

ECLISSI SPAGNOLA

12 Agosto 2026: eclissi totale in Spagna

Storia della Crittografia

Alan Turing: dal codice ENIGMA all'AI

Droni: i protagonisti di una nuova era

70

2026

PROPRIETÀ:

A.P.S. "Il C.O.S.Mo" (Circolo di Osservazione Scientifico-tecnologica di Modena)

C.F.:94144450361

RESPONSABILE:

Davide Borghi

REDAZIONE:

a cura del Consiglio Direttivo

SITO INTERNET:

www.ilcosmo.net

CONTATTI:

info@cosmo.net

COSTO:

Gratuito sul WEB

CONSIGLIO DIRETTIVO:

Leonardo Avella

Davide Borghi

Luigi Borghi

Roberto Castagnetti

Ciro Sacchetti

Questa rivista, le copie arretrate, i suoi articoli e le sue rubriche, non possono essere duplicati e commercializzati.

È vietata ogni forma di riproduzione, anche parziale, senza l'autorizzazione scritta del circolo "Il C.O.S.Mo".

La diffusione all'esterno del circolo è vietata.

Può essere utilizzata solo dai soci per scopi didattici.

SOMMARIO**IN QUESTO NUMERO:****ASTRONOMIA****12 Agosto 2026: eclissi totale in Spagna**

Il COSMo in trasferta

AA.VV. pag. 5

INFORMATICA**Storia della Crittografia**

Le nuove sfide della sicurezza informatica

di Leonardo Avella pag. 18

INFORMATICA**Alan Turing**

Dal codice ENIGMA all'AI

di Davide Borghi.....pag. 36

ASTRONOMIA**Droni: i protagonisti di una nuova era**

Dai quadricotteri agli sciami intelligenti, dai robot terrestri ai rover marziani: come i sistemi senza equipaggio stanno cambiando il nostro mondo

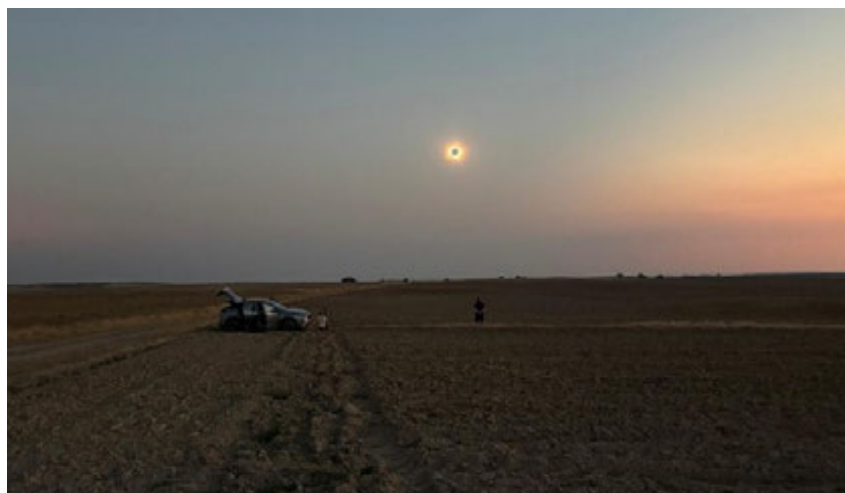
di Luigi Borghi.....pag. 40

GLI EVENTI DEL C.O.S.Mo

L'elenco dei prossimi eventipag. 58

IN COPERTINA

Eclissi a Covarrubias (Spagna). Photo credit: Davide Borghi





Totalità

Le attività della nostra associazione continuano a ritmo incalzante anche durante l'estate.

Negli ultimi tre mesi, dopo gli eventi clou del **Festival della Scienza di San Prospero** e dell'evento **PLAY a Bologna**, abbiamo ospitato al Planetario di Modena **Roberto Mercadini** per una conferenza su Galileo Galilei, facendo il tutto esaurito, abbiamo realizzato diverse interviste su TeleReggio, ad esempio a tema Artemis II, III, IV, Blue Origin, e Space X, ma soprattutto abbiamo organizzato una spedizione speciale del COSMo in Spagna per vedere l'**eclissi totale di sole**. Il meteo ha collaborato e, in perfette condizioni, l'abbiamo osservata da Covarrubias (in diversi gruppi, dal versante di una collina e dal bordo di un campo di girasoli) e dalla Spagna orientale, mentre altri amici l'hanno vista da un luogo a sud di Burgos e dalle Baleari. Un'esperienza unica, anche grazie alle condizioni particolari di questa eclissi: a pochi minuti dal tramonto.

In questo numero trovate un articolo che racconta questo evento con numerose foto di dettaglio scattate da tutti noi nelle diverse località.

Vi proponiamo anche due articoli su un argomento cruciale ma poco conosciuto (anche per ragioni di segretezza): la **crittografia**. Un tema che affrontiamo sia dal punto di vista scientifico e storico, sia con un secondo articolo di approfondimento su **Alan Turing**, che a Bletchley Park (poco a nord di Londra) decrittò il codice nazista Enigma e pose poi le basi dell'Intelligenza Artificiale. Un luogo, Bletchley Park, dove siamo appunto stati in visita con il COSMo-UTE due anni fa.

A settembre ricominciamo con il ciclo di conferenze "**Un altro equinozio con Il COSMo**", aprendo le danze con il grandissimo **Luca Perri**, che ci intratterrà con la Meccanica Quantistica spiegata in modo semplice: "**Smettila di dire a Dio cosa fare coi suoi dadi – la Fisica Quantistica spiegata a me stesso**". Sarà presso l'Auditorium dell'Istituto Istruzione Superiore (I.T.I.S.) "Corni" in via Leonardo da Vinci, 300 (Modena) la sera del 20 settembre alle 21:00.

Lo stesso weekend, sabato 19 e fino al primo pomeriggio di domenica 20 settembre, si terrà anche il **Festival dell'Astronomia di Reggio Emilia**, in cui avrà luogo l'evento speciale "**Terra chiama stazione Terra!**" sul concetto di colonia spaziale orbitante stile O'Neill. Da non perdere!

Continueremo poi, il 6 ottobre alle 21:00, presso il Planetario di Modena, con **Artemis e la nuova corsa alla Luna**: dalla sfida con la Cina alla conquista delle risorse lunari, il primo passo verso la colonizzazione del Sistema Solare. Il programma Artemis segna l'inizio di una nuova era dell'esplorazione spaziale: non più una corsa per piantare una bandiera, ma per costruire una presenza stabile sulla Luna. Stati Uniti e Cina, con i rispettivi alleati, si contendono oggi la leadership di un futuro che intreccia tecnologia, geopolitica e risorse minerarie. La Luna diventa laboratorio e trampolino per l'espansione umana nel Sistema Solare, dove l'estrazione di materiali e la produzione di energia aprono prospettive economiche inedite. Questa volta non torniamo indietro: restiamo, per imparare a vivere fuori dalla Terra e ridefinire il concetto stesso di civiltà spaziale.

Poi il 13 ottobre, sempre alle 21:00: **Droni – Protagonisti di una nuova era**. Con il termine drone si identifica oggi una vasta famiglia di sistemi unmanned, cioè privi di equipaggio a bordo: alcuni volano nei cieli, altri si muovono sulla terraferma, altri ancora navigano in superficie, nelle profondità oceaniche, nello spazio e su altri mondi del Sistema Solare. Esploreremo questo mondo, dai quadricotteri agli sciame intelligenti, dai robot terrestri ai rover marziani, per capire come i sistemi senza equipaggio stiano cambiando il nostro mondo. A proposito: in questo numero troverete una sintesi fedele della conferenza.

La sera del 20 ottobre si continua con **Chernobyl**: il peggior incidente nucleare civile, e punto di svolta tra difetti di progettazione ed errori umani. Chernobyl, Three Mile Island (dove il contenimento ha funzionato) e Fukushima (causata da un evento esterno estremo) sono tre storie molto diverse, da cui nasce il nucleare mo-

dero: reattori ripensati e più sicuri.

Concludiamo la sera del 3 novembre con la **centrale nucleare di Gravelines**, in Francia: un approfondimento sulla centrale nucleare d'oltralpe, con sei reattori da 900 MW ciascuno, che producono il 6% della produzione totale di energia elettrica francese. Un mostro a sei teste, ma anche un esempio di come si possa convivere con questo potente sistema ed essere sicuri che Chernobyl sia molto lontano.

A presto!

Il Presidente

Davide Borghi

davide.borghi@ilcosmo.net



12 AGOSTO 2026: ECLISSI TOTALE IN SPAGNA

Il COSMo in trasferta

di **Davide Borghi, Antonio Melandri, Manuela Mosconi, Arianna Melandri, Daniela Burani, Chiara Corradi, Leonardo Avella, Ciro Sacchetti, Gaia Avella, Viola Avella, Emma Avella**



Che dire, siamo appena tornati dalla spedizione COSMo/REA in Spagna per vedere l'eclissi totale e siamo tutti entusiasti: è andato tutto bene, abbiamo foto spettacolari e il meteo ha collaborato anche stavolta.

Diversi di noi hanno infatti già visto altre eclissi totali (ad esempio Francia 1999, Stati Uniti 2017, Messico e Stati Uniti 2024 fra le altre), ma ogni eclissi è un'esperienza nuova: nuove emozioni e nuove condizioni al contorno dal punto di vista scientifico. Questa, ad esempio, è stata tardi la sera a pochi minuti dal tramonto, che la rende piuttosto particolare.

La spedizione COSMo/REA, si è dipanata in diversi rami: un primo gruppo (Antonio, Davide, Arianna, Daniela e amici dal Trentino) è andato a vederla su un versante di una collina a Ovest di Covarrubias, altri (Leonardo, Alessandro) sono andati poco a Sud di Covarrubias al confine di un campo di girasoli; altri ancora (Ciro) più verso la costa orientale spagnola e infine amici del Planetario (Rita) l'hanno vista al tramonto alle Baleari. Per tutti è andata molto bene, fatto che non era affatto scontato a priori.

Nei paraggi di Burgos e Covarrubias c'era anche la NASA per l'osservazione della totalità e abbiamo anche rischiato di incontrare Elon Musk o dipendenti

di Space X, visto che aveva affittato per tutto il mese di Agosto l'intero castello El Parador de Lerma in provincia di Burgos.

Come si vede dalle foto, ci siamo anche equipaggiati preventivamente con magliette COSMo "Special Edition Total Eclipse 12 August 2026" che hanno avuto un gran successo anche fra gli amici spagnoli.



La famiglia Avella, tutti rigorosamente con maglietta COSMo special edition, foto da Covarrubias. Photo credit: Davide Borghi



Magliette COSMo special edition. Photo credit: Daniela Burani



Dopo la totalità, Covarrubias. Photo credit: Davide Borghi



Totalità, Covarrubias. Photo credit: Davide Borghi



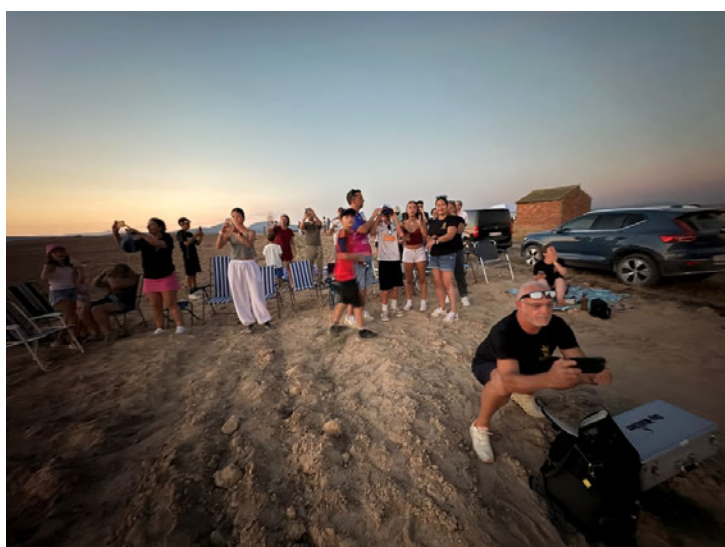
Gli amici spagnoli, Covarrubias. Photo credit: Davide Borghi



Totalità, Covarrubias. Photo credit: Davide Borghi



Sole nero. Photo credit: Alessandro Ferrari,



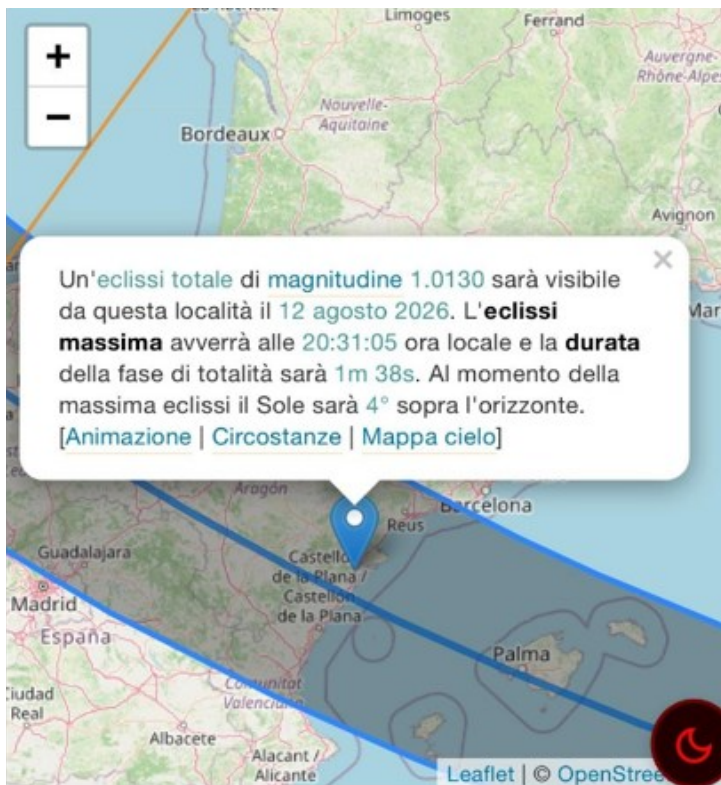
Noi durante la totalità, Covarrubias. Photo credit: Davide Borghi



Facce soddisfatte dopo la totalità, foto da Covarrubias. Photo credit: Daniela Burani

Ciro Sacchetti: la nostra è stata una programmazione molto frettolosa fatta negli ultimi giorni di luglio causa problemi familiari, basti pensare che l'ultima prenotazione di pernottamento l'abbiamo confermata ai primi di agosto, ma ho avuto "due potenti alleati" Cit. STAR WARS, che mi hanno aiutato a trovare il luogo e il modo giusto per osservare questo magnifico spettacolo, e che ringrazio tanto.

Nonostante l'organizzazione di corsa e i tempi strettissimi, siamo riusciti a fare un tour in auto molto bello passando per la Costa Azzurra dove abbiamo fatto tappa nella cittadina di Sainte Maxime, il giorno successivo ci siamo recati in Camargue dove tra natura selvaggia con zone lacustri, cavalli allo stato brado e fenicotteri, abbiamo fatto un'altra splendida tappa. Meta fondamentale è stata Valencia, tra le città più indicate per il passaggio con massima cessione dell'eclissi, avevamo in mente di aggregarci ai due gruppi di Covarrubias, ma voleva dire aggiungere una tratta di oltre 800 Km con tempi ristretti non era ahimè fattibile, ed è qui che Leonardo Avela (primo dei potenti alleati) è entrato in azione passandoci app e consigli utili su come vedere meglio l'eclissi.



Corridoio di massima totalità (Contributo di Leonardo Avela)

Leo aveva già assistito a quella in Nord America 2024 e voleva che anche io e mia Moglie godessimo appieno dello spettacolo ed è stato di enorme aiuto con una immagine che spiegava in modo molto semplice quali fossero le proporzioni da tenere presente rispetto al tramonto del sole nel momento del fenomeno.

Qualche giorno prima della partenza nella chat "A.T.S." del giovanissimo divulgatore Astro Tommy (Tommaso Schiesano) uno dei suoi collaboratori Tommaso Dal Santo affermava che si sarebbe trovato nella zona di Valencia anche lui nei giorni dell'eclissi, questi ragazzi erano parte della comitiva capeggiata da Stefano Pozzato del Circolo di razzo modellisti ACME che assieme a me ha fatto visita alla centrale nucleare di Graveline lo scorso anno (vi rimando all'articolo pubblicato nello scorso numero 69 della nostra rivista). Dopo uno scambio di messaggi, abbiamo convenuto di trovarci in un luogo che avremmo studiato insieme e così è stato.

Dopo il vaglio di alcuni siti seguendo le indicazioni di Leo e i calcoli di Tommaso, lui ha trovato un luogo adatto a 45 minuti da Valencia, proprio nel corridoio ottimale indicato dalle app che Leo mi aveva consigliato situato nei pressi della zona industriale di Burriana Comunità Valenzana.

Il 12 agosto ci siamo ritrovati nel luogo convenuto intorno alle 19.00 dove abbiamo rivisto con piacere Tommaso e abbiamo conosciuto la sua splendida famiglia, circa quarantacinque minuti dopo è iniziata la copertura, sul luogo sono arrivati anche altre persone, abitanti del posto pronti ad ammirare l'eclissi che non ha tardato ad iniziare. Alle 19,45 circa abbiamo iniziato a vedere il disco lunare che dal basso a destra pian piano andava a coprire quello solare, nel giro di alcuni minuti la copertura è stata totale, ed è stato un momento incredibile, la luce è calata e gli uccelli si sono zittiti, è apparso visibile Venere e altre stelle, la temperatura è calata e il disco solare completamente coperto lasciava trasparire una corona dorata tutta intorno, non ho parole per descrivere cosa abbiamo provato ma tutti noi abbiamo alternato momenti in cui esprimevamo il genuino stupore a momenti di silenzio in cui ammiravamo questo splendido spettacolo.



Tommaso e Ciro. Photo credit: Tommaso Dal Santo

Subito dopo ci siamo salutati, Tommaso mi ha promesso che mi avrebbe inviato le immagini da lui scattate. Vorrei evidenziare che ha solo diciotto anni compiuti da pochissimo, ha realizzato in modo artigianale un filtro solare per la sua fotocamera ottenendo immagini di tutto rispetto come potete ben vedere, ed è da poco iscritto al primo anno di Università all'indirizzo di Scienze Astronomiche, i nostri migliori auguri...



Filtro solare. Photo credit: Ciro Sacchetti

Noi del COSMo, subito dopo l'eclissi, abbiamo condiviso a caldo i nostri stati d'animo grazie a una videochiamata organizzata da Leo, che era in compagnia di Alessandro Terzi (ACME/COSMo); a loro si sono poi aggiunti Davide e Antonio. È stato un momento molto bello, in cui l'entusiasmo era evidente:

la dimostrazione di quanta passione proviamo e di quanto questa ci unisca.



Massima copertura. Photo credit: Tommaso Dal Santo

Il giorno successivo io e mia moglie Susanna abbiamo iniziato il viaggio di ritorno, toccando nuovamente la Camargue per una tappa e rientrando in Italia due giorni dopo. Resterà per sempre in noi il ricordo di questa bellissima esperienza.



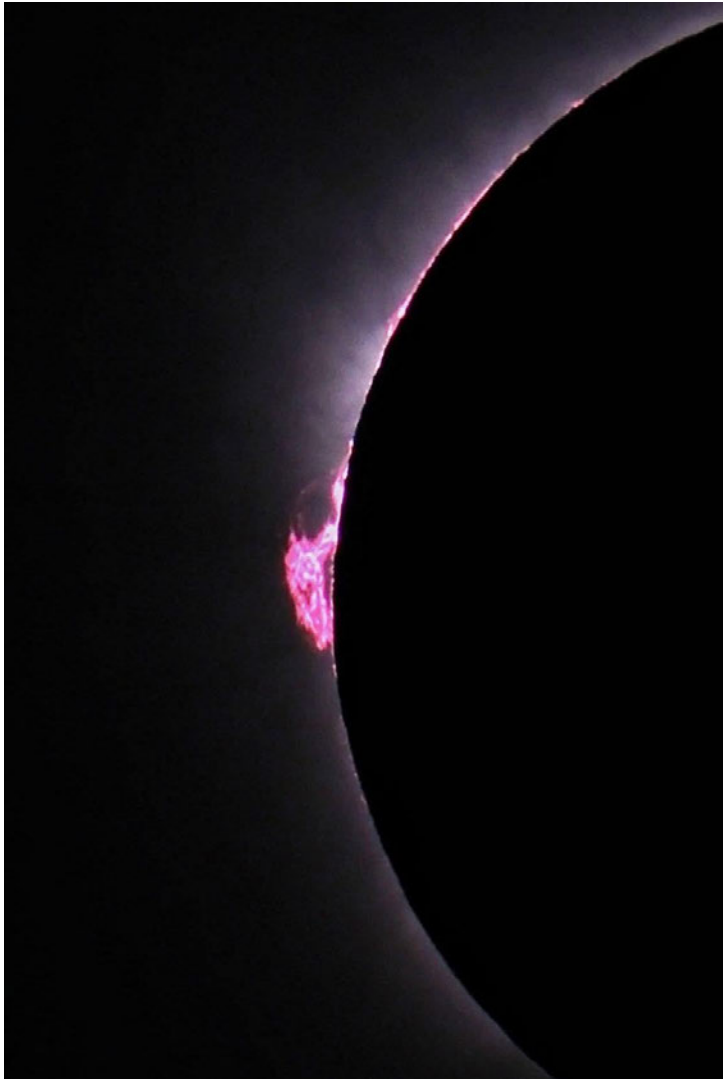
Spagna orientale. Photo credit: Ciro Sacchetti



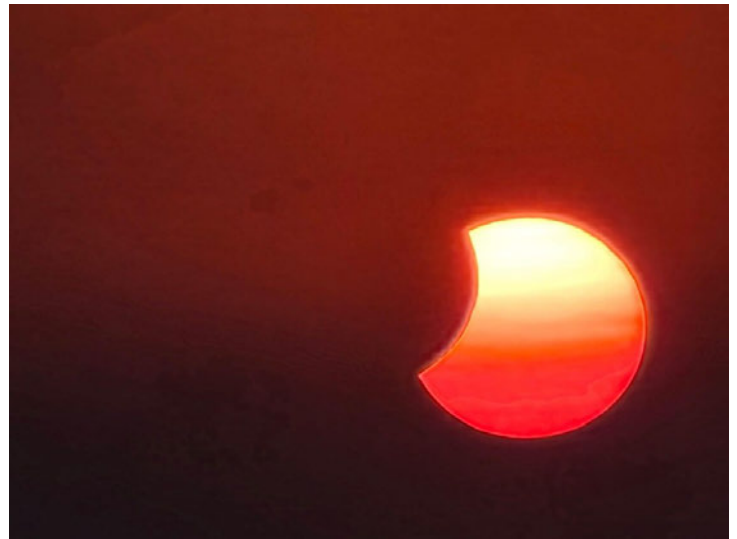
Totalità da Covarrubias - Photo credit: Alessandro Ferrari



*Eclissi parziale poco prima del tramonto, Covarrubias
Photo credit: Alessandro Ferrari*



Totalità da Covarrubias - Photo credit: Massimiliano Di Giuseppe



*Eclissi parziale poco prima del tramonto, Covarrubias
Photo credit: Antonio Melandri*



Photo credit: Antonio Melandri



Covarrubias - Photo credit: Daniela Burani



Composizione di foto NASA – da Burgos, non distante da Covarrubias dove eravamo noi



Breve spuntino dopo la totalità, Covarrubias. Food credit: amici spagnoli

Antonio Melandri, Manuela Mosconi, Arianna Melandri

La programmazione

La programmazione del viaggio in Spagna è iniziata con un anno di anticipo.

Si è cominciato analizzando l'area geografica in cui ci sarebbe stata la visibilità della totalità, escludendo a priori mete affascinanti come Groenlandia e Islanda, che però presentavano rischi meteo elevati.



Della Spagna si è poi esclusa l'opzione isole per le problematiche di accessibilità e alloggio.

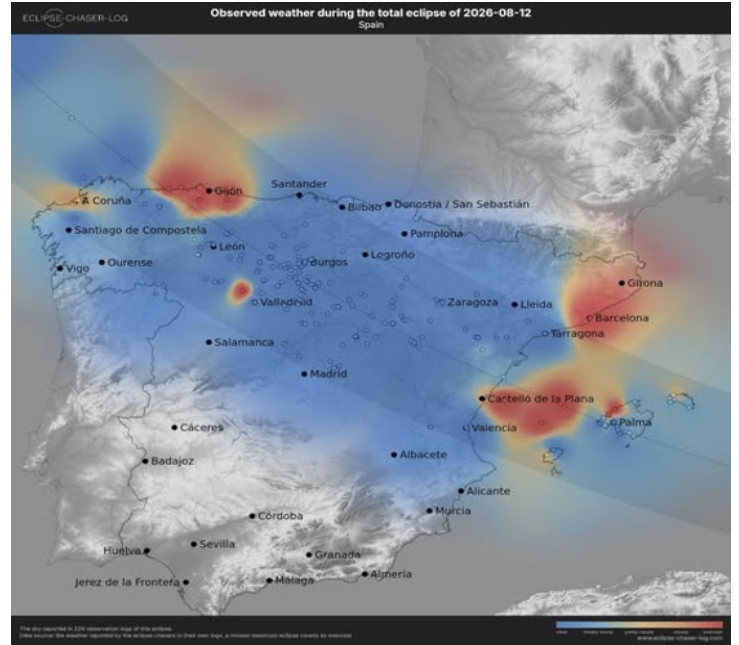
Scelta la Spagna continentale, c'era da definire il luogo più promettente dal punto di vista della statistica sulla nuvolosità.



L'area della costa sul golfo di Biscaglia presentava delle statistiche non promettenti e quindi ci siamo concentrati sulla parte più interna, nella zona di Burgos.

Superate infatti le montagne dei paesi baschi, si raggiunge un altopiano che presenta ottime condi-

zioni climatiche per l'osservazione astronomica.



La strumentazione

La possibilità di viaggiare in automobile, ha garantito la capacità di carico che in passato non avevamo. Abbiamo quindi potuto portare una montatura equatoriale e uno SkyWatcher ED80, che abbiamo usato anche per una improvvisata serata astronomico-



La strumentazione COSMo, Covarrubias - Photo credit: Antonio Melandri

A posteriori la scelta si è dimostrata corretta, visto la distribuzione di nuvole della giornata.

La fortuna ha voluto che dopo aver interpellato un amico spagnolo, ci venisse offerta la possibilità di alloggiare in una casa privata, situata a Covarrubias. L'ospitalità e la gentilezza degli amici spagnoli è stata insuperabile. Non potremo mai ringraziare abbastanza le famiglie di Javier e Rober, per l'accoglienza ricevuta.

ca a Covarrubias. Sull'ED80 e' stata montata una reflex full-frame Pentax K1-II per le fotografie delle varie fasi dell'eclissi.

Su un cavalletto fotografico, abbiamo posizionato la Sony A6000, di mia figlia Arianna, con un 70-200 mm, allo scopo di riprendere un video con il panorama e l'intera fase di totalità.

Sempre Arianna, con un drone DJI ha colto una panoramica a 360 gradi dell'orizzonte al momento della totalità e un po' di immagini del gruppo.

Inutilizzato il teleobiettivo Pentax * 300 f/4.5 che aveva ripreso l'eclissi in Messico e che ci ha seguito solo come soluzione di ripiego, in caso ci fosse stato qualche problema.

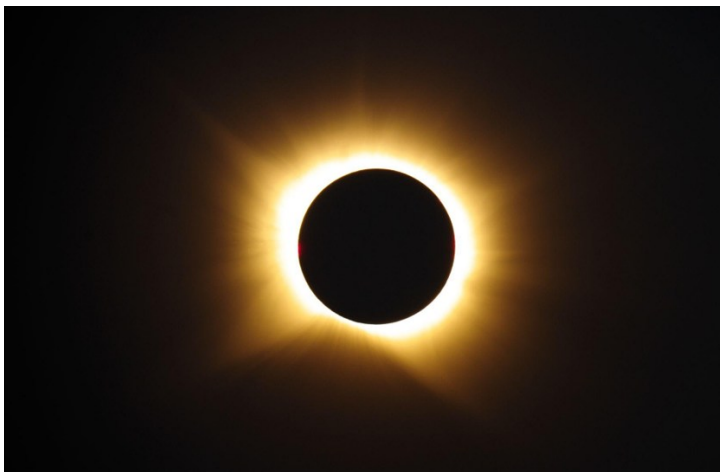
Daniela invece ha usato una macchina fotografica Canon Reflex EOS 600D con obiettivo Canon 70-200mm dove ha montato un filtro K&F ND1000000 20stop OD6.0 che alternava anche sul cellulare iPhone 14PRO con relativa clip in dotazione.

L'eclissi dorata

L'approssimarsi del tramonto ha reso l'eclissi totale particolarmente interessante. Nelle precedenti occasioni abbiamo sempre assistito a fenomeni con tonalità tendenzialmente fredde, con la corona solare di colore bianco-azzurro.



Nell'immagine sopra l'eclissi "americana" del 2017, come si vede nell'immagine sotto, quest'anno, invece, ci siamo ritrovati con una corona dorata.



E con la fase di parzialità in uscita dalla totalità che a molti ha ricordato le affascinanti ambientazioni di Guerre Stellari.



Covarrubias

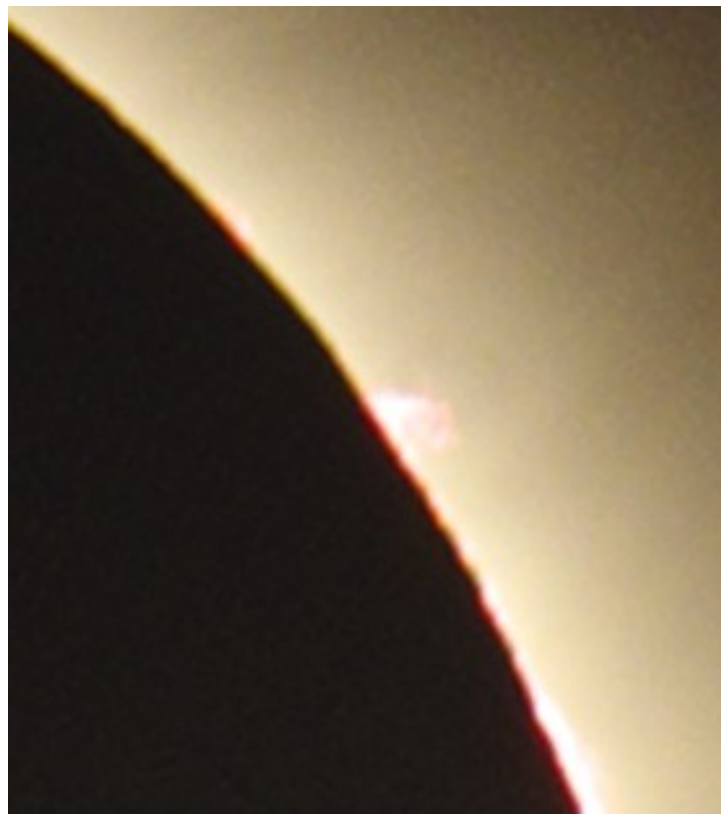
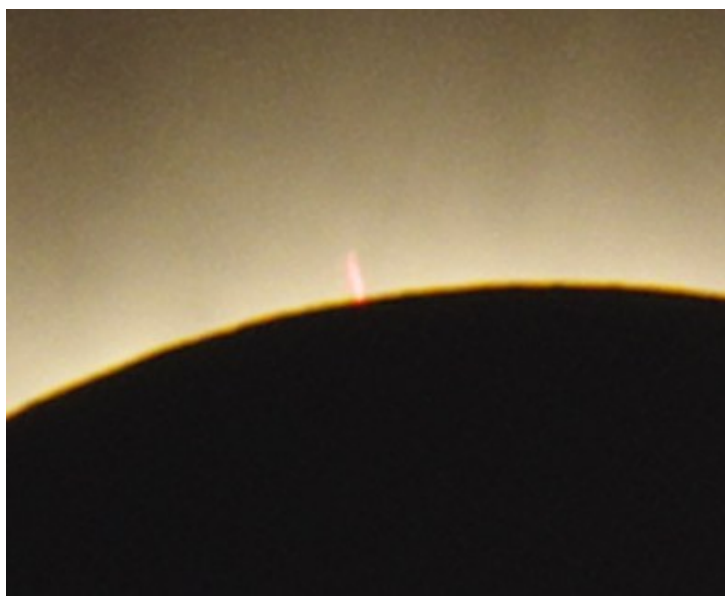
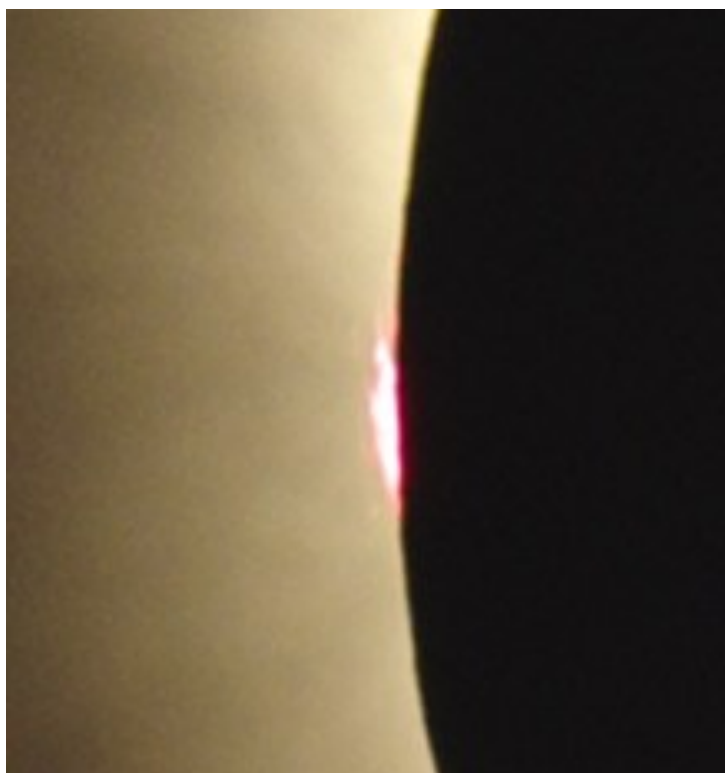


Tatooine

La fase di totalità è durata appena 1 minuto e 40 secondi, molto più corta degli oltre 4 minuti della precedente esperienza in Messico. Personalmente, sono rimasto sorpreso e affascinato da questa totalità e alla fine ho dedicato la maggior parte di questo tempo all'osservazione diretta dell'eclissi, scattando solo 6-7 foto della totalità.



Affascinanti le protuberanze durante l'eclissi:



Ovviamente il viaggio non si è ridotto alla sola osservazione dell'eclissi. Questi viaggi sono sempre una buona scusa per esplorare i paesi che si attraversano per raggiungere la destinazione finale. Nel nostro caso il sud della Francia, dalla Costa Azzurra (Antibes), alla Provenza (Arles e Nimes), la regione di Pirenei (Carcassonne e il Pic du Midi) e i Paesi Baschi (Bayonne, Bilbao, San Sebastian, Vitoria Gasteiz, Burgos). Al ritorno tappa a Toulouse con l'immane visita alla Cité de L'Espace.



Di particolare interesse astronomico l'ascensione in funivia all'osservatorio del Pic du Midi (2877 m slm).



Ma i ricordi che rimarranno più vividi saranno quelli delle esperienze vissute con i compagni di viaggio e l'accoglienza ricevuta dagli amici spagnoli. Grazie!



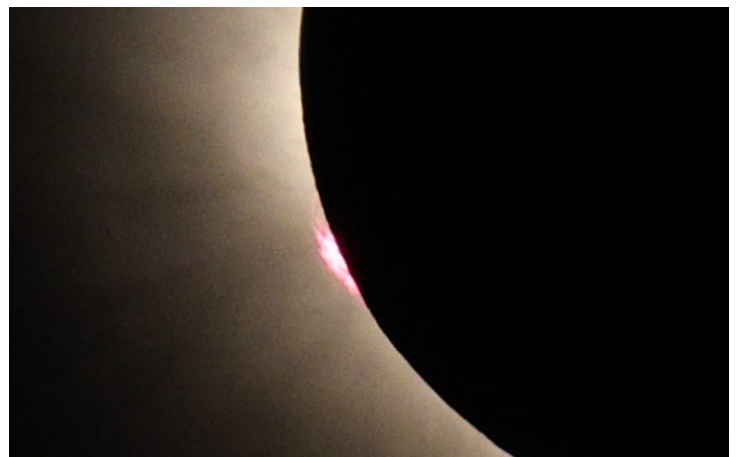
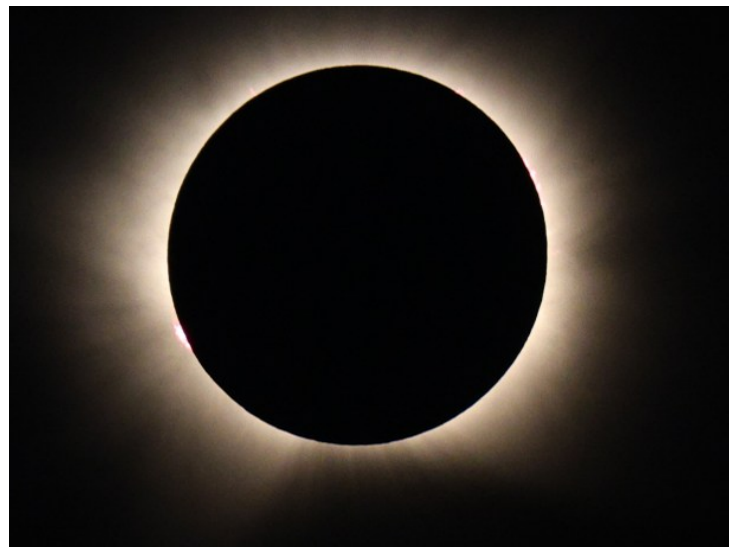
Leonardo Avella: Le vacanze estive della nostra famiglia sono state impostate in funzione dell'eclissi. Abbiamo fatto qualche giorno di vacanza sui Pirenei francesi e su quelli spagnoli, prima e dopo l'eclissi.

Durante l'avvicinamento, in provincia di Torla (Spagna), il 7 agosto ho scattato una foto della Via Lattea di cui vado orgoglioso.

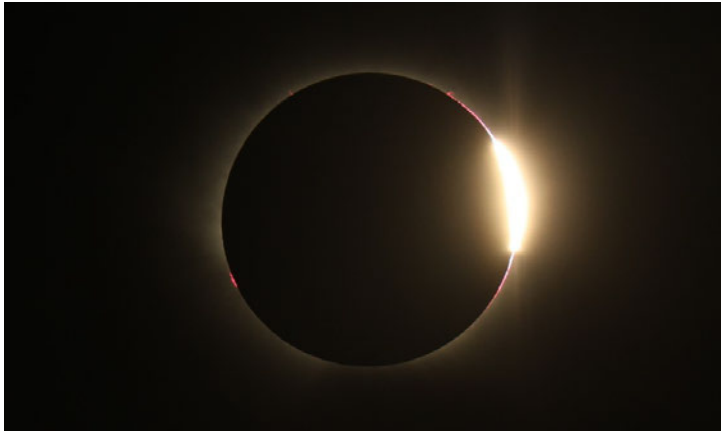


Via Lattea da Torla - Photo credit: Leonardo Avella

L'eclissi è stata diversa da quella americana del 2024, con colori più caldi dovuti probabilmente al tramonto. Molto bella la protuberanza sulla sinistra come si può vedere in questa foto e con il relativo ingrandimento.



Eclissi a Covarrubias - Photo credit: Leonardo Avella



Eclissi a Covarrubias - Photo credit: Leonardo Avella

Molto suggestivo anche il tramonto in fase di parzialità con il sole a *bande* dovuto alla foschia atmosferica.



Eclissi a Covarrubias - Photo credit: Leonardo Avella

Ah... Da noi anche i girasoli hanno voluto godersi lo spettacolo!!!!



Covarrubias - Photo credit: Chiara Corradi

Speriamo di ritrovare questa splendida comunità di appassionati in occasione della prossima eclissi in Egitto!

Daniela Burani: io invece avevo impostato il viaggio in macchina con un amico per fargli scoprire le bellezze dell'astronomia ma, per un cambio dell'ultimo minuto, ho dovuto optare per un viaggio in aereo con Davide Borghi da Bologna su Santander... e così ho pensato: solo 5 gg a disposizione di cui 1 di viaggio!

Invece è stata un'esperienza meravigliosa. Un viaggio a tappe serrate ma vissuto nella massima tranquillità, senza nessun problema e con persone incredibili:

- rendez-vous a Bilbao con famiglia Melandri e già qui dormito sotto le stelle con un abbaino diretto sul mio letto. Visita veloce al Guggenheim Museum e anche qui troviamo all'interno una mostra di bambini sull'astronomia. Tappa veloce sul ponte di Biscaglia-patrimonio UNESCO



- Vitoria Gasteiz capoluogo dei Paesi Baschi nonchè città dei murales e io adoro i murales! Splendida visita immersiva a 360° nella Cattedrale di

Santa Maria. Prima di lasciarla si comincia anche ad assaggiare prelibatezze locali: Antonio prova il "Tinto del Verano"

- Burgos capoluogo della comunità di Castiglia e Leon dove non possiamo perderci la visita alla Cattedrale gotica con all'interno le spoglie di El Cid Campeador figura leggendaria spagnola e punto di passaggio per i pellegrini del Cammino di Santiago
- Infine eccoci a Covarrubias dove incontriamo i ns amici spagnoli INCREDIBILI, un'accoglienza da mille e una notte. Noi arriviamo con le ns magliette speciali da omaggiare loro ed ecco che l'amicizia non ha più confini, diventiamo parte della famiglia anzi loro ormai sono parte della grande famiglia IL COSMO/REA. E via di prelibatezze, paella di pescado e di carne, colazioni da re ed infine poteva mancare un buffet stellare durante l'eclissi ? ah dimenticavo altra scoperta "calimochu" vino rosso & coca cola.
- <Davide sai che qui hanno girato il film "Il Buono, Il Brutto e Il Cattivo" ? <Davvero?> si parte per il set cinematografico ancora in essere e diventiamo tutti "Nessuno" alias Clint Eastwood e un ultimo saltino al parco naturale La Yecla dove con la nostra super attrezzatura vediamo gli avvoltoi
- FINALMENTE LA MIA EMOZIONE PIU' GRANDE, LA MIA 1° ECLISSI DI SOLE TOTALE... non ci crederete ma già la mattina il mio cuore andava a mille, dovevo preparare tutta la mia attrezzatura fotografica e non (ed era la 1a volta anche per questo), dovevamo decidere la posizione perfetta e qui via di sopralluogo... deciso! Emozioni uniche

difficili da spiegare, bisogna viverle e noi l'abbiamo vissuta al massimo, con persone uniche che non finirò mai di ringraziare

- E' ora di tornare ma lo facciamo con il cuore pieno di emozioni, felicità, amicizia e pancia soddisfatta però vuoi non fare un bagno alla Fuente Azul a -10C°? dimenticavo adoro anche le pale eoliche e in questo bellissimo paese ce ne sono veramente un sacco!

Tanti girasoli & un'eclissi solare totale a VOI

Dopo aver gustato i contributi dei nostri Amici associati ricordiamo i prossimi appuntamenti e le ipotesi, tra parentesi, per i luoghi di osservazione: Il 2 Agosto dell'anno prossimo in Egitto (a Luxor o sul Mar Rosso) e il 22 Luglio 2028 in Australia (a Sydney).

Alleghiamo due contributi video che potrete vedere cliccando sui link (Video credit: Arianna e Antonio Melandri):

<https://youtu.be/-BNHqisiuKM?si=MrT5yyEdZGGO82uf>

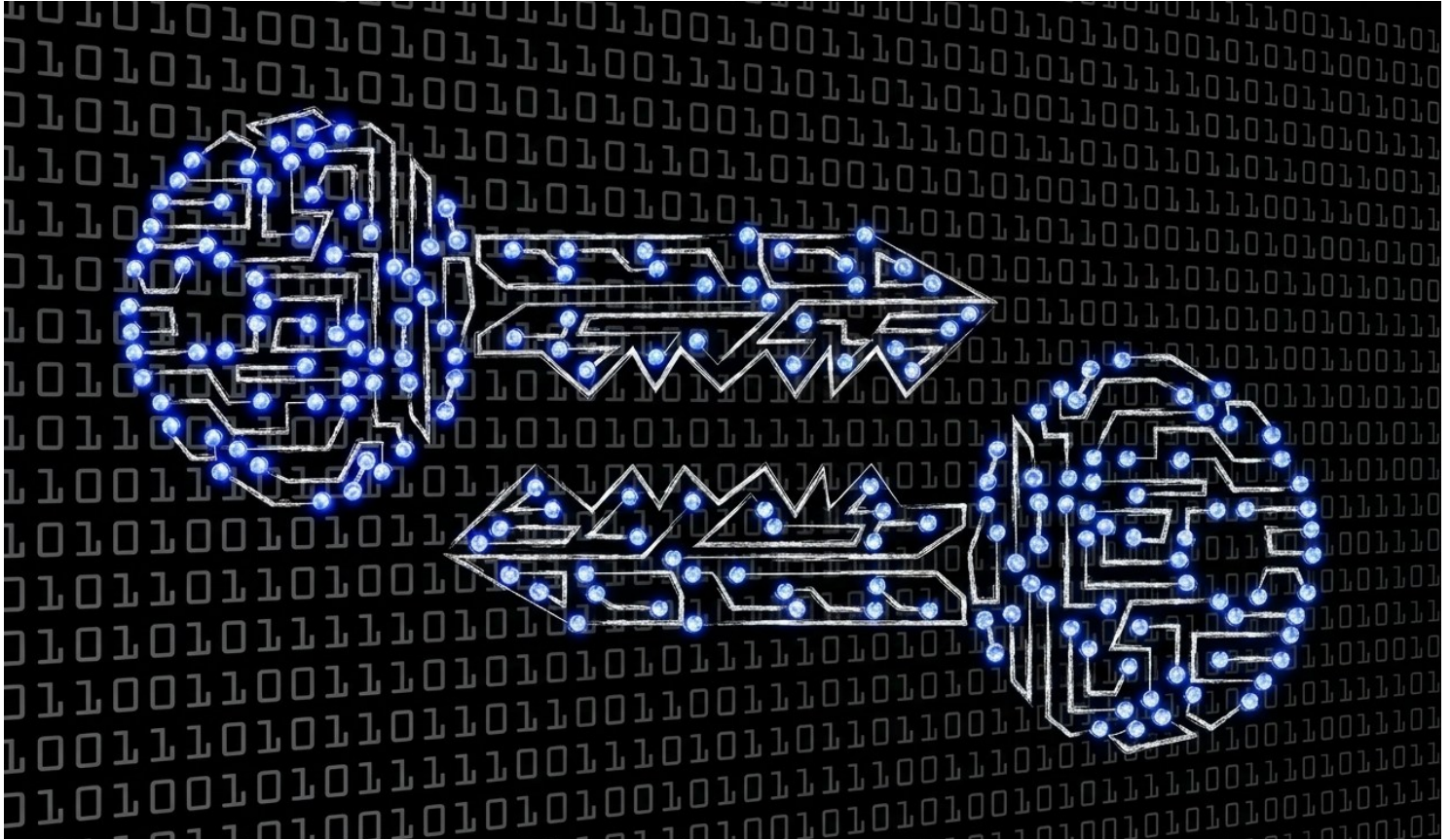
<https://youtu.be/z-eiChlofzc?si=qyN-loHUciyIJJ-K>



STORIA DELLA CRITTOGRAFIA

Le nuove sfide della sicurezza informatica

di **Leonardo Avella**



In questo articolo vi racconterò la storia della crittografia fino ai giorni nostri (crittografia a chiave pubblica) e l'approfondiremo toccando anche le prospettive future.

Vediamo le fonti principali che ho usato per l'articolo:

<https://www.programmiamo.altervista.org/>

<https://www.programmiamo.altervista.org/File/critto/critto1.html>

https://it.wikipedia.org/wiki/Attacco_man_in_the_middle

https://it.wikipedia.org/wiki/Scambio_di_chiavi_Diffie-Hellman

https://it.wikipedia.org/wiki/Crittografia_quantistica

https://it.wikipedia.org/wiki/Algoritmo_di_fattorizzazione_di_Shor

https://it.wikipedia.org/wiki/Teorema_di_Bell

Date queste fonti, introduciamo alcune definizioni.

La **crittografia** (o crittografia, dal greco antico

κρυπτός (kryptós), "nascosto" e γραφία (graphía), "scrittura") è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio non comprensibile o intelligibile a persone non autorizzate a leggerlo. Il suo obiettivo in chiave moderna è garantire il requisito di confidenzialità o riservatezza tipico della sicurezza informatica.

Il **testo in chiaro** è il testo da cifrare, ancora leggibile. Il **testo cifrato** è invece il testo come risulta dopo che è stato eseguito l'algoritmo di cifratura.

L'**algoritmo di cifratura** descrive come si trasforma il testo in chiaro per ottenere testo cifrato. Questa operazione è detta **azione di cifratura** (voce del verbo cifrare) o di crittografia (voce del verbo criptare o crittare. L'algoritmo opposto (di decifratura o di decodifica) è quello che consente di riottenere

re il testo in chiaro a partire dal testo cifrato.

L'algoritmo di cifratura, per poter cifrare il testo, ha quasi sempre bisogno di una **chiave**. A parità di algoritmo e di testo in chiaro, se cambio la chiave allora cambia il contenuto del testo cifrato.

L'algoritmo di decifratura, per decodificare il testo cifrato, ha quasi sempre bisogno di una chiave: tale chiave di decifratura, nel caso degli **algoritmi simmetrici**, coincide con quella di cifratura. Nel caso degli **algoritmi asimmetrici** la chiave per la codifica e quella per la decodifica sono diverse. Gli **algoritmi a chiave pubblica** sono un particolare tipo di algoritmi asimmetrici nei quali non ho bisogno di un canale sicuro per arrivare a condividere la chiave di cifratura.

Per **crittoanalisi** (dal greco *kryptós*, "nascosto", e *analýein*, "scomporre"), o crittanalisi, si intende lo studio dei metodi per ottenere il testo in chiaro a partire solo dal testo cifrato, in altre parole senza possedere la chiave di decodifica.

La crittoanalisi è in sostanza l'altra faccia della crittografia e viene usata da coloro che cercano di "rompere" un codice segreto (break a code) ovvero di "violare" il cifrario: per esempio i nemici che intercettano i messaggi inviati.

La crittoanalisi è molto utile per verificare la bontà di un algoritmo di crittografia.

Oltre alla crittoanalisi ci sono altri modi per cercare di leggere messaggi criptati. Un tipico esempio è l'attacco **man-in-the-middle**.

Tale attacco si ha quando l'attaccante è in grado di intercettare (e modificare) tutte le comunicazioni che avvengono fra le due parti comunicanti, all'insaputa dei legittimi interlocutori.

Un tipo di attacco man-in-the-middle particolarmente devastante è l'**eavesdropping**, nel quale l'attaccante riesce a far credere sia al mittente che al destinatario di essere lui l'interlocutore legittimo, creando connessioni criptate e indipendenti con le vittime. L'attaccante in tal caso è in grado di osservare, intercettare e replicare verso la destinazione prestabilita il transito dei messaggi tra le due ignare vittime.

La sicurezza di un sistema di crittografia è adeguata se:

- Il costo per decodificare i messaggi supera il valore dell'informazione cifrata
- Il tempo richiesto per decodificare i messaggi supera l'arco temporale in cui l'informazione è utile

Uno dei primi esempi documentati di crittografia risale a Giulio Cesare, con il suo cifrario.

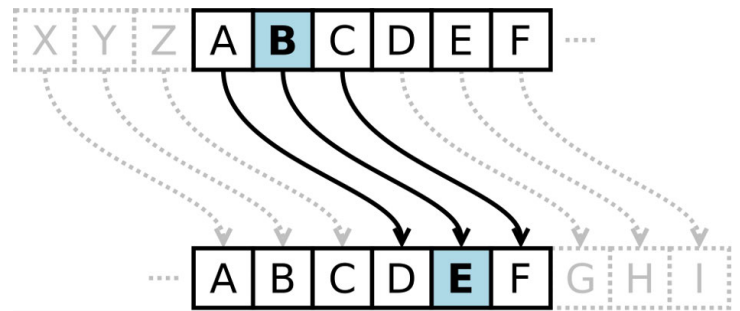


Figura 1: Rappresentazione del cifrario di Cesare

Il cifrario di Cesare, però, è facilmente decodificabile con metodi statistici.

Se si conosce la lingua del testo in chiaro, è possibile ottenere un diagramma delle frequenze delle lettere sia del testo cifrato che di un testo generico in chiaro (sufficientemente lungo) in lingua originale. Fatto questo, è facile individuare il valore della chiave osservandone la frequenza statistica.

Per esempio, in italiano le lettere più frequenti sono la A e la E, che compaiono in media con una frequenza del 12%. In generale le lettere più usate sono le vocali, mentre le consonanti sono meno frequenti (la Z ha una frequenza solo dello 0,5%).

La figura 2 mostra la distribuzione in frequenza delle lettere dell'alfabeto italiano nel primo capitolo dei Promessi Sposi.

Usando un'analisi della frequenza dei vari simboli nel testo cifrato, il crittoanalista può dunque cercare di indovinare a quale lettera corrisponda ogni simbolo. Ciò vale in particolare se il testo cifrato è abbastanza lungo.

Il cifrario di Cesare è definito **monoalfabetico** in quanto ogni simbolo viene sostituito sempre dallo stesso simbolo secondo una tabella di sostituzione

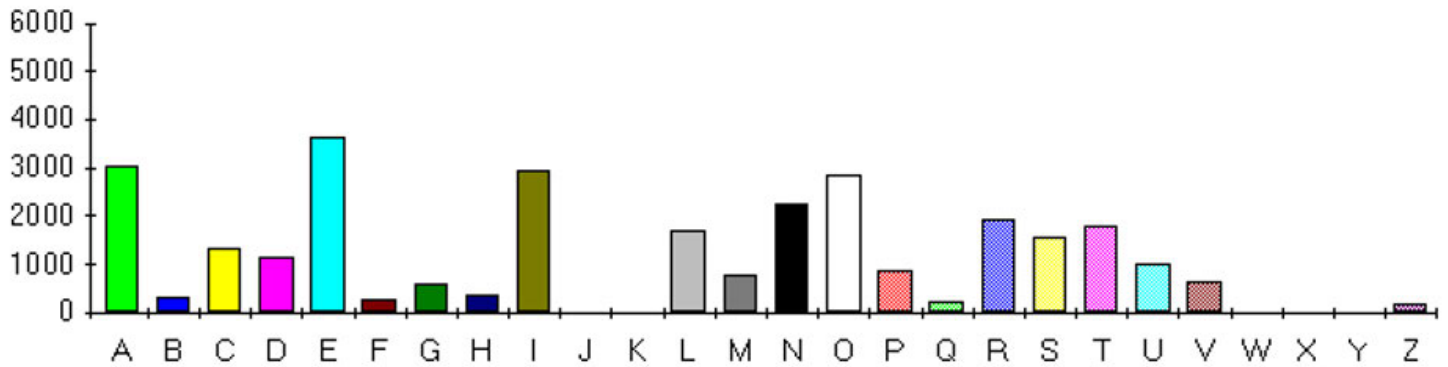


Figura 2: Distribuzione in frequenza delle lettere dell'alfabeto italiano nel primo capitolo dei Promessi Sposi

univoca.

Un maggiore livello di sicurezza si ha con i **cifrari polialfabetici**. I Cifrari polialfabetici si differenziano da quelli monoalfabetici (come il cifrario di Cesare e altri simili) in quanto un dato carattere del testo chiaro (per esempio la A) non viene cifrato sempre con lo stesso carattere, ma con caratteri diversi in base ad una qualche regola, in genere legata ad una parola segreta. La chiave di cifratura deve essere conosciuta solo dal mittente e dal destinatario del messaggio. La sicurezza aumenta dato che non è più così semplice individuare le lettere del messaggio in base alla loro frequenza caratteristica. Un esempio di tale metodo è il **cifrario di Vigenère**. Anche se la sicurezza è molto maggiore rispetto al cifrario di Cesare, si è scoperto che il cifrario di Vigenère non è sicuro in quanto per risalire alla chiave di cifratura si possono ancora fare analisi statistiche.

Un esempio estremo di cifrario polialfabetico è il **cifrario di Vernam**, nel quale la chiave di cifratura è lunga quanto il messaggio stesso e non è riutilizzabile. Tale metodo è stato nominato il cifrario perfetto perché, se non conosco la chiave, è stato dimostrato matematicamente essere inviolabile.

Con il passare del tempo sono stati pensati sistemi di cifratura sempre più sofisticati, come i **cifrari composti**, nei quali il testo cifrato viene cifrato ancora più volte anche con algoritmi diversi tra loro (metodo di sovra-cifratura). Alcuni esempi moderni di tali sistemi sono il 3DES e l'AES che vengono

usati nei sistemi di telecomunicazione moderni per le VPN (Virtual Private Networks) e per la codifica delle trasmissioni WiFi.

La sicurezza del sistema crittografico è basata su questi elementi:

- L'algoritmo o metodo di cifratura
- La chiave di cifratura

La netta separazione concettuale di chiave e algoritmo è uno dei più saldi principi della crittografia, e fu formulata in modo definitivo nel 1883 dal linguista olandese Auguste Kerckhoffs von Nieuwenhof, nel trattato dal titolo "*La cryptographie militaire*".

Ecco quello che scrisse nel suo trattato: «Legge di Kerckhoffs: la sicurezza di un crittosistema non deve dipendere dal tener celato l'algoritmo crittografico. La sicurezza dipenderà solo dal tener celata la chiave».

Detto in parole più semplici: qualsiasi algoritmo di cifratura prima o poi diviene di pubblico dominio (perché viene pubblicato in articoli di ricerca, perché viene trafugato dai servizi di intelligence o perché viene ricostruito tramite reverse engineering). Tenere dunque segreto un algoritmo di cifratura, o ancora peggio affidarsi al fatto che non venga scoperto, non è mai una strategia vincente: conviene piuttosto affidare la sicurezza alla bontà delle chiavi usate.

Ma tutti gli algoritmi di cui abbiamo parlato finora (crittografia simmetrica), hanno una debolezza in comune: la chiave di cifratura deve essere cono-

sciuta sia dal mittente che dal destinatario. In altre parole, devo avere un canale sicuro di comunicazione per inviare la chiave al destinatario. Se poi ho un canale sicuro per inviare una chiave di crittografia lunga come l'intero messaggio e non riutilizzabile (come nel caso di Vernam), allora viene da chiedersi: perché non mandare direttamente il messaggio in chiaro attraverso tale canale sicuro?

Ma qualsiasi canale di comunicazione (telefono, lettera, email, comunicazione radio, incontro di persona, etc.) presenta problemi di sicurezza. C'è sempre la possibilità che qualcuno possa mettersi in mezzo a nostra insaputa o intercettare la chiave.

Il problema è che la chiave non può essere a sua volta cifrata, poiché in tal caso bisognerebbe preventivamente accordarsi sull'algoritmo e sulla chiave di cifratura della chiave, e così via all'infinito. In pratica, mittente e destinatario devono scambiarsi la chiave di cifratura prima di iniziare la corrispondenza e per fare questo devono usare un metodo non cifrato. Per esempio, nel caso semplice del cifrario di Cesare, Cesare potrebbe comunicare a voce la chiave ai propri generali, oppure potrebbe inviarla per mezzo di un messaggero fidato. In entrambi i casi, però, la chiave potrebbe essere intercettata da una spia nemica.

Il problema della condivisione delle chiavi è forse la debolezza principale dei sistemi crittografici tradizionali.

Questo problema è stato superato soltanto con i sistemi di cifratura moderna, i quali richiedono **due chiavi separate** (una **privata** ed una **pubblica**) e non richiedono lo scambio della chiave di decifratura (algoritmi asimmetrici).

Uno dei primi algoritmi di questo tipo fu scoperto da Whitfield Diffie e Martin Hellman.

Il lavoro di Ralph Merkle sulla distribuzione delle chiavi pubbliche (i Puzzle di Merkle) ed il suggerimento da parte di John Gill di utilizzare il problema dei logaritmi discreti come base per la creazione di funzioni unidirezionali servirono da linee guida per lo sviluppo dell'algoritmo Diffie-Hellman. Per tale motivo oggi l'algoritmo è anche detto Diffie-Hellman-Merkle.

La peculiarità dell'**algoritmo Diffie-Hellman-Merkle** è che consente a due entità di stabilire una chiave condivisa e segreta utilizzando solamente un

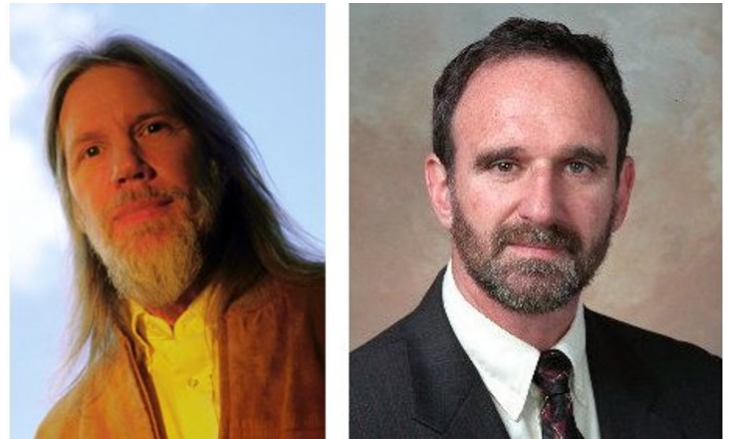


Figura 3: Whitfield Diffie e Martin Hellman

canale di comunicazione insicuro (pubblico).

La prima pubblicazione di tale idea risale a novembre 1976 (fonte: <https://ee.stanford.edu/~hellman/publications/24.pdf>).

Ma come funziona in dettaglio l'algoritmo? Proviamo a spiegarlo con un esempio pratico

Introduciamo innanzitutto la **funzione modulo** (indicata nel seguito con **mod**) che calcola il resto della divisione fra due interi: così per esempio $13 \bmod 5 = 3$, in quanto 13 diviso 5 fa 2 con il resto di 3.

Definiamo che due interlocutori si chiamino Alice e Bob.

L'idea è usare una funzione unidirezionale della forma **$Y^x \bmod P$** .

All'inizio, Alice e Bob si accordano sui valori di Y e P, con P che deve essere un numero primo, e Y che deve essere minore di P.

Non è necessario che i valori in questione siano segreti; perciò Alice può comunicare a Bob su un canale non sicuro che $Y = 7$ e $P = 11$.

In questo modo, Alice e Bob hanno concordato la funzione unidirezionale $7^x \bmod 11$.

A questo punto i nostri interlocutori scelgono la chiave segreta, che denominiamo "A" per Alice e

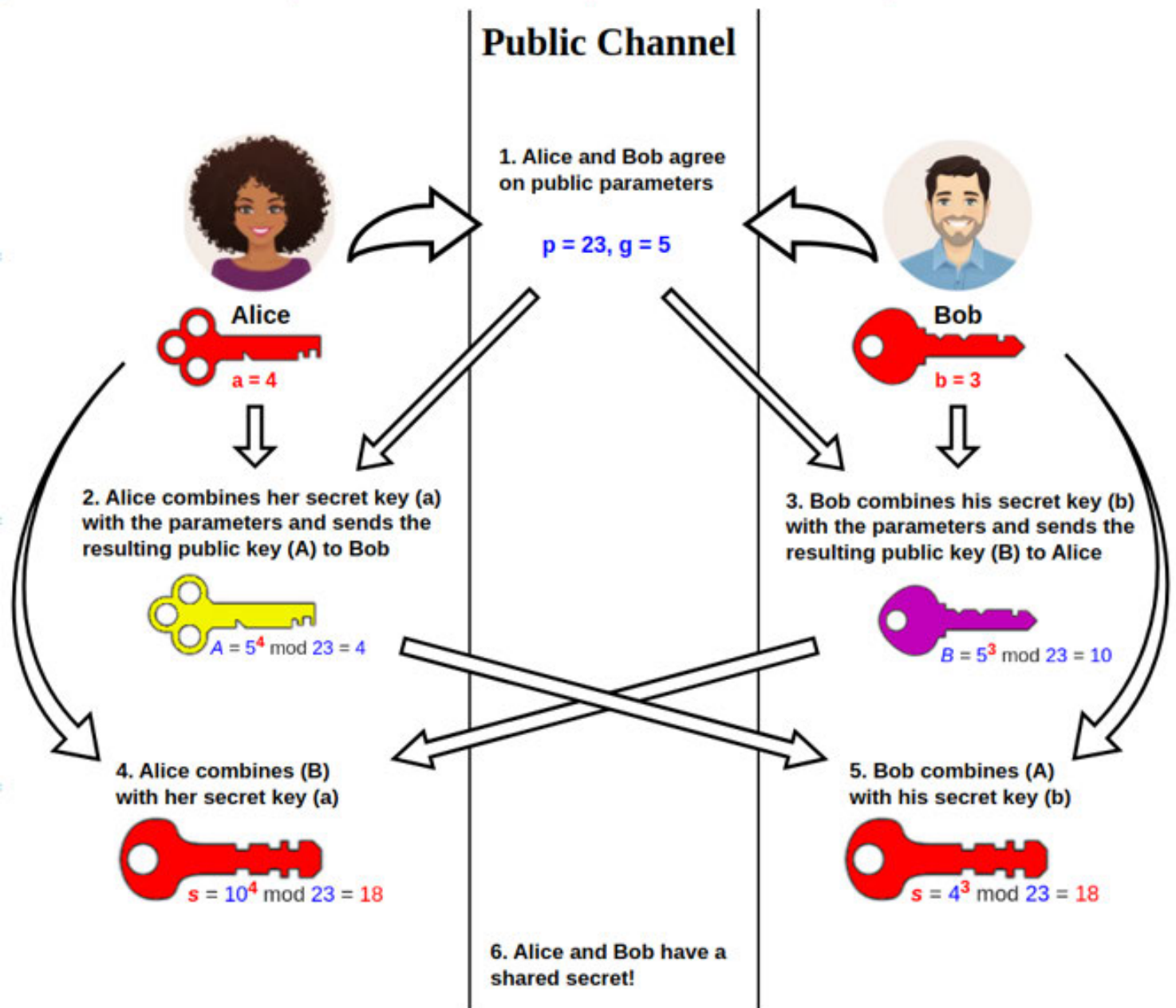


Figura 4: Schema dello scambio di messaggi nel protocollo Diffie-Hellman per la generazione di una chiave segreta comune

"B" per Bob.

Alice sceglie $A=3$. "A" è la parte segreta della chiave privata di Alice, che è la tripletta (7,11,3).

Bob sceglie $B=6$. "B" è la parte segreta della chiave privata di Bob, che è la tripletta (7,11,6).

Alice mette il numero segreto "A" al posto di "x" e calcola:

$$Y^x \bmod P = 7^3 \bmod 11 = 343 \bmod 11 = 2$$

Questo valore, che chiameremo Alfa, fa parte della chiave pubblica di Alice. Come si può notare, grazie alle proprietà delle funzioni unidirezionali, è difficile

ricavare "A" da Alfa. Alfa=2

Bob mette il numero segreto "B" al posto di "x" e calcola:

$Y^x \bmod P = 7^6 \bmod 11 = 117.649 \bmod 11 = 4$. Questo valore, che chiameremo Beta, fa parte della chiave pubblica di Bob. Come si può notare, grazie alle proprietà delle funzioni unidirezionali, è difficile ricavare "B" da Beta. Beta = 4

Alice comunica a Bob il valore di Alfa. A questo punto possiamo dire che la chiave pubblica di Alice sia formata dalla tripletta $(Y, P, \text{Alfa}) = (7, 11, 2)$

Bob comunica ad Alice il valore di Beta. A questo punto possiamo dire che la chiave pubblica di Bob sia formata dalla tripletta $(Y, P, \text{Beta}) = (7, 11, 4)$

A questo punto Alice può usare la sua chiave privata per calcolare una password condivisa con Bob. Alice si serve del risultato Beta di Bob e del suo numero segreto A per calcolare:

$$\text{Beta}^A \bmod P = 4^3 \bmod 11 = 64 \bmod 11 = 9$$

Anche Bob usa la sua chiave privata per calcolare la password condivisa con Alice. Bob si serve del risultato Alfa di Alice e del suo numero segreto B per calcolare:

$$\text{Alfa}^B \bmod P = 2^6 \bmod 11 = 64 \bmod 11 = 9$$

La chiave condivisa sarà dunque il **numero 9**.

Naturalmente nella vita reale i numeri in gioco sono molto più alti in modo che sia impossibile risalire per tentativi alla chiave privata.

Il **metodo Diffie-Hellman-Merkle di scambio delle chiavi**, permette ad Alice e Bob di condividere un segreto scambiandosi informazioni attraverso un canale non sicuro. È stata una scoperta che ha rivoluzionato il mondo della crittografia.

Questo tipo di crittografia è lentissimo, ma è un problema gestibile. Possiamo usare un sistema misto in cui la crittografia a chiave pubblica ci serve solo per scambiare periodicamente in modo sicuro la chiave segreta che andremo ad usare in un algoritmo simmetrico come 3DES o AES, più veloce ed efficiente.

Adesso vedremo un altro algoritmo di crittografia a chiave pubblica denominato **RSA** dalle iniziali dei suoi scopritori: **Rivest, Shamir, Adleman**.

Mentre nel caso dell'algoritmo Diffie Hellman la forza del sistema di crittografia dipende dalla difficoltà di calcolare logaritmi discreti in un campo finito generato da un numero primo molto grosso, l'RSA invece basa la sua sicurezza sulla difficoltà di trovare i fattori primi di un numero intero molto grande.

La fattorizzazione di un numero intero in fattori primi è un altro esempio di quello che i matematici chiamano **funzioni unidirezionali** o **one-way trapdoor function**. Una *one-way trapdoor function*

è una funzione che è facile da calcolare in una direzione, ma è molto difficile da calcolare nell'altra (nel caso specifico è facile calcolare il prodotto di due numeri primi ma è difficile scomporre il prodotto di tali numeri nei suoi due fattori).

Nel caso dell'algoritmo RSA le due chiavi, chiamiamole A e B, possono essere usate alternativamente per cifrare o decifrare un messaggio, nel senso che il messaggio cifrato con A può essere decifrato con B e il messaggio cifrato con B può essere decifrato con A.

Ogni persona coinvolta nello scambio di messaggi possiede dunque una coppia di chiavi che agiscono, di fatto, l'una come l'inverso dell'altra. Una di queste due chiavi viene resa pubblica, cioè nota a tutti. La seconda chiave invece viene mantenuta privata.

Supponiamo ora che Bob voglia mandare un messaggio ad Alice e, temendo che questo messaggio venga intercettato, decide di criptarlo. A tale scopo Bob cripta il messaggio usando la chiave pubblica di Alice, chiave che Alice può tranquillamente mandargli per email o dettargli per telefono. Infatti questa chiave serve solo per criptare il messaggio, ma è completamente inutile per decriptarlo. Dunque, anche se cadesse in mani "nemiche" la chiave non servirebbe a nulla, perché non permetterebbe di decifrare nessun messaggio.

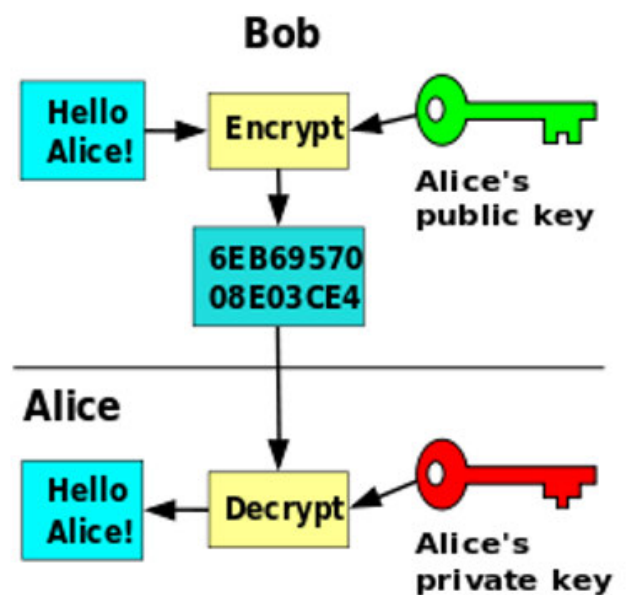


Figura 5: Schema di funzionamento del protocollo RSA (By Davidgothberg - Own work, Public Domain)

Nell'algoritmo RSA chiave pubblica e chiave privata vengono generate insieme e sono strettamente collegate perché servono per le due operazioni opposte di cifratura e decifratura. Pur essendo collegate, è molto oneroso ricavare una dall'altra.

Per un attaccante è praticamente impossibile risalire alla chiave privata partendo dalla chiave pubblica.

Ma come funziona RSA? Tutto comincia dalla scelta di due numeri primi. Supponiamo per semplicità che i due numeri scelti siano:

$$P = 11 \quad Q = 3$$

Definiamo:

$$N = (P \cdot Q) = 11 \cdot 3 = 33$$

il prodotto di questi due numeri

$$R = (P-1) \cdot (Q-1) = (11-1) \cdot (3-1) = 10 \cdot 2 = 20$$

il prodotto dei due numeri diminuiti di una unità.

A questo punto bisogna trovare un terzo **numero casuale E** di valore inferiore a R, tale che E e R siano primi fra loro (cioè non abbiano divisori in comune a parte l'unità).

Il numero più piccolo che ha queste proprietà nel nostro caso è 3.

Infatti i divisori primi di 20 sono 5 e 2 perché

$$20 = 5 \cdot 2 \cdot 2$$

Il più piccolo numero primo che non ha divisori comuni con 5 e 2 è il numero 3.

Quindi:

$$E = 3$$

Nella realtà i numeri scelti sono molto più grandi, ad esempio: si sceglie $E = 2^{16} + 1 = 65537$

Qui per semplicità mostriamo il funzionamento dell'algoritmo con numeri piccoli.

Ora dobbiamo trovare un numero D, tale che

$$1 < D < R$$

Cioè, nel nostro caso, compreso fra 1 e 20.

Questo numero D deve tale per cui il resto di $E \cdot D$ diviso R deve essere 1.

In altre parole: $(E \cdot D) \bmod R = 1$

Si può dimostrare che esiste un solo numero D che ha queste proprietà.

Nel nostro caso dobbiamo trovare D tale per cui

$$3 \cdot D \bmod 20 = 1$$

L'unico numero intero D che soddisfa alla relazione precedente è $D = 7$. Infatti: $7 \cdot 3 = 21$ e 21 diviso 20 produce come resto 1.

Abbiamo dunque ricavato entrambe le chiavi:

- La **chiave pubblica** è formata dalla coppia di valori E,N (nel nostro caso: 3,33)
- La **chiave privata** è formata dalla coppia di valori D,N (nel nostro caso: 7,33).

Le due chiavi, pubblica e privata, condividono il valore di N (il prodotto tra i due numeri primi scelti all'inizio) e tale valore è fondamentale per le operazioni di cifratura e decifratura.

Vediamo ora come avviene la cifratura prendendo come esempio un semplicissimo messaggio costituito da un unico numero $M = 6$.

Il valore 6 potrebbe per esempio essere il codice ASCII di una singola lettera di un messaggio da cifrare. Naturalmente l'esempio è del tutto irrealistico e non ha nessun interesse pratico: serve solo per illustrare il funzionamento del metodo per generare la coppia di chiavi.

Per **cifrare** il messaggio usiamo la chiave pubblica (cioè la coppia E,N = 3, 33) nel seguente modo:

$$Msg_Cifrato = (Msg_Chiaro)^E \bmod N = 6^3 \bmod 33 = 216 \bmod 33 = 18$$

Per **decifrare** il messaggio usiamo la stessa procedura ma con la chiave privata (ovvero la coppia D,N = 7, 33)

$$Msg_Chiaro = (Msg_Cifrato)^D \bmod N = 18^7 \bmod 33 = 612220032 \bmod 33 = 6$$

Nell'esempio è stata usata la chiave pubblica per criptare il messaggio e poi la chiave privata per decriptarlo. Da notare che posso fare anche il contrario: utilizzare la chiave privata per criptare il messaggio, poi decriptarlo con la chiave pubblica. Que-

sto torna molto utile nel caso delle firme dei certificati (come vedremo dopo).

In altre parole partendo dallo stesso messaggio in chiaro riottengo il messaggio in chiaro:

- sia se applico prima la chiave privata per criptare e poi la chiave pubblica per decriptare
- sia se applico prima la chiave pubblica per criptare e poi la chiave privata per decriptare

Proviamo:

- $\text{Msg_Chiaro} = 9$
- Chiave pubblica formata dalla coppia di valori E, N (nel nostro caso: 3,33)
- Chiave privata formata dalla coppia di valori D, N (nel nostro caso: 7,33).

Cifriamo con la chiave pubblica:

$$\text{Msg_Cifrato} = (\text{Msg_Chiaro})^E \bmod N = 9^3 \bmod 33 = 729 \bmod 33 = 3$$

$$\text{Msg_Chiaro} = (\text{Msg_Cifrato})^D \bmod N = 3^7 \bmod 33 = 2.187 \bmod 33 = 9$$

Ho ritrovato il messaggio in chiaro

Cifriamo con la chiave privata:

$$\text{Msg_Cifrato} = (\text{Msg_Chiaro})^D \bmod N = 9^7 \bmod 33 = 4.782.969 \bmod 33 = 15$$

$$\text{Msg_Chiaro} = (\text{Msg_Cifrato})^E \bmod N = 15^3 \bmod 33 = 3.375 \bmod 33 = 9$$

Abbiamo ritrovato il messaggio in chiaro anche cifrando con la chiave privata!

Cerchiamo di capire su cosa si basa la sicurezza dell'algoritmo RSA.

Chi conosce la chiave pubblica sa i valori di E e di N (nel nostro esempio 3 e 33). Per ricostruire da questa la chiave privata, dal momento che N è noto e comune alle due chiavi, un ipotetico attaccante dovrebbe riuscire a calcolare il valore di D (nel nostro esempio 7 supponendo, come accade di solito, che il numero E sia fisso e noto).

Per ottenere questo risultato egli potrebbe partire da N che è il prodotto di P e Q , i due numeri usati all'inizio per generare le chiavi. Se da N potessi ricavare P e Q potrei ricavare R ($R = (P-1)*(Q-1)$) e

da lì potrei risalire a " D ", elemento privato della chiave privata.

Tuttavia, in generale, dato un numero intero, non è semplice scomporlo nei fattori che lo hanno generato, a meno di non voler fare tutte le prove con tutti i numeri.

Per comprendere il problema, si consideri il numero $N = 142.283$. Esso è il prodotto di due numeri primi, ma quali sono questi numeri? L'unico modo per scoprirlo è usare un computer che provi a dividere 142.283 per tutti i numeri primi noti. Nel caso di un numero relativamente piccolo come questo, non occorre molto tempo per un moderno computer per scoprire che $142.283 = 263 * 541$

Se però i due numeri primi P e Q scelti all'inizio sono molto grandi, il compito per un eventuale assalitore si rivela praticamente impossibile.

Vi starete chiedendo tutte queste formule cosa ci azzeccano con il mondo reale. Vorrei rispondere con un esempio pratico.

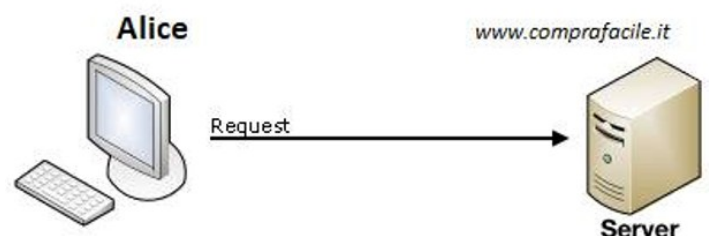
Al giorno d'oggi quando navighiamo in internet di fianco all'indirizzo del sito appare sempre un lucchetto:



Cosa significa questo lucchetto? Che la comunicazione è crittografata con un algoritmo a chiave pubblica che ha gli stessi principi di RSA. Vediamo in dettaglio cosa succede.

La nostra amica Alice vuole andare sul sito *comprafacile.it*, e così scrive l'indirizzo nel suo browser.

Il browser interroga un server DNS per tradurre le lettere dell'indirizzo *comprafacile.it* (comprensibile dagli umani) in un indirizzo IP comprensibile dalle macchine ed invia una richiesta al server che ospita il sito web.



Il server di *comprafacile.it* risponde inviando al computer di Alice la sua chiave pubblica.



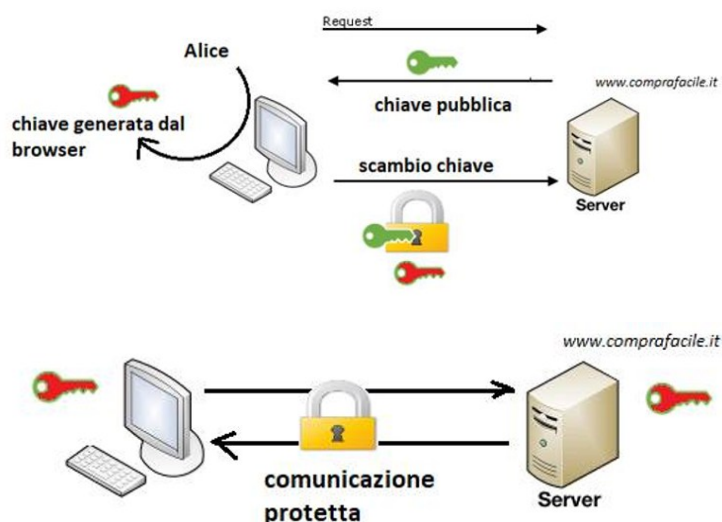
Alice a questo punto usa la chiave pubblica di *comprafacile.it* per comunicare direttamente con il server.

In realtà le cose non stanno proprio così perché:

- Alice potrebbe usare direttamente la chiave pubblica per crittografare tutte le comunicazioni ma gli algoritmi a chiave pubblica sono molto lenti
- Alice deve essere sicura di comunicare con il server *comprafacile.it* e non con un impostore.

Quindi ecco come avvengono realmente le cose:

1. La cifratura a chiave pubblica viene usata solo per scambiarsi una password condivisa e poi si usa un algoritmo simmetrico di crittografia per le successive comunicazioni. Spesso la password condivisa viene aggiornata con una certa periodicità per maggiore sicurezza.



2. In realtà il server non manda semplicemente la chiave pubblica al PC di Alice, ma vi è anche l'intermediazione di una **Certification Authority** che certifica l'identità del server e dunque

Alice può stare sicura di comunicare con il vero sito *comprafacile.it* e non con un impostore. Vedremo più avanti i dettagli di questo aspetto.

Ed ora Approfondiamo perché serve una Certification Authority. Senza tale garante la comunicazione sarebbe suscettibile di un attacco del tipo **man-in-the-middle**.

Supponiamo che Alice voglia comunicare con Bob. Alice deve dunque conoscere la chiave pubblica di Bob. Bob può usare un canale non sicuro per comunicare tale chiave ad Alice.

Supponiamo però che un terzo attore, Eva, possa intercettare le comunicazioni tra Alice e Bob su tale canale non sicuro e sia anche in grado di fermarle mettendosi in mezzo. Eva può mettere in azione un attacco di tipo **eavesdropping**.

Ma come funziona?

Eva riceve e memorizza il messaggio indirizzato ad Alice, messaggio che contiene la chiave pubblica di Bob. Sostituisce tale messaggio con uno identico in cui inserisce la sua chiave pubblica (la chiave pubblica di Eva) e lo manda ad Alice. In questo modo Alice, che non può verificare tramite una CA il vero mittente del messaggio, riceve la chiave pubblica di Eva credendo che sia quella di Bob. Alice userà dunque la chiave pubblica di Eva per cifrare i messaggi indirizzati a Bob. Eva potrà decriptare i messaggi che Alice crede di inviare a Bob e poi criptarli con la chiave pubblica di Bob (o con la chiave simmetrica condivisa nelle comunicazioni con Bob). Alice e Bob crederanno di comunicare tra loro, invece comunicheranno con Eva.

Riassumendo, se una terza persona si inserisce nella distribuzione della chiave, la chiave può essere sostituita compromettendo la sicurezza dell'intero processo di comunicazione.

La cifratura asimmetrica con algoritmi di crittografia a chiave pubblica "di tipo RSA" consente di risolvere anche il **problema dell'identificazione del mittente** tramite il meccanismo della firma digitale e la realizzazione della CA (Certificate Authority).

Si noti che il problema dell'identificazione del mittente è un problema di tipo diverso rispetto a quello della codifica del messaggio. Io potrei voler manda-

re un messaggio in chiaro al mio interlocutore ma facendo in modo che il mio interlocutore sia sicuro di comunicare con me.

Dobbiamo innanzitutto capire come funziona una **firma digitale**.

Nell'algoritmo RSA le chiavi pubblica e privata possono essere usate in modo intercambiabile, ovvero

msg in chiaro -> chiave pubblica -> msg criptato -> chiave privata -> msg in chiaro

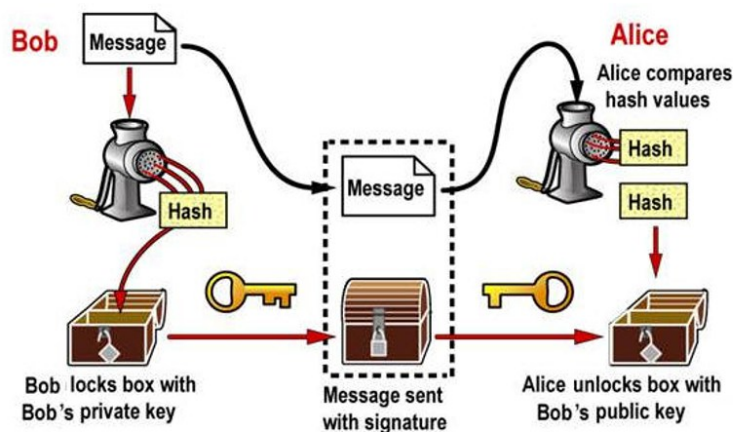
ma anche:

msg in chiaro -> chiave privata -> msg criptato -> chiave pubblica -> msg in chiaro

Supponiamo che Bob voglia mandare un messaggio in chiaro ad Alice, ma facendo in modo che Alice possa essere sicura di riceverlo proprio da Bob. Supponiamo che tramite il meccanismo di CA che vediamo dopo Alice sia sicura che la chiave pubblica di Bob appartenga proprio a lui. Qui non ci stiamo focalizzando sulla crittografia del messaggio, ma sulla verifica del mittente.

Bob scrive il messaggio in chiaro. Una volta che ha finito di scriverlo ne calcola l'**hash** con uno degli algoritmi pubblicamente disponibili (es: MD5, SHA). Prende l'hash ed usa la sua chiave privata per codificarlo. Spedisce quindi ad Alice il messaggio in chiaro e l'hash del messaggio codificato con la sua chiave privata.

Alice riceve il messaggio, ne calcola l'hash e poi decifra la parte crittografata usando la chiave pubblica di Bob.



Se i due hash coincidono Alice può essere sicura che il messaggio sia stato proprio inviato da Bob. Solo lui infatti possedendo la chiave privata può codificare in tal modo il messaggio!

Adesso che abbiamo capito come funziona una firma digitale, se riusciamo a trovare un modo per essere sicuri che la chiave pubblica di Bob sia proprio associata a lui, abbiamo definitivamente risolto il problema dell'identificazione del mittente e dunque ci siamo anche messi al riparo da attacchi di tipo man-in-the-middle o eavesdropping. Per far questo abbiamo bisogno della Certification Authority.

Le **CA** (Certification Authority) sono enti od organizzazioni (pubbliche o private) abilitate a rilasciare certificati digitali. Sono un ente terzo di fiducia che certifica l'identità e la validità dei soggetti che richiedono o offrono un servizio online.

Le CA hanno diversi compiti, tra cui:

- Verificare l'identità del richiedente un certificato digitale.
- Rilasciare il certificato digitale che attesta l'identità del richiedente.
- Firmare digitalmente il certificato con la propria chiave privata, per stabilire la fiducia nella validità del certificato.
- Gestire il registro delle chiavi pubbliche in modo sicuro e protetto da attacchi.
- Revocare o sospendere i certificati in caso di richiesta dell'interessato o in caso di abusi, falsificazioni, ecc.
- Mantenere aggiornata la lista (pubblica) dei certificati revocati o sospesi

Nella crittografia asimmetrica un **certificato digitale** è un documento elettronico che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto (una persona, una società, un computer, etc). In pratica i certificati digitali sono dei file usati per garantire l'identità di un soggetto. Possono essere certificate persone fisiche, organizza-

zioni, server, applicazioni software, siti web, reti di interconnessione, contenuti digitali (ovvero il file che rappresenta il contenuto); ogni CA precisa nel proprio CPS (Certificate Practise Statement) chi sono le entità finali che essa è disposta a certificare e per quali scopi di utilizzo.

Ogni certificato digitale ha un intervallo temporale di validità: di conseguenza ogni certificato scaduto non è più valido e viene revocato. Un certificato può essere revocato prima della sua scadenza se la chiave privata è stata compromessa oppure il soggetto che lo possedeva ha cambiato residenza, email di riferimento, nazionalità, etc..

I certificati digitali vengono rilasciati dalle autorità di certificazione, anche dette Certification Authority o CA. La CA rilascia i certificati a chi ne fa richiesta dopo averne verificato l'identità. La CA svolge il ruolo di garante dell'identità di chi usa il certificato da lei rilasciato, proprio come fanno le autorità di pubblica sicurezza (prefettura, comune, etc...) quando emettono documenti di identificazione quali il passaporto o la carta d'identità.

Chiunque può verificare la validità di un certificato, in quanto le CA mantengono un registro pubblico dei certificati emessi e una lista dei Certificati Revocati disponibile per la verifica per via telematica da parte di tutti gli utenti.

L'elenco delle CA pubbliche italiane è reperibile a questo [LINK](#)

Un certificato emesso da una CA tipicamente contiene:

- la chiave pubblica del possessore;
- il nome del possessore: se il possessore è una persona fisica si tratterà di nome e cognome, data di nascita etc., se invece è un server web sarà presente l'indirizzo web e il nome della compagnia titolare del dominio;
- la data di scadenza della chiave pubblica;
- il nome della CA che ha emesso il certificato;
- la firma digitale della CA che ha emesso il certificato.

Esistono vari standard per la creazione di certificati, attualmente il più affermato è quello definito dallo **standard internazionale X.509**

Ma come funziona nella pratica?

Supponiamo che Mario Rossi, il gestore di *comprafacile.it* voglia un certificato digitale per garantire di essere il legittimo proprietario della chiave pubblica del suo sito.

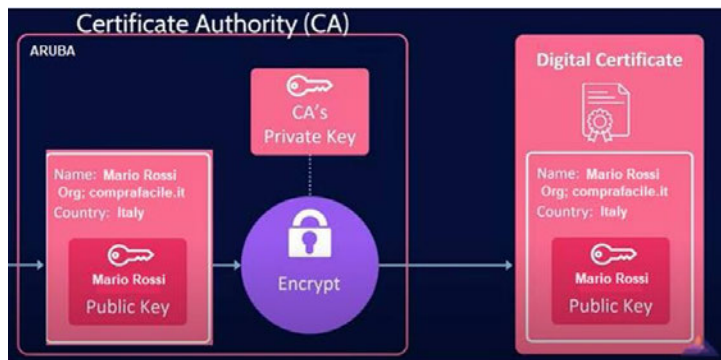
Si rivolge ad una delle CA ufficialmente abilitate (es: Aruba). Invia la richiesta ad Aruba, insieme a una copia della propria chiave pubblica ed a tutti i suoi dati personali.





Aruba verifica attraverso controlli, chiamate telefoniche o anche incontri di persona che Mario Rossi sia davvero il proprietario di comprafacile e della sua chiave pubblica.

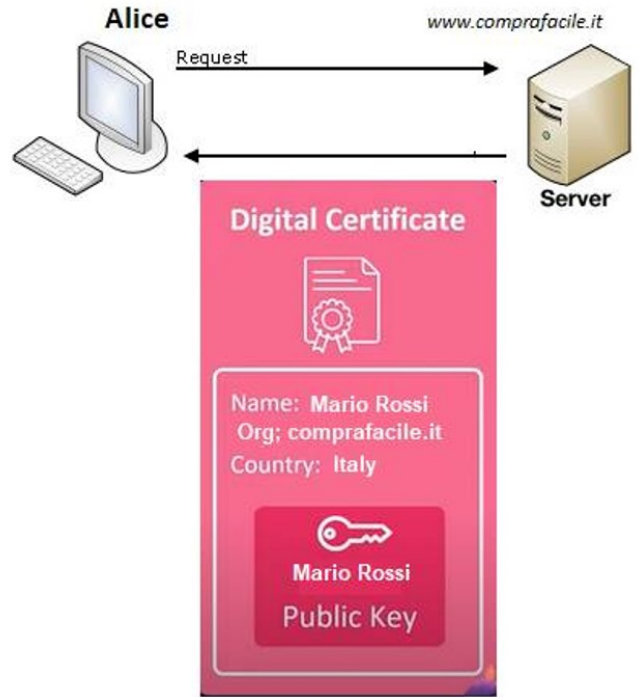
A questo punto Aruba, dopo aver confermato l'identità di Mario Rossi, cifra le informazioni del proprietario (dati personali e chiave pubblica) usando la propria chiave privata (cioè la chiave privata di Aruba).



Questo documento (file) cifrato con la chiave privata dell'Autorità di Certificazione (nel nostro esempio Aruba) è appunto il certificato digitale.

In pratica ogni browser contiene un elenco di tutte le chiavi pubbliche delle Autorità di Certificazione abilitate al rilascio dei certificati digitali. In questo modo il browser è in grado di verificare se il certificato digitale ricevuto è stato davvero autorizzato da una Autorità di Certificazione. Infatti il certificato digitale viene criptato usando la chiave privata dell'ente certificatore: in questo modo chi lo riceve può verificare che si tratta di un certificato originale, decrittandolo con la chiave pubblica del certificatore.

Adesso possiamo finalmente vedere cosa succede quando Alice vuole fare acquisti su comprafacile.it. Alice invia una richiesta al sito e quest'ultimo risponde inviandole una copia del suo certificato digitale.



comprafacile.it non invia ad Alice direttamente la propria chiave pubblica. Invece invia il certificato digitale al cui interno si trova la chiave pubblica di *comprafacile.it*

A questo punto Alice può leggere dentro al certificato digitale la chiave pubblica di *comprafacile.it* ed è quindi in grado di iniziare lo scambio sicuro dei dati. Un eventuale man-in-the-middle che intercettasse il certificato digitale inviato da *comprafacile.it* ad Alice potrebbe provare a sostituirlo con un proprio certificato digitale, ma la sostituzione non funzionerebbe. Alice infatti si accorgerebbe subito che il certificato digitale ricevuto non è l'originale, perché non è stato criptato usando la chiave privata di *comprafacile.it*

Tutto bene?

Sì, ma fino ad oggi.

O meglio fino a quando abbiamo teorizzato la possibilità di costruire computer quantistici.

Un **computer quantistico** è un tipo di computer che utilizza i principi della meccanica quantistica per elaborare informazioni in modo radicalmente diverso rispetto ai computer classici.

A differenza dei computer tradizionali, che utilizzano bit (che possono essere 0 o 1), i computer quantistici usano **qubit** (bit quantistici), che sfruttano due proprietà chiave della meccanica quantistica:

- **Sovrapposizione** → Un qubit può essere sia 0 che 1 contemporaneamente, aumentando enormemente la capacità di calcolo.
- **Entanglement** → Due o più qubit possono essere legati tra loro in modo che lo stato di uno influenzi immediatamente l'altro, indipendentemente dalla distanza.

Grazie a questi fenomeni, un computer quantistico può risolvere alcuni problemi molto più velocemente di un computer classico, come ad esempio la fattorizzazione di numeri primi

Questo lo può fare grazie ad un algoritmo: l'**algoritmo quantistico di Shor** ([Link](#))

E questo metterà in crisi praticamente tutto il mondo dell'informatica dato che i sistemi di crittografia sono usati praticamente ovunque: Bancomat, siti internet, social networks, etc...

Ma l'uomo non sta mai fermo e sta inventando altri metodi per crittografare i propri messaggi.

Una possibile soluzione ci arriva dalla **crittografia quantistica**, che consiste in un approccio alla crittografia che utilizza peculiari proprietà della meccanica quantistica nella fase dello scambio della chiave per evitare che questa possa essere segretamente intercettata da un attaccante.

Qui servono un paio di premesse sui **principi della meccanica quantistica**.

Un **primo principio** è il **principio di indeterminazione di Heisenberg** che dice che non è possibile conoscere, simultaneamente e con precisione assoluta, alcune particolari coppie di caratteristiche di un oggetto quantistico. Queste **grandezze** si definiscono incompatibili. Alcuni esempi di coppie di grandezze incompatibili sono: la posizione e la quantità di moto, lo spin misurato su un asse (es: su-giù) e lo spin misurato su un secondo asse ortogonale rispetto al primo (es: dx-sx), la polarizzazione della luce misurata rispetto ad un asse e quella misurata rispetto ad un secondo asse inclinato di 45 gradi rispetto al primo.

Più in dettaglio se io misuro una delle due grandez-

ze incompatibili, l'altra "si resetta": ad esempio se si cerca di misurare esattamente la posizione di un elettrone, si perde la possibilità di conoscerne la quantità di moto. Se dopo misuro la quantità di moto, l'informazione sulla posizione che ho ricavato con la misura precedente non è più valida.

Il **secondo principio cardine** è che la misura che faccio alla grandezza "resettata" è veramente **casuale**. Supponiamo di aver appena resettato la misura dello spin su-giu tramite ad esempio una misura dx-sx. Lo spin dell'elettrone non è né su né giù fino al momento della mia misura, ma è in una "sovrapposizione di stati" su-giu.

Queste sono limitazioni anche in linea di principio e quindi sussistono indipendentemente dalla bontà dell'apparato di misura. Secondo la meccanica quantistica, per quante tecniche nuove e più precise si possano sviluppare per eseguire queste misure, il limite non è concettualmente eliminabile.

Come possiamo applicare questi principi in crittografia? Una volta individuata una coppia di grandezze incompatibili questa caratteristica, propria di ogni sistema su scala quantistica, può essere utilizzata per valutare se un sistema di cui si conosce lo stato è stato misurato (quindi osservato) da qualcuno.

Niente più man in the middle!

Ecco il perché.

UN PRIMO ESEMPIO

Un **protocollo** che permette lo scambio di una chiave tra due utenti e garantisce che questa non possa essere intercettata da terzi senza che i due se ne accorgano è **il BB84**, dal nome dei suoi ideatori, Bennet e Brassard, che lo realizzarono nel 1984.

Immaginiamo che Alice e Bob dispongano di un canale quantistico e di uno classico (quindi passibile di intercettazione) su cui scambiare dati.

Sul canale quantistico Alice invierà fotoni con una determinata polarizzazione scelta a caso tra quattro possibili, ad esempio: 0 gradi, 45 gradi, 90 gradi, 135 gradi

Queste orientazioni determinano rispettivamente le basi: **+**, **x** incompatibili tra loro.

Per ogni base, un'orientazione è interpretata come convenzionalmente come valore "0" e l'altra come "1" (vedi lo schema in Figura 6).

- In Base "+" le misure potranno avere solo due risultati: orientamento verticale oppure orizzontale. L'orientamento verticale è codificato per convenzione come valore "0" e quello orizzontale come valore "1"
- Anche in Base "x" le misure potranno avere solo due risultati: l'orientamento di polarizzazione a 45° è codificato convenzionalmente come "0" e quello a 135° come "1"

Si veda la figura seguente:

Base	0	1
+		
x		

Figura 6: Basi di misura e interpretazioni dei risultati come "0" e "1"

Bob, ricevuti i fotoni dovrà effettuare una misura su di essi per scoprire con che polarizzazione sono stati spediti.

Sarà quindi costretto a scegliere di fare la misura in una delle due basi che, per il principio di indeterminazione di Heisenberg, non sono compatibili: la base "+" e la base "x".

Se Bob dovesse scegliere la base sbagliata rispetto a quella usata da Alice, il risultato della misura sarà casuale, ovvero valore "0" oppure "1" con probabilità del 50%.

Il punto cruciale è che anche un eventuale attaccante si troverebbe nella stessa situazione di Bob: in-

fatti quando la spia intercetta i fotoni, dovrà scegliere di fare la misura in una delle due basi possibili e, se sceglie quella sbagliata, otterrà un risultato casuale che resetterà il risultato della misura nell'altra base.

Vediamo di capire meglio: se mandiamo un fotone con polarizzazione "0 gradi" e l'attaccante misura il fotone nella base "x", una successiva misura nella base "+" non darà più polarizzazione "0 gradi" ma darà un risultato di polarizzazione casuale tra "0 gradi" e "90 gradi"

Inviata una quantità sufficiente di fotoni, Bob invierà ad Alice pubblicamente le basi che ha utilizzato per le misurazioni (se "+" o "x"), ma non i risultati delle misure. Alice renderà note le basi che ha utilizzato per polarizzare i fotoni, ma non la polarizzazione degli stessi.

I due potranno così scartare tutti i fotoni per i quali Bob ha scelto la base sbagliata.

A questo punto Alice e Bob possederanno una serie di bit comuni ad entrambi che può essere usata per costruire la chiave segreta comune.

Quando Alice e Bob hanno usato la stessa base per la misura, infatti, se nessuno si è messo in mezzo, hanno letto lo stesso risultato e quindi condividono la stessa serie di bit.

Se una spia avesse in qualche modo intercettato i fotoni nel loro tragitto tra Alice e Bob, la metà delle volte avrebbe fatto la misura scegliendo la base sbagliata. Per il principio di indeterminazione, avrà necessariamente "resetato" la polarizzazione dell'altra base, introducendo quindi degli errori nella misura di Bob anche nel 50% dei bit che dovrebbero risultare corretti.

Quindi, se dopo aver scartato tutti i fotoni per i quali Bob ha scelto la base sbagliata, la chiave di Bob risulta diversa da quella di Alice, vuol dire che la spia ha intercettato i fotoni e che la chiave non è sicura.

Come possiamo accorgerci se una spia si è messa in mezzo senza rivelare la chiave segreta?

Alice e Bob possono scegliere insieme metà dei bit comuni e dividerli pubblicamente: se sono uguali, posso essere ragionevolmente sicuro che nessuno

si è messo in mezzo e tenere l'altra metà dei bit per creare la chiave segreta comune. Da notare che non abbiamo usato funzioni di Hash per la verifica in quanto non sono necessarie per la sicurezza della comunicazione.

Sono comunque allo studio funzioni Hash immuni ad attacchi quantistici, come **XMSS (eXtended Merkle Signature Scheme)** e **SPHINCS+**

Se verrà dimostrata l'esistenza di funzioni Hash immuni ad attacchi quantistici, Alice e Bob potrebbero verificare di non essere stati intercettati senza buttare via parte della chiave segreta. Più in dettaglio potrebbero:

- Applicare una funzione di hashing alla chiave segreta, condividere il risultato di tale funzione pubblicamente e vedere se coincide.
- Applicare la funzione di hash ad una parte dei bit comuni, dopo aver concordato su quali bit tra quelli comuni applicare la funzione di hash. Se la funzione coincide allora i bit di partenza sono uguali.

UN SECONDO ESEMPIO DI CRITTOGRAFIA QUANTISTICA

Un'altra possibilità, più recente, è quella di usare l'entanglement quantistico

Il protocollo di Ekert

Un secondo protocollo è stato proposto da Artur Ekert nel 1991. Tale protocollo è nato per consentire lo scambio di una chiave crittografica in modo sicuro tra due utenti e si basa sul principio fisico dell'entanglement quantistico.

Questo algoritmo utilizza coppie di fotoni appunto **entangled**, cioè fotoni con particolari caratteristiche di correlazione.

Supponiamo di avere una sorgente che emette con regolarità, ad esempio ogni secondo, una coppia di fotoni entangled che si propagano in versi opposti, uno verso il mittente del messaggio (Alice) e l'altro verso il destinatario (Bob).

Un sistema così preparato permette di ottenere dei fotoni nello stesso stato di polarizzazione cioè, se il primo fotone ha un certo orientamento di polarizza-

zione, anche il secondo dovrà avere necessariamente lo stesso orientamento di polarizzazione.

Le particelle entangled sono un fenomeno molto strano della meccanica quantistica.

Due particelle sono entangled (o intrecciate) quando il loro stato quantistico è correlato in modo tale che la misurazione di una influenzi istantaneamente lo stato dell'altra, indipendentemente dalla distanza che le separa.

Se io creo una coppia di particelle entangled, le separo a grossa distanza, poi faccio una misura (ad esempio della polarizzazione) su una delle due particelle, istantaneamente se misuro lo stesso parametro dell'altra, leggerò lo stesso valore.

Da notare che, quando la particella è in una sovrapposizione di stati (non c'è ancora stato il collasso della funzione d'onda), il risultato della prima misura è completamente casuale. La particella non ha "deciso" il valore da mostrare prima di separarsi dalla sua gemella. Dopo la prima misura ad una delle due particelle, la prima misura all'altra particella e le misure successive dello stesso parametro saranno uguali.

La descrizione più accurata che riesco a concepire è che è come se fosse la stessa particella, solo separata a km di distanza!

È opportuno capire che con le particelle entangled non posso trasmettere informazioni, ovvero non posso imporre alla particella che la prima lettura sia zero o uno in modo da trasmettere una informazione. E, come scrivevo prima e lo ribadisco, la particella non ha scelto se mostrare zero o uno prima di separarsi dalla sua gemella, ma la prima lettura è completamente casuale.

Come lo sappiamo? Grazie ad una serie di esperimenti denominati disuguaglianze di Bell.

Dobbiamo arrenderci al fatto che la meccanica quantistica è "non locale". Per dirla con le parole di Einstein si ha "spooky action at a distance".

Ma torniamo al **protocollo di Ekert**.

Alice e Bob si dovranno essere precedentemente accordati di eseguire misure di polarizzazione dei fotoni lungo le due direzioni prescelte (appunto 0° e 45°), ma non sulla successione delle misure da ese-

guire. Ciascuno dei due sceglierà quindi in maniera perfettamente casuale la direzione lungo cui eseguire ciascuna misura individuale. Si può notare che la scelta delle due direzioni lungo cui verranno eseguite le misure può essere successivamente resa pubblica (questo algoritmo infatti richiede in molte parti l'utilizzo di comunicazioni non riservate).

Per convenzione Alice e Bob si sono inoltre accordati di scrivere il numero 0 ogni volta in cui il fotone non supera il filtro di polarizzazione e il numero 1 ogni volta in cui esso lo supera.

Entrambi ovviamente dovranno annotare per ciascuna misura il tipo di test eseguito (verticale oppure a 45°). Per maggiore chiarezza riportiamo la situazione in tabella 1.

Alla fine di questo processo (quindi dopo aver eseguito molte misure) ognuno dei due disporrà di una tabella simile a quella mostrata in tabella 1A, in cui vengono evidenziati i fotoni che hanno superato il test e quelli che l'hanno fallito. È importante qui richiamare alcune caratteristiche di questo processo:

- i risultati delle misure sono genuinamente ca-

suali, con probabilità 50% per ciascuna possibilità. I computer tradizionali hanno difficoltà a generare numeri genuinamente casuali.

- nel caso in cui una misura venga eseguita nella stessa direzione (stessa base) da Alice e Bob, i due esiti coincideranno inevitabilmente.

A questo punto del processo sia Alice che Bob annunciano pubblicamente la direzione che hanno scelto per eseguire ciascuna misura.

La spia, se presente, solo in questo momento verrà a sapere come si sono alternate le scelte riguardo alle direzioni di polarizzazione (basi) che hanno caratterizzato le misure.

Per ottenere la chiave segreta comune, Alice e Bob eliminano dall'elenco delle loro misure tutti i casi in cui hanno effettuato misure lungo direzioni diverse l'uno dall'altro (base di misura diversa) e mantengono tutti i rimanenti risultati, che saranno coincidenti, in quanto presi usando la stessa base di misura (Tabella 1B).

Mediante Alice e Bob otterranno delle stringhe di 0 e 1 lunghe circa la metà di quelle originali (Tabella 1C), come si può calcolare facilmente.

La metà delle volte infatti avranno scelto casualmente la stessa base di misura (0° o 45°).

Rimane ancora da capire come gestire l'eventualità che un'ipotetica spia sia in grado di leggere la comunicazione sul canale quantistico.

Per gestire questa eventualità, Alice e Bob annunciano pubblicamente alcuni dei risultati che hanno ottenuto, ad esempio i casi dispari delle combinazioni in cui questi risultano identici (Tabella 2B).

Alice Bob		Alice Bob		Alice Bob	
1			0	1	
	0	1			0
1		1			1
0			1	0	
	0		0		0
	1		1	1	
	0	1			0
1			0	1	
0		0		1	
	0		0		0
0			0		0
1		1			0
	0		0		0
1		1			0
1		1			0
0			0		0
A		B		C	

Tabella 1 (1A, 1B, 1C) Le operazioni necessarie ad Alice e Bob per poter ottenere una successione di bit genuinamente casuale e comune ad entrambi. Nella Tabella A vengono riportate la base ed i risultati delle misure effettuate da Alice e Bob. Il simbolo in testa alla tabella sta ad indicare la base della misura eseguita (verticale oppure a 45°). Nella tabella B vengono invece evidenziati in grigio i casi in cui Alice e Bob ottengano risultati diversi perché hanno misurato secondo una base diversa. Eliminando dunque questi casi si ottengono i risultati in tabella C "

Alice		Bob		Alice		Bob		Alice		Bob	
1		1		1		1			0		0
	0		0		0		0	0		0	
	1		1		1		1	1		1	
0		0		0		0		1		1	
	0		0		0		0				
1		1		1		1					
	0		0		0		0				
1		1		1		1					
1		1		1		1					
A				B				C			

Tabella 2 Il procedimento che consente ad Alice e Bob di essere sicuri che nessuna spia possa aver letto la chiave intercettando i fotoni. Nella colonna A si riprende la chiave ottenuta nella colonna C della Tabella 1. Vengono enunciati pubblicamente tutti gli esiti dispari della chiave (in grigio) e confrontati per verificare che siano uguali. Questi dovranno poi essere rigettati per ottenere quindi una stringa di lunghezza ridotta (colonna C) che corrisponde alla chiave finale

Questo passaggio ha l'unico scopo di verificare che i risultati resi pubblici siano coincidenti per entrambi; essendo stati resi noti non potranno essere utilizzati, e dovranno pertanto essere rigettati, ottenendo la Tabella 2C. Il punto concettualmente rilevante di quest'ultima operazione è dato dal fatto che, effettuando una misurazione sul sistema quantistico, si ha inevitabilmente una certa probabilità di distruggere le correlazioni perfette degli esiti ottenuti da Alice e Bob.

Si può dimostrare che:

- la probabilità che la lettura del canale quantistico da parte della spia passi inosservata è pari a $3/4$ elevato al numero di bit scartati nell'ultimo passaggio.

Analizziamo il caso in cui la spia cerchi di intercettare i risultati (ad esempio) di Bob, ponendo un analizzatore di polarizzazione in una delle due direzioni. Basterà considerare solo i casi in cui Alice e Bob eseguono misure nella stessa direzione in quanto gli altri casi, come abbiamo visto, verranno scartati.

Se la spia effettua una misura, sappiamo dalla teoria che un attimo dopo entrambi i fotoni (in quanto entangled) saranno polarizzati nella direzione scelta

dalla spia stessa. Avremmo quindi due possibilità:

- Sia Alice che Bob hanno scelto la direzione della spia, quindi i loro risultati coincideranno.
- Alice e Bob hanno scelto l'altra direzione

Analizziamo il caso in cui la spia abbia effettuato una misura di polarizzazione verticale e che i nostri protagonisti abbiano scelto invece una polarizzazione a 45° . La probabilità che possano comunque ottenere risultati identici risulta essere pari ad $1/2$, in quanto dopo la polarizzazione verticale effettuata dalla spia, la polarizzazione obliqua sarà resettata dunque Alice e Bob avranno il 50% di probabilità di misurare lo stesso valore di polarizzazione obliqua.

Le casistiche possibili di misura di polarizzazione sono 4:

- Alice 45° , Bob 45°
- Alice 45° , Bob 135°
- Alice 135° , Bob 45°
- Alice 135° , Bob 135°

Come si può vedere da questo elenco, nel 50% dei casi le misure sono uguali e nel 50% dei casi le misure sono diverse.

Avremmo quindi che nella metà dei casi l'intervento della spia non avrà alcun effetto avendo misurato la polarizzazione secondo la stessa base, mentre nell'altra metà dei casi (la spia misura la polarizzazione secondo una base diversa), Alice e Bob misureranno la stessa grandezza la metà delle volte.

Tre volte su quattro Alice e Bob non possono accorgersi dell'intervento della spia.

Ma una volta su 4 (50% di probabilità che la base scelta dalla spia sia diversa moltiplicato per il 50% di probabilità che Alice e Bob misurino valori di polarizzazione diversi) le misure di Alice e Bob saranno diverse.

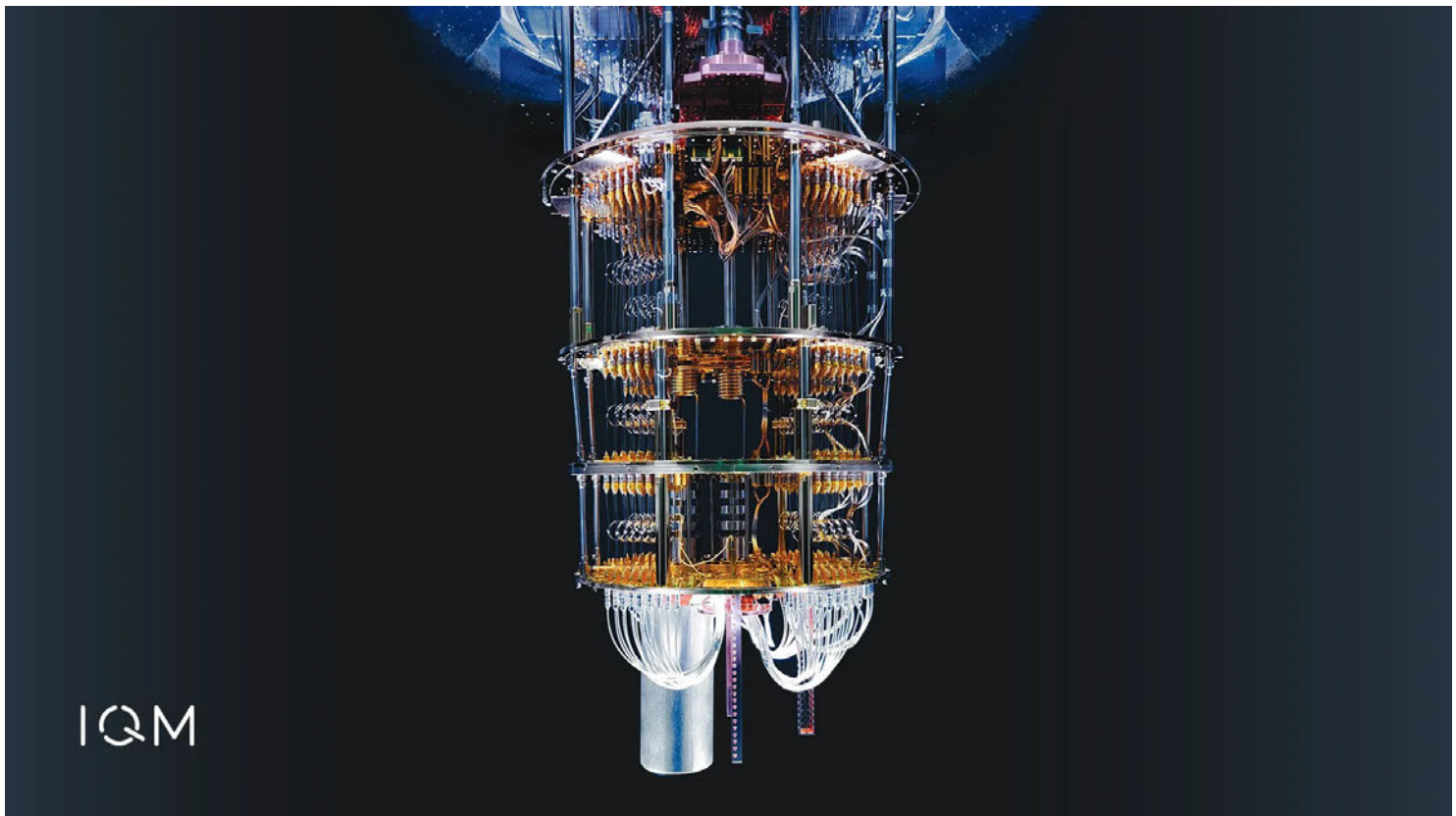
Se Alice e Bob enunciano i risultati di N misure la probabilità che non si presenti alcun esito discorde risulta essere pari alla potenza N -sima di $3/4$. Ad esempio, se Alice e Bob enunciano i risultati di 100 bit la probabilità che non si presenti alcun esito discorde, nonostante vi sia un terzo osservatore tra i due, è di $3/4$ elevato alla 100. Questo numero è molto piccolo, dell'ordine di 10 elevato alla (-13).

In altre parole, la probabilità che 100 esiti risultino coincidenti anche con la presenza di una spia, può verificarsi solo una volta ogni diecimila miliardi di casi. Se le 100 misure coincidono, quindi, Alice e Bob possono essere sicuri al di là di ogni ragionevole dubbio che non vi sia una spia in ascolto.

A questo punto il grosso problema dello scambio delle chiavi è stato risolto e si può procedere a realizzare un cifrario di Vernam, che essendo un cifrario perfetto risulta essere assolutamente inviolabile (se realizzato correttamente).

L'uomo da sempre gioca una eterna partita a scacchi tra inventori di nuovi algoritmi di crittografia ed attaccanti che cercano di decifrarli. Ogni nuovo algoritmo crittografico è una fortezza destinata a incontrare il genio di chi troverà il modo di oltrepassarla.

Questa eterna rincorsa tra guardie e ladri forse non avrà mai fine.

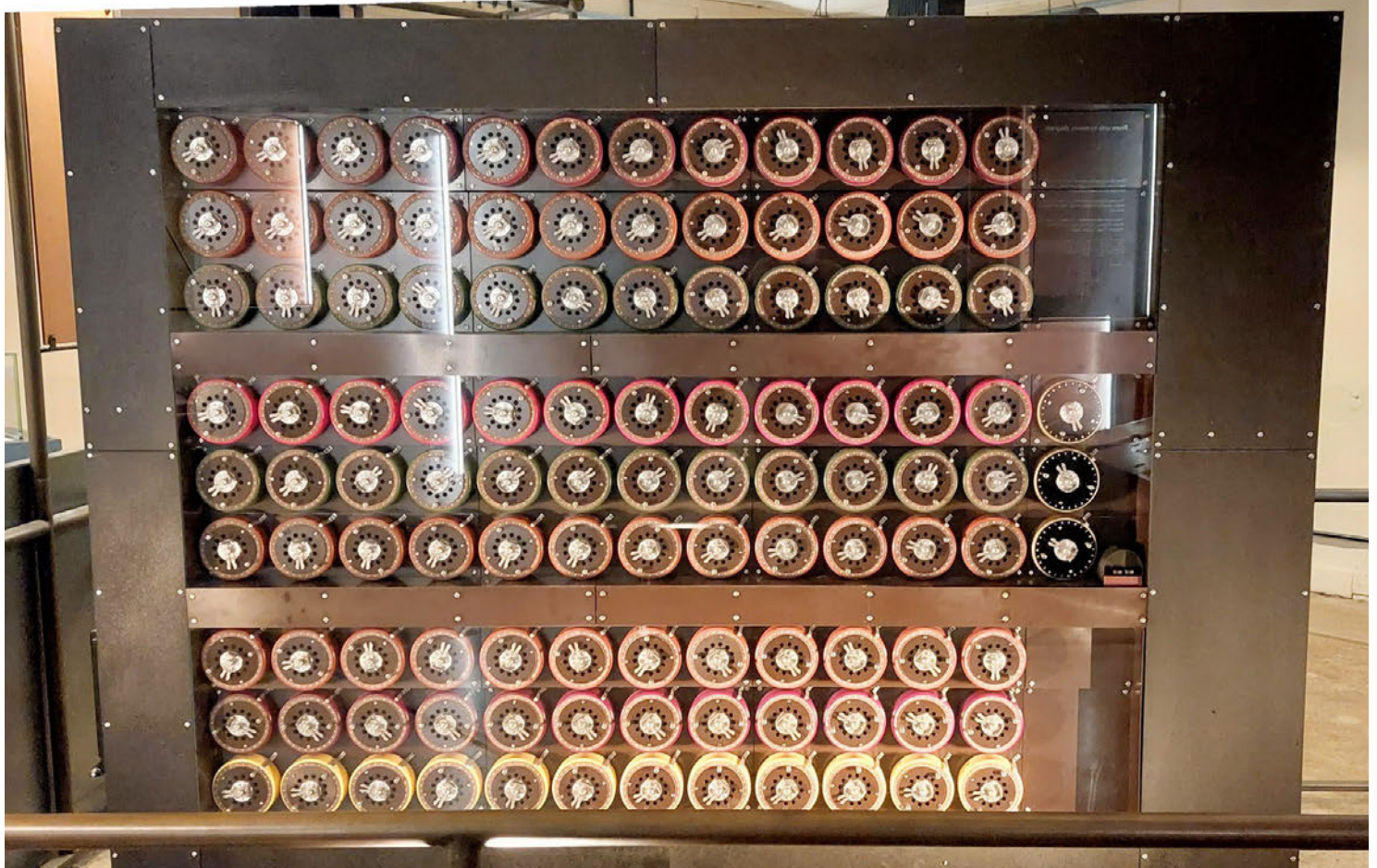


VLQ, il computer quantistico realizzato dall'azienda finlandese IQM e installato a Ostrava, in Repubblica Ceca, è il secondo sistema quantistico operativo in Europa. Interamente progettato e costruito da partner industriali europei nell'ambito del programma Quantum Technologies Flagship, rappresenta un tassello importante nella corsa del continente verso l'autonomia tecnologica nel settore. (Credit: IQM)

ALAN TURING

Dal codice ENIGMA all'AI

di Davide Borghi



A complemento dell'articolo di Leonardo Avella, vorrei contribuire con questo mio approfondimento su Alan Turing e il suo lavoro nel decrittare il codice nazista **Enigma**, durante la Seconda Guerra Mondiale, a Bletchley Park, luogo che è stato anche meta di un nostro viaggio scientifico due anni fa. Alan Turing, che ha anche posto le basi dell'Intelligenza Artificiale e che, per primo, si è chiesto: "Possono le macchine pensare?".

L'Enigma: Il Codice Indecifrabile

All'alba della Seconda Guerra Mondiale, la Germania nazista affidava la sicurezza delle proprie comunicazioni militari a una macchina leggendaria: Enigma. Questo dispositivo elettromeccanico utilizzava un sistema di rotori per trasformare i messaggi in un

groviglio di lettere apparentemente casuale. La complessità del sistema era tale che il numero di combinazioni possibili era nell'ordine dei milioni di miliardi, rendendo un attacco basato sulla "forza bruta" (ovvero provando ogni combinazione a mano) del tutto impossibile per l'epoca, di parecchi ordini di grandezza.

Il primo passo verso la violazione di questo segreto non avvenne però in Inghilterra, ma in Polonia. Già all'inizio degli anni '30, il matematico **Marian Rejewski** e il *Biuro Szyfrow* (ufficio dei servizi segreti polacchi) erano riusciti a decodificare una prima versione di Enigma sfruttando debolezze sistematiche, come la ripetizione delle chiavi all'inizio dei messaggi. Tuttavia, quando i tedeschi aumentarono la complessità della macchina aggiungendo nuovi

rotori, i polacchi si resero conto di non avere più le risorse per continuare. Il 24 luglio 1939, poche settimane prima dell'invasione della Polonia, consegnarono i propri segreti e una replica di Enigma ai servizi segreti britannici e francesi, che furono quantomeno sorpresi dei progressi polacchi in questo campo.



Una macchina crittografica Enigma nazista, sul fronte orientale

Bletchley Park: La Fabbrica dei Codici

Il centro nevralgico della crittografia britannica fu stabilito a **Bletchley Park**, una tenuta a nord di Londra che divenne la sede della *Government Code & Cypher School*. Qui fu reclutato **Alan Turing**, un giovane matematico di Cambridge che era tra i pochissimi al mondo a possedere ricerche approfondite sia sulla logica computazionale che sulla crittografia.

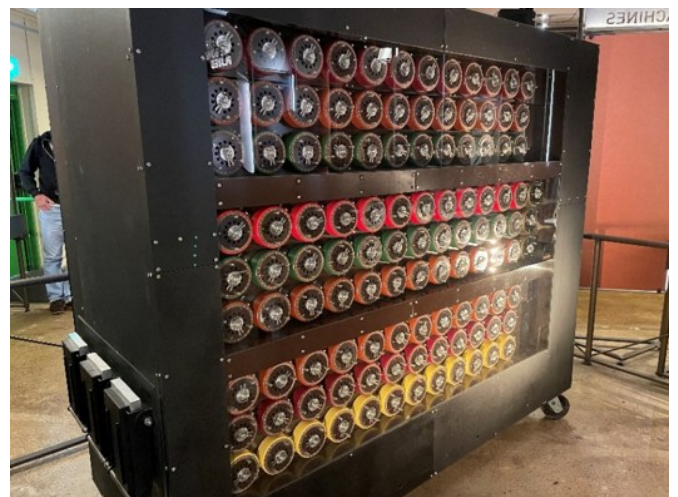
Due anni fa ci siamo andati in visita con un viaggio scientifico Cosmo-UTE, dove ho fatto da guida, viaggio che ci ha anche portato il giorno prima a vedere una manifestazione aerea di velivoli della Seconda Guerra Mondiale a Duxford, UK. Il viaggio

era abbinato al corso UTE da me tenuto a tema Intelligenza Artificiale, che ha completato l'anno scorso la sua terza edizione.

Turing comprese immediatamente che per battere una macchina serviva un'altra macchina. Insieme a Gordon Welchman, ideò la "**Bombe**", un dispositivo elettromeccanico progettato per automatizzare la ricerca delle chiavi di Enigma. La prima "Bombe" entrò in servizio nel marzo 1940, ma fu solo con l'introduzione della "*Diagonal Board*" di Welchman, a metà dello stesso anno, che la macchina divenne davvero efficace nel ridurre i falsi allarmi.

Il lavoro a Bletchley Park fu condotto in totale segretezza da migliaia di persone. Tra queste moltissime donne, fra cui le "**WRENS**" (**Women's Royal Naval Service**). La segretezza del lavoro svolto in questo sito nella brughiera inglese, sarà peraltro tenuto per diversi decenni, ben oltre il termine del secondo conflitto mondiale. Ma il risultato, e forse era proprio questo il segreto ben protetto, ebbe un impatto devastante sull'Asse e su tutta la guerra. Grazie alle intercettazioni denominate **Ultra**, gli Alleati riuscirono ad esempio, fra le altre cose, a:

- Proteggere i convogli nell'Atlantico dai sottomarini U-Boat.
- Anticipare le mosse della Marina italiana, portando alla vittoria di **Capo Matapan** nel 1941.
- Individuare la posizione della corazzata tedesca **Bismark**.
- Ingannare Hitler sullo sbarco in Normandia tramite l'Operazione **Fortitude**.



Una riproduzione della "Bombe" di Alan Turing, Bletchley Park, UK, Settembre 2024

Si stima che gli sforzi di Turing e del suo team abbiano accorciato la guerra di almeno due anni, risparmiando milioni o decine di milioni di vite.

Colossus: L'alba del computer elettronico

Oltre a Enigma, i tedeschi utilizzavano per le comunicazioni di alto comando (tra Hitler e i suoi generali) un sistema ancora più complesso: la telescrivente **Lorenz SZ 40/42**, chiamata in codice "Tunny" dagli inglesi. Per violare questo codice, non bastavano le "Bombe" elettromeccaniche.

Fu così che, su specifiche del matematico **Max Newman**, l'ingegnere telefonico **Tommy Flowers** realizzò il **Colossus**. Entrato in funzione nel febbraio 1944, il Colossus è considerato il **primo computer elettronico digitale della storia**. A differenza delle macchine precedenti, utilizzava migliaia di valvole termoioniche come interruttori velocissimi, arrivando a leggere 5.000 caratteri al secondo da nastri di carta perforata. Nonostante la sua importanza storica, l'esistenza di Colossus rimase segreta per decenni, e Flowers morì nel 1998 senza ricevere il pieno riconoscimento pubblico per la sua invenzione.



Una rappresentazione di Alan Turing a Bletchley Park, Settembre 2024

Le basi dell'Informatica e dell'Intelligenza Artificiale

Mentre lavorava alla decriptazione, Turing stava già gettando le basi teoriche per il futuro. Già nel 1936, nel suo articolo sui "numeri computabili", aveva teorizzato la **Macchina di Turing Universale**: un modello astratto capace di eseguire qualsiasi calcolo matematico se fornito del giusto algoritmo. Questa intuizione eliminò la distinzione tra "numeri che significano cose" e "numeri che fanno cose", definendo il concetto moderno di software.

Nel dopoguerra, Turing si pose una domanda allora rivoluzionaria: **"Le macchine possono pensare?"**. Nel 1950 pubblicò l'articolo, che farà la storia, **Computing Machinery and Intelligence**, in cui propose quello che oggi conosciamo come il Test di Turing (o Imitation Game): se una macchina riesce a conversare in modo indistinguibile da un essere umano, allora può essere definita intelligente. Turing prevede anche la possibilità che le macchine potessero imparare dai propri errori, prefigurando il moderno **Machine Learning**.

Le sue idee sulla memorizzazione dei programmi influenzarono la creazione dei primi computer moderni, come l'**ACE** da lui progettato o l'**EDVAC** di **John von Neumann**, che applicò le teorie di Turing per definire l'architettura dei computer che usiamo ancora oggi. John von Neumann, ovvero **"L'uomo venuto dal futuro"**, come il titolo di una recente biografia su di lui, che consiglio vivamente. Aveva infatti tante caratteristiche di uno scienziato del XXI secolo trapiantato negli anni '40 del XX secolo!



L'immagine di Alan Turing si trova ora sul biglietto da 50 sterline in Gran Bretagna

Eredità e conseguenze attuali

L'eredità di Turing si riflette in ogni aspetto della nostra vita digitale. Dal sistema binario (bit) formalizzato da **Claude Shannon**, alla **crittografia a chiave pubblica** (come l'**RSA**) che protegge oggi i nostri acquisti online, tutto affonda le radici nelle sfide logiche di Bletchley Park.

L'Intelligenza Artificiale (IA in italiano e AI in inglese: Artificial Intelligence), che Turing vedeva come una possibilità concreta, ha oggi raggiunto traguardi incredibili:

- Sistemi di **Deep Learning** superano, ormai da parecchi anni, i campioni umani in giochi complessi come gli scacchi (Deep Blue, AlphaZero) o il Go (AlphaGo).
- Modelli linguistici come **ChatGPT** emulano la conversazione umana in modi che avrebbero sicuramente sorpreso lo stesso Turing.
- L'AI viene utilizzata in medicina per mappare il ripiegamento delle proteine (*AlphaFold*), un compito quasi impossibile per l'uomo.

Tuttavia, Turing non poté vedere i frutti del suo genio. Perseguitato per la sua omosessualità e sottoposto a castrazione chimica, morì suicida il **7 giugno 1954** ingerendo una mela al cianuro.

La sua figura è stata pienamente riabilitata solo decenni dopo, quando il velo di segretezza sulle attività di Bletchley Park è stato finalmente sollevato, rivelando al mondo l'uomo che aveva salvato la de-

mocrazia con la pura forza della logica.

Bibliografia:

- [Cronologia-universale.it](https://cronologia-universale.it) di Davide Borghi
- Bhattacharya, A. (2021). *The man from the future: The visionary life of John von Neumann*. Allen Lane.
- Bhattacharya, A. (2024). *L'uomo venuto dal futuro: La vita visionaria di John von Neumann* (L. Civalieri, Trad.). Adelphi. (Opera originale pubblicata nel 2021)
- Levesque, H. J. (2017). *Common sense, the Turing test, and the quest for real AI*. The MIT Press.
- Ottaviani, J., & Purvis, L. (2016). *The imitation game: L'enigma di Alan Turing*. La Repubblica/L'Espresso — Le Scienze.
- Turing, D. (2014). *Demystifying the Bombe*. The History Press.
- Dewdney, A. K. (1993). *The new Turing omnibus: Sixty-six excursions in computer science*. Owl Books.
- Erskine, R., & Smith, M. (Eds.). (2011). *The Bletchley Park codebreakers*. Biteback.
- Smith, M. (1998). *Station X: The codebreakers of Bletchley Park*. Channel 4 Books.



Repliche della Bombe di Turing nella Hut 11 di Bletchley Park

DRONI: I PROTAGONISTI DI UNA NUOVA ERA

Dai quadricotteri agli sciami intelligenti, dai robot terrestri ai rover marziani: come i sistemi senza equipaggio stanno cambiando il nostro mondo

di Luigi Borghi



10. INTRODUZIONE

Quando sentiamo pronunciare la parola drone, la mente corre immediatamente ai piccoli velivoli multirotores utilizzati per riprese aeree o ai mezzi militari che compaiono quotidianamente nei notiziari. In realtà il concetto di drone è molto più ampio e affascinante.

Con il termine drone si identifica oggi una vasta famiglia di sistemi unmanned, cioè privi di equipaggio a bordo. Alcuni volano nei cieli, altri si muovono sulla terraferma, altri ancora navigano in superficie o nelle profondità oceaniche. Esistono perfino droni che operano nello spazio e su altri mondi del Sistema Solare.

Negli ultimi vent'anni l'evoluzione dell'elettronica, dell'informatica, dei sensori e dell'intelligenza artificiale (AI) ha trasformato questi sistemi da semplici veicoli radiocomandati a piattaforme autonome capaci di svolgere missioni estremamente complesse.

Oggi i droni sono impiegati nell'agricoltura, nella logistica, nella ricerca scientifica, nella protezione civile, nell'esplorazione spaziale e naturalmente nel settore militare.

Più che una nuova categoria di mezzi, rappresentano un nuovo modo di concepire il rapporto tra uomo e macchina.

È un tema che merita un approfondimento, che farò in una conferenza dedicata al Civico Planetario di Modena, nell'ambito del ciclo di ottobre di "Un equinozio con il COSMo", il 13 ottobre alle ore 21.

Si può prenotare qui:

<https://planetariodimodena.it/>

Questo articolo ne offre una sintesi fedele.

2. CHE COS'È REALMENTE UN DRONE?

La definizione moderna di drone non dipende dalla forma del veicolo ma dalla sua modalità operativa.

Un drone è un sistema in grado di svolgere una missione senza la presenza diretta di un essere umano a bordo. Può essere controllato a distanza, seguire un programma prestabilito oppure prendere decisioni autonome grazie a sistemi di intelligenza artificiale.

Le dimensioni possono variare enormemente: si passa dai microdroni grandi quanto il palmo di una mano ai giganteschi velivoli strategici con aperture alari superiori a quelle di un aereo di linea.

Anche il costo può oscillare da poche decine di euro fino a centinaia di milioni di dollari.

I criteri di classificazione sono numerosi:

- livello di autonomia;
- ambiente operativo;
- missione svolta;
- tipo di propulsione;
- capacità di recupero;
- autonomia e carico utile.

La caratteristica comune è sempre la stessa: separare l'operatore dal mezzo.

10. DAI RADIOCOMANDI ALL'INTELLIGENZA ARTIFICIALE

I primi droni erano sostanzialmente modelli radiocomandati evoluti. Ogni movimento veniva deciso dall'operatore attraverso un collegamento radio.

Oggi la situazione è profondamente diversa.

Si distinguono generalmente quattro livelli di autonomia:

- I **sistemi teleguidati** eseguono esclusivamente i comandi ricevuti dall'operatore. Ne fanno parte molti droni civili e i sempre più diffusi **FPV (First Person View)**.
- I **sistemi semi-autonomi** possono seguire rotte programmate, mantenere automaticamente quota e posizione e rientrare alla base in caso di emergenza.
- I **sistemi autonomi** utilizzano algoritmi avanzati per pianificare percorsi, evitare ostacoli e svolgere missioni complesse senza intervento umano continuo.
- Infine, stanno emergendo i **sistemi coopera-**

tivi, nei quali più droni collaborano tra loro condividendo informazioni e prendendo decisioni collettive, in modo simile a quanto avviene negli sciame di insetti sociali.

4. I DRONI VOLANTI: LA RIVOLUZIONE NEI CIELI.

Quando si parla di droni si pensa quasi sempre agli **UAV (Unmanned Aerial Vehicles)**, i sistemi aerei senza pilota.

La loro diffusione è stata resa possibile dall'avvento di motori elettrici efficienti, batterie leggere e sistemi di stabilizzazione elettronica.

I più noti sono i multirotori o **multicotteri**, dotati di quattro, sei o otto eliche. La loro capacità di decollare e atterrare verticalmente (**VTOL: Vertical Take-Off and Landing**) li rende ideali per la fotografia aerea, le ispezioni industriali e le missioni di ricerca e soccorso.

Le configurazioni: dal tricottero all'ottocottero

Nel panorama dei droni ad ala rotante, i **multicotteri** rappresentano oggi la configurazione più diffusa. Velivoli sostenuti da più rotori, ciascuno azionato da un motore elettrico indipendente. La stabilità e il controllo del volo vengono ottenuti variando in tempo reale la velocità dei singoli motori tramite un **flight controller**.

Le configurazioni più comuni sono quelle a **3, 4, 6 e 8 rotori**, ciascuna con caratteristiche specifiche che la rendono adatta a differenti applicazioni (Figura 4.1.).

Il **Tricottero (3 rotori)** è una delle configurazioni più semplici. È composto da tre bracci disposti generalmente a 120°, ciascuno con un motore e un'elica. A differenza di altri multicotteri, il controllo dell'imbardata (vedi di seguito) non avviene solo variando la velocità delle eliche, ma spesso tramite un meccanismo servoassistito che inclina uno dei motori posteriori.

La struttura è relativamente leggera, quindi ha un costo inferiore. È caratterizzato da un consumo energetico minore ed una buona agilità e reattività.

È però un **sistema a ridondanza nulla**, il guasto

di un motore porta alla perdita del velivolo. La stabilità è inferiore rispetto ai quadricotteri ed ha una capacità di carico limitata. Nel caso di due motori per asse (in figura 4.1. distinti da **top** e **bottom**), pur avendo la struttura di un tricottero, di fatto diventa un esacottero, tollerante ad un guasto.

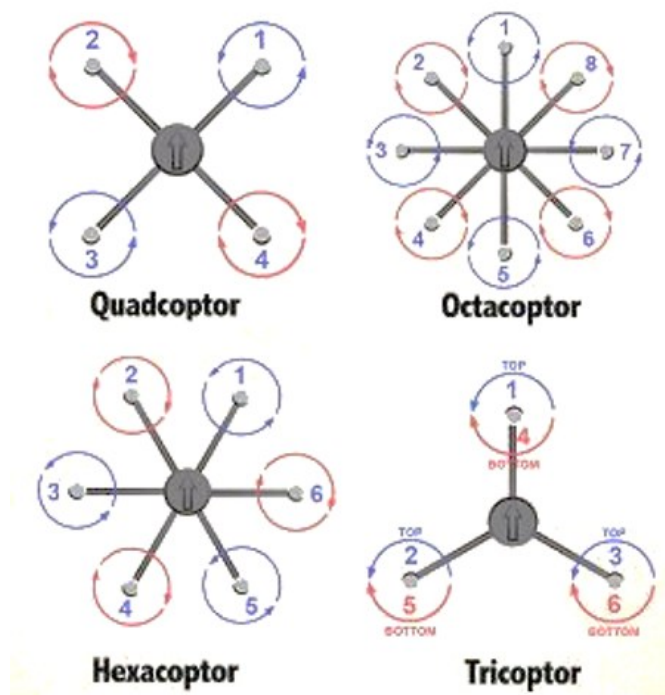


Figura 4.1. le varie configurazioni di un multicottero con i relativi sensi di rotazione delle pale

Il **quadricottero (4 rotori)** è la configurazione più comune e conosciuta. I quattro motori sono disposti ai vertici di una croce o di una X. Due motori ruotano in senso orario e due in senso antiorario, bilanciando la coppia torcente. Il controllo del volo avviene variando la spinta dei singoli rotori.

Una configurazione con un ottimo equilibrio tra semplicità, costo e prestazioni che offre grande stabilità, un controllo relativamente semplice ed una architettura meccanica compatta. È la piattaforma ideale per impieghi generali e rappresenta oggi lo standard di mercato.

Anche il quadricottero non offre alcuna tolleranza al guasto di un motore.

L'**esacottero (6 rotori)** aggiunge due rotori rispetto al quadricottero, generalmente disposti in configurazione esagonale (ma anche a doppio albero di un tricottero). L'aumento del numero di motori mi-

gliora sia la capacità di sollevamento sia la sicurezza quindi:

- Maggiore capacità di carico.
- Migliore stabilità in volo.
- Possibile volo controllato anche con guasto di un motore (in molte configurazioni).
- Migliore resistenza al vento.

Ovviamente tutto questo incide sui costi, appesantisce la struttura aumentandone i consumi. Anche l'elettronica è ovviamente più complessa.

Le sue elevate prestazioni e stabilità ne fanno la piattaforma ideale per le riprese cinematografiche professionali, lidar e rilievo topografico, trasporto sensori avanzati o in molti casi di applicazioni professionali ad alta affidabilità

L'esacottero rappresenta spesso il miglior compromesso tra carico utile e sicurezza.

L'**ottocottero (8 rotori)** è una piattaforma ad alta capacità, pensata per missioni impegnative e carichi importanti. Può avere otto bracci oppure quattro bracci coassiali con doppio motore.

È la configurazione scelta quando priorità assolute sono affidabilità e payload.

Il controllo

Ora prendiamo come esempio il più diffuso, il quadricottero, e cerchiamo di capire come il computer di bordo controlla l'assetto, la direzione e la velocità semplicemente cambiando le velocità di rotazione dei rotori senza dover gestire complicate superfici mobili come nel caso dei droni (o degli aerei) ad ala fissa,

Come si vede dalla figura 4.2. ci sono 3 assi di rotazione a cui l'assetto di un veicolo è assoggettato: roll, pitch e yaw.

Di seguito vediamo come il controllo gestisce ognuno di essi. (figura 4.3.)

Imbardata (Yaw): sfrutta il fatto che due eliche ruotano in senso orario e due in senso antiorario; alterando opportunamente le velocità si genera una coppia che fa ruotare il drone attorno all'asse verticale.

Il controllo del Yaw insieme al Pitch e Roll, determina la direzione e la velocità del veicolo.

Rollio (Roll): maggior spinta dei motori di un lato e minore nell'altro.

Beccheggio (Pitch): aumenta la spinta della coppia anteriore o posteriore.

Naturalmente, con il beccheggio orientato in avanti, aumentando la velocità su tutte e quattro le pale (**throttle**) si aumenta la velocità in avanti (o la salita con pitch a zero). Invertendo il beccheggio si frena o si va indietro (o si scende).

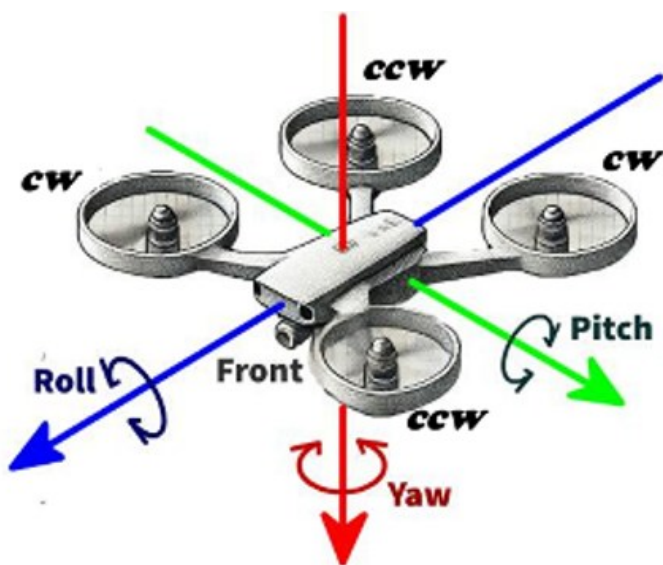


Figura 4.2 Controllo di assetto di un quadricottero

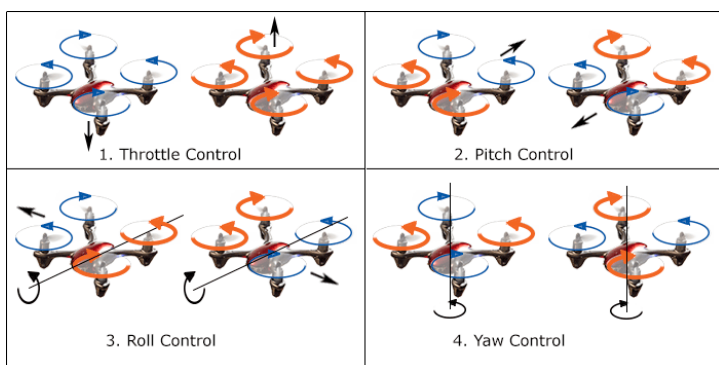


Figura 4.3 I controlli di assetto

I droni ad ala fissa

Nei droni ad ala fissa, assetto e portanza funzionano in modo molto diverso rispetto ai multicotteri: il controllo dipende dalla pressione dell'aria sulle superfici fisse e mobili del velivolo.

Queste superfici sono regolate dal sistema di guida in funzione della velocità di crociera e delle condizioni di volo.

La portanza (figura 4.4. e 4.5.), cioè la forza che sostiene il peso del veicolo, è generata dalla forma e dall'inclinazione delle ali (corda alare), dalla velocità del mezzo e dalla densità dell'aria.



Figura 4.4 Portanza e corda alare



Figura 4.5 Trazione e resistenza

Velocità e densità dell'aria influenzano anche il controllo dell'assetto, che resta però legato alla posizione delle superfici mobili, come gli **alettoni**, l'**equilibratore** e il **timone**.

In figura 4.6. sono riportati gli assi di assetto già considerati sui multicotteri applicato ad un aereo ad ala fissa.

Il tema diventa rapidamente complesso, soprattutto nei velivoli moderni, a volte senza piani di coda, difficili da governare manualmente ma gestibili tramite computer di volo ed il sistema fly-by-wire.

Poiché questo articolo non intende essere un corso

di aerodinamica o controllo dell'assetto, preferisco non approfondire questo specifico argomento.

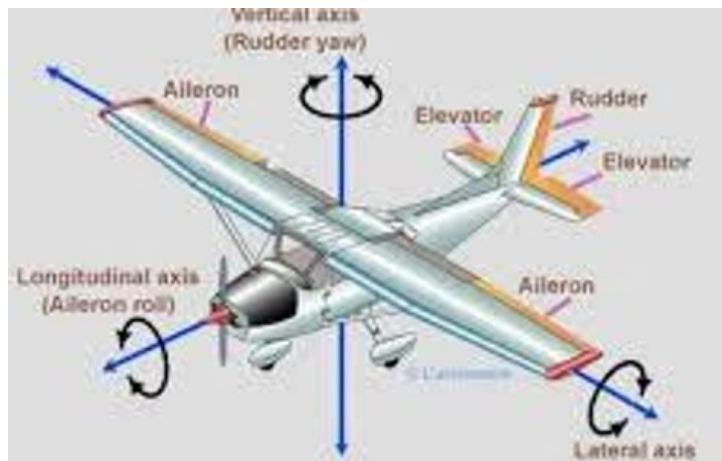


Figura 4.6 Assi di assetto

I droni ad ala fissa, simili ad aeroplani, pur richiedendo generalmente una pista nel caso di droni recuperabili o una catapulta per il lancio, offrono autonomie molto superiori e possono coprire centinaia o migliaia di chilometri.

Nel settore militare si trovano sistemi di ogni dimensione.

I droni "ibridi": convertiplani e multicotteri ad alta velocità

Il confine tra volo ad ala fissa e ad ala rotante non è sempre netto. Due esempi aiutano a chiarire questa zona intermedia e le ragioni che ne hanno favorito lo sviluppo.

Il convertiplano: un aereo ad ala fissa con capacità VTOL (Vertical Take-Off and Landing)

Il convertiplano è nato per superare uno dei principali limiti degli aerei ad ala fissa: la necessità di una pista o di un sistema di lancio per decollare e atterrare (figura 4.7.)

Il **Bell Boeing V-22 Osprey** è un convertiplano militare avanzato ad alta capacità di carico, in grado di trasportare 23 soldati equipaggiati. Grazie ai rotori basculanti, unisce il **decollo e l'atterraggio verticali** tipici di un elicottero alle **prestazioni e alla velocità di crociera** di un aereo a elica, superando i **500 km/h**.

I due motori Rolls-Royce, ciascuno da 6.150 CV,

sono installati in asse con le eliche su un sistema basculante.

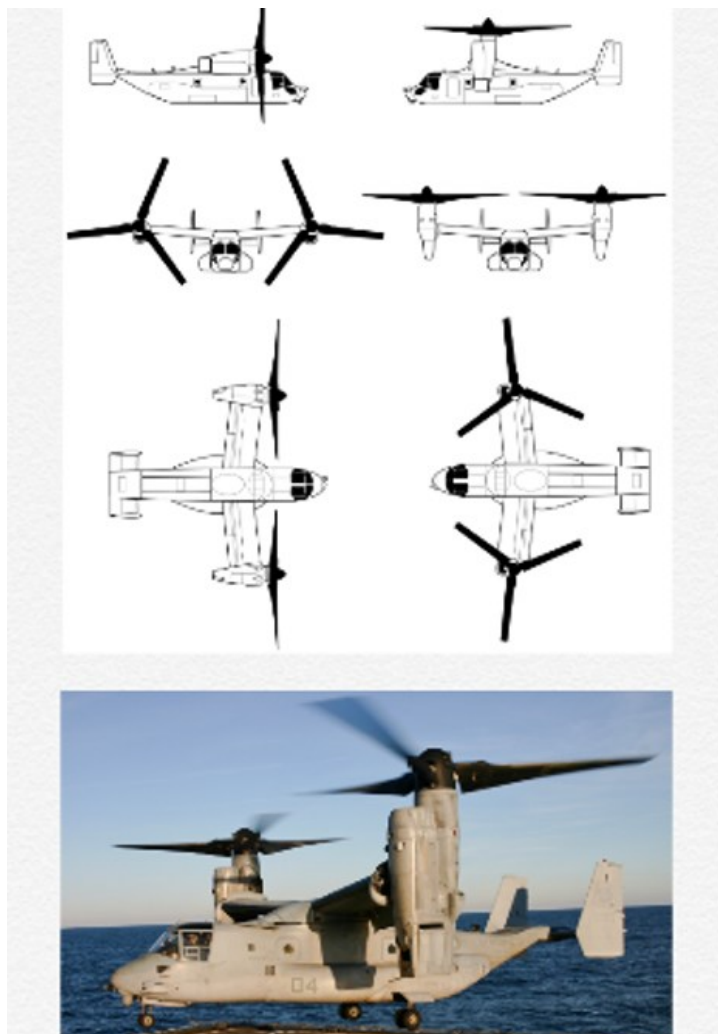


Figura 4.7 Bell Boeing V-22 Osprey

Durante decollo e atterraggio, le eliche lavorano con l'asse verticale, come in un elicottero. In crociera, il sistema ruota progressivamente fino alla posizione orizzontale, trasformando il velivolo in un aereo. In quella configurazione la portanza non dipende più solo dalla rotazione delle pale, ma anche dalle superfici alari aumentandone l'autonomia fino a raggiungere i 1.600 km.

È in servizio presso il Corpo dei Marines degli Stati Uniti e, al momento, non risultano versioni drone in sviluppo.

Questo esempio serve però a introdurre l'approccio opposto che ha portato alla realizzazione del **Black-bird** (figura 4.8.), dove i motori non sono basculanti ma tutta la struttura da assetto verticale al decollo passa ad orizzontale in crociera ad alta velocità.



Figura 4.8 il Blackbird

In questo caso si tratta di un drone elettrico che ha segnato un momento importante nella storia dell'aeronautica sperimentale, superando ufficialmente i **658 km/h** e stabilendo un nuovo record mondiale di velocità.

Realizzato da un team australiano, è uno degli esempi più notevoli di innovazione tecnologica applicata al volo remoto di un drone.



Figura 4.9 Le "ali" del Blackbird

Il quadricottero decolla e atterra come gli altri modelli della sua categoria ed è soggetto alle stesse dinamiche di volo già descritte. Tuttavia, i supporti dei rotori non sono semplici strutture: quando il drone assume un assetto orizzontale ad alta velocità, diventano vere superfici portanti, diventano "ali" fisse.

L'autonomia di un velivolo di questo tipo resta naturalmente limitata a una ventina di minuti, ma la ve-

locità raggiunta lo rende un sistema estremamente performante.

Continuando con i velivoli strani, sul podio va inserito anche il **Black Hornet**.

I piccoli Black Hornet, (figura 4.10.) grandi appena pochi centimetri, vengono utilizzati dalle forze speciali per osservare ciò che si trova oltre un edificio o una collina.



Figura 4.10 Black Hornet

Pesano circa **60 grammi**, possono atterrare sul palmo di una mano e avvicinarsi a meno di dieci metri senza essere sentiti. Sono i piccoli elicotteri nano-droni da ricognizione e volano in sciami nei cieli dell'Ucraina.

Possono tranquillamente essere considerati un'arma alla 007 e, come tutte le armi segrete, di loro si sa ben poco. In pratica si sa solo che «vengono utilizzati in modo molto efficace», come afferma la **Teledyne FLIR Defense**, l'azienda che li costruisce.

Il più strano però forse è **RoBird**. (figura 4.11)

Questo "*uccello meccanico*" è stato sviluppato dall'azienda canadese Aerium Analytics e utilizzato in Australia per ragioni molto "pacifiche": **salvare le coltivazioni dall'invasione degli uccelli**.

Il velivolo utilizza ali battenti che imitano fedelmente il movimento di un falco pellegrino in volo.

Una disciplina che prende ispirazione dai processi e dalle strategie sviluppate dalla natura per risolvere

problemi complessi.

RoBird offre un metodo innovativo, non letale e potenzialmente molto efficace per proteggere i raccolti dai danni causati dagli uccelli.



Figura 4.11 Black Hornet

Su YouTube si trova un interessante video → [Link](#)

Tornando alle applicazioni militari o civili ad alte prestazioni troviamo il **MQ-9 Reaper** statunitense (figura 4.12.). Questo drone può restare in volo per **oltre venti** ore trasportando sensori sofisticati o armamenti.



Figura 4.12 MQ-9 Reaper

Al top della gamma dei droni volanti si collocano i

giganteschi droni strategici come il **Triton** della Marina statunitense (figura 4.13.), capaci di pattugliare vaste aree oceaniche per un'intera giornata



Figura 4.13 Triton

Tutti i droni che abbiamo visto fino ad ora possono rientrare nella categoria **FPV (First Person View)**, anche se nel caso specifico degli ultimi due, il Triton e MQ-9, vengono utilizzati maggiormente in configurazione automatica o semiautomatica.

Il **fenomeno FPV** è uno degli sviluppi più sorprendenti degli ultimi anni ed è rappresentato dai droni dove l'operatore indossa un visore (figura 4.14.) che mostra in tempo reale le immagini provenienti dalla telecamera di bordo, **ottenendo l'impressione di trovarsi fisicamente all'interno del velivolo.**



Figura 4.14

Nati inizialmente come strumenti per competizioni sportive e riprese spettacolari, questi droni hanno assunto un ruolo centrale anche nei moderni conflitti.

La loro combinazione di basso costo, elevata mano-

vrabilità e precisione li rende strumenti estremamente versatili. Possono trasportare sensori, apparati di comunicazione, materiale medico, piccoli carichi logistici e, in ambito militare, anche cariche esplosive.

La loro diffusione dimostra come tecnologie sviluppate per il mercato civile possano trasformarsi rapidamente in strumenti dalle applicazioni molto più ampie.

In un teatro di guerra, un drone **FPV** si trova a operare in un **ambiente estremamente ostile dal punto di vista elettromagnetico**.

Non deve solo trasmettere il video al pilota, ma anche ricevere continuamente i comandi di controllo.

Il problema principale è rappresentato dal **jamming** (disturbo intenzionale), dallo **spoofing** (inganno dei segnali) e dall'**intercettazione**.

Per questo motivo i moderni FPV militari impiegano sistemi di comunicazione molto diversi da quelli normalmente utilizzati dai droni civili.

Per l'**uplink** ed il **downlink** dei dati usano **due canali separati** su bande di frequenza che possono andare da 1,2 fino a 5 GHz.

La tecnica più importante utilizzata è la **Frequency Hopping**.

Invece di trasmettere sempre sulla stessa frequenza, trasmettitore e ricevitore **saltano centinaia o migliaia di volte al secondo, seguendo una sequenza pseudocasuale nota solo ai due apparati**.

Un eventuale jammer dovrebbe disturbare contemporaneamente tutta la banda.

Questa tecnica prende il nome di **Frequency Hopping Spread Spectrum (FHSS)**.

Alcuni sistemi utilizzano anche il **Direct Sequence Spread Spectrum (DSSS)**.

Il segnale viene "spalmato" su una banda molto ampia rendendolo più difficile da intercettare e più resistente al rumore.

Inoltre, le modulazioni della portante cambiano automaticamente in funzione della qualità del collegamento.

Si passa, ad esempio, da QPSK a 8PSK o 16QAM. Per capire meglio questo aspetto consiglio di approfondire attraverso le nostre conferenze sulla comunicazione disponibili sul nostro canale Youtube.

Quando il collegamento peggiora il sistema riduce il **bitrate** (cioè i bit al secondo) per aumentare la probabilità di ricezione.

Infine, abbiamo la **Correzione degli errori (FEC)**. Quasi tutti i sistemi moderni aggiungono ridondanza ai dati.

In questo modo il ricevitore può correggere automaticamente molti errori introdotti dal jamming. I dati sono crittografati.

Per garantire una comunicazione robusta, quando è possibile si usa un ripetitore aereo che consiste nel mantenere in quota un drone dedicato esclusivamente alle comunicazioni.

Il ripetitore può volare anche a 2000 metri da dove vede molto più lontano e aggira gli ostacoli.

Quando però la lotta tra jammer e rete di comando si fa dura ci si pone il problema:

Comunicare senza fili... o con un filo?



Figura 4.15 Drone a fibra ottica

I droni a fibra ottica

Una delle soluzioni più interessanti emerse recentemente è rappresentata dai droni volanti, tipicamente quadricotteri, a fibra ottica (figura 4.15.), capaci di arrivare da 5 fino a 30 km di distanza con capacità di comunicazione bidirezionale fino a ~1Mbps,

attraverso una sottilissima fibra ottica che si srotola mentre il drone viaggia e che mantiene il collegamento tra operatore e drone.

Sebbene possa sembrare una tecnologia anacronistica, offre vantaggi notevoli.

La connessione è totalmente immune alle interferenze radio, non può essere disturbata mediante jamming elettronico e non emette segnali rilevabili dai sistemi di guerra elettronica.

Questa soluzione sta trovando applicazione soprattutto negli scenari dove la sopravvivenza alle contromisure elettroniche è diventata un requisito essenziale.

Per contro, la fibra di un drone kamikaze ovviamente resta sul terreno lungo tutto il percorso generando situazioni di "inquinamento da fibra" come quella rappresentata da questa immagine (fig.4.16.) di una città nella zona di conflitto tra Russia e Ucraina.



Figura 4.16 Un campo di battaglia con i residui delle fibre ottiche lasciate dai droni FPV a filo ottica

Il mondo dei droni evolve rapidamente: mentre scrivo, nel luglio 2026, emergono novità che meritano attenzione. Per questo lascio spazio a due esempi rappresentativi dello stato dell'arte in due tecnologie in forte crescita.

Un **piccolo drone solare italiano "Guardian XL"** (fig.4.17.), sviluppato da **Vector Robotics**, ha stabilito un record mondiale tra i piccoli UAS elettrici con apertura alare inferiore a 3 metri e peso sotto i 3,1 kg:

ha volato per oltre 24 ore senza atterrare, continuando a trasmettere a terra le immagini della tele-

camera di bordo.

Voli solari di lunga durata sono già stati fatti con velivoli senza equipaggio molto più grandi, con aperture alari di 20-30 metri.

La sfida, in questo caso, è stata superare le 24 ore con un drone elettrico piccolo, leggero e molto più economico. Ciò significa quindi la capacità di caricare di giorno, sulle batterie di bordo, l'energia sufficiente per operare di notte.

Il risultato apre prospettive rilevanti: **l'obiettivo è arrivare a missioni autonome senza sosta di giorni, settimane e, in futuro, mesi.**

Le applicazioni sono numerose, sia civili sia militari. Il Guardian XL può trasportare un carico utile di circa 200-300 grammi, tra telecamere, sensori infrarossi o multispettrali e ripetitori radio



Figura 4.17 Guardian XL

Il Guardian XL deriva dal precedente drone solare Guardian, **sviluppato da Vector Robotics con la società emiliana NPC Spacemind**. Quest'ultimo è già impiegato da diverse polizie locali e protezioni civili regionali ed è stato adottato anche da alcune forze armate.

Può essere lanciato a mano da un solo operatore e raggiungere una velocità massima di 90 km/h. Il sistema di trasmissione digitale assicura un segnale stabile e consente di inviare alla stazione a terra le immagini raccolte; una scheda di memoria permette inoltre di registrare i dati e trasferirli dopo l'atterraggio.

Opera con temperature comprese tra -10 e +45 °C e con venti fino a 30 nodi. Il raggio d'azione, legato alla portata della radio di bordo, è di 10-30 km; in missioni autonome può però volare per giorni o settimane e coprire distanze di centinaia o migliaia di chilometri.

Per approfondire → [Link](#)



Figura 4.18 Guardian XL in volo

Concludiamo con due droni che **stanno segnando la storia della guerra in Ucraina** e hanno trasformato le strategie dei conflitti moderni: il drone d'attacco ucraino **FP-1** e l'iraniano **Shahed-136**.

L'FP-1 è un drone d'attacco ucraino a lungo raggio, unidirezionale o "kamikaze", sviluppato e prodotto dalla società di tecnologia per la difesa Fire Point (figura 4.19.).

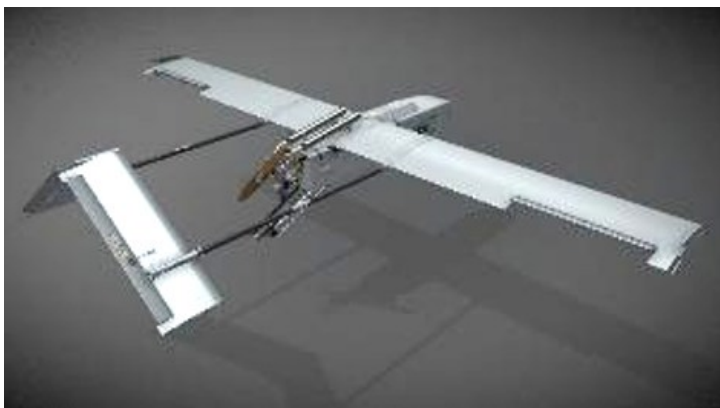


Figura 4.19 FP-1 ucraino

Introdotta alla fine del 2024 in risposta all'invasione russa dell'Ucraina, l'FP-1 è progettato per attacchi in profondità e può trasportare una testata a oltre 2.000 km di distanza.

Le Forze Armate ucraine lo hanno utilizzato per colpire obiettivi militari e logistici di alto valore situati a migliaia di chilometri dal confine.

Il velivolo ha una fusoliera snella, ali fisse dritte, un motore endotermico bicilindrico collegato a un'elica e un razzo ausiliario a propellente solido per il lancio.

L'altro esempio è lo **HESA Shahed-136** (fig. 4.20.), un drone kamikaze a basso costo sviluppato dall'Iran. Conosciuto in Russia come **Geran-2**, è diventato un'arma rilevante nei conflitti moderni grazie alla capacità di colpire bersagli a lunghissima distanza, volando in sciami a bassa quota.



Figura 4.20 Shahed-136

Si tratta, in realtà, di una derivazione del progetto tedesco Dornier DAR (Antiradar Drone), azionata da un motore bicilindrico a due tempi.

Lo Shahed-136 ha una configurazione ad ala volante a delta, è lungo 3,5 metri e ha un'apertura alare di 2,5 metri. Può trasportare un carico esplosivo di 50 kg fino a 2.000 km, con un costo stimato di 20.000 USD

È spinto dal motore MTO MD-550 (fig. 4.21.), un propulsore a scoppio a due tempi e quattro cilindri da 50 CV.

Il successo di questo progetto è dimostrato dalle numerose copie prodotte nel mondo, a partire da una soluzione nata in Germania e in Israele. Oltre alla produzione Dornier, la versione più nota è quella iraniana, lo Shahed-136, affiancata in Russia dal Geran-2.



Figura 4.21 Il motore quattro cilindri due tempi del Shahed-136

Seguono l'India con lo Sheshnang, gli Stati Uniti con il Lucas, l'Ucraina con il Batyar e la Cina con il Sunflower-200.

Una caratteristica comune a molti droni kamikaze ad ala fissa è il sistema di lancio.

Di solito il lancio può avvenire da postazioni terrestri, come camion, oppure navali.

In entrambi i casi si utilizzano una catapulta, cioè una guida inclinata verso l'alto, e razzi a combustibile solido, o booster, che accelerano il drone alla partenza e si staccano dal velivolo una volta esaurito il propellente. A quel punto il drone ha già raggiunto la velocità di crociera, il motore è in funzione e il velivolo prosegue autonomamente.

5. COME FANNO I DRONI AUTOMATICI A SAPERE DOVE SI TROVANO?

Uno degli aspetti più affascinanti riguarda la navigazione.

Molti immaginano che un drone dipenda completamente dal GPS. In realtà i sistemi moderni utilizzano contemporaneamente numerose fonti di informazione.

La navigazione inerziale sfrutta accelerometri e giroscopi per calcolare continuamente posizione, velocità e orientamento.

Le telecamere permettono di riconoscere punti di riferimento sul terreno attraverso tecniche di visione artificiale.

I sistemi **LIDAR** generano mappe tridimensionali dell'ambiente misurando milioni di distanze ogni secondo mediante impulsi laser.

La tecnica chiamata **SLAM (Simultaneous Localization And Mapping)** (fig. 5.1.) consente di costruire una mappa dell'ambiente mentre il drone determina la propria posizione al suo interno.

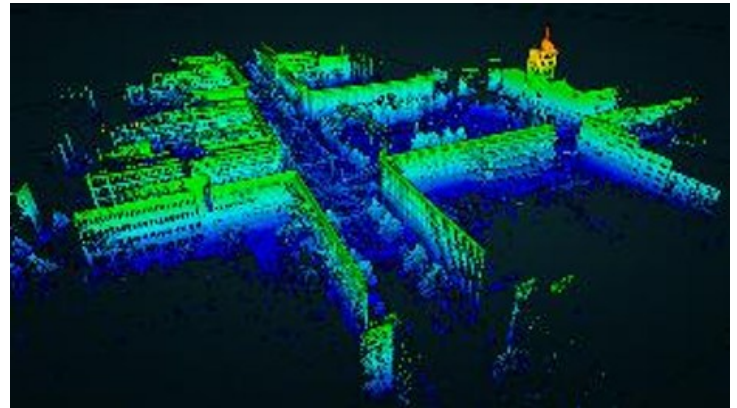


Figura 5.1 "Immagine" creata con la tecnica SLAM

Tutti questi dati vengono combinati attraverso la cosiddetta **sensor fusion** (figura 5.2.), creando una stima molto più affidabile rispetto a quella ottenibile da un singolo sensore.

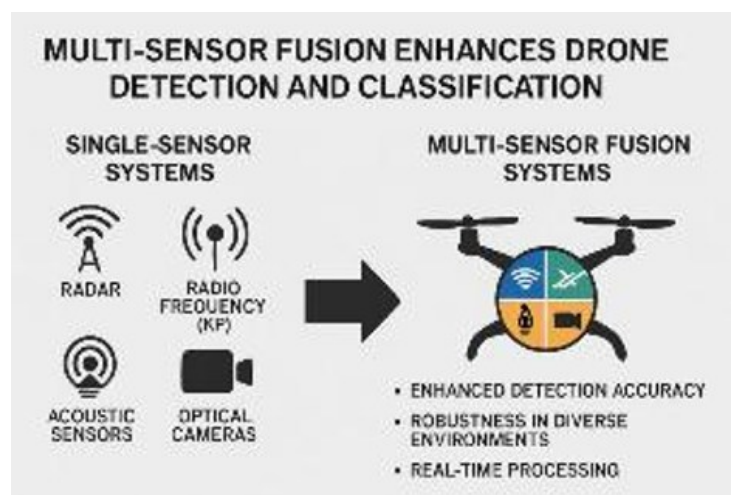


Figura 5.2

L'obiettivo moderno non è più semplicemente utilizzare il GPS, ma **essere in grado di operare anche quando il GPS non è disponibile o viene deliberatamente disturbato.**

6. GLI SCIAMI INTELLIGENTI

La vera frontiera della robotica aerea è rappresentata dagli sciame di droni.

Invece di affidare una missione a un singolo velivolo, si impiega un gruppo composto da decine o addirittura centinaia di unità.

Ogni drone svolge un compito specifico: ricognizione, comunicazione, guerra elettronica, attacco o semplice funzione di esca.

La forza dello sciame risiede nella cooperazione.

Se un elemento viene perso, gli altri possono riorganizzarsi automaticamente e redistribuire i compiti. In alcuni casi non esiste nemmeno un vero centro di controllo: ciascun drone prende decisioni locali basandosi sulle informazioni condivise dagli altri membri del gruppo.

Il comportamento ricorda quello di uno sciame di api o di uno stormo di uccelli, ma applicato a sistemi tecnologici.

Questa capacità potrebbe rivoluzionare non soltanto il settore militare ma anche le operazioni di soccorso, il monitoraggio ambientale e l'esplorazione di aree estese.

7. DALLA TERRA AGLI OCEANI: QUANDO I DRONI CAMBIANO AMBIENTE

Se il cielo è stato il primo ambiente a essere associato ai droni, oggi la tecnologia *unmanned* si sta diffondendo in ogni contesto operativo.



Figura 7.1 Centaur Unmanned Ground Vehicle (USA)

I veicoli terrestri senza equipaggio, indicati con la sigla **UGV (Unmanned Ground Vehicle)**, sono progettati per operare in ambienti pericolosi, ostili o semplicemente poco adatti alla presenza umana. (figura 7.1.)

I loro impieghi spaziano **dal settore militare alla protezione civile**, dalla logistica industriale all'agricoltura di precisione.

Robot cingolati vengono utilizzati per disinnescare ordigni esplosivi o per entrare in edifici pericolanti dopo terremoti e incendi.

Altri sistemi trasportano materiali in magazzini automatizzati, ispezionano oleodotti, gallerie o impianti industriali.

Negli ultimi anni sono comparsi anche i cosiddetti "**cani robotici**" (figura 7.2.), quadrupedi capaci di muoversi su terreni accidentati dove un mezzo a ruote avrebbe difficoltà.

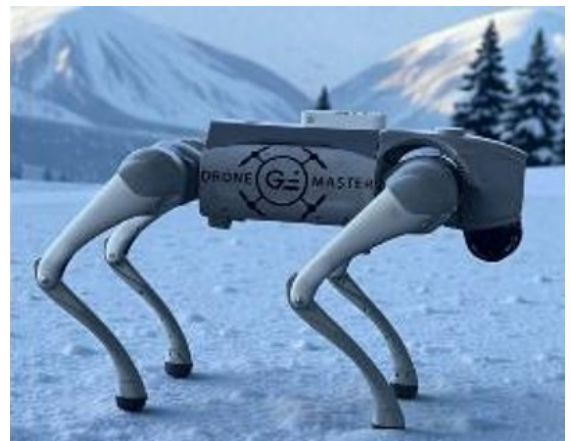


Figura 7.2 Cane robotico

Grazie a sofisticati algoritmi di controllo riescono a mantenere l'equilibrio, superare ostacoli e recuperare la stabilità anche dopo urti o spinte improvvise.

Ancora più impressionante è l'evoluzione dei robot umanoidi.

Dopo decenni di sviluppo, il 2026 potrebbe essere ricordato come l'anno della loro effettiva introduzione nel mondo del lavoro. Aziende statunitensi, europee e cinesi stanno sviluppando macchine capaci di muoversi in ambienti progettati per gli esseri umani, utilizzare utensili, trasportare materiali e collaborare con operatori umani. (Figura 7.3.)

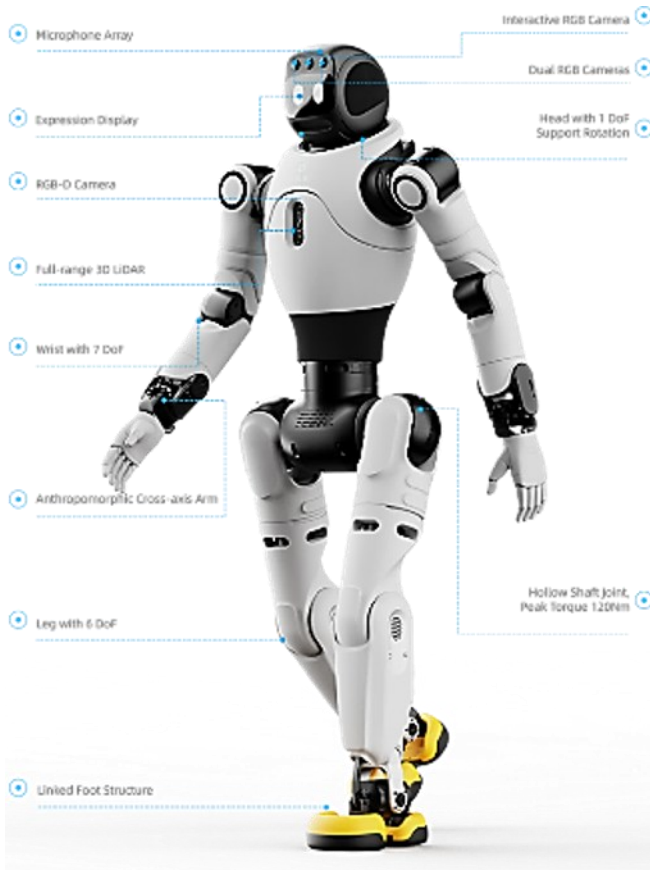


Figura 7.3 Agibot di SIR

Pur non essendo droni nel senso tradizionale del termine, condividono la stessa filosofia: sostituire o affiancare l'uomo nelle attività più ripetitive, pericolose o gravose.

Il system integrator modenese **SIR Robotics** ha annunciato una partnership strategica con **Agibot**, leader cinese nella robotica umanoide, e **Wolong Electric**, mettendo a disposizione del mercato umanoidi progettati per accoglienza commerciale e hospitality.

Ad esempio, il modello **A2 Ultra** (anche denominato G2 in alcune configurazioni): è robot umanoide alto 170 cm e dal peso di 70 kg,

Può scattare foto con gli ospiti, servire bevande e snack e muoversi in sicurezza tra le persone.

Ogni mano può sollevare carichi fino a 5 kg.

Oppure **X2 Ultra**: specializzato nell'intrattenimento e nell'interazione dinamica con il pubblico, offre esperienze coinvolgenti e personalizzate.

Non è escluso che uno di questi signori "artificiali" ci faccia compagnia nella conferen-

za che COSMo terrà su questo tema, come ho già detto, il 13 ottobre 2026 presso il planetario di Modena. In tal caso avremo modo di interagire con lui.

8. I DRONI DEL MARE

Un altro settore in forte crescita è quello dei droni marini. Si distinguono generalmente due categorie principali.

I veicoli di superficie, denominati **USV (Unmanned Surface Vehicle)**, navigano sull'acqua come piccole imbarcazioni autonome per uso civile (figura 8.1) o per uso militare (figura 8.2)



Figura 8.1 Mirai robotics (Italia)



Figura 8.2 Magura V5, forze armate ucraine

Alcuni sistemi moderni sono persino in grado di trasportare missili o piccoli droni aerei, trasformandosi in vere e proprie piattaforme multifunzione.

Purtroppo anche nel settore militare i droni marini stanno assumendo un'importanza crescente.

I recenti conflitti hanno dimostrato come piccoli ed economici mezzi navali autonomi possano rappre-

sentare una minaccia significativa anche per navi molto più grandi e costose.

I veicoli subacquei (figura 8.3.) o **UUV (Unmanned Underwater Vehicle)**, operano invece nelle profondità marine.



Figura 8.3 "DEEP" drone subacqueo di Fincantieri

Le applicazioni civili sono numerosissime: monitoraggio ambientale, oceanografia, ispezione di piattaforme offshore, controllo di cavi e condotte sottomarine, ricerca scientifica e studio degli ecosistemi marini.

9. IL PROBLEMA DELLA NAVIGAZIONE SOTT'ACQUA.

Se per un drone aereo o terrestre o comunque di superficie il GPS rappresenta normalmente la principale fonte di localizzazione, per un drone subacqueo la situazione è ovviamente molto più complessa.

Le onde radio utilizzate dai sistemi satellitari non penetrano efficacemente nell'acqua. Di conseguenza il GPS diventa inutilizzabile già a pochi centimetri sotto la superficie.

Per risolvere il problema vengono impiegate diverse tecnologie.

Tra queste la più comune è quella degli **accelerometri o sistemi inerziali**. Essi calcolano continuamente la posizione partendo da un punto noto. Tuttavia, gli errori tendono ad accumularsi nel tempo molto velocemente.

Per correggerli vengono utilizzati **sonar Doppler** che misurano la velocità rispetto al fondale marino (ma rivelano al nemico la posizione) e **sistemi acu-**

stici basati su reti di trasmettitori installati sul fondo o su navi di appoggio note (Sistemi Acustici di Baseline (LBL, SBL, USBL)).

Anche in questo caso parliamo di **sensor fusion**.

Molti droni subacquei emergono periodicamente per ricevere un aggiornamento GPS e correggere la propria posizione.

Queste limitazioni rendono la **navigazione sottomarina una delle sfide tecnologiche più impegnative** dell'intero settore unmanned.

Anche le **comunicazioni** sott'acqua rappresentano un elemento fondamentale.

Le portanti radio diventano quasi inutilizzabili e vengono sostituite da **modem acustici che trasmettono dati attraverso onde sonore**.

Questi sistemi consentono collegamenti a lunga distanza ma con velocità molto inferiori rispetto alle comunicazioni radio.

Poi vi sono i **modem Ottici (Laser/LED)** che utilizzano la luce blu o verde per trasmettere enormi quantità di dati ma solo a cortissimo raggio (poche decine di metri).

Nelle applicazioni civili si usa un **cavo ombelicale** in fibra ottica.

Ma ci sono anche approcci via radio a bassissima frequenza.

Tra queste abbiamo le **onde VLF (Very Low Frequency, 3 kHz - 30 kHz)** dove tramite un lungo cavo antenna agganciato al sottomarino (che però si può notare da un ricognitore) una emittente aerea può **penetrare per decine di metri l'acqua del mare**.

Oppure le **ELF (Extremely Low Frequency, > 3 kHz giù fino a 45 Hertz)**.

Grazie all'ottima capacità di penetrazione nell'acqua salata, sono impiegate dalle marine militari mondiali per comunicare con i sottomarini nucleari a grandi profondità.

A causa delle bassissime frequenze, la velocità di trasmissione dati è estremamente ridotta, pari a 450 parole al minuto), permettendo solo l'invio di messaggi molto brevi o codificati.

Infine, ma non per questo meno importante, abbiamo il laser. Un raggio laser sparato da satellite può penetrare per decine di metri sotto il livello del mare garantendo però in download standard di comunicazione elevatissimi.

10. L'INTELLIGENZA ARTIFICIALE PRENDE IL COMANDO

Uno degli aspetti più innovativi riguarda il ruolo crescente dell'intelligenza artificiale nel settore militare.

I primi droni erano piattaforme controllate dall'uomo; oggi molti sistemi sanno riconoscere oggetti, evitare ostacoli, classificare bersagli e pianificare in autonomia il percorso più adatto.

Combinando telecamere ottiche, sensori infrarossi, radar e sistemi LiDAR, un drone moderno può ricostruire con precisione l'ambiente circostante e adattare il proprio comportamento in tempo reale.

In alcuni casi, il livello di autonomia è tale da permettere il completamento della missione anche senza comunicazioni con l'operatore.

È una trasformazione paragonabile a quella introdotta nell'automobile dalla guida assistita e, in prospettiva, dalla guida autonoma.

Nel volo senza equipaggio, però, questa rivoluzione è già in corso. I dettagli su modalità e diffusione restano limitati, ma è evidente che il futuro delle missioni militari farà sempre più affidamento su queste capacità, con l'obiettivo di ridurre il rischio per il personale umano. Allo stesso tempo, l'autonomia decisionale dell'AI introduce interrogativi nuovi e delicati.

Decisioni che possono incidere sulla vita o sulla morte di persone considerate ostili rischiano infatti di essere affidate, almeno in parte, ad algoritmi.

Le decisioni umane in ambito militare non sono certo prive di errori o limiti, ma l'introduzione dell'intelligenza artificiale apre scenari ancora difficili da prevedere e quantificare con chiarezza.

11. LA SFIDA DELLA DIFESA ANTI-DRONE

L'enorme diffusione dei droni ha generato anche

nuove problematiche.

Una delle più importanti è la difesa contro questi sistemi.

Il problema principale è economico.

Un piccolo drone può costare poche centinaia o poche migliaia di euro, mentre il missile necessario per intercettarlo può costare decine o centinaia di volte di più.

Lo squilibrio diventa ancora più evidente nel caso degli sciami, dove decine di droni possono saturare le difese di un obiettivo.

Per affrontare questa sfida si stanno sviluppando nuove tecnologie.

I sistemi di guerra elettronica cercano di disturbare i collegamenti radio o satellitari.

I cannoni automatici impiegano munizionamento relativamente economico.

Sempre maggiore interesse suscitano le armi a energia diretta, in particolare i laser (figura 11.1).



Figura 11.1 DragonFire da 50 kW, (UK): Sviluppato con tecnologia italiana (Leonardo)

Questi sistemi concentrano grandi quantità di energia su un bersaglio per alcuni secondi, danneggiandone sensori, batterie o strutture. Una volta installati, il costo di ogni ingaggio può essere estremamente basso (un paio di dollari) rispetto a quello dei missili tradizionali.

La vera sfida del futuro non sarà semplicemente abbattere un drone, ma farlo in modo economicamente sostenibile.

12. MODENA, NELLA MOTOR VALLEY UNA FABBRICA DI DRONI

Una collaborazione tra Regno Unito e Italia in uno degli ambiti più sensibili e "attuali" della difesa, quello dei droni. Una sinergia che fa leva sull'esperienza unica, riconosciuta a livello mondiale, che l'Italia ha maturato nella produzione di motori di auto e moto.

Giovedì 4 giugno 2026 è stata presentata a Roma a Villa Wolkonsky, residenza ufficiale dell'ambasciatore britannico in Italia, una nuova società, **MGI Italia**, nata dalla joint venture tra un'azienda britannica, la **MGI Engineering Ltd**, e una italiana, la **Vigilar Group Spa**. (figura 12.1. e 12.2.)

L'accordo prevede di realizzare a Modena una linea di produzione che potrebbe arrivare a produrre circa 200 droni al mese, per un costo che dovrebbe aggirarsi attorno ai **€ 500.000 l'uno**.



Figura 12.1



Figura 12.2

Sette piccole imprese della regione, con la collaborazione di **Thales Alenia Space** e dell'Università di

Bologna hanno già presentato nell'ottobre scorso il progetto **ERIS-Emilia-Romagna in Space** finalizzato a creare, con base a Forlì, una filiera nel settore spaziale italiano per lo studio di tecnologie altamente innovative e la successiva industrializzazione di prodotti, a partire dalle antenne a maglie e cabling flessibili per l'osservazione della terra, da installare sui satelliti.

13. I DRONI CONQUISTANO LO SPAZIO

Il concetto di drone non si ferma all'interno dell'atmosfera terrestre.

Anche nello spazio esistono sistemi autonomi che svolgono missioni senza equipaggio.

Uno degli esempi più noti è rappresentato dagli spaziplani automatici, capaci di operare in orbita per mesi o anni e rientrare successivamente sulla Terra come il **Boeing X-37B (OTV: Orbital Test Vehicle)** (figura 13.1 e 13.2).



Figura 13.1 X-37B in orbita



Figura 13.1 X-37B al lancio (sinistra) e dopo l'atterraggio (a destra)

L'X-37 è uno spaziosplano sperimentale non pilotato sviluppato per la U.S. Space Force. Una volta posizionato in orbita è in grado di volare ed atterrare autonomamente. Il programma vede la partecipazione sia della Forza Spaziale statunitense, che di DARPA e NASA.

È un drone che può avere in orbita una autonomia notevole. Il 7 marzo 2025 X37-B è rientrato sulla terra terminando la missione OTV-7 dopo 434 giorni di orbita.

Il 21 agosto 2025 è iniziata l'ottava missione OTV-8 con un Falcon 9 di Space X.

Le forze armate cinesi ne hanno già operativo uno simile.

Droni interplanetari

Ma è soprattutto nell'esplorazione planetaria che il concetto di drone assume un'importanza fondamentale. Quando un rover si trova su Marte, le comunicazioni con la Terra richiedono da alcuni minuti fino a oltre venti minuti per tratta.

Un controllo in tempo reale è impossibile! Per questo motivo i rover devono essere in grado di prendere autonomamente molte decisioni operative.

I rover **Spirit** e **Opportunity** furono tra i primi a utilizzare sistemi di navigazione autonoma per evitare ostacoli e pianificare i percorsi.

Curiosity ha introdotto capacità avanzate di analisi scientifica e selezione automatica degli obiettivi di studio.

Perseverance (figura 13.2.) rappresenta oggi uno degli esempi più sofisticati di robot autonomo extra-terrestre.



Figura 13.3 Perseverance

Dragonfly: il primo elicottero completamente autonomo su un altro mondo

Nel 2021 un veicolo ha compiuto un'impresa destinata a entrare nella storia dell'esplorazione spaziale: **Ingenuity**, un piccolo elicottero trasportato su Marte dal rover Perseverance, ha effettuato il primo volo controllato e motorizzato su un altro pianeta.

L'impresa è stata particolarmente difficile a causa della rarefattissima atmosfera marziana, che possiede una densità pari a circa l'uno per cento di quella terrestre.

Molti consideravano il progetto un semplice dimostratore tecnologico.

In realtà Ingenuity ha superato ogni aspettativa, compiendo decine di voli e dimostrando che l'esplorazione aerea di altri mondi è possibile.

Il prossimo grande passo sarà rappresentato dalla **missione Dragonfly** della NASA. (figura 14.1. e 14.2.)



Figura 13.4 Dragonfly

Utilizza **otto rotori coassiali** (disposti a coppie su quattro bracci) dotati ciascuno di **tre pale rigide**, ottimizzati per volare su Titano, la più grande luna di Saturno, in un'atmosfera densa (azoto e metano) con una gravità bassissima, circa 1/7 di quella terrestre: condizioni ideali per il volo.

Dragonfly potrà spostarsi da un sito all'altro percorrendo decine di chilometri, analizzando la superficie e studiando una delle realtà più affascinanti dell'intero Sistema Solare.

Le comunicazioni tra Titano e la Terra hanno un tempo di volo di oltre un'ora e mezza per tratta.

Ciò significa che il veicolo dovrà essere estremamente autonomo.

In un certo senso rappresenta il punto di arrivo dell'evoluzione dei droni: una macchina capace di esplorare da sola un mondo distante oltre un miliardo di chilometri.



Figura 13.5 Luglio 2026, Dragonfly in assemblaggio (Crediti: NASA/Johns Hopkins APL/Ed Whitman)

14. CONCLUSIONI

Dai piccoli quadricotteri civili ai rover marziani, dai robot terrestri agli sciami intelligenti, i droni stanno modificando profondamente il nostro rapporto con la tecnologia e con l'ambiente.

Essi estendono la presenza umana in luoghi pericolosi, remoti o inaccessibili. Permettono di raccogliere informazioni, effettuare misure scientifiche, svolgere attività operative e persino esplorare altri mondi senza esporre direttamente persone ai rischi.

La loro evoluzione è ancora agli inizi. Sensori più avanzati, batterie migliori, comunicazioni più efficienti e sistemi di intelligenza artificiale sempre più sofisticati renderanno questi strumenti ancora più autonomi e versatili.

Forse il modo migliore per definire un drone non è considerarlo un semplice veicolo senza pilota, quanto **un'estensione tecnologica delle nostre capacità**: occhi che osservano dove non possiamo arrivare, mani che operano dove sarebbe troppo rischioso andare e, sempre più spesso, intelligenze artificiali che collaborano con noi nell'esplorazione del mondo.

E, domani, di altri mondi.



GLI EVENTI DEL C.O.S.MO

Di seguito l'elenco (parziale) dei prossimi eventi del C.O.S.Mo. Sono quelli che sono già organizzati, ma altri potrebbero essere realizzati, per questo restate sintonizzati con i nostri social (trovate i link in fondo a questa sezione).



**Sabato 19 Settembre e fino al pomeriggio di
Domenica 20 Settembre 2026**
**Presso TecnoPolo Reggiane Parco Innovazione
a Reggio Emilia**

**Festival dell'Astronomia di Reggio Emilia –
IV edizione**



**Relatori: associazioni REA (Reggio Emilia
Astronomia) e COSMo**

Domenica pomeriggio, nell'ambito del Festival, è inoltre in programma l'evento speciale "Terra chiama stazione Terra!", sul concetto di colonia spaziale orbitante stile O'Neill. Da non perdere!

Domenica 20 Settembre 2026 – Ore 21:00
Conferenza presso l'Auditorium dell'I.T.I.S.
"Corni" in via Leonardo da Vinci, 300 - Modena

**Smettila di dire a Dio cosa fare coi suoi
dadi**

La Fisica Quantistica spiegata in modo semplice.



Secondo i fisici esiste un mondo ancora più assurdo di quello descritto da Einstein nella sua Relatività. Anche perché è parzialmente impossibile da descrivere. È quello della Fisica Quantistica, dell'infinitamente piccolo. Un reame incantato e misterioso capace di smontare ogni certezza e mettere tutto in dubbio, compreso il fatto che esista una realtà oggettiva.

Difficile crederci, eppure funziona. Vale la pena capirne almeno le basi: non si sa mai che un giorno ci chiedano di spiegarle.

Relatore: Luca Perri

Martedì 6 Ottobre 2026 – Ore 21:00

Conferenza del ciclo: "Un altro equinozio con Il COSMo" presso Planetario di Modena

Artemis e la nuova corsa alla Luna

La frontiera che ridisegna il potere nello spazio. Dalla sfida con la Cina alla conquista delle risorse lunari: il primo passo verso la colonizzazione del Sistema Solare. Il programma Artemis apre una nuova era dell'esplorazione: non più piantare una bandiera, ma costruire una presenza stabile sulla Luna. Stati Uniti e Cina, con i rispettivi alleati, si contendono la leadership di un futuro che intreccia tecnologia, geopolitica e risorse minerarie. La Luna diventa laboratorio e trampolino verso il Sistema Solare, dove estrazione di materiali e produzione di energia aprono prospettive economiche inedite. Questa volta restiamo, per imparare a vivere fuori dalla Terra e ridefinire il concetto stesso di civiltà spaziale.

Relatori: Davide Borghi, Ciro Sacchetti

Martedì 13 Ottobre 2026 – Ore 21:00

Conferenza del ciclo: "Un altro equinozio con Il COSMo" presso Planetario di Modena

Droni – Protagonisti di una nuova era

Con il termine drone si identifica oggi una vasta famiglia di sistemi *unmanned*, cioè privi di equipaggio a bordo. Alcuni volano nei cieli, altri si muovono sulla terraferma, altri ancora navigano in superficie, nelle profondità oceaniche, nello spazio e su altri mondi del Sistema Solare.

Dai quadricotteri agli sciame intelligenti, dai robot terrestri ai rover marziani: come i sistemi senza equipaggio stanno cambiando il nostro mondo.

Relatore: Luigi Borghi

Martedì 20 Ottobre 2026 – Ore 21:00

Conferenza del ciclo: "Un altro equinozio con Il COSMo" presso Planetario di Modena

Chernobyl 40 anni dopo

Chernobyl: il peggior incidente nucleare civile, nato

dall'intreccio fatale tra difetti di progettazione ed errori umani. Chernobyl, Three Mile Island (dove il contenimento ha retto) e Fukushima (innescata da un evento esterno estremo) sono tre storie molto diverse tra loro. Da questi errori nasce il nucleare moderno: reattori ripensati e più sicuri.

Relatore: Roberto Castagnetti

Martedì 3 Novembre 2026 – Ore 21:00

Conferenza del ciclo: "Un altro equinozio con Il COSMo" presso Planetario di Modena

La centrale nucleare di Gravelines in Francia

Un approfondimento sulla centrale nucleare d'oltralpe, con sei reattori da 900MW ognuno, che producono il 6% della produzione totale di energia elettrica francese. Un mostro a sei teste ma anche un esempio di come si può convivere con questo potente sistema ed essere sicuri che Chernobyl sia molto lontano.



Autunno 2026 un altro equinozio con il C.O.S.Mo.

Il Circolo di Osservazione Scientifico-tecnologico di Modena (COSMo),
in collaborazione con il Civico Planetario "F. Martino"
presentano una nuova serie di conferenze presso la sala del
Civico Planetario "F. Martino", Viale Barozzi, 31

Domenica 20 Settembre ore 21: La Fisica Quantistica – con Luca Perri
Smettila di dire a Dio cosa fare coi suoi dadi – la Fisica Quantistica spiegata a me stesso. Un reame incantato e misterioso capace di smontare ogni certezza e mettere tutto in dubbio, compreso il fatto che esista una realtà oggettiva.
Relatore: Luca Perri

Martedì 6 Ottobre ore 21:00: Artemis e la nuova corsa alla Luna
Dalla sfida con la Cina alla conquista delle risorse lunari: il primo passo verso la colonizzazione del Sistema Solare. USA e Cina, coi relativi alleati, si contendono la leadership di un futuro che intreccia tecnologia, geopolitica e risorse minerarie.
Relatori: Davide Borghi e Ciro Sacchetti

Martedì 13 Ottobre ore 21:00: Droni – Protagonisti di una nuova era
Sistemi unmanned, cioè privi di equipaggio a bordo nei cieli, sulla terraferma, sul mare, nelle profondità oceaniche, nello spazio e su altri mondi del Sistema Solare. Dai quadricotteri agli sciame intelligenti, dai robot terrestri ai rover marziani.
Relatore: Luigi Borghi

Martedì 20 Ottobre ore 21:00: Chernobyl 40 anni dopo
Chernobyl: il peggior incidente nucleare civile e punto di svolta tra difetti di progettazione e errori umani. Con Three Mile Island (dove il contenimento ha funzionato) e Fukushima (causata da evento esterno estremo) sono 3 storie molto diverse. Da ciò nasce il nucleare moderno: reattori ripensati e più sicuri.
Relatore: Roberto Castagnetti

Martedì 3 Novembre ore 21:00: La centrale nucleare di Gravelines
Un mostro a 6 teste, in Normandia. Un esempio di come si può convivere con questo potente sistema ed essere sicuri che Chernobyl sia molto lontano.
Relatori: Stefano Pozzato, Ciro Sacchetti.

Note: Occorre arrivare 10' prima: a conferenza iniziata non si potrà accedere.
Biglietto: 7 € (15 € per conferenza del 20 Settembre), ridotto (fino a 18 anni e studenti universitari): 5,5 € (10 € per la conferenza del 20 Settembre).
È richiesta prenotazione on-line: www.planetariodimodena.it - sezione "eventi".

con il Patrocinio del



GLI EVENTI DEL C.O.S.MO

Relatori: Stefano Pozzato, Ciro Sacchetti

**Altre attività ed altri eventi sono in fase di organizzazione
Per essere informati è possibile utilizzare il nostro sito**

[Clicca qui per andare alla pagina Eventi](#)

RESTATE AGGIORNATI!

Ma non solo sul sito

SEGUITECI SUI NOSTRI SOCIAL

[Clicca qui per l'elenco dei social](#)

Per Info e Contatti

Sito: www.ilcosmo.net



Email: info@cosmo.net

