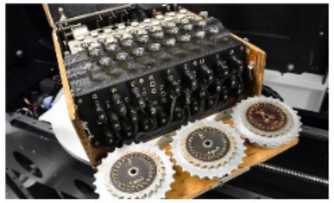
CODICI SEGRETI

da Enigma ai giorni nostri



Gianluca Salvalaggio

26 marzo 2025

UNIVERSITÀ POPOLARE MESTRE 1921

M9 museum

Contenuti

- Introduzione
- Cenni storici
- Crittografia Moderna
  - Crittografia a Chiave pubblica
- PGP e I Crypto War
- II Crypto War
- Crittografia End-to-End
- *Going Dark*

Introduzione

Sin dall'antichità, alla diffusione della **scrittura** si è affiancata l'esigenza di proteggere la riservatezza delle proprie comunicazioni. Per millenni reali, generali e governi, temendo intercettazioni *ostili*, hanno promosso lo sviluppo di codici e *scritture segrete*.
Usando termini contemporanei diciamo che hanno fatto ricorso a tecniche **crittografiche** sempre più sofisticate.

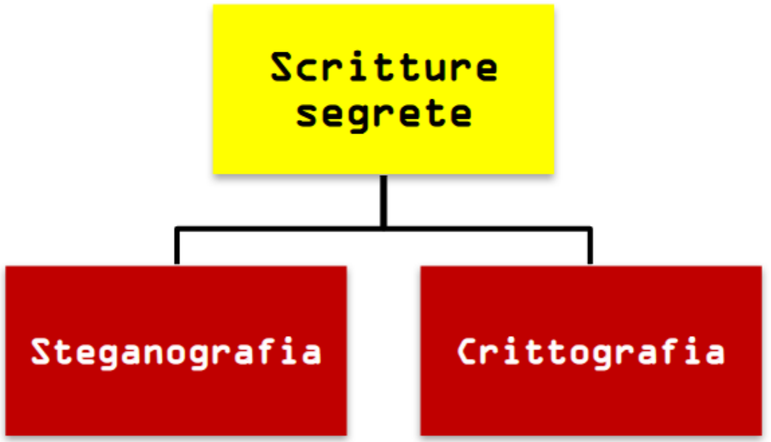
Il termine **crittografia** deriva dalle parole greche *kryptós* (nascosto) e *graphía* (scrittura) ed è la scienza delle *scritture segrete*. Nell'ambito di una comunicazione, il messaggio da inviare viene alterato (cifrato) utilizzando un procedimento concordato da **mittente** e **destinatario** in modo che risulti incomprensibile ad un eventuale avversario che riesca ad intercettare il messaggio.

Mittente e destinatario condividono segretamente una conoscenza che consente al primo la cifratura del messaggio in chiaro e al secondo la decifratura del testo cifrato. Tale conoscenza segreta **NON è il processo di alterazione ma è la chiave**: *un parametro del processo di alterazione stesso*.
La chiave può essere una parola o un numero (es: abracadabra, 00712845, …)..

Introduzione

La crittografia si distingue dalla **steganografia** (dal greco *steganos*, coperto) che invece mira a nascondere il messaggio, in modo che NON sia rivelata la presenza del messaggio stesso.

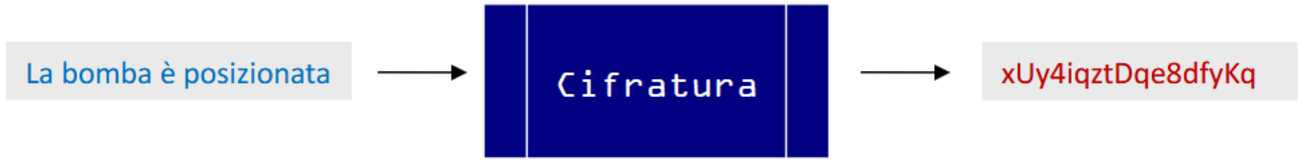
Mentre la **crittografia** si concentra sul *rendere incomprensibile* il messaggio attraverso la cifratura, la **steganografia** punta a *mascherare l'esistenza stessa* del messaggio, per esempio inserendolo all'interno di un contesto diverso come un'immagine.

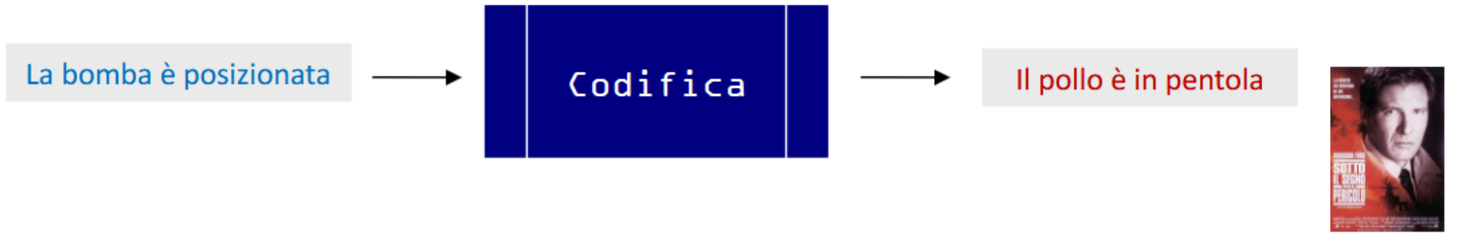


Introduzione

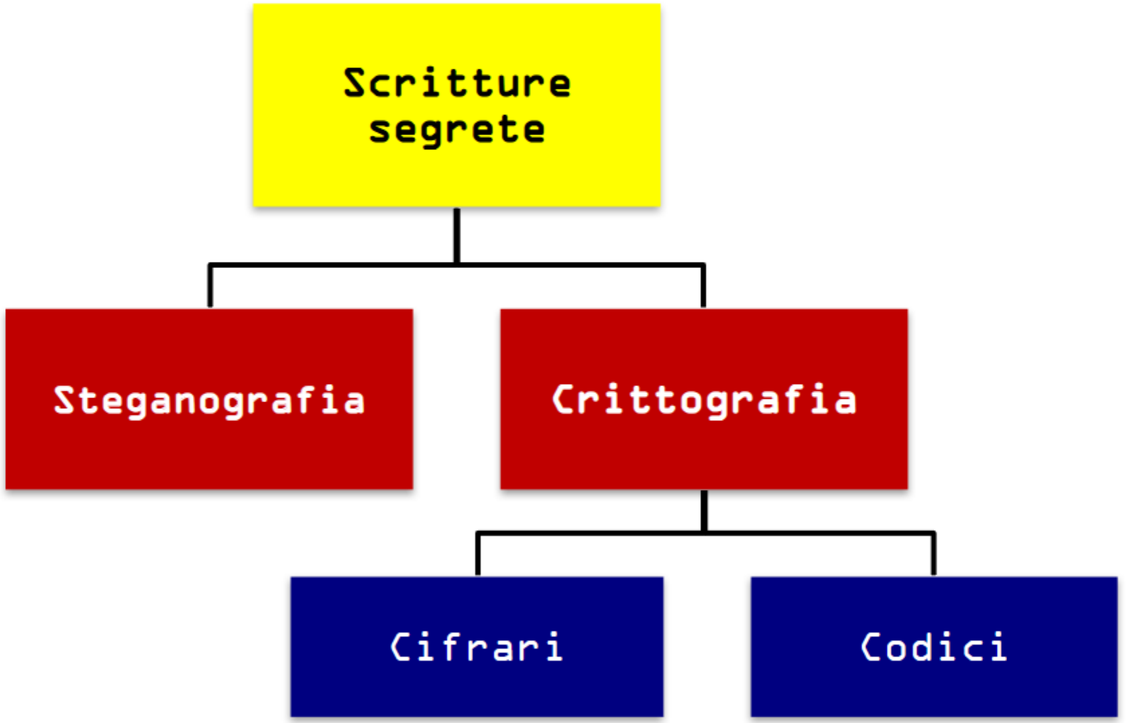
Spesso i termini ***sistema di cifratura*** (cifrario) e ***codice*** vengono usati in modo interscambiabile.
In realtà si riferiscono a meccanismi diversi.

I ***cifrari*** modificano le singole lettere (o bit nelle tecniche odierne) che compongono un messaggio.
I ***codici*** sostituiscono intere parole (o frasi) con altre parole.





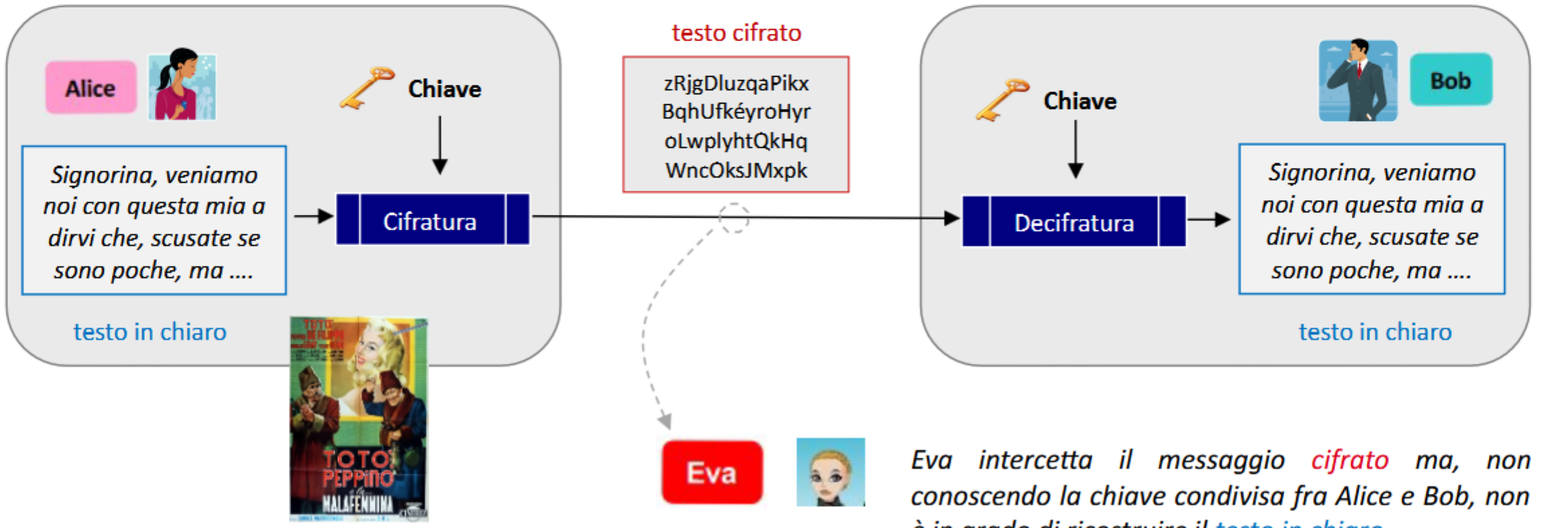
Riepilogando …



Introduzione

Un imagine dice più di mille parole. Vediamo un esempio di **cifratura**.

Alice spedisce a Bob un messaggio cifrato con una Chiave che è nota anche a Bob

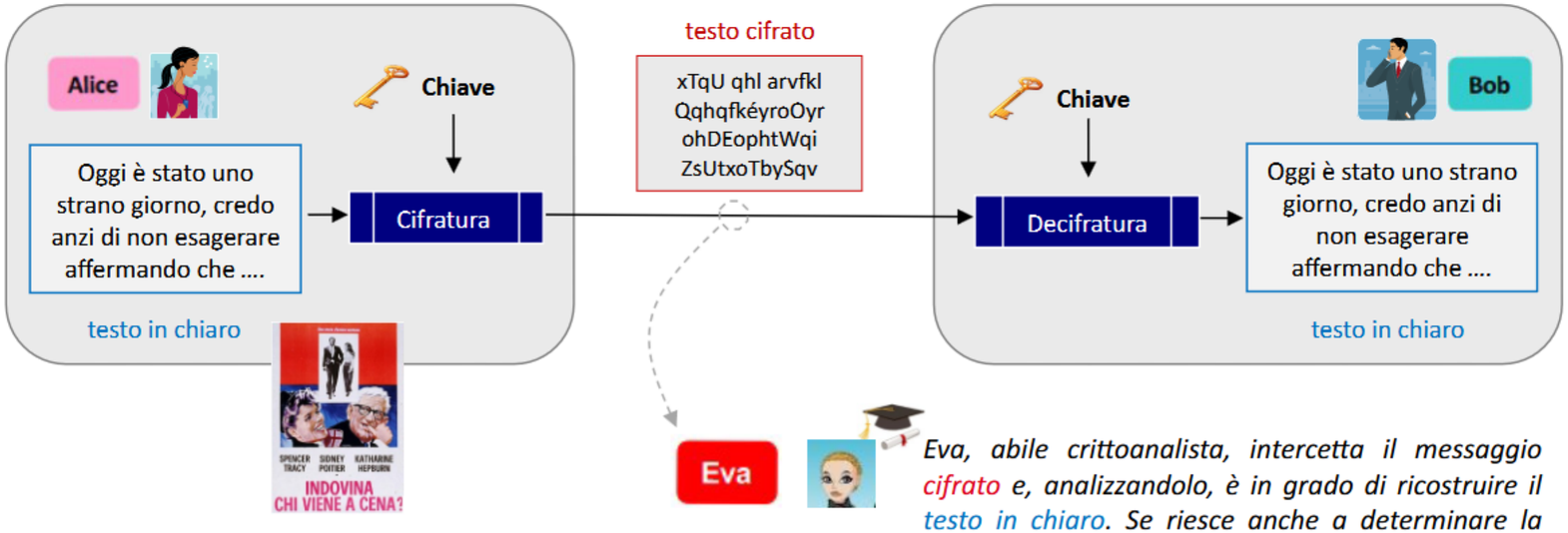


Eva intercetta il messaggio cifrato ma, non conoscendo la chiave condivisa fra Alice e Bob, non è in grado di ricostruire il testo in chiaro.

Introduzione

La **crittoanalisi** è la disciplina che mira a *violare* un cifrario riuscendo, senza conoscere la *chiave*, a ricostruire il messaggio in chiaro, o la chiave stessa, conoscendo solo il testo cifrato.

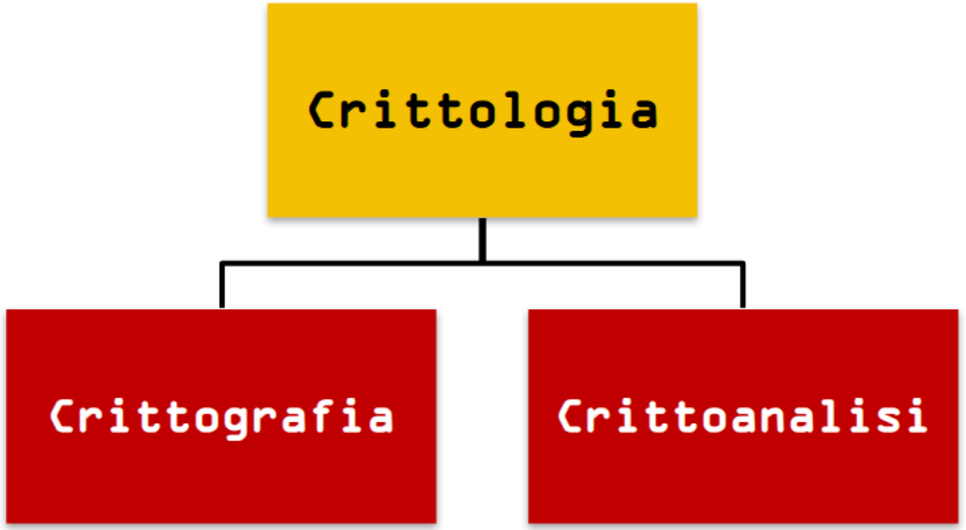
In alcune circostanze l'attaccante riesce a recuperare il testo in chiaro senza essere in grado di ricostruire la chiave. Se però viene scoperta la *chiave* il cifrario si dice *compromesso* (*broken*).



Eva, abile crittoanalista, intercetta il messaggio cifrato e, analizzandolo, è in grado di ricostruire il testo in chiaro. Se riesce anche a determinare la chiave ha compromesso il cifrario.

Introduzione

La crittografia e la crittoanalisi insieme vanno sotto il nome di **crittologia**



Principio di Kerchoffs


JOURNAL
DES
SCIENCES MILITAIRES.
Janvier 1883.
LA CRYPTOGRAPHIE MILITAIRE.
« La cryptographie est un auxiliaire puissant de la tactique militaire. »
(Général LEWAL. Études de guerre.)
I.
LA CRYPTOGRAPHIE DANS L'ARMÉE


Auguste Kerchoffs

"*La cryptographie militaire*", *Journal des sciences militaires*, 1883

"La sicurezza di sistema di cifratura (cifrario) non deve essere compromessa se il nemico conosce le specifiche del cifrario"

Ciò che deve rimanere segreta è la **chiave**!

Nel XX secolo Claude Shannon riformulò questo principio affermando che:

"il nemico conosce il sistema"

Cenni storici

Scitala spartana [~ 400 A.C, Grecia]: il messaggio veniva scritto, in senso longitudinale, su un nastro di stoffa avvolto su un bastone. Solo riavvolgendo il nastro su un bastone dello stesso diametro, il messaggio era ricostruibile.

Codice Atbash : utilizzato anche all'interno della Bibbia per codificare il nome di Babele. La prima lettera dell'alfabeto (in ebraico, *aleph*) viene scambiata con l'ultima (*taw*), la seconda (*beth*) con la penultima (*shin*) e così via …

Chiaro: a b c d e f g h i j k l m n o p q r s t u v w x y z
Cifrato: Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

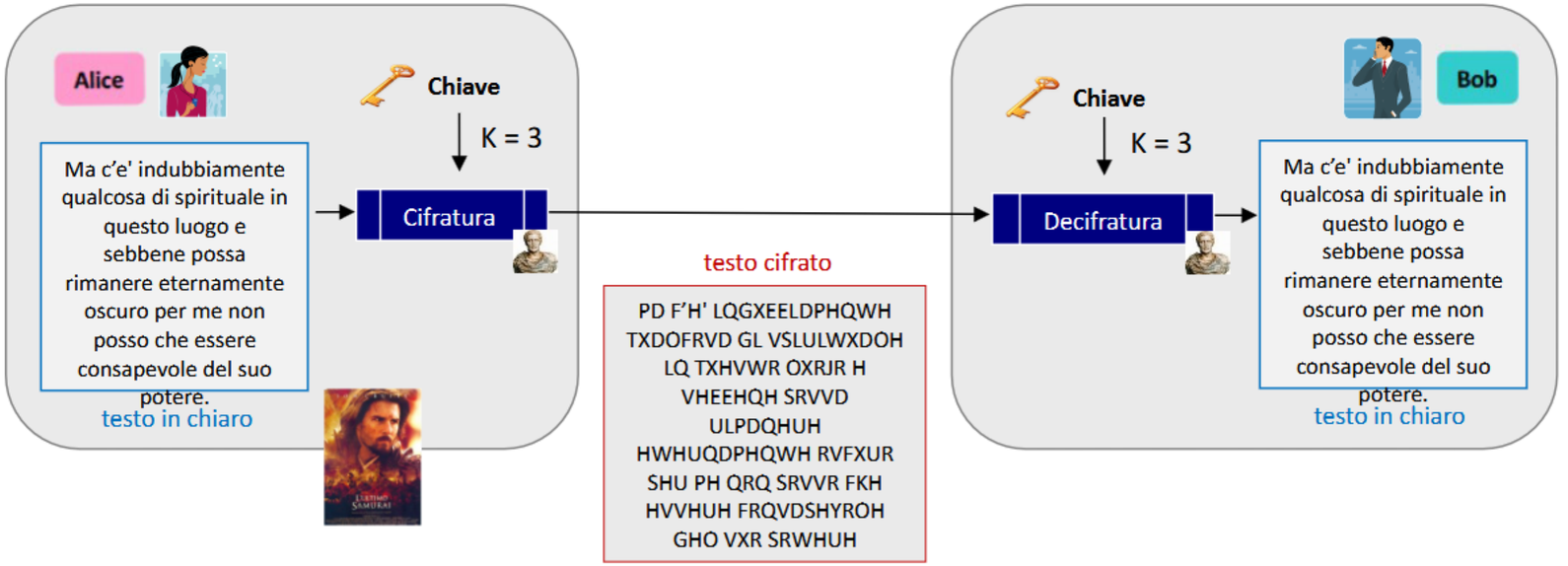
Esempio: ciao a tutti → XRZL Z GFGGR

Cenni storici

Giulio Cesare [100 A.C.]: il cifrario di Cesare[1] prevede che ogni lettera venga sostituita con quella più avanti di *K* posizioni (in origine era *K*=3, quindi 'a' → 'D', 'b' → 'E', …).

Chiaro: a b c d e f g h i j k l m n o p q r s t u v w x y z
Cifrato: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

K = 3

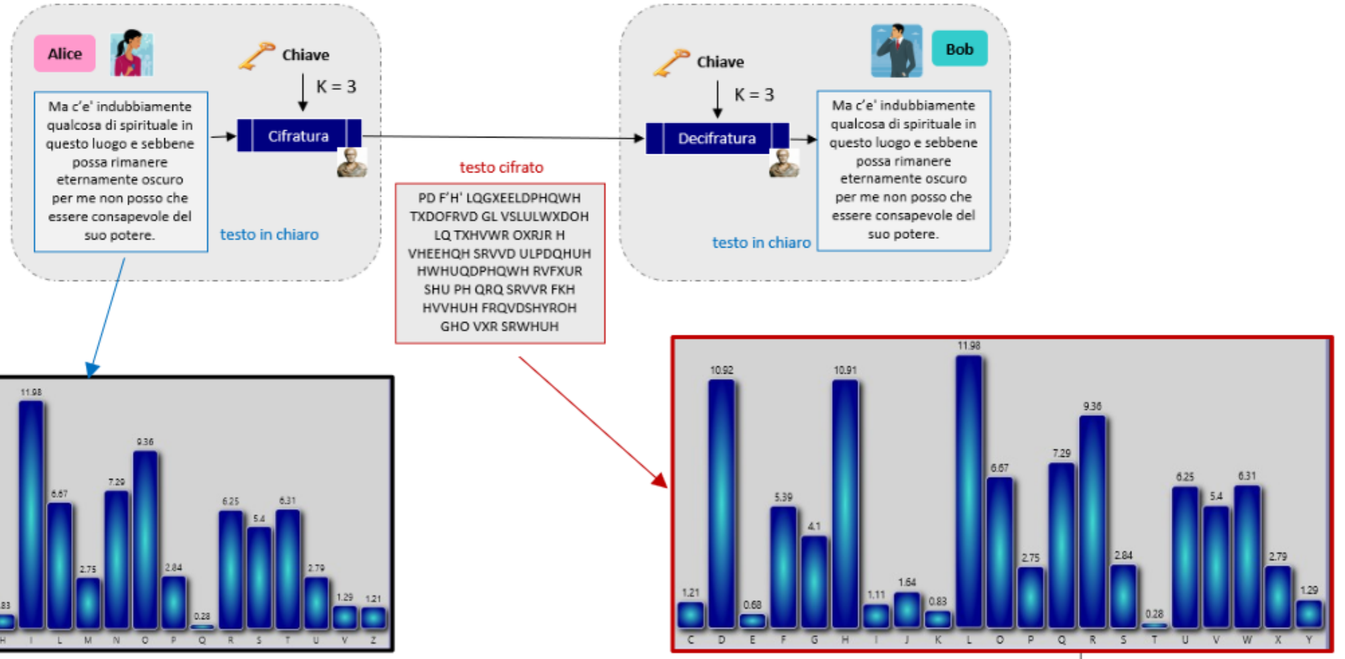


[1] E' un esempio di *cifrario monoalfabetico*: ogni lettera viene sostituita sempre con la stessa lettera (es: 'a' → 'D')

Cenni storici

Nel Medioevo **[IX secolo]** gli Arabi inventarono la tecnica dell'**Analisi delle Frequenze** che studia la distribuzione delle lettere in una lingua.

Ogni lingua ha una propria frequenza caratteristica delle lettere: in italiano, ad esempio, le lettere più comuni sono la **E**, la **A** e la **I**.



Cenni storici

Una celebre vittima della crittoanalisi dei cifrari monoalfabetici è stata **Maria Stuarda** (1542-1587), regina di Scozia e pretendente al trono d'Inghilterra detenuto dalla regina Elisabetta I.

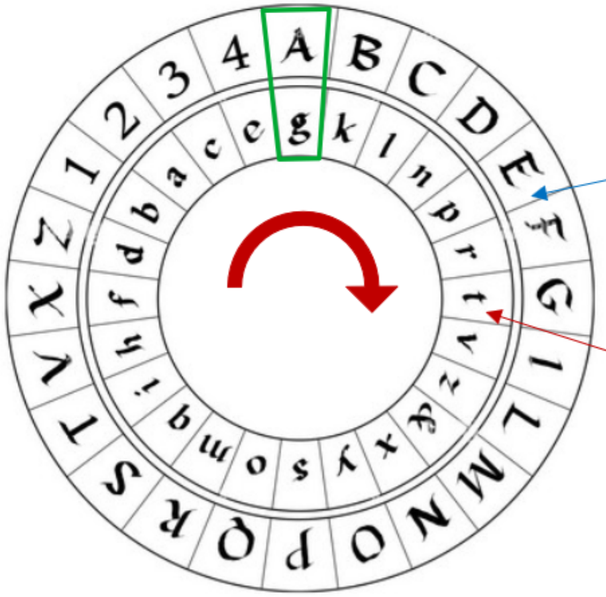
Maria Stuarda si avvia al patibolo,
Scipione Vannutelli, 1861

Venne processata e condannata alla decapitazione perché in un messaggio cifrato, ma sapientemente decifrato, emerse il suo coinvolgimento nella cospirazione che mirava all'uccisione della regina di Inghilterra Elisabetta I.

L'esecuzione avvenne l'8 febbraio 1587.

Leon Battista Alberti [1404-1472] progettò il *disco cifrante*. Due dischi concentrici: uno esterno detto *stabile* con lettere maiuscole, per il testo in chiaro ed uno interno detto *mobile* con lettere minuscole per il testo cifrato.

Si fissa come chiave iniziale la corrispondenza fra un carattere del disco esterno ed uno di quello interno (nella figura A,g). Nel testo in chiaro vengono inserite a caso le cifre 1,2,3,4 che servono per far ruotare opportunamente il disco interno e cambiare quindi le associazioni fra lettere maiuscole e minuscole.



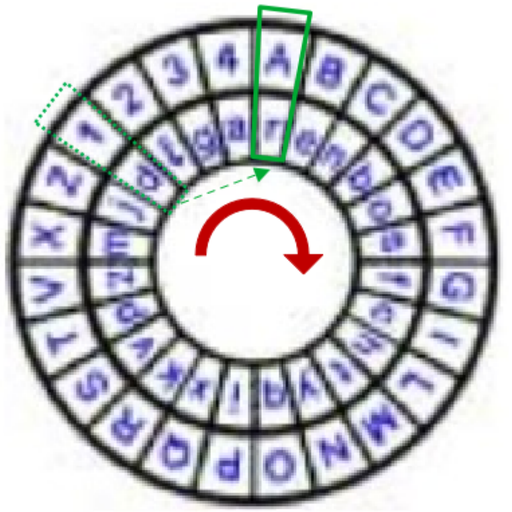
Disco esterno: testo in chiaro (stabile)

Disco interno: testo cifrato (mobile)

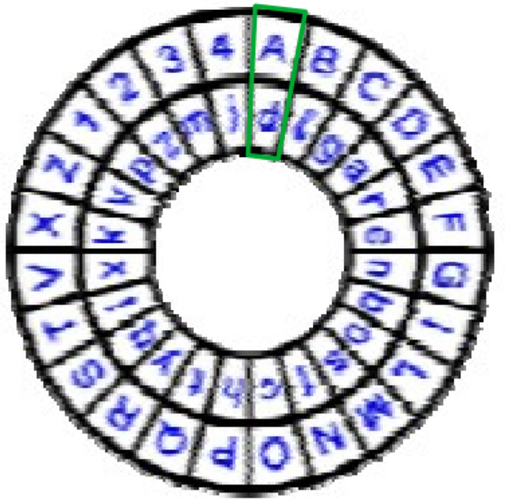
Cenni storici

Esempio (Disco di Alberti):

Configurazione iniziale: (A,r)
Messaggio: CON CORAGGIO PROCEDETE
Testo in chiaro: CON1CORAG2GIOPROCEDE4TE



Quando si incontra la cifra 1, la lettera (d) corrispondente al numero 1 determina la nuova posizione: si ruota il disco interno e si fa corrispondere alla lettera A proprio questa lettera (d), ottenendo la nuova configuraz. (A,d)



Cifratura
In chiaro: C O N 1 C O R A G 2 G I O .....
Cifrato: n q y **d** g c y d n **z** a r o .....

Il **disco di Alberti** era un esempio di *cifrario polialfabetico* e non risultava attaccabile con l'analisi delle Frequenze.

Cenni storici

La geniale intuizione di Alberti venne ripresa da altri (Trithemius, Della Porta) e in particolare fu il francese **Blaise de Vigenère** (1523-1596) a sviluppare una cifrario polialfabetico dalla forma compiuta.
Nel cifrario di Vigenerè la chiave è una sequenza di numeri che determinano gli alfabeti con cui cifrare (sostituire) ogni lettera del messaggio in chiaro. Più lunga è la sequenza più sicura è la cifratura.

Nel XVIII secolo (I Rivoluzione Industriale) ogni nazione europea si dotò di una propria "*camera nera*": centro strategico di decifrazione dei messaggi in codice. La loro efficienza crittoanalitica rese ormai non più utilizzabili i cifrari monoalfabetici.

Si cominciò ad impiegare la più macchinosa ma più sicura **cifratura di Vigenère**, che venne soprannominata *le chiffre indéchiffrable*.

Cenni storici

Nel 1837 **Samuel Morse** inventò il **telegrafo elettrico** e l'omonimo codice.

Nella seconda metà del XIX secolo venne inventato il **telefono** (Meucci, Bell)

Nel 1895 Guglielmo Marconi inventò la comunicazione via **radio**

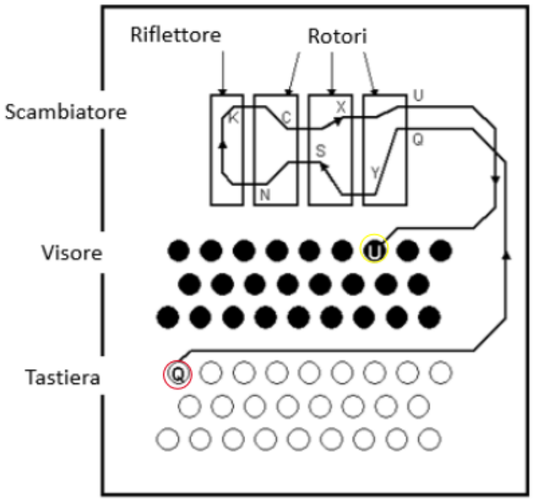
Sempre nella seconda metà dell' 800 venne sviluppata (Charles Babbage, Friedrich Wilhelm Kasiski) una tecnica crittoanalitica che violava il cifrario di Vigenerè.

Le chiffre indéchiffrable era diventato *déchiffrable*.

Cenni storici

Nella prima metà del XX secolo vennero proposte le prime macchine cifranti elettromeccaniche. La più famosa è senza dubbio **Enigma** (1918), usata dai tedeschi durante la seconda Guerra mondiale. Era dotata di un certo numero di rotori (inizialmente erano 3) che deviavano il segnale elettrico, generato dalla tastiera e determinavano il carattere cifrato da visualizzare.

- Negli anni '30 un gruppo di crittoanalisti polacchi, guidati da Marian Rejewsky, riuscì a *violare la crittografia* di Enigma.
- Nel 1939 a Bletchley Park (UK) venne istituita l'unità di Crittoanalisi del Regno Unito, dove vennero decifrati migliaia di messaggi cifrati con Enigma. A tale progetto lavorò il matematico Alan Turing.



Cenni storici

Nel corso del secondo confllitto mondiale i Marines degli Stati Uniti, per proteggere le comunicazioni radio, utilizzarono i **Navajo Code Talkers**: Navajo che trasmettevano le informazioni usando le loro lingua nativa, nota a pochissimi e non documentata in forma scritta.

Caccia	Colibrì	Da-he-tih-hi
Aereo spia	Gufo	Ne-as-jah
Aerosilurante	Rondine	Tas-chizzie
Bombardiere	Poiana	Jay-sho
Cacciabombardiere	Sparviero	Gini
Bombe	Uova	A-ye-shi
Veicolo anfibio	rospo	Chal
Portaerei, corazzata o incrociatore	Balena	Lo-tso
Cacciatorpediniere	Squalo	Ca-lo
Sottomarino	Pesce ferro	Besh-lo

Parole militari in codice Navajo

A	Ant	(formica)	Wol-la-chee	N	Nut	(noce)	Nesh-chee
B	Bear	(orso)	Shush	O	Owl	(gufo)	Ne-ahs-jsh
C	Cat	(gatto)	Moasi	P	Pig	(maiale)	Bi-sodih
D	Deer	(cervo)	Be	Q	Quiver	(faretra)	Ca-yeilth
E	Elk	(alce)	Dzeh	R	Rabbit	(coniglio)	Gah
F	Fox	(volpe)	Ma-e	S	Sheep	(pecora)	Dibeh
G	Goat	(capra)	Klizzie	T	Turkey	(tacchino)	Than-zie
H	Horse	(cavallo)	Lin	U	Ute	(indiani Ute)	No-da-ih
I	Ice	(ghiaccio)	Tkin	V	Victor	(vincitore)	A-keh-di-glini
J	Jackass	(asino)	Tkele-cho-gi	W	Weasel	(donnola)	Gloe-ih
K	Kid	(capretto)	Klizzie-yazzi	X	Cross	(croce)	Al-an-as-dzoh
L	Lamb	(agnello)	Dibeh-yazzi	Y	Yucca	(yucca)	Tsah-as-zih
M	Mouse	(topo)	Na-as-tso-si	Z	Zinc	(zinco)	Besh-do-gliz

Codice alfabetico Navajo

Crittografia Moderna

Nel 1949 il matematico **Claude Shannon**, padre della Teoria dell'Informazione, pubblicò sul *Bell System Technical Journal* l'articolo "*Communication Theory of Secrecy System*" nel quale pose le basi teoriche della **Crittografia Moderna**.

Negli anni '50 nacque l'Informatica commerciale e negli anni '60 i calcolatori diventarono alla portata delle aziende private per elaborare e cifrare le informazioni. Nacque l'esigenza di **standardizzare** i sistemi di cifratura. Nel 1975 nacque il sistema **DES** (Data Encryption Standard)

Nel 1976 **Whitfield Diffie** e **Martin Hellman** proposero, nel famoso articolo *New Directions in Cryptography*, il rivoluzionario concetto di crittografia a chiave pubblica (PKC, *public-key cryptography*).

Nel 1977 Gli studiosi **Rivest**, **Shamir** e **Adleman** svilupparono **RSA**, quello che ad oggi è l'algoritmo di cifratura a *chiave pubblica* più utilizzato.

Crittografia a Chiave pubblica

Ribadiamo il concetto: *è fondamentale che la Chiave rimanga segreta fra mittente e destinatario di una comunicazione* (i nostri amici Alice e Bob)
Ma come fa Alice a scambiare la chiave con Bob? E se Alice deve scambiare messaggi confidenziali anche con Tom, dovrà utilizzare una chiave differente. In linea di principio dovrà impiegare una **chiave diversa** per ogni conoscente!!!!

La **crittografia a chiave pubblica** si basa sui seguenti punti:

- il destinatario (Bob) possiede due chiavi: una pubblica K_{pub}, nota a tutti e una privata K_{pri} che conosce solo lui. La prima può solo cifrare la seconda può solo decifrare.
- il mittente (Alice) usa la chiave pubblica di Bob K_{pub} per cifrare il messaggio da spedire. Con questa chiave NON è possibile effettuare la decifratura.
- Bob utilizza la propria chiave privata K_{pri} per decifrare il messaggio ricevuto.
- Le chiavi, pubblica e privata, sono due numeri tra loro *correlati* tali che è molto *difficile* risalire alla chiave privata, conoscendo la chiave pubblica. La difficoltà è legata alla risoluzione un Problema matematico *particolarmente difficile*.

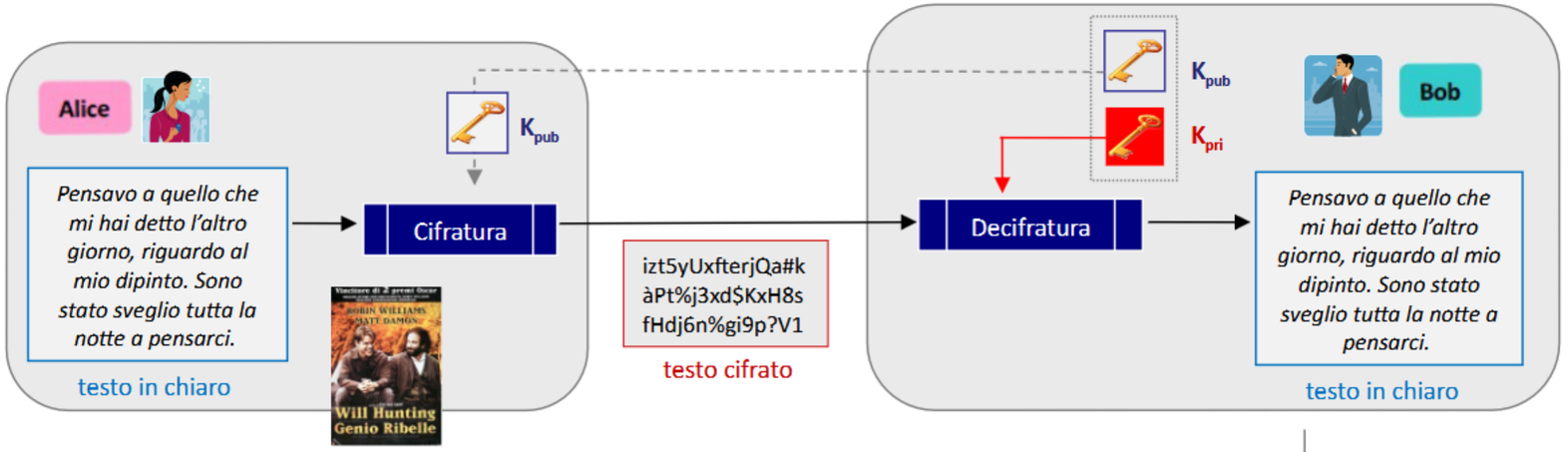
Crittografia a Chiave pubblica

Vediamo come una comunicazione fra Alice e Bob viene protetta con la **Crittografia a Chiave pubblica**.

Bob genera una coppia di chiavi (K_{pub}, K_{pri})

- K_{pub}: chiave *pubblica*, usata per cifrare (nota a tutti)
- K_{pri}: chiave *privata*, usata per decifrare (nota solo a Bob)

- Bob spedisce ad Alice, senza timori, la sua chiave pubblica K_{pub}
- Alice usa chiave pubblica di Bob K_{pub} per cifrare il messaggio destinato a Bob
- Bob usa la propria chiave privata K_{pri} per decifrare il *testo cifrato* inviato da Alice



Crittografia a Chiave pubblica

L'algoritmo di crittografia a chiave pubblica più utilizzato è senza dubbio **RSA** (1977). La sicurezza di RSA si basa sul problema della **Fattorizzazione Intera**: dato $N=p\times q$, ottenuto moltiplicando due grandi numeri primi p e q, determinare questi ultimi.

Noto N=827.371 trovo p=937 e q=883 tali che $N=p\times q$

Noto N=152260502792253336053561837813263742971806811496138068865790849458012296325895289765400035069200613 9 [1]

Compito per casa: trovare p e q 😜

Nel generare la propria coppia di chiavi privata/pubblica Bob seleziona a caso due numeri primi molto grandi p e q e li moltiplica fra loro per ottenere $N=p\times q$.

Il numero N è noto a chiunque, perchè è contenuto nella chiave pubblica (K_{pub}), però per valori grandi di N è *molto, molto* difficile trovare i due primi p e q conoscendo il loro prodotto N.

Se infatti si riuscisse ad ottenere i due numeri primi p e q, con semplici calcoli si potrebbe calcolare la chiave privata (K_{pri}) di Bob.

[1] https://en.wikipedia.org/wiki/RSA_numbers#RSA-100

PGP, Zimmermann e la I *Crypto War*

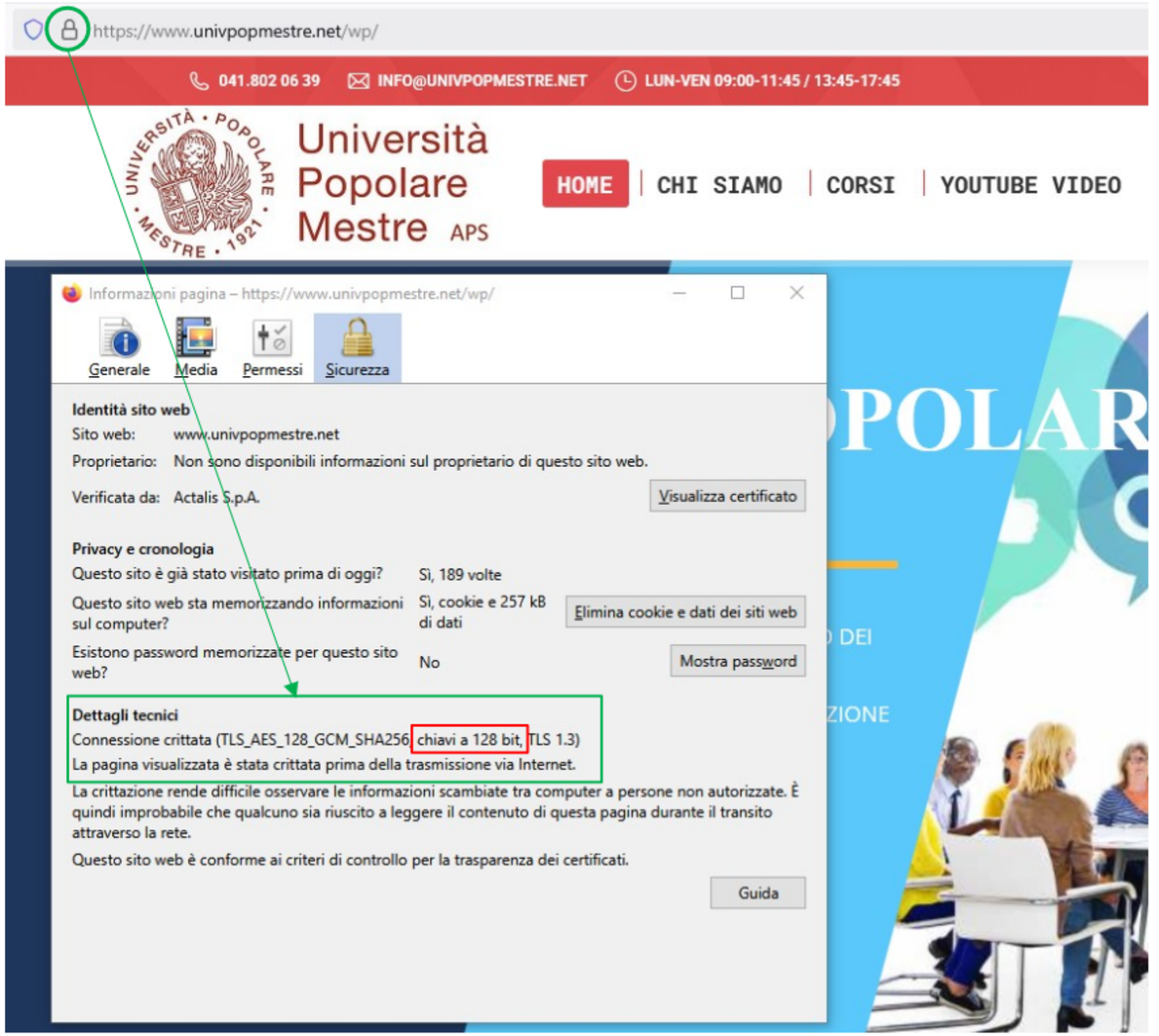
Nel 1991 Phil Zimmermann rese pubblico **PGP** (*Pretty Good Privacy*), un programma di crittografia che permetteva di proteggere la posta elettronica con l'utilizzo della crittografia a chiave pubblica (RSA).

Venne incriminato per violazione del brevetto con cui era protetto RSA ma soprattutto per esportazione illegale di **materiale bellico**. A quel tempo per il Governo statunitense il software crittografico era un'arma, al pari di missili e mitragliatrici. Nel 1996 la crittografia venne rimossa dalla lista delle munizioni e, dopo tre anni di indagini, si decise di rinunciare all'incriminazione di Zimmermann.

Il *caso* Zimmermann accese il dibattito sui *pro* e *contro* della Crittografia e si inserì nel periodo (anni '80 e '90) i cui si consumò la I ***Crypto War***.
Il governo degli Stati Uniti cercò di limitare e controllare l'utilizzo della crittografia da parte sia dei privati cittadini che degli altri paesi :

- utilizzo del Clipper chip nei telefoni (1993 NSA, abbandonato nel 1996)
- restrizioni nell'esportazione di tecnologie crittografiche: non solo hardware ma anche software e … lunghezza delle chiavi (rimosse nel 2000)

PGP, Zimmermann e la I *Crypto War*



Negli anni '90 l'esportazione di algoritmi crittografici con chiavi più lunghe di 40 bit era soggetta a severe restrizioni.

La II *Crypto War*

Agli inizi degli anni 2000 iniziarono a diffondersi gli smartphone

La II ***Crypto War*** *scoppiò* nel secondo decennio degli anni 2000, con l'esplosione delle comunicazioni attraverso i dispositivi mobili (WhatsApp nacque nel 2009) e soprattutto dopo il 2014, anno in cui Apple e Google iniziarono a cifrare gli smartphone di default.

Agosto 2010: gli Emirati Arabi chiesero, e ottennero, le chiavi per decifrare i BlackBerry

https://www.punto-informatico.it/emirati-arabi-blackberry-funzioner/

Puntoinformatico

Emirati Arabi, BlackBerry funzionerà

Sicurezza Antivirus

Raggiunto l'accordo tra il governo di Abu Dhabi e RIM. L'azienda canadese fa un passo indietro fornendo i codici di cifratura degli smartphone. Restano oscuri i dettagli dell'intesa

Chiunque abbia intenzione di recarsi negli Emirati Arabi potrà stare tranquillo sul funzionamento del proprio BlackBerry: è stato raggiunto l'accordo tra RIM e il governo locale.

Cristina Sciannamblo
Pubblicato il 8 ott 2010

La vicenda ha finalmente trovato il suo epilogo, dopo mesi di botta e risposta tra le parti in causa. Tutto ha inizio quando le autorità dell'emirato annunciano di voler monitorare gli strumenti di messaggistica dello smartphone canadese per motivi di sicurezza nazionale: si teme che a **sfruttare certi canali di comunicazione siano anche alcune cellule terroristiche di Al Quaeda.**

Dopo che la Commissione per le Comunicazioni e l'IT ha annunciato il blocco dei dispositivi, RIM ha risposto sostenendo di rispettare le regolamentazioni locali dei 170 paesi in cui opera, insistendo sulla necessità di compiere un'indagine approfondita sulla faccenda. La partita, almeno per il momento, si conclude con la **vittoria di Abu Dhabi** .

Febbraio 2016: l'FBI chiese ad Apple di sbloccare l'iPhone di un attentatore

di Fabio Massa

Il recente caso investigativo americano ha suscitato numerose discussioni di carattere tecnico, giuridico etico e sociale in merito alla disputa tra la Apple inc., la Federal Bureau of Investigation e la DOJ (U.S. Department of Justice), generata dalla richiesta di sblocco di un Iphone 5C utilizzato da uno dei killer della strage di San Bernardino in California del dicembre 2015, dove sono rimaste uccise 14 persone e ferite gravemente 22. il telefono dell'attentore è stato recuperato intatto, ma risultava bloccato da un codice di blocco a 4 cifre e impostato per il wiping dei dati dopo 10 tentativi falliti nell'inserimento del codice di blocco, opzione presente nei dispositivi iPhone. La Apple inc. adducendo diverse motivazioni, tecniche e giuridiche, ha rifiutato la disponibilità nella creazione di un software che avrebbe consentito di bypassare i sistemi di sicurezza dei loro dispositivi, nodo cardine delle politiche commerciali dell'azienda.

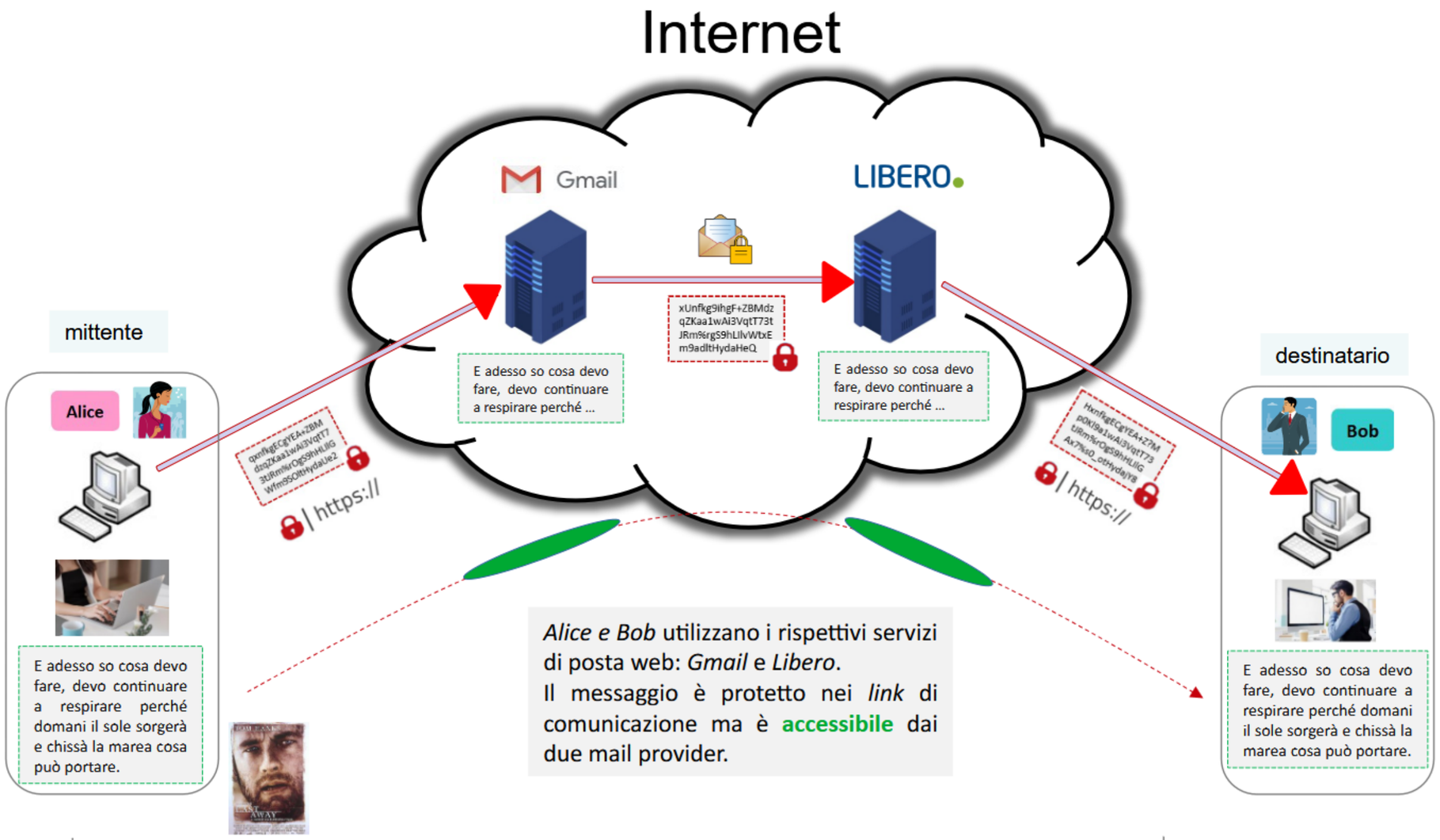
Going Dark

Nell'ottobre del 2014 il Direttore dell'FBI James B. Comey evocò il rischio della sindrome **Going Dark**: *l'incapacità, a causa della crittografia, delle agenzie governative di proteggere i cittadini dai criminali e dai terroristi*.

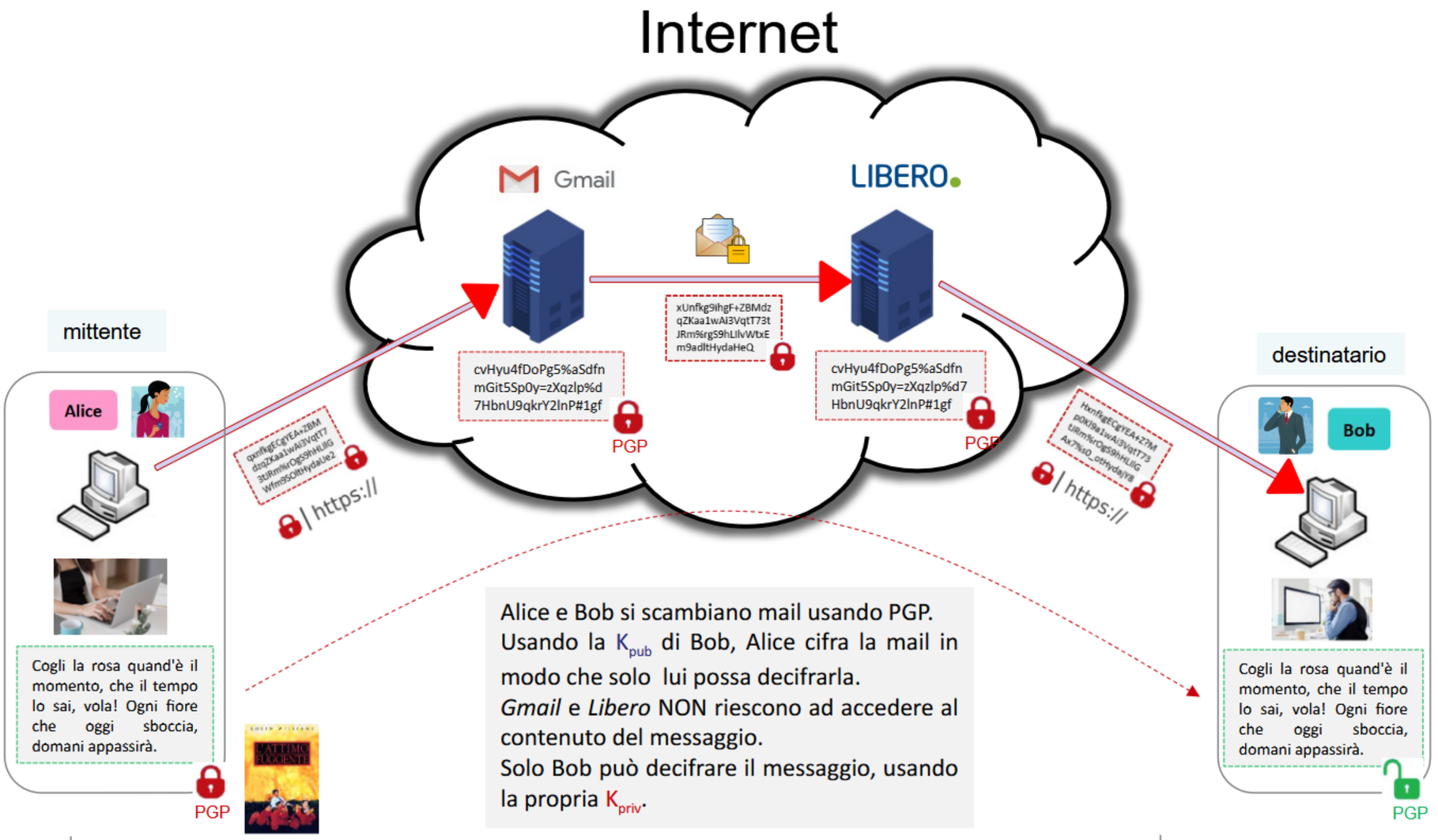
*"Sfortunatamente, la legge non ha tenuto il passo con la tecnologia e questa disconnessione ha creato un problema significativo di sicurezza pubblica. Lo chiamiamo "**Going Dark**" e il suo significato è questo: coloro che sono incaricati di proteggere la nostra gente non sono sempre in grado di accedere alle prove di cui abbiamo bisogno per perseguire i crimini e prevenire il terrorismo, anche con l'autorità legale. (…)*
*Ci troviamo di fronte a due sfide sovrapposte. La **prima** riguarda l'intercettazione in tempo reale ordinata dal tribunale di ciò che chiamiamo "dati in movimento", come telefonate, e-mail e sessioni di chat in tempo reale. La **seconda** sfida riguarda l'accesso ordinato dal tribunale ai dati archiviati sui nostri dispositivi, come e-mail, messaggi di testo, foto e video, o ciò che chiamiamo "dati a riposo". E sia le comunicazioni in tempo reale che i dati archiviati sono sempre più crittografati."*

In particolare, per l'intercettazione delle comunicazioni, la crittografia **End-to-End** (E2E) si stava rivelando *un osso particolarmente duro*.

Crittografia di collegamento



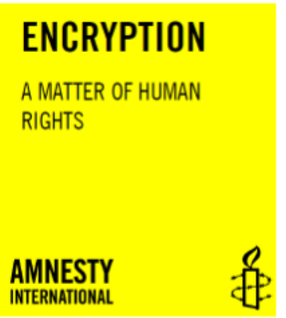
Crittografia End-to-End



Alice e Bob si scambiano mail usando PGP.
Usando la K_{pub} di Bob, Alice cifra la mail in modo che solo lui possa decifrarla.
Gmail e *Libero* NON riescono ad accedere al contenuto del messaggio.
Solo Bob può decifrare il messaggio, usando la propria K_{priv}.

Going Dark

A marzo 2016 **Amnesty International** ha pubblicato il documento "*Encryption, A matter of human rights*".



*"Nell'era digitale, l'accesso e l'uso della crittografia sono un abilitatore del **diritto alla privacy**. (...). La crittografia è quindi anche un abilitatore dei **diritti alla libertà di espressione**, informazione e opinione, e ha anche un impatto sui diritti alla libertà di riunione pacifica, associazione e altri diritti umani."*

*"Costringere le aziende a fornire "**backdoor**" alla crittografia implementata nei loro prodotti o servizi (che potenzialmente incide su tutti gli utenti) costituisce una significativa interferenza con i diritti degli utenti alla privacy e alla libertà di espressione. "*

Aprile 2022: **Meta** ha publicato un report commissionato a *Business for Social Responsibility* (BSR) nel quale emerge che la crittografia end-to-end ha un effetto fondamentale ed estremamente positivo per la tutela dei diritti umani.

https://www.wired.it/article/privacy-rapporto-meta-crittografia-diritti-umani/

WIRED SCIENZA ECONOMIA CULTURA GADGET SECURITY DIRITTI IDEE VIDEO PODCAST

LILY HAY NEWMAN SECURITY 19.04.2022

La crittografia end-to-end è fondamentale per i diritti umani

Un nuovo rapporto commissionato da Meta sottolinea il ruolo della tecnologia per la tutela della privacy, e potrebbe aiutare la società superare l'opposizione dei governi che vogliono più controlli

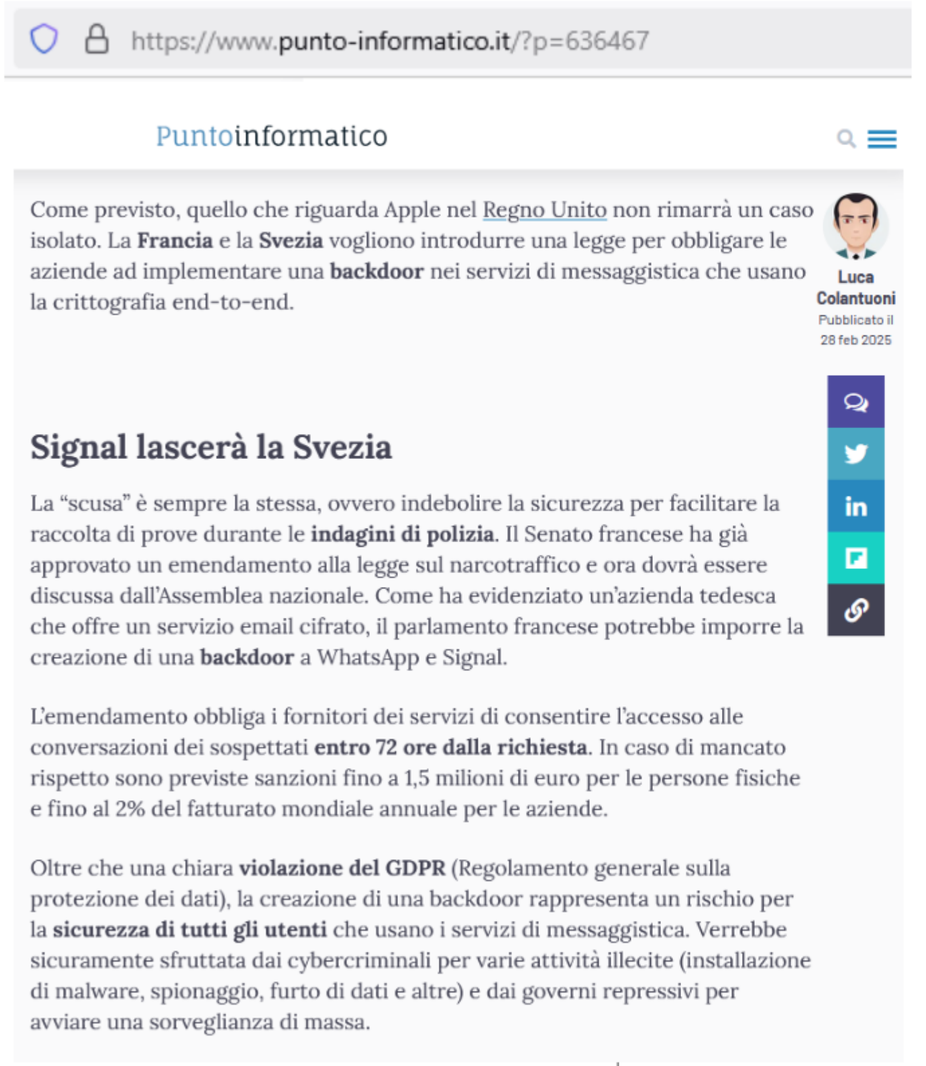
Lunedì 4 aprile Meta ha pubblicato un rapporto sugli impatti della crittografia end-to-end sui diritti umani, realizzato da Business for Social Responsibility (Bsr), una no-profit che si occupa di responsabilità sociale d'impresa. Oltre ad averlo commissionato, Meta ha anche pubblicato un documento di risposta al rapporto indipendente di Bsr. Nello studio, che ha richiesto più di due anni per essere completato, Bsr rileva che **la crittografia end-to-end ha un effetto fondamentale ed estremamente positivo per la tutela dei diritti umani**, e approfondisce allo stesso tempo il tema di come le attività criminali ed l'estremismo violento possano trovare rifugio sicuro sulle piattaforme criptate grazie alla tecnologia. Il rapporto elenca anche alcune raccomandazioni su come mitigare questi impatti negativi.

Going Dark

Agli inizi del **2023** l'UE affrontò il tema "Going dark"

Going Dark

febbraio 2025: La Francia e la Svezia vogliono introdurre una legge per obbligare le aziende ad implementare una *backdoor* nei servizi di messaggistica che usano la crittografia end-to-end.



https://www.punto-informatico.it/?p=636467

Puntoinformatico

Come previsto, quello che riguarda Apple nel Regno Unito non rimarrà un caso isolato. La **Francia** e la **Svezia** vogliono introdurre una legge per obbligare le aziende ad implementare una **backdoor** nei servizi di messaggistica che usano la crittografia end-to-end.

Luca Colantuoni
Pubblicato il 28 feb 2025

Signal lascerà la Svezia

La "scusa" è sempre la stessa, ovvero indebolire la sicurezza per facilitare la raccolta di prove durante le **indagini di polizia**. Il Senato francese ha già approvato un emendamento alla legge sul narcotraffico e ora dovrà essere discussa dall'Assemblea nazionale. Come ha evidenziato un'azienda tedesca che offre un servizio email cifrato, il parlamento francese potrebbe imporre la creazione di una **backdoor** a WhatsApp e Signal.

L'emendamento obbliga i fornitori dei servizi di consentire l'accesso alle conversazioni dei sospettati **entro 72 ore dalla richiesta**. In caso di mancato rispetto sono previste sanzioni fino a 1,5 milioni di euro per le persone fisiche e fino al 2% del fatturato mondiale annuale per le aziende.

Oltre che una chiara **violazione del GDPR** (Regolamento generale sulla protezione dei dati), la creazione di una backdoor rappresenta un rischio per la **sicurezza di tutti gli utenti** che usano i servizi di messaggistica. Verrebbe sicuramente sfruttata dai cybercriminali per varie attività illecite (installazione di malware, spionaggio, furto di dati e altre) e dai governi repressivi per avviare una sorveglianza di massa.

Going Dark

febbraio 2025: Il Regno Unito ha ordinato a Apple di creare una *backdoor* che consenta di recuperare tutti i dati salvati su iCloud di qualsiasi utente Apple nel mondo.

La richiesta si concentra sul servizio **Advanced Data Protection** (ADP) di Apple, che utilizza la crittografia end-to-end, rendendo i dati accessibili solo al proprietario dell'account.

Apple ha smesso di offrire il servizio ADP ai nuovi utenti nel Regno Unito e richiederà agli utenti esistenti di disattivare questa funzione in futuro.

https://www.rivista.ai/2025/02/22/apple-rimuove-la-protezione-avanzata-dei-dati-nel-regno-unito-una-mossa-per-salvaguardare-la-privacy

Apple rimuove la protezione avanzata dei dati nel regno unito: una mossa per salvaguardare la privacy degli utenti

DI REDAZIONE / IL 22 FEBBRAIO 2025 / IN BUSINESS

Apple ha recentemente deciso di ritirare la funzionalità di sicurezza "Advanced Data Protection" (ADP) per gli utenti nel Regno Unito. Questa decisione è una risposta diretta alle richieste del governo britannico, che ha ordinato all'azienda di Cupertino di creare una "backdoor" nei suoi sistemi di crittografia, consentendo l'accesso ai dati degli utenti da parte delle autorità.

L'ADP, introdotta da Apple alla fine del 2022, offre una crittografia end-to-end per i dati archiviati su iCloud, garantendo che solo il titolare dell'account possa accedervi. Tuttavia, secondo quanto riportato dal Financial Times, il governo britannico ha emesso un "technical capability notice" in base all'Investigatory Powers Act del 2016, noto anche come "Snooper's Charter", che richiede alle aziende di fornire accesso ai dati dei clienti per scopi di sicurezza nazionale. Questa legge impedisce alle aziende di discutere pubblicamente tali richieste, rendendo la decisione di Apple di ritirare l'ADP un'ammissione implicita della situazione.

Crittografia al Cinema

I signori della Truffa

The Imitation Game

Enigma

U-571

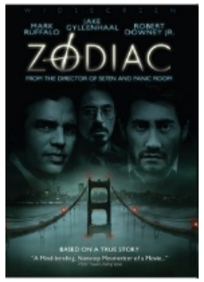
Windtalkers

Codice Mercury

Codice Swordfish

Nemico pubblico

Zodiac



Crittografia in libreria

[Guglielmo]: *"Se Venanzio fosse stato un ingenuo avrebbe usato l'alfabeto zodiacale più comune: A uguale a Sole, B uguale a Giove... La prima linea si leggerebbe allora... prova a trascrivere: RAIQASVL..." S'interruppe. "No, non vuole dire nulla, e Venanzio non era ingenuo. Ha riformulato l'alfabeto secondo un'altra chiave. Dovrò scoprirla."*

[Adso]: *"E' possibile?" domandai ammirato.*
[Guglielmo]: *"Sì, se si conosce un poco della sapienza degli arabi. I migliori trattati di* ***criptografia*** *sono opera di sapienti infedeli, e a Oxford ho potuto farmene leggere qualcuno. Bacone aveva ragione a dire che la conquista del sapere passa attraverso la conoscenza delle lingue. (...)*

[Adso]: *"E quale di questi sistemi avrà usato Venanzio?"*
[Guglielmo]: "Bisognerebbe provarli tutti, e altri ancora. Ma la prima regola per ***decifrare*** *un messaggio è indovinare cosa voglia dire."*
[Adso]: *"Ma allora non c'è più bisogno di decifrarlo!" risi.*
[Guglielmo]:*"Non in questo senso. Si possono però formulare delle ipotesi su quelle che potrebbero essere le prime parole del messaggio, e poi vedere se la regola che se ne inferisce vale per tutto il resto dello scritto "*

Crittografia in libreria

Langdon si guardò attorno e si accorse di essersi fermato a metà della scala, paralizzato da un'improvvisa rivelazione. "O, Draconian devil! Oh, lame saint!" […]Laggiù, nelle viscere del Louvre, con il pensiero di phi e di Leonardo, Robert Langdon aveva ***decifrato*** *all'improvviso, senza volerlo, il codice di Saunière.*
«O, Draconian devil» mormorò. «Oh, lame saint. È proprio il tipo di codice più semplice...!» […]
«L'ha detto lei» spiegò Langdon, con la voce piena di eccitazione. «I numeri di Fibonacci hanno significato solo se sono nel loro giusto ordine. Altrimenti sono solo nonsense matematici. Prese di tasca la stampata del computer ed esaminò nuovamente il messaggio del nonno.

13-3-2-21-1-1-8-5
O, Draconian devil!
Oh, lame saint!

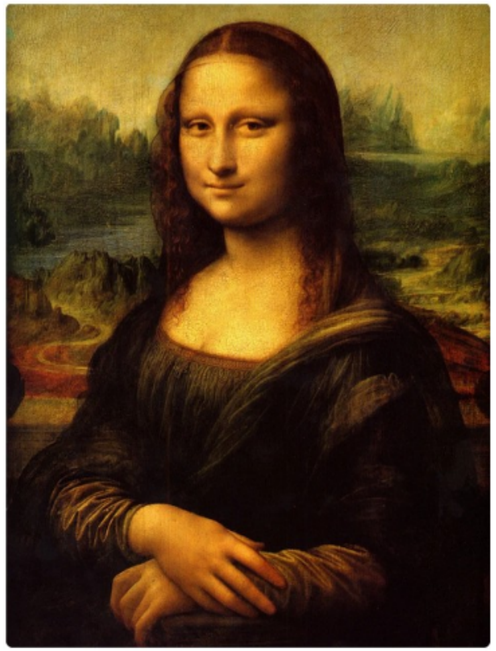
"Che significato possono avere questi numeri?" «La sequenza di Fibonacci cambiata di ordine è un indizio» disse Langdon, facendosi dare il foglio. «I numeri suggeriscono come decifrare il resto del messaggio. Saunière ha scritto la sequenza non in ordine per dirci di applicare lo stesso concetto al testo. "O, Draconian devil! Oh, lame saint!" Queste righe non significano nulla. ***Sono semplicemente lettere scritte non nel loro giusto ordine****.»*
Langdon incrociò lo sguardo con quello di Sophie. «Il significato del messaggio di suo nonno è sempre stato davanti ai nostri occhi, e lui ci ha lasciato abbondanti indizi per scoprirlo.» Senza altre parole, prese una penna dal taschino e ricombinò le lettere di ciascuna riga.

O, Draconian devil!
Oh, lame saint!

era un perfetto anagramma di:

Leonardo da Vinci!
The Mona Lisa!

Sorriso enigmatico ...



*“ La crittografia e l'anonimato sono necessari come abilitatori sia della **libertà di espressione** e di opinione, sia del **diritto alla privacy**. Non è né fantasioso né esagerato affermare che, senza strumenti di crittografia, le vite potrebbero essere messe in pericolo. Nei casi peggiori, la capacità di un governo di entrare nei telefoni dei suoi cittadini potrebbe portare alla persecuzione di individui che stanno semplicemente esercitando i loro **diritti umani fondamentali**.”*

Nazioni Unite, Alto Commissario per i Diritti Umani[1]

[1] https://www.ohchr.org/en/press-releases/2016/03/apple-fbi-case-could-have-serious-global-ramifications-human-rights-zeid

Grazie per l'attenzione!

Gianluca

Domande?