
Liceo Galvani – commissione BOLII2004

Classe VN – indirizzo internazionale scientifico

Percorso individuale

Esame di Stato anno scolastico 2017/18

Giulio Cesare avrebbe WhatsApp?

Crittografia: un'arte antica
nel nostro quotidiano

Discipline coinvolte:
Matematica, Storia, Inglese

Gioele Buriani

INDICE

INTRODUZIONE	2
COS'È LA CRITTOGRAFIA.....	3
Algoritmo e chiave.....	3
Classificazione dei cifrari.....	3
UN PO' DI STORIA.....	5
In principio	5
La crisi.....	6
Nuove soluzioni.....	6
Una brusca accelerazione	8
Ormai indispensabile.....	9
L'uomo non basta più.....	10
EDGAR ALLAN POE	13
A passion for cryptography.....	13
The Gold-Bug.....	13
CRITTOGRAFIA MODERNA.....	16
Crittografia a chiave pubblica	16
Troppo presto e nel posto sbagliato	16
Asimmetria per tutti	17
Algoritmi a chiave pubblica	17
Chiavi e lucchetti	18
Scambiare un messaggio.....	19
Scambiare un messaggio identificando il mittente.....	19
Tutto ciò ci riguarda?	21
HTTPS e Home Banking	21
Posta elettronica certificata e smart card.....	22
Messaggistica istantanea, WhatsApp & C.	23
Criptomonete, Bitcoin & C.	23
Algoritmo RSA	24
Aspetti matematici	24
Un semplice esempio numerico	26
CONCLUSIONI	29
BIBLIOGRAFIA	30

INTRODUZIONE

Il mio interesse per la crittografia è nato inizialmente dalla passione per i rompicapo e gli enigmi di logica tra cui, appunto, la decifrazione di messaggi. Se però da bambino avevo considerato la crittografia quasi come un gioco, negli ultimi anni mi sono reso conto della sua importanza nella realtà quotidiana odierna. Uno stimolo ulteriore è arrivato dal film di Morten Tyldum *The Imitation Game*, che tratta dell'importanza della decifrazione della macchina Enigma nel corso della Seconda Guerra Mondiale.

Da quel momento ho cominciato a notare diverse notizie riguardanti la crittografia, ad esempio il cambio di politiche di Whatsapp che molti hanno letto senza realmente capirne il significato. L'evento più recente che mi ha convinto ad approfondire questo argomento è stato l'esplosione del Bitcoin, la criptovaluta che ultimamente ha fatto tanto parlare di sé: anche il funzionamento di questa moneta virtuale è basato sulla crittografia.

Spesso, sentendo parlare di crittografia, si pensa a un passatempo per amanti di enigmi e rompicapi, al pari di un cruciverba. Non a tutti, però è noto che questa disciplina ha origini molto antiche ed è stata di grande importanza per lo sviluppo della storia umana, influenzandone numerosi eventi.

La rivoluzione più significativa riguardante l'impiego di questa disciplina si è verificata alla fine del ventesimo secolo, per poi presentare una crescita esponenziale negli ultimi anni. Questo ben più ampio utilizzo della crittografia è stato dettato dalla rivoluzione dell'informatica: con la nascita dei computer e di Internet si è rivelato necessario individuare sistemi grazie ai quali i miliardi di informazioni trasmesse dagli utenti tramite la rete non cadessero in mani di terzi. Inoltre si doveva dare la possibilità di mandare e ricevere informazioni cifrate anche, e soprattutto, a coloro che di crittografia non sapevano nulla. Si sono così sviluppati dei sistemi automatici in grado di cifrare e decifrare le comunicazioni tra tutti gli utenti. Questi automatismi fanno però sì che l'utente medio spesso non sia consapevole del fatto che la crittografia entra più volte nel suo quotidiano.

COS'È LA CRITTOGRAFIA

La crittografia (dal greco κρυπτός [kryptós] "nascosto" e γραφία [graphía] "scrittura") è la scienza che si occupa delle tecniche per cifrare un messaggio, ovvero trascriverlo in modo tale che esso possa essere decifrato e letto solamente dal destinatario.

Algoritmo e chiave

Nella crittografia esiste l'algoritmo, cioè il procedimento che viene applicato al messaggio, ed esistono le chiavi che permettono all'algoritmo di variare il risultato ogni volta. Gli algoritmi in crittografia si chiamano cifrari o cifre. Nel banalissimo cifrario di Cesare l'algoritmo è "sposta ogni lettera in avanti di un certo numero di posti nell'alfabeto" e la chiave è il numero: al variare di questo numero, lo stesso messaggio di partenza darà messaggi cifrati diversi.

La netta separazione concettuale di algoritmo e chiave è uno dei più saldi principi della crittografia e fu formulata in modo definitivo nel 1883 dal linguista olandese Auguste Kerckhoffs von Nieuwenhof: "La sicurezza di un crittosistema non deve dipendere dal tener celato il critto-algoritmo. La sicurezza dipenderà solo dal tener celata la chiave"¹.

Detto in parole ancora 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 decrittato) e dunque tenere segreto un algoritmo di cifratura non è mai una strategia vincente. Conviene piuttosto affidare la sicurezza alla bontà delle chiavi usate.

Un algoritmo si dice sicuro se l'attacco più efficace contro di esso è un attacco a forza bruta, (Brute Force Attack) cioè che consiste nel provare tutte le possibili chiavi.

Il testo originale si chiama testo in chiaro, mentre quello ottenuto in seguito all'operazione di cifratura è detto testo cifrato.

Classificazione dei cifrari

Per poter classificare i diversi tipi di cifrario occorre innanzitutto definire i concetti di chiave simmetrica e chiave asimmetrica.

Un cifrario a chiave simmetrica è un algoritmo che cifra e decifra usando la medesima chiave. La crittografia simmetrica è anche definita tradizionale poiché fu l'unica utilizzata fino all'avvento dei computer.

Un cifrario a chiave asimmetrica, invece, è un algoritmo che per cifrare e decifrare necessita di una coppia di chiavi diverse tra loro. Questo tipo di cifrario nasce con la diffusione dei computer.

Il problema della classificazione dei cifrari è piuttosto complesso, qui diamo una definizione delle tipologie più comuni.

¹ Auguste Kerckhoffs, *La Cryptographie militaire*, Journal des sciences militaires, vol. IX, Parigi, Jan. 1883, pp. 5–38

Per ciò che riguarda i cifrari a chiave simmetrica abbiamo:

- Trasposizione
i simboli del testo cifrato sono ottenuti “mescolando” quelli originari secondo una qualche regola reversibile. Es. scitola spartana.
- Sostituzione
i simboli del testo di partenza vengono sostituiti da un simbolo diverso nel testo cifrato.
Questi cifrari si dividono in:
 - Monoalfabetici
ogni simbolo di partenza viene sostituito sempre dallo stesso simbolo secondo una regola di sostituzione unica da concordare. Es. Cifrario di Cesare.
 - Polialfabetici
ogni simbolo di partenza viene sostituito non sempre dallo stesso simbolo, ma da simboli diversi che vengono determinati da una chiave segreta da concordare. Es. Disco cifrante di Leon Battista Alberti.
- Composti
uniscono le due tipologie precedenti: il testo chiaro viene cifrato con un metodo ottenendo un testo cifrato che viene a sua volta cifrato con un altro metodo; questa operazione si chiama sovracifratura e può essere ripetuta molte volte. Es. AES.

I cifrari a chiave asimmetrica si basano su strumenti matematici più complessi e meno intuitivi delle trasposizioni e sostituzioni tipiche dei cifrati simmetrici in quanto fanno tutti uso di funzioni facili da computare ma difficili da invertire, cioè risalire agli elementi di partenza, a meno di non conoscere un particolare dato. Una classificazione di base si limita quindi a indicare le principali funzioni utilizzate:

- Fattorizzazione: dati due numeri primi p e q è facile calcolare $n = pq$, ma dato n è difficile risalire ai suoi fattori p e q se p e q sono abbastanza grandi. Es. RSA.
- Logaritmo discreto: è facile calcolare un esponenziale (elevamento a potenza di un numero) mentre lo è molto meno trovare l'esponente da dare alla base nota per ottenere l'argomento noto. Es. Diffie Helmann.
- Logaritmo Discreto su Curve Ellittiche: è una generalizzazione del Logaritmo discreto sui punti di una curva ellittica. Es. ElGamal.

UN PO' DI STORIA

In principio

Le prime forme di crittografia nascono subito dopo la scrittura umana, più di 4000 anni fa.

Lo storico greco Erodoto ci parla di casi nelle civiltà antiche in cui un messaggio veniva scritto e poi celato grazie a diversi stratagemmi (strato di cera, ricrescita dei capelli sul cuoio capelluto rasato,...). In questi casi però si tratta non di crittografia, dove il testo del messaggio viene mutato secondo un determinato criterio, bensì di steganografia, dove il messaggio può anche rimanere leggibile, ma ne viene celata l'esistenza.

Il primo caso rilevante di vera e propria crittografia risale invece all'inizio del VI secolo a.C. nel Libro di Geremia della Bibbia, dove compare una parola cifrata secondo il metodo detto Atbash. Questo cifrario fu usato esclusivamente per occultare la parola "Babele", ma ricopre comunque un importante ruolo storico: rappresenta il primo esempio di cifrario della storia che ci sia pervenuto. In particolare si tratta di un semplice cifrario per sostituzione monoalfabetica in cui la prima lettera dell'alfabeto ebraico (Aleph) era sostituita con l'ultima (Taw), la seconda (Beth) con la penultima (Shin) e così via. Da qui nasce il nome del cifrario: A + T + B + Sh, che con il tempo è diventato Atbash.

Un altro esempio famoso di metodo di comunicazione che può essere considerata cifrata proviene dagli spartani che, dall'inizio del V secolo a.C., impiegavano l'uso della Scitala: un bastone su cui veniva arrotolata una striscia di pelle che, a seconda del diametro bastone stesso, rendeva leggibile o meno il messaggio. Si tratta di un esempio di cifrario a trasposizione.



Figura 1 - Scitala spartana

Con l'evolvere delle civiltà si rese necessario l'utilizzo di un metodo di comunicazione sicuro da usare in ambito militare. Quello più celebre fu introdotto proprio dal popolo che con la strategia militare riuscì a conquistare l'intero Mediterraneo: i Romani. In particolare questo metodo di cifratura prende il nome da Giulio Cesare che, come scrive lo storico Svetonio in *La vita dei dodici Cesari*, fu il primo ad utilizzarlo abitualmente. Il Cifrario di Cesare si basa ancora una volta su una sostituzione monoalfabetica, ma questa volta ogni lettera viene sostituita con quella che si trova tre posizioni successive nell'alfabeto (la A diventava D, la B diventava E,...). Pur essendo una forma molto semplice, rimane uno dei primi, se non proprio il primo, esempio dell'impiego della crittografia in campo militare, quindi fu comunque di grande successo vista l'incompetenza dei

nemici a riguardo. Nonostante Cesare utilizzasse esclusivamente il cifrario in chiave tre, oggi si definisce Cifrario di Cesare qualsiasi cifrario per sostituzione monoalfabetica che si ottenga cifrando una lettera con la sua corrispondente traslata nell'alfabeto di un numero fisso di posti.

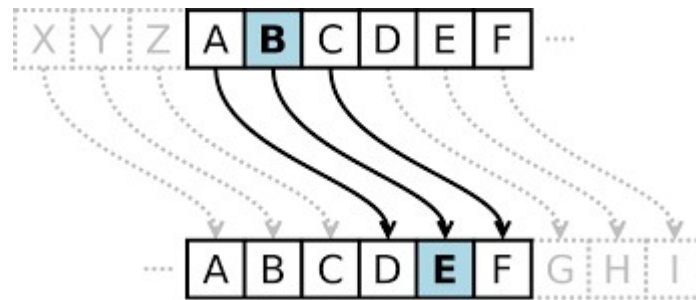


Figura 2 - Schema di cifratura con Cifrario di Cesare

Risulta anche interessante notare come già nel I secolo d.C. la crittografia avesse una sorta di rilevanza sociale, oltre a quella militare: veniva spesso usata negli scritti religiosi come forma di critica velata alle istituzioni dominanti. L'esempio forse più emblematico è l'utilizzo del numero 666, oggi ricollegato a Satana, che si pensa fosse usato per riferirsi all'imperatore Nerone, responsabile di numerose persecuzioni nei confronti dei cristiani.

La crisi

Dopo il I secolo d.C., i cifrari a sostituzione monoalfabetica, come quello di Cesare, furono quelli largamente più diffusi, nonostante la loro sostanziale semplicità. Questo sistema, però, venne messo in crisi nel IX secolo dal matematico, filosofo e musicista arabo al-Kindi.

Nel suo libro *Epistola sulla decifrazione dei messaggi crittati* introdusse un metodo di decifrazione che fece sostanzialmente crollare la sicurezza della sostituzione monoalfabetica. Questo metodo è usato ancora oggi con il nome di crittoanalisi statistica e si basa sull'analisi della frequenza di apparizione di ogni singola lettera nelle varie lingue.

Questo tipo di decifrazione, che viene spiegato approfonditamente da Edgar Allan Poe nel suo racconto *The Gold-Bug*, permette di decifrare praticamente qualsiasi tipo di cifrario a sostituzione monoalfabetica, indipendentemente da quale sia la chiave.

Nuove soluzioni

Il primo cifrario in grado di resistere alla crittoanalisi statistica apparve solamente all'inizio del Rinascimento, precisamente nel 1467, anno di pubblicazione del *De cifris* di Leon Battista Alberti. L'artista di origine fiorentina era infatti anche matematico e crittografo, nonché inventore del primo cifrario a sostituzione polialfabetica. Questo metodo si basava sull'utilizzo di un disco cifrante, ora noto come Disco di Alberti: due dischi concentrici che, ruotando, permettono di sostituire una stessa lettera del messaggio in chiaro con diverse lettere nel messaggio cifrato, poiché ad ogni parola il disco interno viene ruotato di un numero di posti dato da una chiave concordata in precedenza.

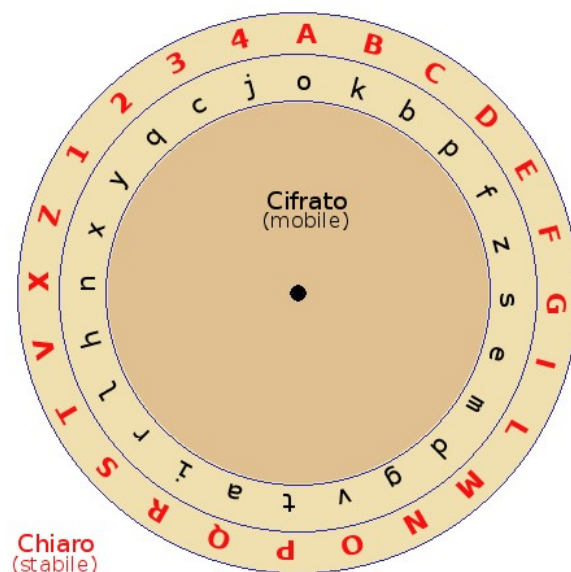


Figura 3 - Rappresentazione schematica del dico cifrante di Leon Battista Alberti

I sostanziali problemi legati al metodo di Alberti erano l'impiego di una chiave complessa, quindi difficile da trasmettere al destinatario, e l'esigenza materiale di possedere e saper utilizzare un disco cifrante uguale a quello del mittente.

Per questo motivo nel 1553 il crittografo bresciano Giovan Battista Bellaso introdusse un nuovo cifrario a sostituzione polialfabetica meno sicuro di quello di Alberti, ma molto più pratico da utilizzare in quanto la chiave era rappresentata da un versetto di origine letteraria preconcordato: le parole di questi versetti determinavano lo slittamento dei due alfabeti utilizzati per cifrare il messaggio.

Il più semplice dei cifrari a sostituzione polialfabetica fu paradossalmente introdotto per ultimo, ma fu proprio la sua semplicità a renderlo il più utilizzato. Si tratta del Cifrario di Vigenère, comparso per la prima volta nel 1586. Il funzionamento è simile a quello delle Cifre di Bellaso, ma il processo di cifratura e decifrazione risulta sostanzialmente più immediato, purtroppo anche per coloro intenzionati a intercettare il contenuto del messaggio.

Tuttavia, si dovette aspettare il 1863 per assistere al primo metodo di decifrazione del Vigenère: il metodo Kasiski, basato sull'osservazione delle sequenze di lettere ripetute nel messaggio. Oggi, con l'ausilio di un computer, la decifrazione si può svolgere in una frazione di secondo.

La crittografia si rese anche protagonista di alcune vicende socio-politiche nell'Europa del XVI e XVII secolo. In particolare in Inghilterra nel 1586 fu pianificato il complotto Babington, il cui obiettivo era l'omicidio della regina Elisabetta I con conseguente ascesa al trono della regina di Scozia Maria Stuarda. È poco noto, ma il fallimento dell'operazione e la conseguente esecuzione di Maria Stuarda furono causate da una scarsa sicurezza nei messaggi cifrati scambiati fra la regina di Scozia, allora in prigione, e gli attentatori: i messaggi vennero facilmente intercettati e decifrati dalle spie di Elisabetta che ebbero così tutte le prove per processare e condannare Maria Stuarda.

La crittografia ebbe un ruolo importante anche nel 1898 nel corso del processo a Alfred Dreyfus, capitano francese accusato di essere una spia della Germania. Per incastrare il militare francese

venne diffuso un telegramma cifrato risalente al 1894, il *Telegramma Panizzardi*, che si diceva contenesse un messaggio inviato da un militare italiano in cui veniva confermata la colpevolezza di Dreyfus. In realtà il messaggio era stato decifrato in maniera volutamente errata e in seguito ad una decifrazione corretta risultò che il messaggio aveva significato completamente opposto a quello diffuso in precedenza: testimoniava infatti l'innocenza di Dreyfus.

Una brusca accelerazione

A fare esplodere l'esigenza della crittografia fu la Prima Guerra Mondiale.

Fu il primo grosso conflitto che si svolse dopo le invenzioni nel campo delle telecomunicazioni di inizio secolo. I militari approfittarono subito delle nuove tecnologie, infinitamente più veloci dei corrieri o dei piccioni viaggiatori, ma c'era un problema: mentre prima il nemico doveva avere la fortuna di intercettare il messo o abbattere il piccione, adesso è sufficiente mettersi in ascolto con un ricevitore e le nostre comunicazioni sue sue.

Il messaggio non poteva quindi essere spedito in chiaro, ma occorreva crittografarlo: solo alcuni paesi europei entrarono in guerra con l'adeguata preparazione.

I francesi furono i primi a rendersi conto dell'importanza di avere un ufficio cifra e grazie a questo furono in grado di decifrare numerosi messaggi tedeschi. In particolare sul fronte francese si distinse un professore di paleontologia, Georges Painvin, che fu in grado di rompere la cifra ADFGVX, un sistema crittografico tedesco a trasposizione, decrittando il famoso *Radiogramma della vittoria* che aiutò i Francesi nel 1918 a respingere la *Offensiva di Primavera* del generale Erich Ludendorff e iniziare l'avanzata che li avrebbe portati alla vittoria.

Anche gli inglesi non furono da meno in questo campo con l'istituzione della Room 40, l'ufficio cifra della marina britannica, dove si intercettavano e decifravano centinaia di comunicazioni tedesche. Una delle più significative fu il *Telegramma Zimmermann* con cui i tedeschi chiedevano un'alleanza ai messicani in funzione anti-USA: questo telegramma, poi trasmesso al Congresso statunitense, fu uno dei fattori che spinsero gli USA ad entrare in guerra nel 1917.

Il terzo membro della Triplice Intesa, la Russia, contrariamente ai due paesi alleati, entrò in guerra completamente impreparata. Addirittura inizialmente non si preoccupava neanche di cifrare i messaggi che diventavano quindi facile preda di tedeschi e austriaci: il caso più eclatante fu la rovinosa sconfitta russa nella battaglia di Tannenberg dove i tedeschi conoscevano in anticipo il piano russo.

Gli imperi centrali pagarono il fatto che le loro conoscenze in campo crittografico, seppur di buon livello, erano comunque inferiori a quelle anglo-francesi. Sia gli austriaci, guidati dal capitano Pokorny, sia i tedeschi, guidati dal professor Deubner, sovrastarono facilmente i Russi in campo di comunicazioni, ma dovettero sottostare agli altri due membri dell'Intesa.

L'Italia, nonostante precedenti storici eccellenti (Alberti, Bellaso,...) a inizio 1900 si ritrovava in una situazione critica in campo crittografico. Il 24 maggio 1915 l'Italia, nonostante riuscisse ad intercettare i messaggi austriaci, non disponeva di un ufficio cifra. Il capitano Luigi Sacco si recò quindi a Chantilly per cercare una collaborazione con l'avanzato ufficio cifra francese. L'Italia cominciò così ad inviare in Francia i messaggi intercettati affinché venissero decifrati, ma

l'operazione si rivelò lenta e insoddisfacente. Così Sacco, istituito un ufficio radiotelegrafico a Codroipo, cominciò ad occuparsi autonomamente sia di radio-intercettazione, sia di decifrazione. Solo nell'ottobre del 1916 lo Stato Maggiore dell'Esercito italiano istituì un ufficio cifra a Roma: l'esercito italiano cominciò ad ottenere i primi successi e a competere in campo crittografico con le altre potenze europee. Paradossalmente, però, si dovette aspettare il novembre 1917 con la Battaglia di Caporetto affinché lo SME decidesse di utilizzare cifre più sicure, prima considerate troppo complicate, per le proprie comunicazioni militari. La decifrazione di diversi messaggi austriaci si rivelò fondamentale per il successo italiano nella seconda Battaglia del Piave.

Durante la guerra, nel 1917, l'ingegnere statunitense Gilbert Vernam teorizzò e due anni dopo realizzò un nuovo cifrario: il cifrario di Vernam. Quest'ultimo consiste in un cifrario di Vigenère con una chiave casuale, lunga quanto il testo in chiaro e non riutilizzabile, in modo da rendere completamente inefficaci i metodi usati fino ad allora. Nel 1949 il matematico Claude Shannon dimostrò nel suo lavoro *Communication Theory of Secrecy Systems* che questo cifrario è l'unico teoricamente sicuro e inattaccabile. L'unico problema di questo sistema è ovviamente, la trasmissione della chiave lungo un canale sicuro. La soluzione migliore fu quella di passare tramite due corrispondenti una chiave abbastanza lunga da servire per numerosi messaggi, ma il sistema mancava comunque di praticità.

Ormai indispensabile

Ormai nota a tutti l'importanza fondamentale del possesso di un ufficio cifra, con lo scoppio della Seconda Guerra Mondiale i vari paesi concentrarono numerose energie per ideare metodi che permettessero sia di rendere sicure le proprie comunicazioni, sia di carpire quelle nemiche.

Il caso sicuramente più celebre è quello della macchina tedesca *Enigma* (di cui parleremo nel prossimo paragrafo). La decifrazione di questa macchina da parte degli Alleati avrebbe fornito informazioni fondamentali, influenzando fortemente l'esito di alcune battaglie. Una di esse fu, ad esempio, la battaglia di capo Matapan, in cui fu intercettato un messaggio tedesco che forniva l'esatta posizione della flotta italiana che venne poi nettamente sconfitta.

Altro esempio molto conosciuto è quello dello Sbarco in Normandia, in cui gli Inglesi, dopo aver diffuso la falsa notizia di uno sbarco nei pressi di Calais, decifrarono messaggi tedeschi che testimoniavano massicci spostamenti di truppe verso la città francese. Erano quindi certi che avrebbero incontrato ben poca resistenza sulle spiagge della Normandia e decisero di sbarcare in quel punto.

Anche sul fronte del Pacifico la crittografia si rivelò fondamentale. L'alto comando giapponese utilizzava una macchina, conosciuta con il nome di *Purple*, per cifrare i messaggi. La macchina, ritenuta inattaccabile, venne presto decifrata dallo Special Intelligence Service, una frazione dell'FBI, capeggiata dal crittografo William Friedman che ideò la macchina *Magic* appositamente per decifrare il codice nipponico. La superiorità crittografica statunitense risultò fatale per i Giapponesi in diverse occasioni.

La battaglia delle Midway, punto di svolta per la guerra sul fronte pacifico, venne vinta dagli USA anche grazie ad ingente apporto crittografico: gli americani avevano intercettato i messaggi giapponesi che descrivevano nel dettaglio il loro piano di battaglia. L'ammiraglio americano Nimitz

poté quindi preparare la sua strategia conoscendo già perfettamente quella nemica. Vennero inoltre diffusi falsi piani americani, cifrati con un codice che si sapeva essere noto ai giapponesi, in modo da facilitare ulteriormente la vittoria.

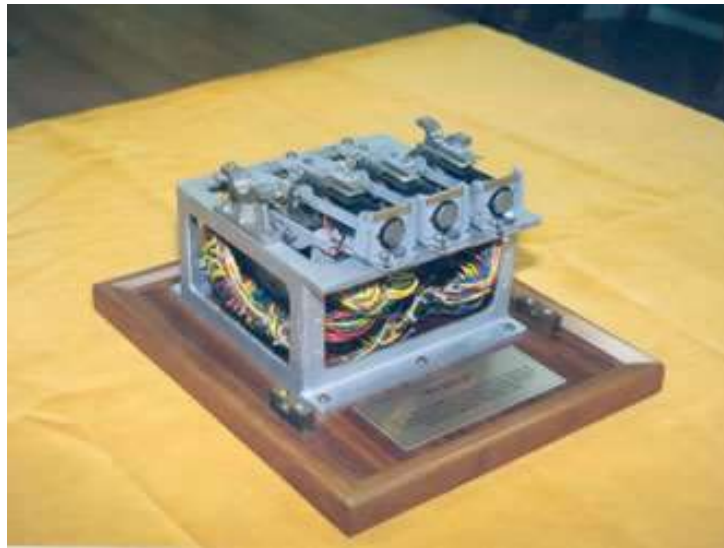


Figura 4 - Macchina cifrante giapponese detta Purple

Un altro episodio chiave dello scontro fra giapponesi e statunitensi fu la morte dell'ammiraglio giapponese Isoroku Yamamoto, ideatore e comandante dell'attacco a Pearl Harbor. Gli americani decifrarono un messaggio che rivelava il giorno e l'ora esatta in cui Yamamoto sarebbe passato per un determinato tratto di mare: il 14 aprile 1943 il suo aereo fu intercettato e abbattuto dall'aviazione americana. Questo fatto venne tenuto segreto per diversi anni, in quanto la morte fu attribuita ad un semplice incidente aereo.

Vi è anche una teoria riguardante l'attacco al porto di Pearl Harbor che coinvolge l'impiego di crittografia. Secondo alcuni storici, grazie a *Magic* gli statunitensi erano a conoscenza dell'imminente attacco, ma decisero di non impedirlo: avevano bisogno di un casus belli per convincere l'opinione pubblica e il parlamento della necessità dell'entrata in guerra al fianco degli Alleati. A sostegno di questa tesi vi è il fatto che le portaerei americane, considerate le navi più importanti di stanza alla base hawaiana, vennero allontanate dal porto nei giorni precedenti l'attacco. Questo potrebbe essere un caso, come succederà anche in Europa con i codici tedeschi, in cui fu necessario sacrificare molte vite umane (ci furono ca. 3.000 vittime), pur di non rivelare al nemico i propri successi in campo crittoanalitico.

In generale, la superiorità crittografica degli Alleati, come nel caso della Prima Guerra Mondiale, si rivelò molto importante per l'esito del conflitto e per la sconfitta della Germania e dei suoi alleati.

L'uomo non basta più

Al termine della Prima Guerra Mondiale, ormai nota l'importanza della crittografia in campo militare, l'ingegnere tedesco Arthur Scherbius aveva iniziato a sviluppare una macchina elettromeccanica per cifrare e decifrare messaggi sulla base del disco di Alberti: *Enigma*. Questa macchina, che nella sua versione definitiva poteva generare un numero di chiavi dell'ordine di 10^{16} (10 milioni di miliardi), fu di largo impiego sul fronte tedesco nel corso della Seconda Guerra

Mondiale. Fu proprio l'immenso numero di combinazioni possibili, unito al fatto che la chiave cambiava ogni 24 ore, a far credere, erroneamente, che la macchina fosse indecifrabile.

Il primo prototipo venne brevettato 1918, per poi essere continuamente migliorato e potenziato negli anni successivi: l'esercito tedesco decise di cominciare ad utilizzare la macchina per le proprie comunicazioni solo nel 1929.

Nel 1931 Hans-Thilo Schmidt, un impiegato tedesco che poteva accedere alla macchina, fornì ai francesi due documenti che permettevano di ricostruire il funzionamento di *Enigma*. Tuttavia questi ritennero la macchina troppo complessa e non prestarono ad essa particolare attenzione. Al contrario, i polacchi, sapendo a ragione che in caso di guerra sarebbero stati la prima preda della Germania, si concentrarono sulla decifrazione della macchina dopo aver chiesto ai francesi le informazioni in loro possesso. Nel 1932 l'intelligence polacca, guidata dal matematico Marian Rejewski, riuscì a decifrare *Enigma*, progettando una macchina apposita chiamata *Bomba* che simulava il funzionamento di *Enigma* e permetteva di trovare la chiave del giorno.



Figura 5 – Una delle versioni di Enigma

Enigma assomiglia ad una macchina da scrivere: c'è una tastiera sulla quale si batte il messaggio; ad ogni pressione di tasto si accende una lettera che va a comporre il messaggio cifrato. Il legame tra la lettera battuta e quella che si accende è creato tramite alcuni dischi meccanici e collegamenti elettrici che 'mescolano' le lettere e cambiano il modo di mescolarle ad ogni lettera (altrimenti diventerebbe un cifrario di Cesare monoalfabetico...). La chiave è costituita dall'ordine dei rotori, dallo schema dei collegamenti e dalla posizione iniziale. La chiave viene cambiata ogni 24 ore in base ad una tabella che viene inviata ogni mese ai reparti.

I tedeschi si resero comunque conto che il loro sistema era stato violato e decisero quindi migliorare la macchina moltiplicando per 60 le possibili combinazioni, rendendo così *Bomba* insufficiente. Nel 1939, alla vigilia dell'invasione della Polonia, Rejewski passò agli inglesi tutti gli studi fatti in

Polonia nella speranza che essi potessero forzare la versione più sofisticata di *Enigma*. I britannici istituirono quindi a Bletchley Park la sede del loro ufficio cifra, guidato da diversi matematici e ingegneri, tra cui il campione di scacchi Hugh Alexander e il ben più noto matematico Alan Turing. Cominciò così il progetto Ultra. Un punto di svolta avvenne nel 1941, con l'operazione *Primrose*: la marina inglese, catturando un sommergibile tedesco, riuscì ad impossessarsi di un modello di *Enigma*. Non restava che trovare un modo per individuare sistematicamente la chiave del giorno. Fu proprio Turing a ideare una macchina, prendendo come modello la *Bomba* polacca, in grado di svolgere questa operazione.

Nel 1942 la marina inglese era in grado di decifrare più di 80.000 messaggi tedeschi al mese. Ormai però si presentava anche un problema etico riguardo al modo in cui utilizzare le informazioni ottenute: se si fosse intervenuti in situazioni particolarmente sospette, i tedeschi avrebbero capito che la macchina era stata decrittata e avrebbero cambiato nuovamente il suo funzionamento, rendendo tutto il lavoro inutile. Tuttavia, non intervenire quando si era in possesso di informazioni significava in genere lasciare che i soldati e i civili coinvolti perdessero la vita. Alla fine fu adottata una procedura che permettesse di utilizzare le informazioni ottenute senza far insospettare i tedeschi e, si spera, cercando di minimizzare il numero di "sacrificati". Alcuni storici stimano che il successo dell'operazione Ultra abbia accorciato la guerra di quasi due anni, salvando circa 14 milioni di vite umane. Tuttavia l'operazione venne tenuta top secret fino agli anni '70.

Meno nota di *Enigma* ma altrettanto importante fu un'altra macchina usata dai tedeschi: la macchina *Lorenz*. Questo dispositivo, usato prevalentemente per le comunicazioni fra gli alti gerarchi nazisti, era basato sul cifrario di Vernam, considerato inattaccabile, e quindi paradossalmente molto più sicuro di *Enigma*.

Questa macchina venne prodotta nel 1941 dalla ditta tedesca Standard Elektrik Lorenz AG, su ordine del Terzo Reich, sulla base di *Enigma*. Essendo la macchina basata sul cifrario di Vernam, il suo punto debole era ovviamente la trasmissione della chiave. Per ovviare a ciò, i progettisti del dispositivo pensarono di sostituire la chiave casuale con una chiave pseudo-casuale generata da un dispositivo meccanico secondo una procedura ovviamente segreta. Ma a questo punto la chiave diventò la procedura stessa.

Fu proprio grazie a questa debolezza di sistema, e all'ingenuità di un cifratore tedesco, che gli inglesi di Bletchley Park, in particolare John Tiltman, riuscirono a decifrare un messaggio per poi risalire alla struttura interna della macchina. Tuttavia a questo punto la decifrazione manuale dei messaggi richiedeva ben quattro giorni, lasso di tempo in cui le informazioni contenute diventavano obsolete: per questo motivo nacque la necessità di sviluppare un sistema automatico di decifrazione.

Questo in pratica spinse il gruppo di lavoro al superamento dell'approccio elettromeccanico nell'opera di decifrazione e alla scelta di una trattazione puramente elettrica del problema, dove la parte meccanica veniva simulata da opportuni collegamenti. Ciò portò alla nascita del primo (o secondo per alcuni) computer programmabile della storia.

Nel 1944 il matematico Max Newman progettò *Colossus*, una macchina automatica realizzata sulla base di *Bomba* e della macchina di Turing. Finita la guerra, lo stesso Alan Turing progettò uno dei primi elaboratori elettronici programmabili nel Laboratorio Nazionale di Fisica del Regno Unito. Era nata l'informatica ovvero la trattazione automatica dell'informazione.

EDGAR ALLAN POE

A passion for cryptography

It might sound strange to find Edgar Allan Poe in this work on cryptography, as everybody associates his name to well-known Gothic stories. However not many people know that this famous American writer of the 19th century had also a keen interest in cryptography.

In 1840 he started publishing some articles in the *Alexander's Weekly (Express) Messenger*, a newspaper from Philadelphia, in which he boasted about his ability in deciphering and asked the readers to challenge him by sending him some coded messages.

In July 1841, Poe published an essay called “A few words on secret writing” in *Graham Magazine*. In this essay Poe proved to be extremely informed about cryptography: he started the essay talking about the scytala, at the time considered the first form of cypher, but stating that maybe there were some older ones he still didn't know (and he was right!). He then showed some deciphering methods, but only regarding monoalphabetic substitution cyphers. This essay was a starting point for the creation of the Room 40, the decoding office of the British Army during WWI.

As the public was becoming interested in and amused by this new form of “art” (as Poe defines it), the writer decided to publish a short story called *The Gold-Bug* based on the decryption of a specific cypher. The cypher, as we will see, is fairly simple: the success of this story is not particularly due to Poe's knowledge of cryptography, but to the clever way in which he explains to the reader the method used to decipher the message.

The sensation that Poe created with his cryptography stunts played a major role in popularizing cryptograms in newspapers and magazines.

William Friedman, probably the greatest cryptologist of the USA, said that his interest in cryptology started when as a child he read *The Gold-Bug*. Maybe, if it wasn't for Poe, Friedman would have never deciphered Japan's PURPLE code during World War II, significantly changing the outcome of the war.

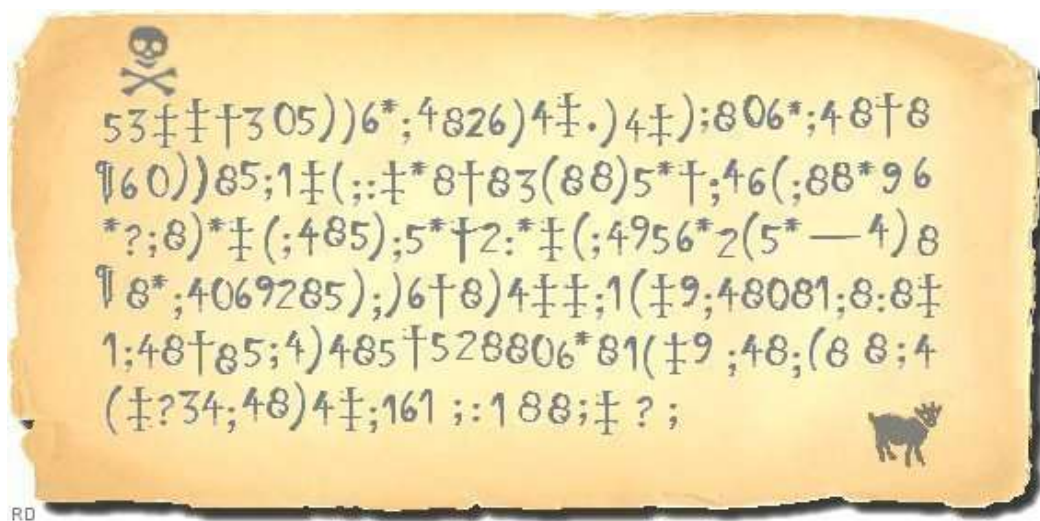
The Gold-Bug

This mystery story follows the adventure of William Legrand, the poor descendant of a once-wealthy family, as he goes treasure hunting on a remote island in South Carolina. Legrand, who lives in a hut with his black servant Jupiter, is visited by the nameless narrator of the story. The protagonist tells the narrator-friend that he has found a wonderful golden bug, but he has lent it to a soldier, so he draws it on a piece of parchment to show it to his friend who, however, only sees a skull.

From that moment Legrand starts behaving strangely and, a month later, asks the narrator to come back to his hut. The two men with the servant then leave on a journey on the island, as if they were following precise instructions. They find a tree and Legrand asks Jupiter to climb the tree and drop the golden bug from the eye of a skull stuck on the branches of the tree. Legrand then walks 50 feet from the spot where the bug was dropped and starts digging. After the first attempt turns out to be a

failure, they try again with the other eye of the skull. This time, by digging in the ground, they find a chest full of gold and jewels of the value of about 1.5 million dollars. After taking the chest back to the hut, Legrand starts explaining the confused narrator how he has managed to find the treasure.

When Legrand had found the bug, he had also picked up a peace of parchment sticking up from the sand and wrapped the dead bug in it. This was the same parchment on which the protagonist drew the bug to show his friend, who however only saw a skull. Legrand then understood that, with the heat of the fireplace, a message appeared on the parchment that looked white before. Legrand then heated the parchment to reveal the full message:



Here Poe starts describing the deciphering process used by Legrand.

First Legrand tried to understand the symbols at the corners of the parchment: having found the message near a shipwreck he interpreted the skull as a pirate symbol. For what concerns the animal on the bottom corner, it looks like a little goat, but it actually is a kid: the protagonist explains “You may have heard of one Captain Kidd. I at once looked on the figure of the animal as a kind of punning or hieroglyphical signature”². Therefore the little animal represents the enigmatic signature of the terrible Captain Kid, famous for having left a great treasure that was never found.

Having understood the author of the message, Legrand then started focusing on understanding its strange form:

"And yet, the solution is by no means so difficult as you might be led to imagine from the first hasty inspection of the characters. These characters, as any one might readily guess, form a cipher - that is to say, they convey a meaning; but then, from what is known of Kidd, I could not suppose him capable of constructing any of the more abstruse cryptographs. I made up my mind, at once, that this was of a simple species - such, however, as would appear, to the crude intellect of the sailor, absolutely insoluble without the key."³

² Edgar Allan Poe, *The Gold-Bug*, CreateSpace Independent Publishing Platform, Columbia, 2017, p. 12

³ Edgar Allan Poe, *The Gold-Bug*, CreateSpace Independent Publishing Platform, Columbia, 2017, p. 13

Legrand has understood that this can only be a simple monoalphabetic substitution cypher and, as we know, the best way to decipher it is statistical cryptanalysis, based on the study of the frequency of the letters in each language.

Poe explains each and every passage of the process:

- We need to know the language to use: “The pun on the word 'Kidd' is appreciable in no other language than the English”⁴ says Legrand
- We now have to start by counting the symbols in the cyphered text and determine which of them are the most common. In our message the most frequent character is the 8 that appears 33 times.
- We combine the information acquired with the frequency of the letters in the language you need. In this case we know that in the English language the order of appearance of the different letters is e a o i d h n r s t u y c f g l m w b k p q x z
- We then start by assuming that the character 8 represents the letter e
- We consider the most frequent word in the English language: the. We now look for a sequence of three symbols ending with 8 that appears several times in the message: there are seven ;48.
- We can now assume that ; represents the letter t and 4 represents the letter h
- We now consider the sequence ;48;(88;4 and we rewrite it as the t(eeth. We understand that there isn't a word ending with -eeth, so we must assume that the word t(ee is alone and the best guess is the word tree
- We can now assume that (represents the letter r
- Keeping on with the sequence we can write: the tree thr‡?3h the. In this case the most evident word is through
- We can now assume that ‡ represents o, ? represents u and 3 represents g
- The more letters we understand, the easier it is understanding the others
- Using this method we can understand the full text of the message, which is: “A good glass in the bishop's hostel in the devil's - twenty-one degrees and thirteen minutes - northeast and by north - main branch seventh limb east side - shoot from the left eye of the death's-head - a bee-line from the tree through the shot fifty feet out”⁵

Legrand then explains to his friend how, by interpreting this message, he managed to find out the place where the treasure was buried and the instructions on where to dig.

What about the bug? Why drop the bug instead of anything else? Legrand answered “Why, to be frank, I felt somewhat annoyed by your evident suspicions touching my sanity, and so resolved to punish you quietly, in my own way, by a little bit of sober mystification”⁶. A little joke from Poe to end his story.

⁴ Edgar Allan Poe, *The Gold-Bug*, CreateSpace Independent Publishing Platform, Columbia, 2017, p. 14

⁵ Edgar Allan Poe, *The Gold-Bug*, CreateSpace Independent Publishing Platform, Columbia, 2017, p. 16

⁶ Edgar Allan Poe, *The Gold-Bug*, CreateSpace Independent Publishing Platform, Columbia, 2017, p. 19

CRITTOGRAFIA MODERNA

I metodi di crittografia a chiave simmetrica si sono evoluti per secoli fino a giungere a risultati eccellenti: un documento cifrato con uno dei moderni algoritmi è praticamente inespugnabile. Resta però un grande limite: la chiave è unica e quindi occorre che entrambi i protagonisti dello scambio di informazioni siano in possesso della stessa. I due devono scambiarsela, dunque occorre incontrarsi di persona o usare un canale sicuro, ma se avessimo sempre disponibile un canale sicuro non avremmo tanto bisogno di crittografare i messaggi. Inoltre occorre avere pianificato in anticipo la possibilità di scambiare messaggi proprio con un preciso interlocutore.

Crittografia a chiave pubblica

Il problema che la crittografia a chiave pubblica vuole risolvere si può sintetizzare in questo modo: Alice deve poter comunicare con Bruno in modo sicuro, anche senza conoscerlo utilizzando unicamente un canale pubblico cioè, per definizione, non sicuro.

A partire dagli anni '70 un gran numero di novità tecnologiche (nuove tecniche, firma digitale, scambio di chiavi e altre) furono sviluppate nel campo della crittografia asimmetrica. Alcuni erano metodi ideali e praticamente irrealizzabili come l'algoritmo del puzzle di Merkle che però influenzò Whitfield Diffie e Martin Hellman per la realizzazione del sistema di scambio chiavi che porta il loro nome. Il sistema di crittografia ElGamal, inventato da Taher ElGamal si basa sull'alto livello di difficoltà del problema logaritmo discreto, così come lo strettamente correlato DSA, che è stato sviluppato presso l'US National Security Agency (NSA).

Lo sviluppo della crittografia asimmetrica ebbe una partenza lenta perché richiede grande potenza di calcolo che nei primi anni non era disponibile relegando i concetti ad argomento di studio accademico o militare.

Più avanti approfondiremo l'algoritmo RSA in quanto ad oggi è probabilmente il più utilizzato al mondo.

Troppo presto e nel posto sbagliato

Nel 1970, James H. Ellis immaginò la possibilità di una "crittografia non segreta", (adesso chiamata crittografia a chiave pubblica), ma non riusciva a vedere alcun modo di implementarla.

Nel 1973, il suo collega Clifford Cocks realizzò quello che è diventato poi noto come algoritmo di crittografia RSA, dando un metodo pratico di "cifatura non segreta".

Nel 1974 Malcolm J. Williamson sviluppò quello che oggi è noto come 'scambio chiavi di Diffie-Hellman'.

Il progetto fu passato anche alla National Security Agency (NSA) americana, ma in un'ottica militare e con bassa potenza di calcolo disponibile, le potenzialità della crittografia a chiave pubblica non furono comprese a pieno: i vecchi e collaudati sistemi erano ancora sufficienti dato che le strutture militari o diplomatiche erano ancora in grado di scambiarsi le chiavi in sicurezza.

Ma perché questi scienziati hanno fatto scoperte che oggi sono note con i nomi di altre persone? Perché tutti lavoravano al Government Communications Headquarters (GCHQ) britannico e le loro scoperte rimasero quindi segrete e furono rese di dominio pubblico solo nel 1997 quando le ricerche furono declassificate dal governo.

Asimmetria per tutti

Nel 1977, la generalizzazione del sistema di Cocks è stata indipendentemente inventata da Ron Rivest, Adi Shamir e Leonard Adleman all'epoca al MIT. Questi ultimi hanno pubblicato il loro lavoro nel 1978 e l'algoritmo è da allora conosciuto con il nome RSA, dalle loro iniziali. RSA utilizza l'elevamento a potenza in modulo di due numeri primi molto grandi moltiplicati tra loro, per la cifratura e decifratura, eseguendo sia la crittografia a chiave pubblica sia la firma digitale a chiave pubblica. La sua sicurezza è collegata alla estrema difficoltà di fattorizzare, cioè scomporre in fattori primi, grandi numeri, un problema per cui non è nota una tecnica generale efficiente.

Occorrerà però ancora del tempo perché la crittografia asimmetrica esca dai laboratori e dalle aule ed entri nelle case. Teniamo anche presente che la crittografia 'forte' come si presenta la crittografia in chiave pubblica era vietata in molti paesi a partire dagli Stati Uniti.

All'inizio degli anni '90 fece rumore la vicenda di PGP (Pretty Good Privacy), la prima famiglia di software di crittografia per autenticazione e privacy che venne resa disponibile al grande pubblico.

L'americano Phil Zimmermann produsse la prima versione del PGP nel 1991. Era stato per molto tempo un attivista anti-nucleare e creò il PGP in modo che i suoi compagni potessero usare sistemi BBS (Bulletin Board System una sorta di bacheche elettroniche raggiungibili da casa via modem) e memorizzare messaggi e file in tutta sicurezza. Non era richiesta licenza se l'uso non era commerciale, non c'era spesa neanche simbolica e veniva fornito il codice sorgente. PGP si diffuse su Usenet (una rete di computer antenata di Internet) e di qui poi su Internet che si stava diffondendo.

In breve tempo il PGP iniziò a diffondersi al di fuori dei confini degli USA e nel febbraio 1993 Zimmermann fu incriminato dal governo degli Stati Uniti con l'accusa di "esportazione di armi senza apposita licenza" (un sistema di crittografia con chiave maggiore di 40 bit era considerato come munizionamento da guerra, PGP aveva sempre avuto chiavi di almeno 128 bit). PGP ebbe anche una lunga e travagliata storia di cause ed accuse per violazione di brevetti.

Ma la strada era ormai aperta...

Algoritmi a chiave pubblica

Abbandonando la storia, vediamo più da vicino i concetti base di questo tipo di cifrario facendo una premessa importante: quando parliamo di chiavi o di lucchetti, stiamo parlando di strumenti matematici gestiti da un computer.

Come dice il nome, nella cifratura a chiave pubblica, c'è una chiave che è nota a tutti, ma questa non è l'unica chiave. Le chiavi infatti sono due e vengono create nello stesso momento perché sono legate tra loro: una qualsiasi delle due (poi detta pubblica) viene distribuita, ad esempio

memorizzandola presso uno dei “depositi” a ciò dedicati, mentre l’altra viene tenuta segreta (e viene detta privata). Le due chiavi devono ovviamente essere fatte in modo che da una non si possa risalire all’altra in un tempo ragionevole: diciamo che nella migliore delle ipotesi occorrerebbero anni.



Essenziale è che la chiave privata rimanga segreta e che quella pubblica sia nota; in seguito, una chiave servirà per codificare il messaggio e l’altra per decodificarlo.



Chiavi e lucchetti

Una metafora classica usata per spiegare il meccanismo della crittografia a chiave pubblica utilizza chiavi fisiche e lucchetti a doppia chiave: con una chiave della coppia si chiude e con l’altra si apre.




Si noti che, come accennato, le due chiavi (pubblica e privata) sono strettamente legate e sono necessarie entrambe: se chiudo il lucchetto (codifico un messaggio) con una, solo l’altra potrà aprirlo (decodificare il messaggio); neppure la chiave che lo ha chiuso può riaprirlo.

Si considera che lucchetti e chiavi pubbliche siano sempre a disposizione di tutti e ovviamente che ognuno possieda l’unica copia della propria chiave privata.

	chiave privata di Alice
	chiave pubblica di Alice

	chiave privata di Bruno
	chiave pubblica di Bruno

Per capire un po’ come può funzionare una crittografia a chiave pubblica prendiamo quindi due persone, Alice e Bruno, che si vogliono scambiare messaggi riservati e dotiamoli di questi strumenti ideali:

ALICE possiede	
	tanti lucchetti
	propria chiave privata
	chiave pubblica di Bruno

BRUNO possiede	
	tanti lucchetti
	propria chiave privata
	chiave pubblica di Alice

Scambiare un messaggio

Se Alice deve spedire un messaggio a Bruno e vuole essere sicura che venga letto solo da lui, blocca il messaggio con un lucchetto, che chiude con la chiave pubblica di Bruno, e glielo spedisce anche usando un canale non sicuro.

Il lucchetto che blocca il messaggio di Alice, chiuso con chiave pubblica di Bruno, potrà essere aperto solo dalla chiave privata di Bruno che solo lui possiede: Alice è sicura che il messaggio in chiaro non verrà letto da altri.

Notare che, in questo caso, Alice non ha utilizzato la propria chiave privata.


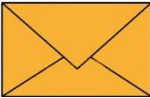


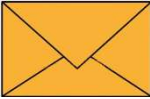


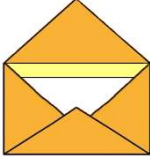

			Alice scrive il messaggio
			Alice chiude con la chiave pubblica di Bruno
SPEDIZIONE SU CANALE NON SICURO			
			Bruno apre con la propria chiave privata
			Solo Bruno può leggere il messaggio

Tabella 1 – Cifratura semplice a chiave pubblica

Scambiare un messaggio identificando il mittente

Continuiamo a giocare con i nostri lucchetti e le nostre chiavi e complichiamo un po' il problema dopo avere fatto una considerazione: Bruno ha ricevuto un messaggio, ma il lucchetto con cui era bloccato è stato chiuso con la sua chiave pubblica che è a disposizione di tutti e quindi chiunque può avergli mandato quel messaggio. Se Bruno volesse essere sicuro che a mandare il messaggio è stata Alice, come si dovrebbero comportare?

In questo caso, dopo avere scritto il messaggio, Alice usa un primo lucchetto che chiude con la propria chiave privata e un secondo che chiude con la chiave pubblica di Bruno poi lo spedisce a Bruno sempre sul canale non sicuro.

Ricevuto il messaggio, Bruno apre il secondo lucchetto con la propria chiave privata, cosa che solo lui può fare, e apre il primo con la chiave pubblica di Alice: a questo punto Bruno è certo che il messaggio lo ha scritto Alice.





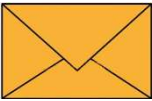



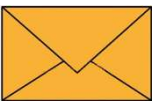







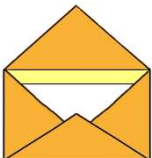


				Alice scrive il messaggio
				Alice chiude con la propria chiave privata
				Alice chiude con la chiave pubblica di Bruno
SPEDIZIONE SU CANALE NON SICURO				
				Bruno apre con la propria chiave privata
				Bruno apre con la chiave pubblica di Alice
				Solo Bruno può leggere il messaggio ed è certo che l'ha inviato Alice

Tabella 2 – Doppia cifratura a chiave pubblica

Osserviamo ancora due cose:

la prima è che la sequenza con cui Alice chiude la busta è ininfluente: può usare prima la propria chiave e poi quella di Bruno o viceversa, Bruno potrà sempre aprirla usando le due chiavi in suo possesso in un ordine o nell'altro.

La seconda è che Alice non può sostenere di non avere scritto il messaggio dato che è stato chiuso con la chiave che solo lei possiede (chiave privata) e vedremo che questa è una caratteristica importante.

Tutto ciò ci riguarda?

Più avanti vedremo uno dei vari modi utilizzati per costruire queste chiavi e questi lucchetti (sono oggetti matematici), ma adesso ci possiamo chiedere se quanto illustrato ora è solo un buffo gioco ideale o un passatempo da enigmisti.

Lo schema che prevede lo scambio di messaggi con l'identificazione certa dei partecipanti è alla base di praticamente tutti i più recenti protocolli di comunicazione cioè l'insieme delle regole formalmente descritte che definiscono le modalità di scambio di informazioni tra due o più entità, su Internet o meno.

HTTPS e Home Banking

Il protocollo **HTTPS** (HyperText Transfer Protocol over Secure Socket Layer) è utilizzato in Internet per i collegamenti sicuri ad un server. Un server Web (un computer che fornisce "pagine" a cui si accede per mezzo di un browser) che usa HTTPS è in possesso di una chiave pubblica (certificata da un apposito Ente) che identifica il sito e permette di codificare la trasmissione. L'**home banking** che ormai tutti usiamo è un esempio di servizio che si serve di questo protocollo che garantisce:

1. un'autenticazione del sito web visitato (certificazione)
2. protezione della privacy (codifica della trasmissione)
3. integrità dei dati scambiati tra le parti comunicanti (codifica della trasmissione)



Figura 6 – Protocollo HTTPS - Home page di una banca

I browser generalmente indicano i siti che usano HTTPS visualizzando un lucchetto chiuso a significare che la comunicazione è sicura, in caso contrario, il lucchetto è aperto. A partire dal mese di Luglio 2018, il browser Chrome, non apporrà più l'etichetta 'Sicuro' ad un sito che usa HTTPS

come nella figura sotto, ma mostrerà “Non sicuro” per tutti siti che non lo usano. Un sito web che non usa HTTPS usa HTTP: già dal nome gli manca Secure.

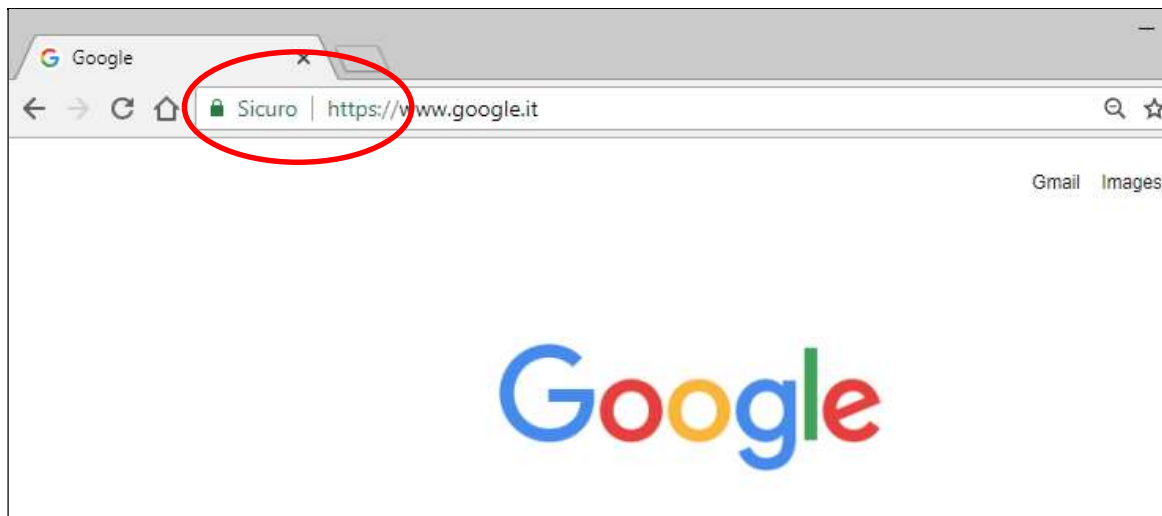


Figura 7 – Protocollo HTTPS - Home page di Google Italia

Posta elettronica certificata e smart card

Anche la posta elettronica certificata pretende di conoscere con certezza mittente e destinatario dei messaggi. I protocolli di posta certificata permettono poi di garantire che il contenuto del messaggio non sia stato alterato facendo uso di speciali funzioni dette di hashing il cui risultato viene criptato e, infine, come accennato, garantiscono la non ripudiabilità del messaggio stesso: chi lo ha scritto non lo può negare.

Uno dei metodi più diffusi per utilizzare la firma digitale prevede l'uso di una smart card che contiene la chiave privata e il deposito della chiave pubblica presso l'ente che gestisce il servizio.

La Carta Nazionale dei Servizi è una di queste smart card. E' possibile averla o rinnovarla on-line seguendo una semplice procedura. Sul sito dell'ente gestore, prima della conferma finale dell'operazione, viene mostrata la videata qui sotto; si noti cosa c'è scritto nel testo evidenziato.

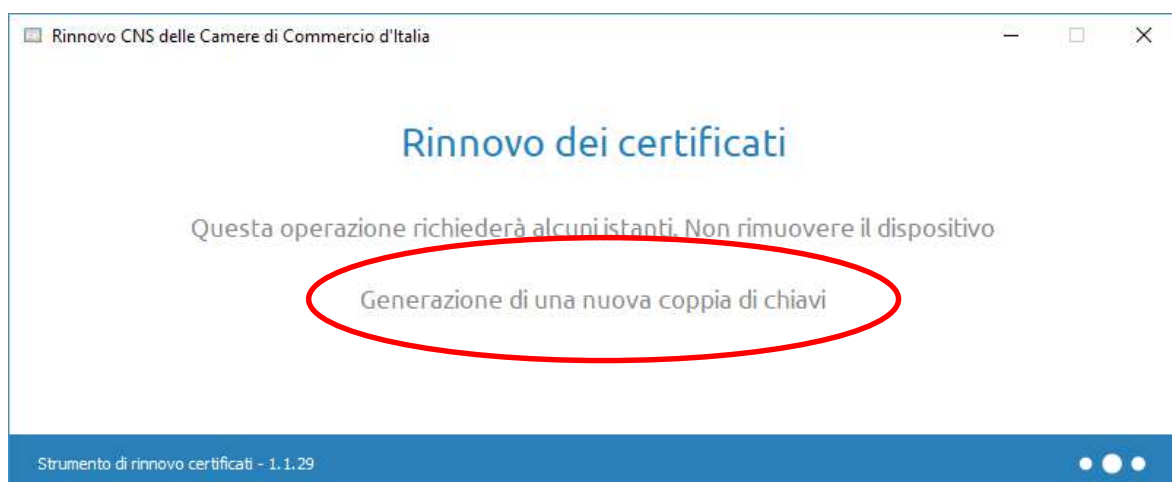


Figura 8 - Generazione di nuove chiavi per una smart card

Messaggistica istantanea, WhatsApp & C.

I programmi di messaggistica istantanea ormai di uso comune come **WhatsApp** o **Telegram** usano la crittografia ‘end to end’ basata su metodi a chiave pubblica. Nella codifica ‘end to end’ i messaggi vengono codificati e decodificati direttamente dal dispositivo dell’utente e neppure il provider Internet o il gestore dell’App li vedono mai in chiaro.

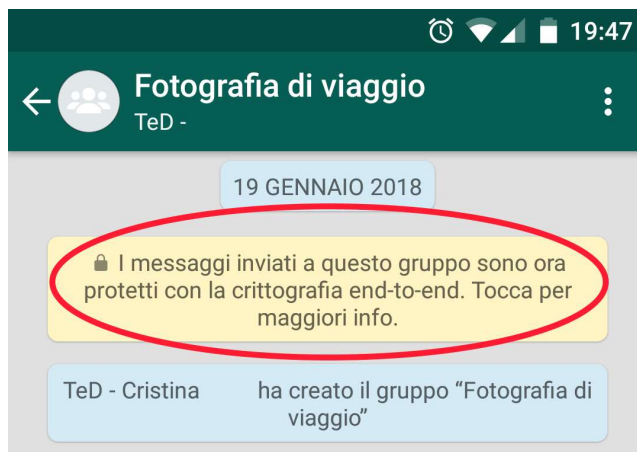


Figura 9 - Schermata alla creazione di un nuovo gruppo WhatsApp

Criptomonete, Bitcoin & C.

Anche la Blockchain (tipo di database crittografato, distribuito e replicato su migliaia di computer) su cui si appoggiano tutte le nuove criptomonete come il Bitcoin si basa sulla crittografia a chiave pubblica. Se volete inviare Bitcoin a qualcuno dovete avere la sua chiave pubblica, mentre se volete ricevere Bitcoin da qualcuno dovete fornire la vostra chiave pubblica.

Nella figura sotto si può vedere la pagina di un sito web dal quale si possono gestire le criptomonete del proprio borsellino (wallet) e, ad esempio, si possono inviare bitcoin a WikiLeaks come donazione.



Figura 10 – Pagina da dove è possibile inviare Bitcoin a Wikileaks

Algoritmo RSA

Per applicare gli schemi a chiavi e lucchetti visti in precedenza, è necessario trovare una funzione matematica (il lucchetto) la cui trasmissione su canali insicuri non compromette l'algoritmo, che sia facile da applicare (chiudere il lucchetto) ma difficile da invertire (aprire il lucchetto), a meno di non possedere un determinato elemento (la chiave del lucchetto)

Useremo come esempio la cifratura RSA.

Aspetti matematici

Utilizzeremo, senza dimostrazioni, questi concetti:

- Aritmetica finita
- Funzione di Eulero
- Teorema di Fermat-Eulero
- Inverso di un numero nell'Aritmetica finita
- Metodo RSA
- Esempio

Aritmetica finita

L'aritmetica ordinaria opera su insiemi infiniti di numeri come l'insieme \mathbb{N} dei numeri naturali: $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$ o quello degli interi $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}$.

Nella realtà però si ha spesso a che fare con situazioni nelle quali i numeri possibili sono finiti; l'orologio ha solo 12 o 24 ore; e anche i numeri gestiti da un computer sono sempre limitati.

Si definisce allora aritmetica finita un'aritmetica che opera su un insieme limitato di numeri, di solito un sottoinsieme di \mathbb{N} . Si dice anche aritmetica modulare o circolare, in quanto una volta raggiunto l'ultimo numero si ricomincia dal primo.

Esempio classico quello dell'orologio; le ore si susseguono da 0 a 23, il 24 coincide con il punto di partenza, quindi con lo 0; e con la mezzanotte si ricomincia da 0. L'insieme è $\{0,1,2,3,\dots,22,23\}$. L'aritmetica dell'orologio è quindi definita un'aritmetica modulo 24.

In generale un'aritmetica finita modulo n si basa sull'insieme $\{0,1,2,\dots,n-1\}$; questi numeri possono vedersi come i possibili resti di una divisione per n .

Ad esempio 44 in un'aritmetica modulo 6 vale 2, come ben sapeva la famosa canzone: quarantaquattro gatti in fila per sei col resto di due...

Molti ambienti e linguaggi informatici prevedono un operatore per il calcolo del resto; il simbolo è mod (linguaggio Pascal) o % (linguaggio C e simili). Es. $19 \bmod 7 = 5$; $19 \% 7 = 5$.

Funzione di Eulero

In matematica, la funzione Φ di Eulero è una funzione definita, per ogni intero positivo n , come il numero degli interi compresi tra 1 e n che sono coprimi con n cioè non hanno divisori comuni.

Ad esempio, $\varphi(8) = 4$ poiché i numeri coprimi di 8 sono quattro: 1, 3, 5, 7. Notare che la funzione di Eulero di un prodotto è il prodotto delle funzioni di Eulero: $\varphi(a*b) = \varphi(a)*\varphi(b)$.

Deve il suo nome al matematico svizzero Eulero, che per primo la descrisse.

Teorema di Fermat-Eulero

Dati due qualsiasi numeri m ed N primi tra di loro allora è:

$$m^{\Phi(N)} = 1 \bmod N$$

Se poi N è primo allora $\Phi(N) = N - 1$ (piccolo Teorema di Fermat: è quello che interessa a noi)

Inverso di un numero nell'Aritmetica finita

L'inverso di un numero x in un'aritmetica finita modulo N è quel numero y per il quale risulta $xy = 1 \bmod N$. Un metodo di calcolo è fornito, quando x ed N sono primi tra di loro, dal teorema di Eulero-Fermat che, come visto sopra, asserisce:

$$x^{\Phi(N)} = 1 \bmod N$$

dove $\Phi(N)$ è la funzione di Eulero.

Allora l'inverso è semplicemente il numero

$$y = x^{\Phi(N)-1} \bmod N$$

Infatti moltiplicando modulo N ambo i membri dell'uguaglianza per x si ha:

$$xy = x * x^{\Phi(N)-1} = x^{\Phi(N)} = 1 \bmod N$$

e, se N è primo:

$$xy = x * x^{\Phi(N)-1} = x^{\Phi(N)} = x^{N-1} = 1 \bmod N$$

Va rilevato che il calcolo della funzione di Eulero per numeri elevati ha la stessa complessità della fattorizzazione, cioè la ricerca di un insieme di numeri interi positivi tali che il loro prodotto sia il numero originario.

Esempio:

Si prenda il numero 5 in un aritmetica finita di ordine 18; si calcoli la funzione di Eulero $\Phi(18) = 6$ (1, 5, 7, 11, 13, 17), e l'inverso di 5 viene ad essere $5^5 \bmod 18 = 3125 \bmod 18 = 11$. E in effetti $5 * 11 = 55 = 1 \bmod 18$.

A questo punto, gli strumenti li abbiamo tutti e possiamo costruire i nostri lucchetti e le nostre chiavi.

Un semplice esempio numerico

RSA è un cifrario a chiave pubblica che permette di cifrare un messaggio attraverso un procedimento che sfrutta le proprietà dei numeri primi nell'aritmetica finita. Supponiamo di avere come corrispondenti i soliti Alice e Bruno.

Nell'illustrare il metodo, forniamo un esempio basato su numeri molto piccoli; nella realtà, i numeri utilizzati hanno svariate decine di cifre. Di questo non ci dobbiamo preoccupare perché, tutta la trattazione della crittografia in chiave pubblica, compresi tutti gli usi a cui abbiamo accennato, viene gestita da applicazioni che nascondono completamente all'utente la complessità computazionale.

Alice genera le sue chiavi

- Alice genera due numeri primi distinti **p** e **q** e li moltiplica tra di loro ottenendo **il numero N che viene reso pubblico**, mentre **p** e **q** devono restare segreti (non fanno parte della chiave, ma permetterebbero di ricostruirla).
 - Esempio:

<p>p = 5</p> <p>q = 11</p> <p>p*q = 5*11 = 55</p>
<p>N = 55 (chiave pubblica 1)</p>

- Alice calcola **b** che è la funzione di Eulero di **N**: $b = \Phi(N) = (p-1)*(q-1)$. Il numero **b** deve restare segreto.
 - Esempio:

$\Phi(55) = (5 - 1) * (11 - 1) = 4*10 = 40$
b = 40 (serve per calcolare la chiave pubblica 2)

- Alice calcola il primo intero **e** che sia primo con **b** (non abbia divisori in comune, ovvero $MCD(e, b) = 1$). Il numero **e** è la seconda chiave pubblica.
 - Esempio:

$e = 2 \rightarrow MCD(2, 40) = 2$ NO $e = 3 \rightarrow MCD(3, 40) = 1$ SI
e = 3 (chiave pubblica 2)

- Alice calcola il numero d inverso di e nell'aritmetica finita di ordine **b**, che è il più piccolo x per cui sia $e*d \bmod b = 1$; il numero **d** è la chiave per decifrare e deve restare segreto. Si potrebbe usare il metodo basato sulla funzione di Eulero ma per numeri grandi la complessità sarebbe proibitiva; molto più efficiente un'estensione del classico algoritmo di Euclide per l'MCD; qui a titolo esemplificativo usiamo un semplice metodo a tentativi:
 - Esempio:

$d = 2 \rightarrow 2*3 \bmod 40 = 6$ NO $d = 3 \rightarrow 3*3 \bmod 40 = 9$ NO $d = 4 \rightarrow 4*3 \bmod 40 = 12$ NO ... $d = 26 \rightarrow 26*3 \bmod 40 = 78 \bmod 40 = 38$ NO $d = 27 \rightarrow 27*3 \bmod 40 = 81 \bmod 40 = 1$ SI
d = 27 (chiave privata)

Bruno invia un messaggio ad Alice

- Per trasmettere un messaggio ad Alice, Bruno lo scompone inizialmente in una sequenza di numeri (in precedenza ci si è accordati riguardo alla modalità di "traduzione"; potrebbero essere p.es. i codici ASCII dei singoli caratteri ma così il cifrario degenererebbe in un banale cifrario monoalfabetico): (m_1, m_2, \dots, m_r).
- Quindi Bruno legge le chiavi pubbliche di Alice **N** ed **e** e trasmette i numeri **m** uno alla volta cifrandoli con la formula $c = m^e \bmod N$.
 - Esempio: per trasmettere il numero 7, Alice calcola $c = m^e \bmod N = 7^3 \bmod 55 = 343 \bmod 55 = 13$; il numero da trasmettere è quindi 13.

Alice decifra il messaggio cifrato di Bruno

- Alice usa per questo la chiave di decifrazione d , segreta, che permette di recuperare m grazie alla formula $m = c^d \bmod N$; infatti si dimostra che $c^d \bmod N = m$.
 - Esempio: $m = c^d \bmod N = 13^{27} \bmod 55 = 7$

Osservazioni

- Tutte le operazioni che abbiamo visto vengono eseguite automaticamente senza nessun intervento dell'utente e in genere senza che lui se ne renda conto.
- Come si può immaginare, per numeri molto grandi i calcoli sono molto impegnativi anche per un computer moderno e stiamo parlando solo della codifica, non di un tentativo di forzarla. L'uso che si fa oggi della crittografia a chiave pubblica non è quindi quello, troppo impegnativo, di codificare tutto il messaggio, ma "solo" quello di trasmettere una chiave su un canale non sicuro. Questa chiave è la chiave di un molto più veloce e certo non meno robusto algoritmo SIMMETRICO. Ad esempio, trasmetto con RSA (algoritmo asimmetrico) una chiave AES (algoritmo simmetrico) e codifico il messaggio con questa: unisco la non necessità di scambiare preventivamente una chiave comune con la velocità di codifica/decodifica degli algoritmi simmetrici che invece usano proprio una chiave comune.

CONCLUSIONI

Abbiamo visto come la crittografia, da strumento per pochi, sia alla fine entrata nella vita quotidiana di tutti noi. Abbiamo citato alcuni esempi, ma oggi anche chi preleva denaro con il Bancomat, chi effettua acquisti su internet con la carta di credito, chi fa una telefonata con il cellulare fa uso, in genere senza rendersene conto, di tecniche crittografiche.

Cosa si può prevedere per il futuro?

Gli algoritmi simmetrici oggi sono molto potenti e robusti e anche quelli asimmetrici godono di ottima salute. Potrà esserci un nuovo al-Kindi che con la sua analisi delle frequenze sconfisse i cifrari a sostituzione?

Se qualche matematico trovasse una “regola” per fattorizzare grandi numeri, la crittografia asimmetrica tremerebbe e assieme ad essa tutto il mondo tecnologico, ma ormai non sembra molto probabile: sono secoli che i matematici ci provano invano.

Un pericolo più grosso per gli algoritmi di crittografia è probabilmente l’aumento della potenza di calcolo dei computer. Già in passato cifrari ritenuti robusti sono stati rapidamente resi deboli dai grandi progressi dell’hardware degli elaboratori: l’algoritmo DES è diventato uno standard del governo degli Stati Uniti nel 1976, ma alla fine degli anni ‘90 era già considerato insicuro e oggi nessuno si sognerebbe di usare DES per qualcosa che deve restare riservato. Si può usare il 3DES che applica tre volte consecutive DES rendendolo più robusto, ma è un ritorno alla sfida tra cannone e corazza.

Il futuro computer quantistico di cui si favoleggia dovrebbe aumentare di migliaia di volte la capacità di calcolo dei computer. Vedremo.

Per concludere, vorrei rispondere alla domanda del titolo di questo mio lavoro: Giulio Cesare avrebbe WhatsApp? In fondo la risposta è semplice: la sua sensibilità al problema della sicurezza dei messaggi gli farebbe sicuramente apprezzare le qualità crittografiche delle ultime applicazioni di messaggistica istantanea, quindi sì, sono certo che Giulio Cesare avrebbe WhatsApp.

BIBLIOGRAFIA

- David Kahn, *The Codebreaker*, Scribner, New York, 1997.
- Auguste Kerckhoffs, *La Cryptographie militaire*, Journal des sciences militaires, vol. IX, Parigi, Jan. 1883
- Luigi Sacco, *Manuale di crittografia*, Youcanprint, Lecce, 2014.
- Edgar Allan Poe, *A few word on secret writing*, CreateSpace Independent Publishing Platform, Columbia, 2014.
- Edgar Allan Poe, *The Gold-Bug*, CreateSpace Independent Publishing Platform, Columbia, 2017.
- Andrew S. Tanenbaum, *Reti di calcolatori*, Pearson Education Italia Srl, Milano, 2003

FILMOGRAFIA

- Ron Howard, *A beautiful mind*, 2001
- Morten Tyldum, *The Imitation Game*, 2014

SITOGRAFIA

- Crittografia.eu <http://crittografia.eu/index.htm> (ultima consultazione 07/06/2018)
- La Crittografia da Atbash a RSA <http://www.crittologia.eu/index.html> (ultima consultazione 07/06/2018)
- Crittografia e trigonometria nello *Scarabeo d'oro* di Poe <http://keespopinga.blogspot.com/2012/07/crittografia-e-trigonometria-nello.html> (ultima consultazione 28/05/2018)
- Enigma: ecco come funzionava <https://www.focus.it/scienza/scienze/enigma-come-funzionava?gimg=56505#img56505> (ultima consultazione 23/05/2018)
- RSA Algorithm https://www.di-mgt.com.au/rsa_alg.html#keygen (ultima consultazione 01/06/2018)
- Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia <https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/> (ultima consultazione 03/06/2018)
- Whatsapp attiva la crittografia end-to-end <https://www.webnews.it/2016/04/05/whatsapp-attiva-la-crittografia-end-to-end/> (ultima consultazione 03/06/2018)