dossier

TOP SECRET

di PASQUALE EMANUELE SCOPELLITI

Lungo tutta la storia dell'uomo i segreti di re, capi di stato e generali hanno avuto un potentissimo alleato: la matematica. Algoritmi matematici sono infatti alla base di tutte le tecniche crittografiche che consentono di rendere un messaggio incomprensibile a chiunque, tranne a chi possiede la chiave necessaria a decifrarlo

Gli algoritmi crittografici sono come una cassaforte che può essere aperta solo da chi ne ha la chiave. Senza di essa, in molti casi, l'unico modo per conoscere il contenuto del messaggio cifrato è utilizzare la tecnica della *forza bruta*, che consiste nel provare tutte le possibili chiavi fino a trovare quella corretta. Il numero di combinazioni possibili, però, può essere talmente grande da rendere inutile all'impresa anche il supporto del più potente calcolatore. Se consideriamo, per esempio, una chiave di 27 caratteri, composta da numeri compresi tra 0 e 9, come 435167719261406529939035128, le possibili combinazioni sono 10^{27}, cioè 1.000.000.000.000.000.000.000.000.000. Un computer moderno, molto potente, in grado di svolgere un miliardo di tentativi al secondo, per provare tutte le combinazioni impiegherebbe circa 30 miliardi di anni, più del doppio dell'età dell'Universo. La probabilità di trovare la combinazione giusta è paragonabile a quella di individuare un determinato granello di sabbia in una spiaggia lunga 1000 km.

La forza bruta però non è sempre l'unico modo per forzare un codice, infatti i crittoanalisti hanno sviluppato tecniche più raffinate e ingegnose, che permettono di attaccare alcuni tipi di cifrari. La storia è ricca di episodi affascinanti che narrano proprio la sfida fra crittologi, coloro che elaborano algoritmi sempre più sicuri ed efficienti, e crittoanalisti, che invece cercano modi per *crackare* gli algoritmi crittografici. Proprio questo meccanismo di sfida, insieme allo sviluppo delle nuove tecnologie, ha alimentato l'evoluzione della crittografia, a partire dal primo cifrario introdotto da Giulio Cesare fino ad arrivare ai complessi algoritmi che caratterizzano oggi l'era delle comunicazioni digitali.

IL CIFRARIO DI CESARE

Uno dei primi sistemi crittografici risale al I sec a.C. e prende il suo nome da Giulio Cesare, che lo impiegava frequentemente per trasmettere in modo sicuro informazioni riservate. Il *cifrario di Cesare* è basato sulla sostituzione di ogni lettera del testo da trasmettere con una lettera successiva, nell'alfabeto del messaggio originale, a distanza fissa *n*: sia per cifrare che per decifrare un messaggio è sufficiente conoscere *n*, che è la chiave crittografica. In questo esempio abbiamo utilizzato come chiave *n*=3 per creare l'alfabeto cifrato e per cifrare un messaggio.

Testo in chiaro:

ATTACCHIAMO QUANDO SORGE IL SOLE

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

Testo cifrato:

DZZDFFMNDPRTADQGRVRULHNOVROH

CRITTOGRAFIA: COME LA MATEMATICA PROTEGGE I SEGRETI


Giulio Cesare

Sebbene molto efficace agli scopi di Cesare, oggi questo cifrario appare estremamente debole perché, dato un alfabeto di N lettere (nel caso dell'alfabeto italiano N=21, per quello inglese invece N=26), è infatti possibile generare solo N-1 chiavi, basta quindi qualche tentativo sulle prime parole del testo cifrato per trovare la chiave corretta.
Questo perché, vista la ciclicità dell'operazione di traslazione per passare dall'alfabeto in chiaro a quello cifrato, una qualunque chiave n è equivalente a tutte le chiavi d=(n mod N)+kN, dove k è un qualunque numero intero non negativo. Questo implica che esistono solo N classi differenti di chiavi. Inoltre, dato che la chiave d=0 darebbe l'alfabeto originale, le chiavi effettivamente utilizzabili sono N–1.

Le notizie che abbiamo sulla crittografia romana sono molto scarse, ma grazie a Svetonio sappiamo per certo che sia Cesare sia Augusto utilizzavano per la loro corrispondenza un alfabeto spostato di un certo numero di posti.
In Vita dei dodici Cesari (§56), Svetonio infatti scrive:

Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.

[Restano quelle *[lettere]* a Cicerone, così come quelle ai familiari sugli affari privati, nelle quali, se doveva fare delle comunicazioni segrete, le scriveva in codice, cioè con l'ordine delle lettere così disposto che nessuna parola potesse essere ricostruita: se qualcuno avesse voluto capire il senso e decifrare, avrebbe dovuto cambiare la quarta lettera degli elementi, cioè D per A e così via per le rimanenti.].

CIFRARIO A SOSTITUZIONE MONOALFABETICA

La generalizzazione del codice di Cesare è rappresentata dal cifrario a sostituzione monoalfabetica. In questa tecnica ogni lettera è sostituita da un'altra dello stesso alfabeto in modo autonomo e senza una legge fissa. Per esempio:

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
Q	A	Z	S	P	D	C	R	F	V	T	G	B	H	N	U	M	I	O	L	E

Per tentare di forzare questo cifrario non è possibile utilizzare la forza bruta, perché in questo caso il numero di chiavi è incredibilmente elevato e corrisponde a 21! (nel caso del nostro alfabeto), cioè a tutte le permutazioni di tutte le lettere dell'alfabeto, che corrisponde a circa $5 \cdot 10^{19}$: un cinque seguito da 19 zeri. Esiste però una tecnica molto efficace per decifrare questo tipo di codice chiamata *analisi in frequenza*. Questa tecnica si basa sul fatto che, statisticamente, in un testo ogni lettera viene ripetuta con una certa frequenza caratteristica. Per esempio, la lettera E nell'alfabeto italiano, è la più utilizzata e in media ha una frequenza del 12%. Esistono inoltre delle sequenze di lettere che sono frequentemente ripetute, come *qu* e *ch*, i bigrammi *la*, *il* e *lo* e i trigrammi *per*, *con*, *dal* e *del*. Dato un testo cifrato monoalfabetico, si può dunque effettuare una statistica sulla frequenza delle lettere e associare a ciascuna lettera cifrata la lettera in chiaro con la frequenza più simile.

LE CHIFFRE INDECHIFFRABLE

Il matematico francese Vigenère nel XVI sec., riprendendo il lavoro iniziato da Leon Battista Alberti, sviluppò un cifrario a sostituzione che non è attaccabile da una semplice analisi in frequenza, infatti ciascuna lettera viene codificata in modo differente ogni volta, rompendo così la corrispondenza diretta fra alfabeto in chiaro e


Leon Battista Alberti

VII sec. a.C.

Codice Atbash

Il libro di Geremia nella Bibbia usa un semplicissimo codice monoalfabetico per cifrare la parola Babele; la prima lettera dell'alfabeto ebraico (Aleph) viene cifrata con l'ultima (Taw), la seconda (Beth) viene cifrata con la penultima (Shin) e così via; da queste quattro lettere è derivato il nome di Atbash (A con T, B con SH) per questo codice.

V sec. a.C.

La scitale spartana

Primo esempio di crittografia per trasposizione, in cui cioè un testo viene crittato invertendone l'ordine delle lettere. La scitale consisteva in un bastone su cui veniva avvolto ad elica una striscia di cuoio; il testo del messaggio viene scritto lungo l'asse più lungo del bastone, una lettera per ciascuna colonna formata dalla striscia di cuoio. Tolto il nastro dal bastone il testo vi risultava trasposto in modo regolare ma sufficiente per evitare la lettura senza un secondo bastone uguale al primo.

I sec. a.C

Cifrario di Cesare

Codice monoalfabetico introdotto da G. Cesare per lo scambio di informazioni riservate.

XI sec.

Nasce la crittoanalisi

Lo studioso Abu Yousuf ibn Ishaq al-Kindi, chiamato il "Filosofo degli Arabi" nel trattato "Sulla decifrazione dei messaggi crittati" illustra per la prima volta la tecnica dell'analisi in frequenza.

1466

Primo esempio di cifrario Polialfabetico

Leon Battista Alberti inventa un cifrario basato sull'utilizzo di due dischi concentrici. Sul disco esterno, che è fisso, è scritto l'alfabeto in chiaro, sul disco interno, che è invece mobile, l'alfabeto cifrato, ruotando i dischi si cambia continuamente la corrispondenza fra i due alfabeti. Oltre ad essere uno dei primi esempi di cifrario polialfabetico, il disco cifrante di Alberti è anche il progenitore delle "macchine cifranti".

2002-2003

Lancio dei primi prototipi commerciali da parte di Id Quantique

1994

Zbinden, Gautier, Gisin, Huttner, Muller, Tittel implementano un sistema di Crittografia Quantistica sulla distanza di 23 km sotto il lago di Ginevra usando fibre ottiche Telecom.

1992

Bennett, Bessette, Brassard, Salvail, Smolin implementano per la prima volta un sistema di Crittografia Quantistica in laboratorio.

1984

Bennett e Brassard pubblicano il primo e principale protocollo della Crittografia Quantistica, il BB84.

1977

Viene inventato l'algoritmo RSA Una vera e propria rivoluzione per la crittografia, nasce infatti la crittografia a chiave pubblica.

1976

Un articolo di Diffie ed Hellmann per la prima volta propone l'idea di una crittografia a chiave pubblica.

1863

Il colonnello Kasiski trova il modo di forzare il codice di Vigenère, sfruttando la ricorrenza delle lettere a una certa distanza una dall'altra.

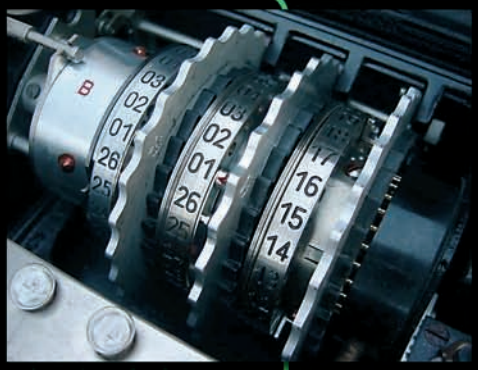
1883

Auguste Kerckhoffs Von Nieuwenhof nel trattato dal titolo La cryptographie Militaire formula uno dei principi cardine della crittografia: "La sicurezza di un crittosistema non deve dipendere dal tener celato il critto-algoritmo. La sicurezza dipenderà solo dal tener celata la chiave".

1918

· ***Vernam*** modifica il cifrato di Vigenère, migliorando grazie all'utilizzo di chiavi lunghe almeno quanto il messaggio da trasmettere e generate in maniera casuale.

· ***Viene inventata la macchina Enigma*** la macchina cifrante più famosa della storia, che è stata utilizzata dai tedeschi fino alla fine della II guerra mondiale.



XVI sec.

Introdotto il codice di Vigenère, ritenuto inattaccabile per quasi tre secoli.

1932

I matematici Marian Rejewski, Henryk Zygalski e Jerzy Rozicki dell'ufficio CIFRA polacco scoprono incredibili leggerezze nelle procedure di codifica tedesche e forzano i messaggi prodotti con Enigma, che era considerata dai tedeschi inattaccabile.

1939

Da una collaborazione Polacca -Inglese nasce il progetto ULTRA per una sistematica decifrazione dei messaggi Tedeschi crittati con Enigma. Grazie anche alla partecipazione del noto matematico inglese Alan Turing furono sviluppati nuovi metodi di crittoanalisi che portarono nel 1942 a decrittare 80000 messaggi tedeschi al mese. Aver forzato sin dall'inizio della guerra Enigma fu un elemento decisivo per la vittoria degli anglo-americani nella II guerra mondiale.

1943

Viene assemblato in Inghilterra quello che è considerato da molti il primo calcolatore elettronico Colosso Mark I – per decifrare i messaggi crittati con la macchina di Lorenz. Un forte impulso alla nascita dei calcolatori elettronici è dato proprio dalla necessità delle autorità americane di forzare la seconda macchina cifrante dei tedeschi, la macchina di Lorenz, molto più complicata di Enigma, che veniva utilizzata dagli alti comandi di Hitler.

1949

Shannon dimostra l'inviolabilità del cifrario di Vernam.

1975

L'IBM presenta il D.E.S. (Data Encryption Standard) che è un cifrario composto che prevede 16 cifrature successive (trasposizioni e sostituzioni di bit) e che è tuttora il cifrario a chiave segreta più usato negli ambienti informatici.

alfabeto cifrato. Per fare ciò viene utilizzata una tavola in cui in ogni riga viene riscritto l'alfabeto sfasato di un certo numero di lettere:

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B
I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C	D	E	F	G	H
A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
O	P	Q	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	L	M	N

Le prime lettere di ogni riga, esclusa la prima, rappresentano la nostra chiave (che nell'esempio è CIAO) e il messaggio viene cifrato utilizzando ciclicamente le corrispondenze fra la prima riga e una delle successive, in questo modo:

A	T	T	A	C	C	H	I	A	M	O
C	I	A	O	C	I	A	O	C	I	A
C	E	T	O	E	M	H	Z	C	U	O

In questo caso, alla prima lettera del testo, **A**, corrisponde la lettera C, trovata all'incrocio tra la prima colonna e la prima riga. Alla lettera **T** corrisponde la E, trovata all'incrocio tra la colonna della T e la riga della I. Si prosegue di questo passo utilizzando la chiave in un ciclo continuo, fino a cifrare tutto il testo.

Per oltre due secoli il codice di Vigenère è stato considerato inattaccabile, fino a quando il colonnello prussiano Kasiski nel 1863 escogitò una tecnica di attacco che consisteva in una analisi in frequenza multipla. L'attacco di Kasiski sfrutta il fatto che esistono lettere ricorrenti a una certa distanza una dall'altra. Notate, per esempio, che nel nostro testo la prima **A** è cifrata con una **C** mentre la seconda **A** con una **O**; tuttavia, la terza **A** è ancora cifrata con la lettera **C**. Questa, che a prima vista potrebbe sembrare una pura casualità, è invece la principale debolezza del cifrario di Vigenère. Nel testo in chiaro, infatti, lettere uguali che si trovano a una distanza pari a un multiplo della lunghezza della chiave vengono cifrate con la stessa lettera. Partendo da questo principio, il colonnello Kasiski ha sviluppato un attacco al cifrario di Vigenère, dimostrando di fatto la possibilità di romperlo.

Nel 1917 Gilbert Vernam perfezionò il metodo di Vigenère, con il metodo chiamato *One Time Pad*, proponendo l'idea di usare chiavi lunghe quanto il messaggio e generate in modo casuale, eliminando così ogni possibilità di attacco di Kasiski.

Nel 1949 Claude Shannon, il padre della Teoria dell'Informazione, dimostrò che il cifrario di Vernam è assolutamente sicuro e che si tratta dell'unico sistema inattaccabile dalla crittoanalisi.

Alan Mathison Turing (Londra 1912; Manchester 1954) matematico e logico, considerato uno dei padri dell'informatica (tra le sue invenzioni, si ricordano sempre la macchina ideale e il test che portano il suo nome).

Durante la sua giovinezza e fino al raggiungimento del diploma i suoi risultati scolastici non furono affatto eccezionali: gli insegnanti si lamentavano per il suo disinteresse per il latino e le Sacre Scritture e non concepivano come potesse invece preferire letture riguardanti la teoria della Relatività di Einstein, i calcoli astronomici, gli esperimenti di chimica o il gioco degli scacchi. A partire dal 1931, quando venne ammesso al King's College dell'Università di Cambridge, il genio di Turing cominciò a emergere: si laureò con il massimo dei voti e ottenne il Ph.D, nel 1936 si trasferì alla Princeton University per difendere la propria tesi di dottorato e pubblicò l'articolo che lo rese famoso "On computable Number, with an application to the Entscheidungsproblem", in cui descrisse per la prima volta, quella che in seguito è stata definita la macchina di Turing.

Alan Turing è noto al grande pubblico soprattutto per il ruolo fondamentale che ebbe durante la seconda guerra mondiale, quando si mise a completa disposizione del Department of Communications inglese per decifrare i codici usati nelle comunicazioni scambiate tra i nemici degli Alleati. Essi, infatti, aveva sviluppato un macchina crittatrice, Enigma, capace di generare un codice che mutava costantemente, così da rendere insufficiente agli Alleati il tempo di decodifica dei messaggi nemici. Nel 1942 Turing riuscì nell'impresa realizzando una macchina chiamata Colossus , che decifrava in modo veloce ed efficiente i codici tedeschi creati con Enigma, e permise all'esercito inglese di cambiare le sorti della guerra.

La scultura di Turing, in memoria del matematico inglese (City College of Manchester)