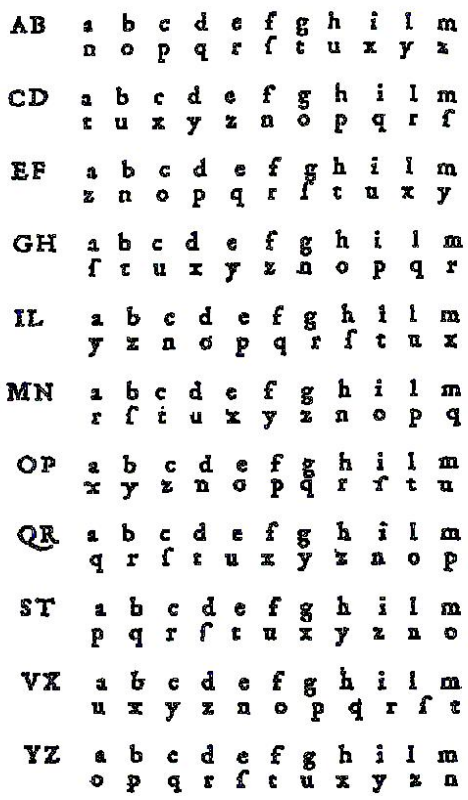
QUINTA TAPPA

La guerra, purtroppo, ha sempre fatto parte della storia del mondo. E come si dice bisogna “fare di necessità virtù”, ed è proprio per questo che nacquero i primi codici segreti. L’uomo aveva bisogno di comunicare informazioni e comandi a distanza, senza però che questi venissero intercettati e letti dal nemico. Ed è così che nacque la crittografia, cioè la ricerca di metodi sempre più elaborati per impedire che le informazioni potessero finire nelle mani sbagliate.

Tra i metodi più antichi ricordiamo il *codice di atbash* degli Ebrei, che consisteva nello scambiare le lettere associando all’alfabeto il suo opposto: facendo un esempio con il nostro alfabeto, la A diventa la Z, la B diventa la V, la C diventa la U e così via. Gli spartani invece utilizzavano la scitala che consisteva in una bacchetta attorno alla quale veniva avvolta una pergamena; veniva quindi scritto il messaggio. Poi, una volta tolta la pergamena dalla bacchetta, questo diventava indecifrabile, a meno di possedere una bacchetta delle stesse esatte misure (che veniva fornita solo a chi doveva leggere il messaggio). Uno dei primi algoritmi crittografici di cui si hanno fonti scritte, fu il *cifrario di Cesare*, così chiamato perché utilizzato da Giulio Cesare. A differenza della scitala o del codice atbash, si tratta di un vero e proprio metodo per la cifrazione e decifrazione di messaggi militari. Nel caso del codice di atbash infatti ogni lettera aveva sempre la stessa corrispondente, perciò una volta individuata la costruzione del metodo era possibile decifrare qualsiasi messaggio. La scitala invece non era un vero e proprio metodo, ma più un espediente che necessitava di strumenti adeguati (bacchette delle stesse dimensioni, appunto). Il *Cifrario di Cesare* consisteva nel sostituire ogni lettera del messaggio con la sua corrispondente, definita da un certo numero, che chiameremo *chiave*. Svetonio, storico romano, ci racconta che Cesare utilizzava sempre per le sue cifrature il numero 3:

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

ad ogni lettera corrisponde quella che si trova 3 posizioni avanti nell’alfabeto. Il fatto che Cesare usasse sempre la stessa chiave non deve far pensare che fosse uno sprovveduto: i suoi avversari spesso non erano neanche in grado di leggere un testo in chiaro, men che mai un testo cifrato.



Col progredire della civiltà però, tutti questi metodi si rivelarono abbastanza fragili, perché una volta capito il loro funzionamento, rendevano il messaggio facilmente decifrabile. Per questo sono state ideate soluzioni sempre più complesse.

Il primo passo nella crittografia moderna avviene grazie a Leon Battista Alberti e al suo disco cifrante: si tratta di un disco con una parte stabile, il chiaro, e una mobile, il cifrato. Ruotando opportunamente il disco era possibile ottenere messaggi cifrati che cambiavano chiave di lettura ogni 2/3 parole, e rendeva quindi più complicata la decifratura. Fu poi il bresciano Giovan Battista Bellaso, nel 1553, a portare una vera svolta nella cifratura, grazie all’introduzione di diversi alfabeti per la cifratura. Utilizzando il cosiddetto *contrassegno*, ad ogni lettera del messaggio veniva

attribuito un diverso alfabeto di decifrazione. Mostriamo un esempio:

contrassegno:	VIRTVTIOMNIAPARENTVIRTVTIOMNIAPARENTVI
chiaro:	larmataturchescapartiraacinquediluglio
cifrato:	fyboueyldanuofszlpiincupnshmlrnxoiznrd

Nell'esempio abbiamo che la "l" iniziale del messaggio viene cifrata con l'alfabeto VX, dove "l → f"; la "a" invece utilizza l'alfabeto IL, per cui "a → y"; procedendo in questo modo si ottiene il messaggio cifrato.

Sull'esempio di Bellaso, il francese Vigenère, utilizzando il contrassegno e una tavola ad alfabeti regolari, generò un sistema che rimase indecifrabile per tre secoli. Fino a quando nel 1863 il colonnello prussiano Friedrich Kasiski riuscì a ideare un metodo di decrittazione, chiamato in suo onore *Metodo Kasiski* (o Babbage-Kasiski). Il maggiore Kasiski notò che spesso in un crittogramma di Vigenère si possono notare sequenze di caratteri identiche, poste ad una certa distanza fra di loro; questa distanza può, con una certa probabilità, corrispondere alla lunghezza della chiave, o a un suo multiplo. Una volta stabilita la lunghezza della chiave, la decrittazione si riduce a quella di un cifrario di Cesare, e diventa quindi abbastanza banale. Circa una ventina di anni dopo l'olandese Auguste Kerckhoffs stabilì una delle leggi fondamentali sull'uso dei metodi crittografici, tuttora ritenuta valida, la quale afferma che la sicurezza di un crittosistema non deve dipendere dal tenere celato l'algoritmo crittografico ma solo dal tenere celata la chiave. Proprio sull'onda di quest'idea, a quarant'anni di distanza, nel 1918, il maggiore dell'esercito statunitense Gilbert Vernam riprese il metodo di Vigenère introducendo però chiavi lunghe almeno quanto il messaggio e non riutilizzabili. Il cifrario di Vernam, così viene chiamato il sistema così ottenuto, è detto anche cifrario perfetto, in quanto è l'unico sistema crittografico la cui sicurezza sia stata provata da una dimostrazione matematica. Purtroppo però ha lo svantaggio di richiedere chiavi di grandi dimensioni e quindi difficili da distribuire: le spie venivano equipaggiate con dei taccuini contenenti una lunga chiave per pagina, da poter strappare una volta utilizzata.

Durante la seconda guerra mondiale la crittografia ha svolto un ruolo centrale. In Germania, prima la macchina Enigma e poi la macchina Lorenz, furono fondamentali per la cifratura dei messaggi militari: si tratta di due macchine che si basano teoricamente sul cifrario di Vernam utilizzando però anche dei rotori, ispirati al disco cifrante di Leon Battista Alberti. La differenza sostanziale delle due è che la seconda permette di inviare e ricevere messaggi in chiaro, che risultano cifrati solo in caso di intercettazione. Si tratta però di una macchina molto più ingombrante e quindi meno pratica. La macchina Purple invece fu costruita dai giapponesi e si differenziava dalle macchine tedesche in quanto al posto dei rotori utilizzava degli switch telefonici, che rendevano la cifratura più casuale. Le capacità di decifrazione degli avversari però, permisero agli Alleati di intercettare messaggi cruciali e vincere così la guerra.

Al giorno d'oggi la crittografia è fondamentale: tutto ciò che facciamo online deve essere protetto, dai nostri dati personali a ciò che scriviamo. La maggior parte delle applicazioni di messaggistica sfruttano sistemi di crittografia in modo che solo chi invia e riceve i messaggi sia in grado di leggerli.

FONTI QUINTA TAPPA

- Crittografia - Wikipedia
- Crittografia: Cos'è e come funziona | Guida per principianti (outofbit.it)
- crittografia nell'Enciclopedia Treccani
- Disco cifrante - Wikipedia

Cifrario di Vernam - Wikipedia
Metodo Kasiski - Wikipedia
Cifrario di Vigenère - Wikipedia
ARPINATI_MUSIANI_CRITTOGRAFIA.pdf (zanichelli.it)