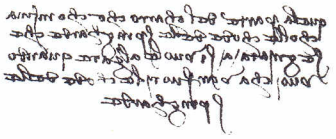
MODULO H



La strategia del codice segreto

PRESENTAZIONE

Come trasmettere segreti tramite codici e cifrari

Durante la seconda guerra mondiale, alla vigilia dell'attacco giapponese alla base americana di Pearl Harbour nel Dicembre 1941, un messaggio, apparentemente innocente, di previsioni del tempo («Vento dell'est, pioggia – vento del nord, nuvole – vento dell'ovest, sereno») allertò i diplomatici giapponesi in tutto il mondo che la guerra era imminente.

Il messaggio era una delle più semplici forme di codice – un messaggio predisposto in modo da avere un significato speciale per coloro che lo ricevono.

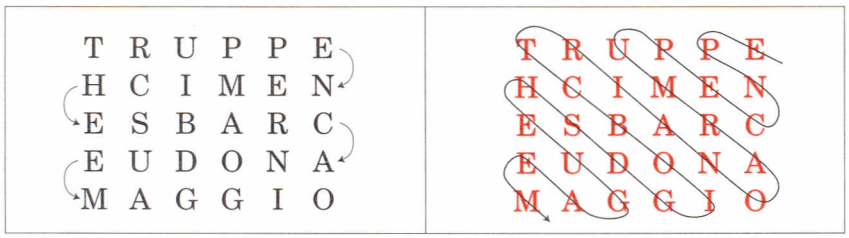
Messaggi simili vennero trasmessi dalla BBC durante la seconda guerra mondiale alla Resistenza francese. Una frase come «Romeo abbraccia Giulietta» or «Benedictine è un liquore dolce» potevano trasmettere informazioni sul lancio di paracadutisti o rifornimenti. Il primo verso di una poesia dello scrittore francese Paul Verlaine («I lunghi singhiozzi dei violini d'autunno») comunicò alla Resistenza che il D-Day (il giorno dello sbarco in Normandia) era imminente.

In codici più complessi, le parole e le frasi vengono sostituite da altre parole e frasi; oppure vengono usati gruppi di lettere scollegate per creare un intero dizionario di parole e frasi. Ad esempio, l'ordine «Forniteci un fuoco d'appoggio» potrebbe essere comunicato tramite le lettere GYPHC. Lunghi rapporti militari possono essere trasmessi con simili gruppi di cinque lettere – comprensibili soltanto a coloro che sono in grado di interpretarli.

L'altro modo principale di inviare informazioni segrete consiste nell'utilizzare un cifrario. In una «cifra» le vere lettere dell'alfabeto vengono sostituite da altre lettere, numeri o simboli. Il codice Morse è di fatto un cifrario, in quanto trasmette ogni lettera tramite combinazioni di segnali lunghi e brevi che possono essere inviati per radio, telegrafo o segnali luminosi. La lettera E, ad esempio, è un punto fermo (.), mentre la Q è lineetta, lineetta, punto, lineetta (— — . —).

Un'altra comune forma di «cifra» viene elaborata per mezzo di una griglia. Il messaggio «Truppe nemiche sbarcano due maggio» potrebbe essere scritto in una griglia di, poniamo,

sei colonne, scrivendolo alternativamente da sinistra a destra e da destra a sinistra. Le lettere vengono poi riscritte in gruppi di cinque seguendo un percorso diagonale sulla griglia:

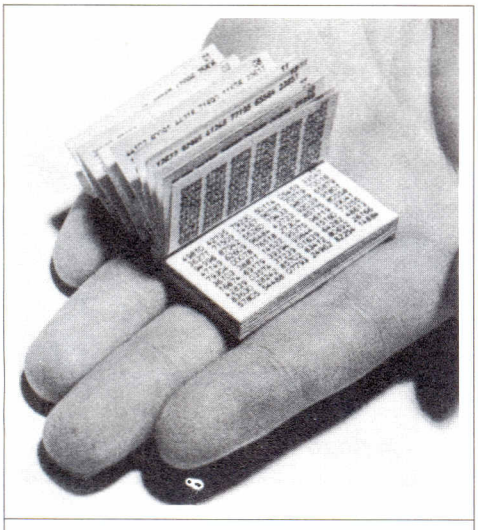


In tal modo la «cifra» trasmessa risulterà:

EPNCE PUMRA ONAIR TCBOI GDSHE UGAEM

La persona che riceve il messaggio userà una griglia simile per decifrarlo.

Un punto debole di questo sistema consiste nel fatto che la frequenza delle lettere e delle combinazioni di lettere rimane uguale a quella del linguaggio comune. La E, ad esempio, è una delle lettere più comuni, e la Z una di quelle più rare, per cui una persona che volesse decifrare il codice può presumere che la lettera che compare con maggiore frequenza rappresenti la E – e così via.



Minuscoli blocchetti vengono usati dalle spie per decifrare messaggi segreti. Delle istruzioni in codice inviate via radio fanno riferimento a gruppi di numeri a cinque cifre in una pagina specifica del blocchetto. Una volta che il messaggio è stato ricevuto e decifrato, il destinatario e il mittente strappano la relativa pagina dai loro blocchetti.

Durante la seconda guerra mondiale il governo tedesco utilizzava una macchina per generare codici chiamata «Enigma». Con qualunque frequenza si digitasse una particolare lettera, la macchina non ripeteva mai la stessa «cifra». Ogni giorno veniva creato un nuovo cifrario, secondo un programma noto solo ai tedeschi.

Un gruppo di matematici e linguisti delle università inglesi riuscirono a decifrare il codice di «Enigma» nel 1940. Il loro lavoro fu molto importante per la vittoria finale, in quanto fornì ai comandi alleati un quadro aggiornato dei piani tedeschi nella campagna nordafricana e nella guerra aerea.

Con l'avvento dei computer, i codici sono diventati molto più complicati e difficili da decifrare. Programmi complessi usano migliaia di calcoli, e senza conoscere la sequenza dei comandi da immettere, potrebbero essere necessari migliaia di anni per decifrarli!

(Da: *How Is It Done?*, The Reader's Digest, Londra 1990. Traduzione di L. Mariani)