Nicola Marras Manfredi

CRYPTORAMA

www.nicolamarras.it

a new life for old technologies: ensuring the future by preserving the past

La crittografia è indispensabile per mantenere il segreto: da minuscoli brandelli di informazione il nemico può infatti ricostruire le nostre mosse!

La crittografia e i regoli cifranti

La crittografia sembra un tema estraneo alla storia del calcolo ma ebbe una grande importanza nello sviluppo dei calcolatori. Il primo computer moderno fu inventato da AlanTuring, il padre dell' informatica, per decifrare le comunicazioni tedesche nel centro di *Bletchley Park* in Inghilterra ed oggi si studiano i calcolatori quantistici proprio per disporre della potenza di calcolo indispensabile a garantire la riservatezza nelle transazioni su internet. Nessuno darebbe il suo numero di carta di credito ad un sistema non a *"prova di bomba"*. *"Bombe"* era il soprannome dei primi computer meccanici costruiti per decifrare i messaggi criptati tedeschi e da qui deriva questo modo di dire.

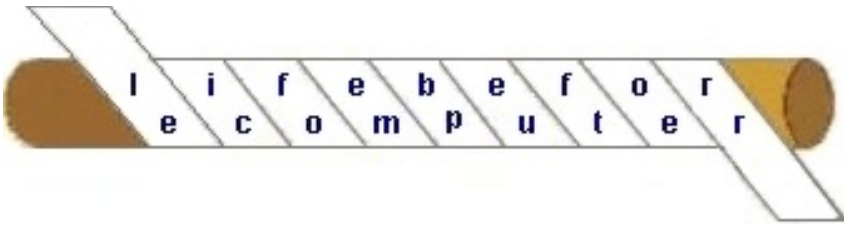
E' chiaramente impossibile parlare di crittografia in poche pagine, una trattazione breve ne richiederebbe almeno 400, ma cercherò comunque di dare una idea sommaria del suo sviluppo e delle sue problematiche.

Un primo esempio di messaggio segreto si trova nelle storie di Erodoto che riporta come un tal Demarato, accortosi che Serse costituiva una grande flotta per conquistare la Grecia, tolse la cera ad una tavoletta di scrittura, marcò il messaggio sul legno e rimise la cera scrivendovi sopra una lettera poco importante. La inviò quindi agli ateniesi, questi capirono dal contesto che era necessario leggere il fondo ed ebbero il tempo di prepararsi: nel 480 Serse fu sicuro di aver imbottigliato le forze greche nella baia di Salamina senza rendersi conto di essere caduto in una trappola.

La tecnica di scrittura segreta usata da Demarato si chiama *steganografia*, dalle parole greche *steganós* (coperto) e *gráphein* (scrivere). Fu un sistema molto usato nell'antichità, i cinesi per esempio scrivevano i messaggi su strisce di seta finissime che ricoprivano di cera e facevano mangiare al messaggero. Nel XVI° secolo Giambattista della Porta spiegò come comunicare con un uovo sodo: si prepara un inchiostro con 30 grammi di allume e mezzo litro di aceto e si scrive sul guscio, che è poroso, senza lasciare tracce mentre il testo rimarrà impresso sull'albume solidificato e si potrà leggere sbucciando l'uovo. Il punto debole della *steganografia* è però evidente: se il testo viene scoperto il nemico viene subito a conoscenza del suo significato. Questo sistema è comunque ancora in uso, per esempio inserendo messaggi nascosti all'interno di immagini digitali, ma il livello di protezione è molto basso.

Per ovviare a questo inconveniente nacque la *crittografia*, dal greco *kriptos* che significa nascosto, che intende rendere incomprensibile il messaggio modificandolo con un procedimento concordato fra mittente e destinatario. I metodi utilizzati furono principalmente la *trasposizione* e la *sostituzione.*

La *trasposizione* consiste nel rimescolare i caratteri del testo chiaro secondo una qualche regola reversibile. Le più antiche notizie sono quelle sulla *scitala lacedemonica*, data da Plutarco come in uso presso gli spartani. I messaggi venivano criptati utilizzando lo *scitale*, un cilindro di legno (in greco skutale significa bastone) di un diametro dato: vi si avvolgeva il nastro attorno e si scriveva sopra; una volta sciolto il nastro il testo era *trasposto* e non era leggibile senza disporre di un cilindro di uguale diametro. Erano tempi più ingenui dei nostri.



"life before computer" sulla scitala, sciogliendo il nastro si leggerà: LEICFOEMBPEUFTOERR

Questa striscia di cuoio veniva spesso indossata come una cintura aggiungendo così un trucco *stenografico*, ma la *trasposizione* è facile da decifrare e fu usata molto poco.

La *sostituzione* consiste invece nel cifrare ogni lettera con una diversa utilizzando un *alfabeto cifrante* concordato tra mittente e destinatario. Nel Libro di Geremia alcuni nomi sono cifrati sostituendo la prima lettera dell'alfabeto ebraico (Aleph) con l'ultima (Taw), la seconda (Beth) con la penultima (Shin) e così via. In pratica si utilizzava l'alfabeto al contrario e da queste prime quattro lettere è derivato il nome di Atbash per questo sistema, ma la moderna *sostituzione* fu inventata da Giulio Cesare che riprese quanto consigliato nel Kāma Sūtra (ca. 400 a.C.) per inviare messaggi agli amanti.

Vediamo come funziona la *sostituzione* di Giulio Cesare: supponiamo di avere due righelli come questi, molto utilizzati durante la seconda guerra. In alto troviamo l'alfabeto *chiaro*, in basso quello *cifrante*.

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

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

L'ordine da inviare è “attaccate immediatamente”: sgrammatichiamo e nascondiamo la lunghezza delle parole, dividendolo in *gruppi* di 5 lettere senza punteggiatura o spazi: “attik catei nxmed iotem xente”. La **x** è una lettera *nulla*, inserita per completare i gruppi. Ora decidiamo la lettera chiave, per esempio “**F**”, e spostiamo il righello superiore (*chiaro*) fino a far combaciare la “**A**” con la “**F**” dell' inferiore (*cifrante*).

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

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

Scambiamo quindi le lettere del righello in chiaro con quelle del cifrante, si usa scrivere i messaggi in chiaro in minuscolo blu e quelli cifrati in maiuscolo rosso.

a t t i x c a t e i n x m e d i o t e m x e n t e

F Y Y N C H F Y J N S C R J I N T Y J R C J S Y J

Il destinatario deve solo conoscere la chiave ed effettuare il procedimento inverso coi suoi righelli. La sgrammaticatura non gli impedirà di comprendere il significato del messaggio, ma renderà più difficile il lavoro di chi proverà a decifrarlo analizzandone le frequenze, come vedremo nella prossima pagina.

Decifrazione dei dispacci radio, notare i righelli in mano all'operatore

Ovviamente non è un cifrario a *“prova di bomba”,* ma ha il vantaggio di avere una chiave semplice da comunicare e ricordare. Ai computer moderni basta poco tempo per *forzarlo*, però fino alla seconda guerra mondiale il lavoro doveva essere svolto manualmente dai pochi specialisti disponibili, sovraccaricati di dispacci da decifrare, e i nostri soldati avrebbero avuto il tempo di compiere l'attacco sorprendendo il nemico. Giulio Cesare utilizzava solo la chiave “D”, ma con l'alfabeto internazionale sono disponibili 26 chiavi. Le buone idee durano a lungo: oggi questo cifrario si chiama ROT (rotation) ed è abbastanza diffuso nei newsgroup, dove si "*rotta*" il testo sempre in chiave “N” (ROT13). Una curiosità: decifrate HAL, il nome del supercomputer di *2001 Odissea nello spazio*, con la chiave ”B”!
Questi esempi mettono in evidenza le basi dei sistemi tradizionali di crittografia: il *metodo* e la *chiave*. Nel primo caso il metodo è il cilindro che costituisce la scitala, la chiave la misura del suo diametro; nel secondo il metodo è la traslazione lineare delle lettere, la chiave l'entità della traslazione (una “a” che cifrata diventa “F” significa una traslazione di 5 a sinistra, chiave “F” o “5S”). E' ininfluente che il nemico conosca il metodo: anche sapendo che abbiamo usato il Codice di Cesare, dovrà comunque conoscerne la chiave per decifrare il crittogramma.

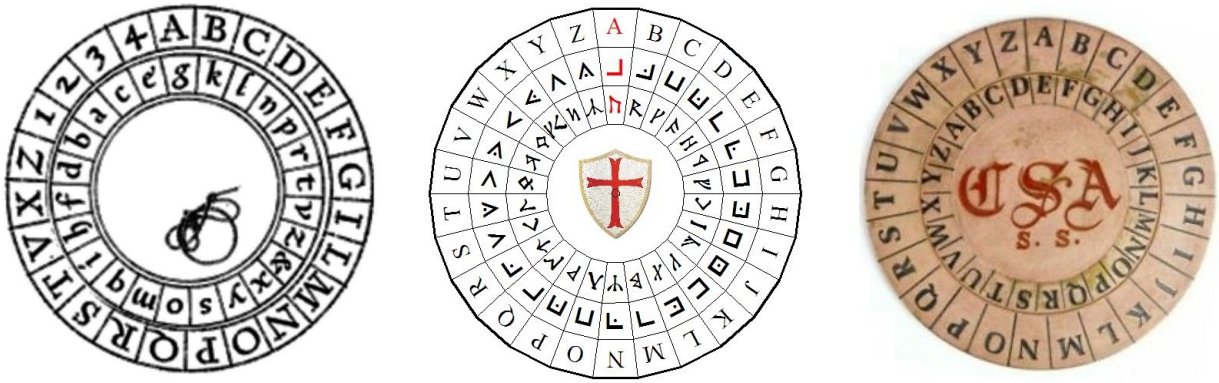
Esiste però il metodo dell'analisi delle frequenze, che permette di decifrare qualunque messaggio così cifrato. Sentiamolo direttamente dal suo inventore Abū Yūsuf Yaʿqūb ibn Ishāq al-Kindī, conosciuto in Occidente col nome latinizzato di Alchindus, eclettico filosofo e matematico arabo del IX° secolo:

"Un modo di svelare un messaggio cifrato consiste nel trovare un testo chiaro nella stessa lingua e calcolare la frequenza con cui appare ciascuna lettera. Chiamiamo "prima" quella che appare più spesso, "seconda" quella che la segue per frequenza e così via fino ad esaurire tutte le lettere. Esaminiamo poi il testo in cifra che vogliamo interpretare ordinando in base alla frequenza anche i suoi simboli: troviamo il simbolo più comune e rimpiazziamolo con la "prima" lettera dell'esempio chiaro, il simbolo che lo segue per sequenza con la "seconda" e così via fino alla fine".

In realtà le frequenze rappresentano valori medi che non sempre corrispondono a quelli riscontrabili in un brano specifico, specie se molto corto. Esaminiamo il testo di Alchindus: le frequenze delle principali lettere sono E=13% - A=12% - I=10% - O=9%, contro i valori considerati standard per la lingua italiana di E=11,8 %, A=11,7 %, I=11,2 %, O=9,8 %. Vi è una piccola differenza percentuale ma le lettere mantengono sempre la loro posizione relativa come *"prima"*, *"seconda"* ecc. e se avessimo criptato il brano le lettere in cifra che sostituiscono le originali apparirebbero con la stessa frequenza, permettendo ad un analista di risalire facilmente al significato. Una volta scoperto il 60% dell'alfabeto è intuitivo ricostruire le parole *"cote nai cvutivepba"*.

Dagli studi di Leon Battista Alberti si sono poi sviluppate tecniche che semplificano il lavoro in quanto ogni lettera ha una identità che consiste sia nella frequenza media sia nella tendenza a prediligere la vicinanza di altre lettere: la *"q"* è sempre seguita alla *"u"*, le doppie più usate sono *"tt"*, *"pp"*, *"nn"* e *"ll"*, mentre le vocali non sono mai doppie. Un individuo che cambiasse nome e aspetto continuando a frequentare gli stessi luoghi ed amicizie prima o poi verrebbe certamente scoperto.

Per il nostro esempio abbiamo usato il Codice di Cesare, chiamato *sostituzione monoalfabetica* in quanto l'alfabeto utilizzato per tutto il messaggio è sempre lo stesso, ma l'Alberti propose di usare più alfabeti cifranti (*sostituzione polialfabetica*) utilizzando il suo regolo. Si tratta di un disco composto di due cerchi concentrici: uno esterno per il testo chiaro, detto *stabile,* con 24 caselle contenenti 20 lettere latine maiuscole messe in ordine alfabetico ed i numeri 1, 2, 3, 4 (sono escluse le lettere J, K, Y, W, Q, H, che hanno una bassa frequenza) ed uno interno, detto *mobile*, con tutte le 24 lettere latine minuscole e in disordine (esclusa W e U=V) per il testo cifrato.



Il disco cifrante di Alberti, la versione templare e un modello americano dell'800

E' un metodo complesso: decisa una lettera maiuscola come chiave (ad es. *"A"* nel disco in alto a sinistra) si deve spostare il disco mobile interno e scrivere, come prima lettera del crittogramma, la lettera minuscola (nel nostro caso "*g"*) che corrisponde alla *"A"*; quindi cifrare come nel precedente esempio col regolo. Sembrerebbe un semplice Codice di Cesare ma l'Alberti suggerisce di usare uno dei quattro numeri per segnalare nel messaggio il cambio di alfabeto; la lettera minuscola corrispondente al numero sarà la nuova chiave e la stessa lettera in chiaro sarà cifrata con diverse lettere ogni volta che si cambia alfabeto. Il risultato è molto più difficile da decifrare e l'Alberti scriveva: "*Ma nessuno, se non chi è consapevole dell'accordo, potrà riuscire da sé a comprendere qualche cosa di quelle che si trovino scritte con questa cifra".*

Alberti disegnò anche un disco per l'alfabeto templare ed il suo regolo fu utilizzato per centinaia di anni, spesso nella versione semplificata da Vigenère.

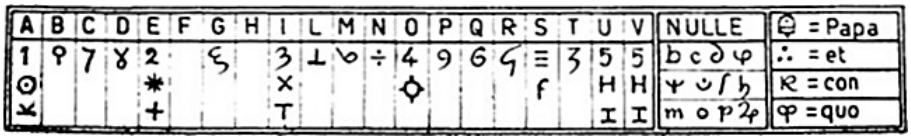
Le scoperte di Alberti passarono inosservate per la sua decisione di non pubblicare il manoscritto, che fu stampato solo nel 1568 a Venezia con il titolo "*La Cifra".* Da quel momento ne vennero a conoscenza vari studiosi, come Johannes Tritemius e Giambattista della Porta, ma fu il diplomatico francese Blaise de Vigenère che nel 1586 ne propose una versione più semplice anche se meno sicura.
Si basa sul Codice di Cesare, migliorando la sicurezza con l'uso di più *alfabeti cifranti* stampati su di una tavola. Cifriamo di nuovo "attix catei nxmed iotem xente" usando come chiave "DUX" ed evidenziando gli alfabeti che cominciano con queste lettere: la "a" di attix sarà criptata con la chiave "D", la "t" con la chiave "U", la seconda "t" con la chiave "X" e ricominceremo daccapo fino alla fine. Il risultato è: DNQHR ZDNBL HUPYA LIQHG UHHQL.

Chiave	Testo chiaro	Testo in cifra

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

Il messaggio così criptato nasconde meglio le frequenze, per esempio la doppia "t" è cifrata con due lettere diverse, ma ancora si può decifrarlo in quanto ogni 3 lettere la sequenza ricomincia riformando degli schemi. L'unica soluzione è avere una parola chiave lunga come il messaggio da usare una sola volta: in questo caso la cifra è assolutamente inviolabile ed ancora serve per le comunicazioni fra i presidenti degli USA e della Russia, ma non è certo praticabile sul campo di battaglia dove si possono scambiare centinaia di messaggi al giorno.
Questo sistema fu ampiamente utilizzato in quasi tutti i conflitti, talvolta impiegando un disco cifrante simile a quello dell'Alberti al posto della tavola. Spesso comunque si preferiva per semplicità la vecchia sostituzione *monoalfabetica,* ed i Rossignol, padre e figlio, riuscirono ad elaborarne una versione quasi inattaccabile. Il sistema, chiamato *omofonico*, fu utilizzato da Re Sole per la sua corrispondenza di stato. Alla sua morte si persero le chiavi e le lettere di Luigi rimasero inaccessibili agli storici per oltre 2 secoli, fino a quando il crittografo Étienne Bazeries riuscì venirne a capo nel 1889.
Fra i tanti documenti finalmente *in chiaro* uno sembra svelare il mistero della Maschera di Ferro, la cui identità fu attribuita ad un gemello del Re tenuto nascosto per evitare pretese al trono. Una lettera indica che potesse invece trattarsi del generale Vivien de Bulonde, accusato di codardia durante l'assedio di Cuneo. La missiva riporta infatti: *"Sua Maestà desidera che arrestiate subito il generale Bulonde e lo facciate condurre alla fortezza di Pinerolo, dove di notte resterà chiuso in una cella mentre di giorno potrà passeggiare sugli spalti portando una maschera"*. Data e luogo corrispondono anche se i romantici preferiscono ancora oggi versioni più fantasiose.

Intorno al 1400 si diffuse anche l'uso del *nomenclatore*, sistema nel quale si utilizza un alfabeto di fantasia concordato fra mittente e destinatario. Il nome deriva dall'addetto che presentava i nobili e i dignitari al Re: all'inizio si cifravano infatti solo i nomi dei personaggi importanti ma in seguito, per rendere difficoltosa l'analisi delle frequenze, anche le vocali e le consonanti più ricorrenti. Alcune parole venivano sostituite con un solo simbolo, diventando più propriamente dei nomi in codice, ma neanche con queste complicazioni aggiuntive il *nomenclatore* resiste all'analisi delle frequenze.



Il nomenclatore dell'ambasciatore veneziano Michele Steno, 1411

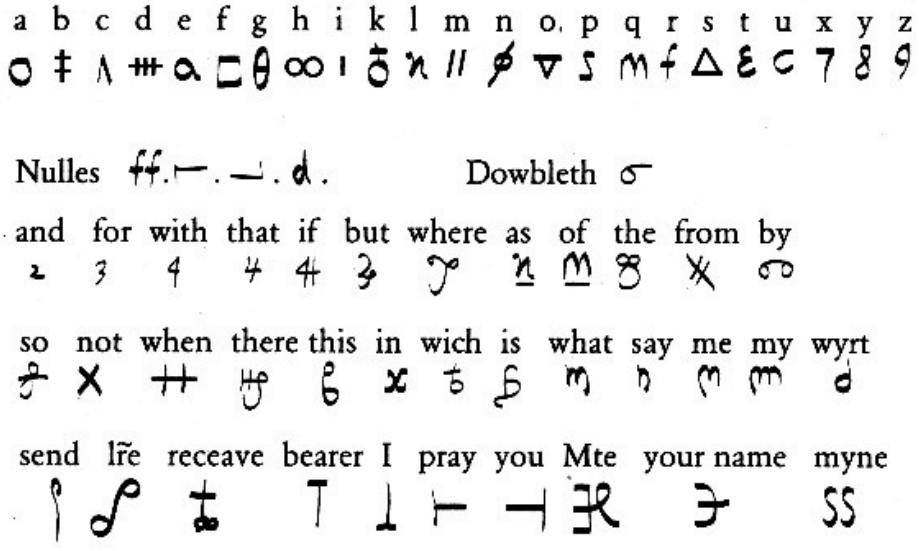
Il codice non è una vera forma di crittografia, ma piuttosto una lingua in cui le parole hanno un significato diverso da quello usuale. In pratica cifrando sostituiamo le lettere, codificando le parole. Se nel nostro codice “attaccare” = “sole” e “immediatamente” = “nero” il messaggio diverrà “SOLE NERO”, indecifrabile senza consultare il *nomenclatore* corrispondente. Sembrerebbe un vantaggio, ma bisogna distribuire voluminosi *nomenclatori* e se uno solo fosse scoperto bisognerebbe riscriverlo e ridistribuirlo.

Solo gli agenti segreti, come James Bond = 007, hanno quindi nomi in codice in quanto questo metodo è utilizzato principalmente per nascondere le identità o per aumentare la sicurezza di altri sistemi: criptando per *sostituzione* di lettere possiamo inserire delle parole in *codice* per confondere gli analisti.

Scheda - Il nomenclatore di Maria Stuarda

Durante la sua lunga prigionia Maria Stuarda criptava tutta la corrispondenza con i suoi alleati, capeggiati da Anthony Babington, che la volevano porre sul trono d'Inghilterra uccidendo Elisabetta I.

La Regina di Scozia utilizzava un misto di *nomenclatore*, *codice* e cifratura per *sostituzione* inserendo inoltre svariate lettere *nulle*, ma il crittoanalista di corte Thomas Phellipes usò con destrezza l’analisi delle frequenze riuscendo a decifrare le sue missive. Non vi erano però mai accenni diretti all'assassinio di Elisabetta, e quindi Phelippes aggiunse un poscritto compromettente prima di consegnare l'ultima lettera decifrata agli inquisitori. Pochi giorni dopo Babington fu arrestato e condotto nella Torre di Londra dove confessò l'intero piano. L'esecuzione della cospiratrice avvenne l’8 febbraio 1587, ma Elisabetta morì senza eredi e il figlio di Maria divenne il primo Re Stuart d'Inghilterra, avverandosi così il motto della madre: *En ma Fin gît mon Commencement* (Nella mia Fine è il mio Principio).



La complicata cifra di Maria Stuarda non fu sufficiente a salvarle la vita

Nel ‘700 ogni grande potenza europea aveva la sua *camera nera* per la decifrazione dei messaggi in codice e la raccolta di informazioni riservate. La più organizzata fu la viennese *Geheime Kabinettes Kanzlei*, che funzionava in base ad una ferrea tabella di marcia: la corrispondenza per le ambasciate era dirottata alla *camera nera*, trattenuta il tempo necessario alla copiatura e consegnata entro le sette di mattina. Le copie venivano quindi passate ai crittoanalisti per la decrittazione.

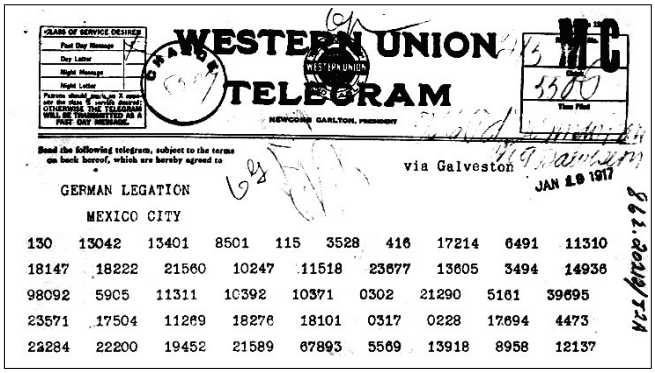
Dalla metà del XIX secolo la crittografia assunse un ruolo determinante nella trasmissione dei messaggi: l'uso del telegrafo e della radio rendevano infatti facili le intercettazioni, ma rimanevano in uso le varianti della tavola di Vigenere, di cui da tempo Friedrich Kasiski aveva scoperto un metodo rapido di decrittazione. In pratica i sistemi per criptare erano rimasti al palo mentre i crittoanalisti sfornavano nuovi metodi per *forzarli*. I Governi continuavano però ad illudersi di poter comunicare senza essere scoperti, causando incidenti anche clamorosi: nel gennaio del 1917 un telegramma inviato dal Ministro degli Esteri dell’Impero Tedesco, Arthur Zimmermann, all’ambasciatore tedesco in Messico venne intercettato dagli inglesi e decifrato in pochi giorni nella loro *camera nera*, la famosa *“Room 40”*.

Il contenuto era esplosivo: i tedeschi preparavano un attacco sottomarino globale e, temendo che gli Stati Uniti entrassero in guerra, proponevano ai Messicani di attaccarli a sud per distrarne le forze.

La situazione era imbarazzante per gli inglesi: il messaggio era sotto copertura diplomatica USA e desideravano non far sapere ai tedeschi che potevano decifrare le loro comunicazioni diplomatiche.

Il telegramma venne quindi passato agli americani, che dichiararono di averlo intercettato e decrittato in Messico (senza quindi violare la copertura diplomatica negli USA), ed il 1 marzo 1917 il presidente Wilson ne divulgò il contenuto. Zimmermann dovette ammettere di esserne stato l’autore e gli americani, già esacerbati per la morte di molti concittadini nell'affondamento del transatlantico Lusitania da parte del sommergibile tedesco U-20*,* dichiararono guerra alla Germania. Un risultato esattamente opposto al desiderato ed anche un errore strategico: il Messico, in piena rivoluzione, non poteva intraprendere la *“Reconquista”* dei territori perduti con l'invasione statunitense del 1846.

Scheda - Il Telegramma Zimmermann



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
22284	22200	19452	21589	67893	5569	13918	8958	12137	

Particolare del telegramma originale e la proposta tedesca di aumento territoriale per il Messico: in verde il territorio originale, in rosso gli Stati da riconquistare

A partire dal 1° febbraio intendiamo avviare una guerra sottomarina ad oltranza. Nonostante ciò cercheremo di mantenere gli Stati Uniti neutrali. Nel caso ciò non si verificasse faremo al Messico una proposta di alleanza sulle seguenti basi: gestione congiunta della guerra, gestione congiunta della pace, offerta di un generoso aiuto economico e il nostro riconoscimento della riconquista del Texas, del Nuovo Messico e dell'Arizona. I dettagli conclusivi potrà definirli Lei.

Lei informerà il Presidente (del Messico) di quanto sopra con la massima segretezza non appena l' entrata in guerra degli Stati Uniti sarà certa, aggiungendo che egli dovrebbe, di sua iniziativa, invitare il Giappone ad aderire immediatamente e nello stesso tempo mediare tra noi e il Giappone.

Richiami l'attenzione del Presidente sul fatto che l'impiego ad oltranza dei nostri sottomarini offre l'opportunità di costringere l'Inghilterra a firmare la pace entro pochi mesi. Accusare ricevuta. Zimmermann.

La fine di questi antichi sistemi arrivò nella seconda guerra mondiale: i messaggi diretti ai sommergibili tedeschi contenevano spesso istruzioni valide per più di un mese: vi era quindi il tempo per *violarli* ed occorreva una cifra che potesse reggere ad attacchi così prolungati.

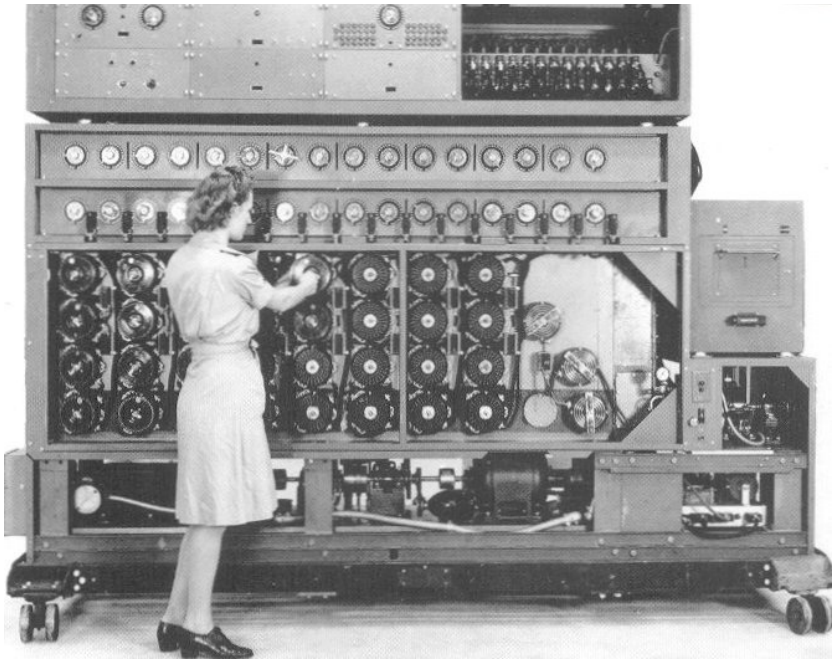
La tattica della guerra lampo (blitzkrieg) di Hitler si basava proprio sulla velocità di spostamento e la segretezza nelle comunicazioni. Per raggiungere questo scopo i tedeschi utilizzarono il disco di Alberti ed il sistema di Vigenère coniugati alle moderne tecnologie creando Enigma, una macchina che permetteva cifrature molto più sicure. I primi esemplari avevano solo tre dischi cifranti e si poteva sperare di accedere al messaggio ogni 10 milioni di miliardi di tentativi, ma nei successivi modelli i dischi montati erano 8 …
Il funzionamento è complicatissimo, ma in sintesi la macchina era composta da una tastiera, tre o più dischi rotanti per immettere la chiave, un display per leggere il risultato e degli spinotti che avevano l'effetto di scambiare tra loro due lettere (con l'uso dei 6 spinotti la complessità saliva di circa 100 miliardi di combinazioni). In pratica battendo una lettera questa veniva criptata con un altra e si accendeva la corrispondente lampadina per indicarla. Il messaggio veniva quindi scritto a penna lettera per lettera ed inviato. Per decifrarlo bisognava disporre di una macchina uguale e conoscere la posizione iniziale dei rotori e degli spinotti: battendo il crittogramma si accendevano una ad una le lampadine del testo in chiaro. Una comunicazione come questa *"avvistati 16 - 20 mercantili nella griglia ca 9133, firmato u-999"* diveniva "RDF QRLE ATMG SIKR ODX RDF" (inutile contare le lettere, in tedesco il messaggio è più sintetico): davvero impenetrabile!

Enigma: si notano la tastiera, le lampadine, i rotori e un particolare degli spinotti

Decrittare i messaggi prodotti da Enigma era quasi impossibile e, poiché gli attacchi dei sommergibili stavano seriamente impedendo i rifornimenti all'Inghilterra, il governo creò il centro di *Bletchley Park* dove radunò i migliori matematici, enigmisti e linguisti. Fu qui che Alan Turing, considerato il padre del computer, riuscì a costruire le famose *Bombe*, elaboratori analogici in grado di venire a capo delle cifrature tedesche decifrando oltre 4.000 messaggi al giorno. Un compito titanico.

Operatore Enigma sul sottomarino tedesco U-124

Oltre che alla potenza di calcolo ci si appigliava ad ogni più piccolo indizio, si supponeva per esempio che un sommergibile comunicasse per prima cosa la posizione, e quindi le prime lettere del messaggio potevano essere “latitudine” o “lat”, e si provavano migliaia di queste combinazioni. In questo modo si riuscirono a decifrare molti dispacci tedeschi ed italiani ma il compito era così difficile che, trovata la chiave, i comandi lasciavano talvolta silurare navi poco importanti pur di non far insospettire il nemico facendogliela così cambiare. Un serio problema morale, ma si stima che il lavoro svolto a *Bletchley Park* abbia accorciato la guerra di almeno due anni salvando così innumerevoli vite. Nel 1944 venne infine realizzato, da parte di Tommy Flowers e Max Newman, un computer della potenza equiparabile ad un notebook dei primi anni '90. Chiamato Colossus per le sue dimensioni era così potente da poter decifrare i messaggi super criptati dello stato maggiore tedesco. Distrutto per motivi di segretezza alla fine della guerra è oggi ricostruito al museo di *Bletchley Park.*

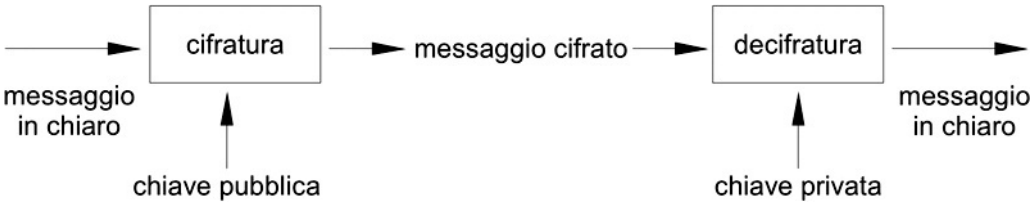


Una “bomba” al lavoro per decrittare un messaggio. Il curioso soprannome era dovuto al continuo ticchettare dei meccanismi

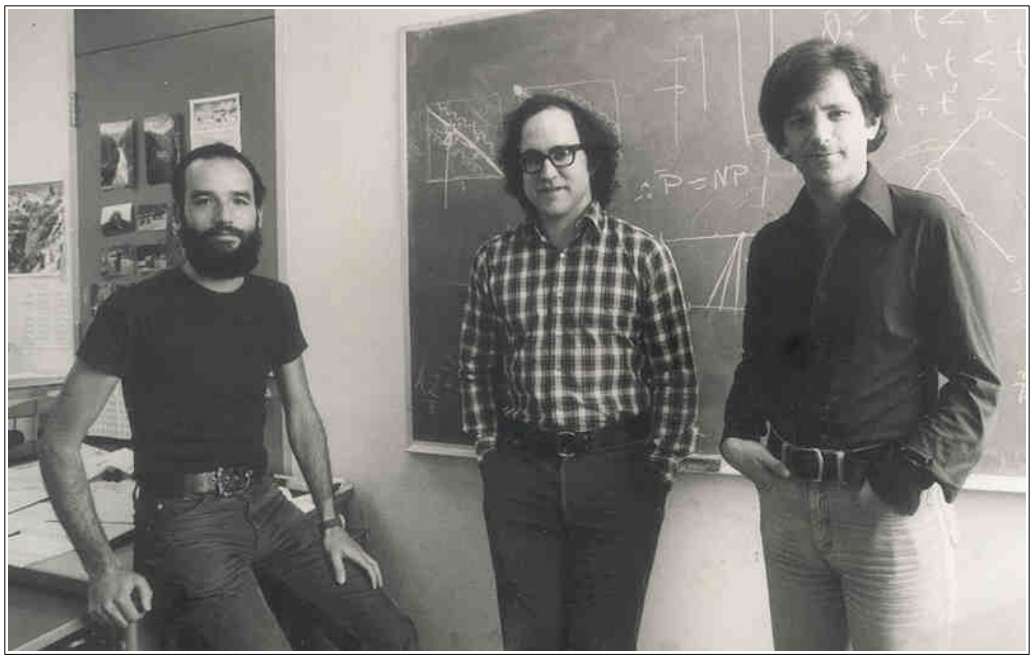
Divertente ricordare come talvolta le barriere linguistiche siano assolutamente insuperabili: durante la velocissima avanzata nel Pacifico le truppe americane scambiavano migliaia di messaggi al giorno e non vi era tempo per criptare, decrittare o distribuire macchine tipo Enigma. Utilizzarono quindi radio operatori di etnia Navajo, la loro lingua non era mai stata studiata e nessuno ne aveva compilato un dizionario: i dispacci trasmessi in navajo rimasero sempre incomprensibili per i giapponesi!

Operatori radio Navajo

Dopo la guerra i computer permisero di elaborare ottime crittografie, sempre derivate dai sistemi di Alberti e di Vigenère, ai quali si applicava una chiave, o *verme*, molto lunga. Negli anni '70 però la diffusione delle carte di credito rese necessarie innumerevoli transazioni protette, ma per l'invio della chiave si doveva ricorrere a corrieri privati che non garantivano sufficiente rapidità e sicurezza. I computer, inoltre, permettevano ormai di tentare milioni di chiavi in tempi brevissimi.
Era considerato un assioma che, dato un sistema di cifratura, la chiave per criptare e decriptare dovesse essere sempre la stessa: nel 1976 Withfield Diffie, Martin Hellman e Ralph Merkle immaginarono che si potesse scomporre il procedimento in due parti, creando una chiave solo per cifrare da rendere pubblica, ed una solo per decifrare, o privata, da conservarsi. In pratica è come se distribuissi diversi lucchetti aperti di cui solo io conosco la combinazione: chiunque può prendere una scatola, inserirci il messaggio, chiudere il lucchetto e spedirmela. Mi arriveranno tante scatole chiuse con lucchetti di cui solo io posseggo la combinazione in grado di aprirli.



Non si conosceva però il modo pratico per creare una chiave di questo tipo e nel 1977 Ronald Rivest, Adi Shamir e Leonard Adleman proposero questo sistema: si prendono due numeri primi e si moltiplicano (es. 17.159 x 10.247), il numero ottenuto, 175.828.273, non è facilmente scomponibile nei fattori usati per produrlo e questa sarà la chiave che posso distribuire a tutti affinché criptino un messaggio e me lo inviino. Per risalire ai due numeri primi usati come fattori, se questi sono abbastanza grandi, un computer necessiterebbe di milioni di anni.
La semplicità di questa spiegazione non deve far sottovalutare lo sforzo intellettuale che fu necessario per creare l'attuale sistema di *cifratura asimmetrica*, chiamato RSA dal nome degli inventori, e se questi studiosi hanno raggiunto fama planetaria negli ambienti scientifici il pubblico ignora chi ha creato i suoi strumenti di uso quotidiano. Questa tecnologia permette infatti i quotidiani acquisti con la carta di credito, la firma digitale e la posta elettronica certificata.

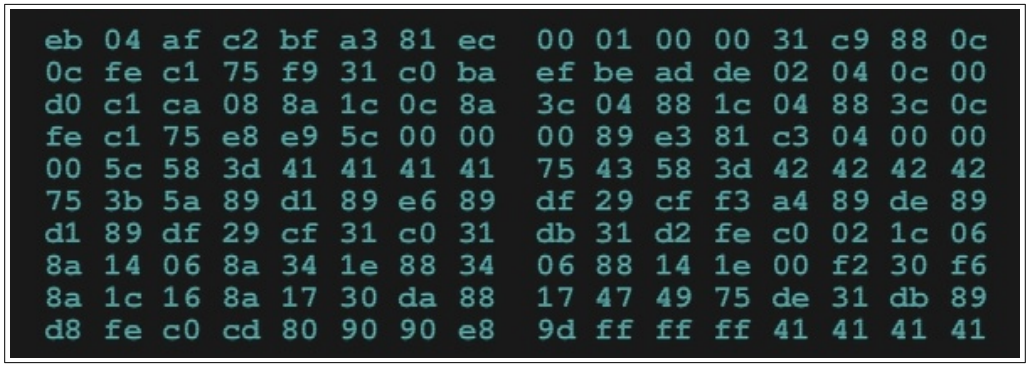


Shamir, Rivest e Adleman hanno rivoluzionato il mondo degli acquisti

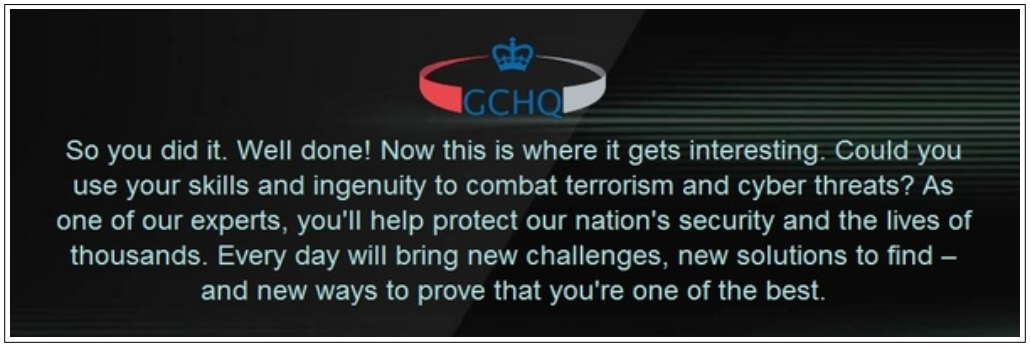
La guerra fra crittografi e crittoanalisti non è ancora finita e prosegue con lo sviluppo dei computer quantici, nei quali i bit sono sostituiti da qubit (quantum-bit) capaci di aumentare la potenza di calcolo al punto di poter scomporre in poche ore chiavi pubbliche lunghissime.

Il computer quantico di Google lavora alla temperatura di -232 celsius!

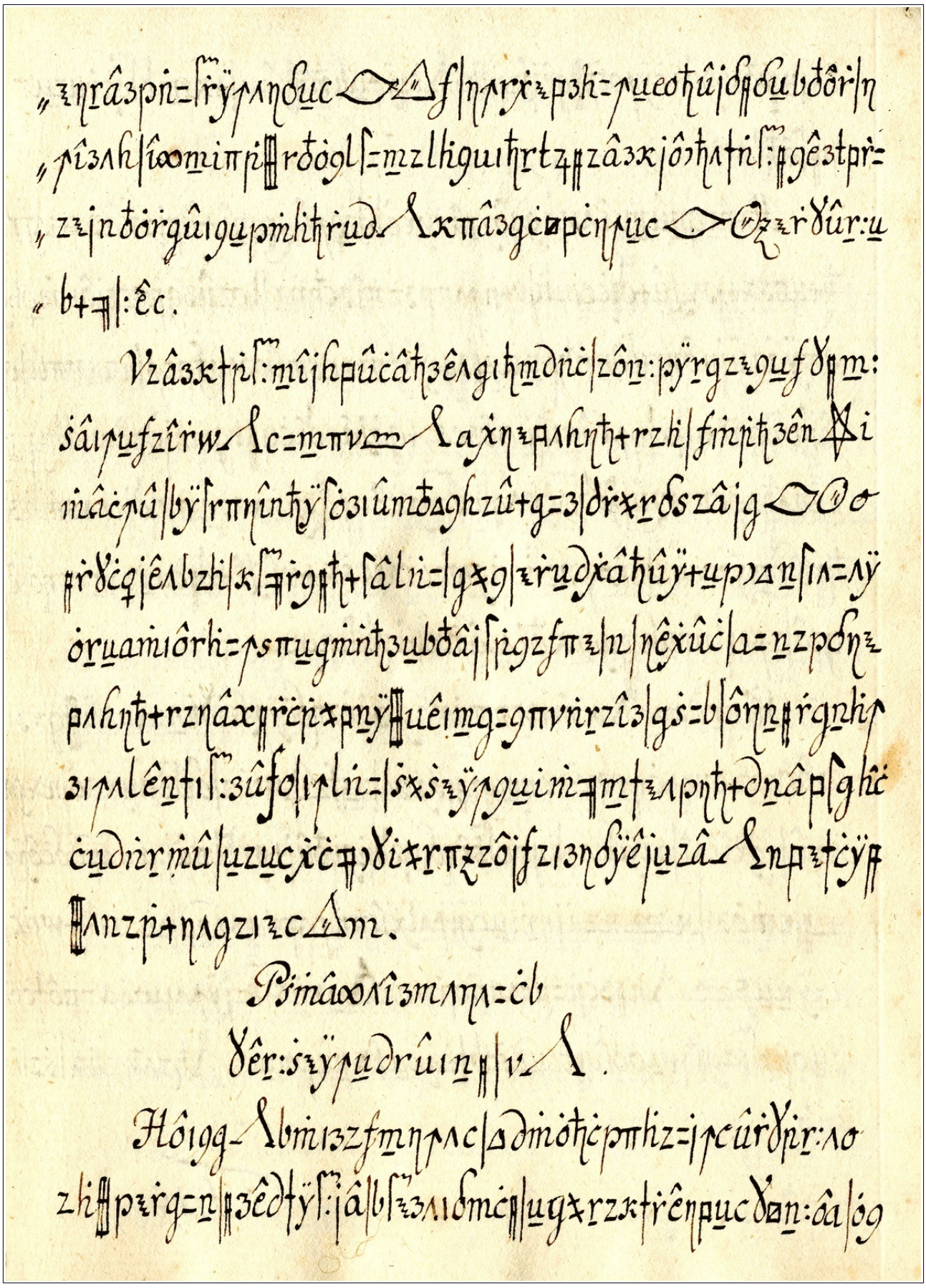
Il concetto di computer quantico fu ipotizzato da Richard Feynman nel 1982 e, nonostante la sua base teorica sembri una sfida al buon senso, dal 2011 la D-Wave Systems commercializza (per 10 milioni di dollari) un modello a 512 qubit subito acquistato dalla Lockheed Martin proprio per creare un nuovo sistema di sicurezza informatica. E' una competizione agguerrita che assomiglia ad una lotta evolutiva e già si profila la post-quantum cryptography, che non potrà essere decifrata con i computer quantici: cosa mai ci riserverà il futuro?



Questo è il test online per essere assunti come analisti al GCHV (Quartier Generale Governativo per le Comunicazioni inglese). Volete provare?



Nel caso riusciste a risolverlo apparirà questa schermata: è un lavoro duro per gente motivata, ma gli stipendi sono altissimi



Il manoscritto del *Copiale Cypher*, 1730: venne criptato con tanta perizia che fu possibile decifrarlo recentemente solo con l'ausilio del computer

Kryptos, scultura di Jim Sanborn posta nell'ingresso della CIA a Langley nel 1990: contiene un messaggio di 869 lettere, che gli analisti non sono ancora riusciti a decifrare integralmente