

CRITTOGRAFIA: IL PASSATO

Introduzione

La crittografia è una parola di origine greca col significato di “scrittura nascosta o segreta”. L’arte di scrivere messaggi segreti che potevano essere letti esclusivamente da coloro a cui erano diretti risale all’antichità. La più antica forma conosciuta di crittografia è la *scitala lacedemonica*, secondo Plutarco usata ai tempi di Licurgo (IX secolo a.C.) ma più sicuramente a quelli di Lisandro (verso il 400 a.C.). Però già ai tempi degli antichi Egizi si tendeva a modificare volontariamente il testo delle tombe (faraone Knumotete II 1900 a.C.).

Nel tempo questa arte è stata di quasi esclusivo appannaggio dei militari e dei diplomatici, e i metodi crittografici erano specifici per l’invio di messaggi materiali affidati a corrieri.

Nel XX secolo, però, prima l’invenzione della radio e quindi la possibilità di trasmettere informazioni attraverso l’uso di onde elettromagnetiche, e poi quella del computer con la possibilità di raggiungere tramite collegamento Internet qualunque zona del mondo, ha radicalmente modificato lo scenario. La necessità di comunicare informazioni in modo riservato si è ampliata notevolmente. Oggi l’utente del Bancomat, chi acquista su Internet con carta di credito e chi ha conti bancari su Internet fa uso, spesso senza saperlo, di tecniche crittografiche.

La sicurezza nella trasmissione dei dati anche attraverso una rete locale richiede di adottare misure atte alla protezione dei dati da intrusioni o da un loro utilizzo non consono da parte degli operatori e legittimi possessori. In questo periodo sono due le forme di crittografia più utilizzate: la crittografia a chiave simmetrica o segreta e la crittografia a chiave pubblica o asimmetrica, cui sono strettamente legati argomenti quali la firma digitale e la certificazione.

Informazioni o file trasmessi attraverso un supporto elettronico senza protezione possono essere intercettati, letti e/o modificati senza che i diretti interessati, trasmittente e ricevente, si accorgano di nulla. Per evitare queste possibilità si utilizzano degli algoritmi che criptano tali informazioni.

Va detto che non esiste una soluzione che garantisca la sicurezza dei dati al 100% ma esistono vari metodi con diversi gradi di sicurezza a cui corrispondono ovviamente diverse tipologie di

CRITTOGRAFIA: IL PASSATO

costo. Sta all'utente valutare il giusto rapporto tra costo e grado di sicurezza. C'è da dire che esistono software Open Source e/o con licenza GPL che garantiscono il massimo di sicurezza con costo nullo sfruttando quello che è al momento il sistema operativo migliore in assoluto perché free e in continuo miglioramento sia per reti sia su desktop (GNU/Linux).

Tutte le diverse tecniche sempre più ricercate, utilizzate per un sicuro invio di un messaggio, (inteso in generale come unità informativa da trasmettere e da proteggere) fanno parte della crittografia. Invece, lo studio dei metodi d'attacco o "brute force" atti a ricavare le chiavi di decifrazione dai messaggi cifrati viene chiamato crittanalisi. L'insieme della crittografia e della crittanalisi formano la crittologia.

Cenni storici

Si è detto che la prima forma conosciuta di crittografia è la *scitala lacedemonica*. Consisteva in un bastone su cui si avvolgeva ad elica un nastro di cuoio. Su tale nastro si scriveva per colonne parallele all'asse del bastone, lettera per lettera, il testo da rendere nascosto. Tolto il nastro dal bastone, il testo vi risultava trasposto in modo regolare ma sufficiente per evitare la lettura del messaggio senza un altro bastone di dimensioni uguali al primo. Si tratta di una forma di crittografia a **trasposizione**.

Tra il 360 ed il 390 fu compilato da Enea il tattico, generale della lega arcadica, il primo trattato di cifre il cui XXI capitolo tratta proprio di messaggi segreti. In questo viene descritto un disco con 24 fori nella sua parte esterna, ciascuno corrispondente ad una lettera dell'alfabeto e con un foro centrale. Un filo, partendo dal foro centrale, si avvolgeva passando per i fori delle successive lettere del testo. All'arrivo, riportate le lettere sul disco, si svolgeva il filo segnando le lettere indicate. Il testo si doveva poi leggere al contrario. Spesso gruppi di puntini sostituivano le vocali.

Vennero ideati codici cifrati indiani ed ebraici utilizzati per celare nomi innominabili o sacrileghi.

CRITTOGRAFIA: IL PASSATO

Numerosi testi greci antichi contengono tratti cifrati, specialmente nomi propri, ma si trovano anche interi scritti cifrati con sostituzione semplice.

Cifrari per trasposizione

I sistemi di trasposizione letterale consistono nel rimescolare secondo una regola reversibile i caratteri di un testo chiaro. In altre parole il testo cifrato è un anagramma ovvero una permutazione del testo originale.

La permutazione può basarsi su una parola chiave (trasposizione con chiave) o su un qualche dispositivo meccanico come il bastone di Licurgo o su griglie.

Mostriamo un esempio di cifrario basato sulla trasposizione con chiave dei caratteri di un testo.

Si sceglie la parola chiave di n caratteri e possibilmente senza doppie; si divide il messaggio in chiaro¹ in gruppi di n caratteri riempiendo eventualmente di x l'ultimo gruppo per completarlo ed eliminando tutti gli spazi. Si riordinano le colonne così ottenute in ordine alfabetico relativo alla parola chiave e si ottiene il messaggio cifrato o criptato leggendo le colonne così ordinate.

Esempio: la scuola inizia a settembre

Parola chiave: nicola

n i c o l a

l a s c u o

l a i n i z

i a a s e t

t e m b r e

Riordinamento:

a c i l n o

¹ Significa che il messaggio non è stato ancora criptato.

CRITTOGRAFIA: IL PASSATO

o s a u l c

z i a i l n

t a a e i s

e m e r t b

Il messaggio cifrato è il seguente: **aoztecsiamiaaaeluiernllitocnsb.**

La trasposizione con chiave produce un codice cifrato molto debole, ma è stata spesso usata insieme ad altre cifrari per rafforzarne la sicurezza. Si parla in questo caso di sovracifratura.

Sistemi a griglia sono stati proposti anche in tempi recenti come è il caso della griglia Patronen-Geheimschrift inventata nel secolo scorso da Eduard von Fleissner, e delle griglie indefinite inventate da Luigi Sacco durante la I Guerra Mondiale.

Le griglie

Le griglie sono sistemi per trasposizione semplici; consistono in un cartoncino o lamina di legno o metallica con una serie di fori. Il messaggio in chiaro viene scritto nei fori secondo una certa regola e il messaggio cifrato si ottiene leggendo i caratteri secondo una diversa regola o muovendo la griglia secondo un ordine stabilito. Per decifrare si segue ovviamente il procedimento inverso.

Le griglie classiche sono: le griglie quadrate a rotazione e le griglie rettangolari indefinite.

Le prime permettono di cifrare un messaggio per trasposizione; consistono in un quadrato di cartone o altro materiale con una serie di fori quadrati. I fori devono essere un quarto del numero totale di caselle disponibili e devono essere disposti in modo da coprire tutte le caselle del quadrato una e una sola volta in quattro successive rotazioni di 90°.

Per cifrare si deve disporre la griglia su un foglio di carta e si scrive la prima parte del messaggio nei fori disponibili per righe fino ad esaurimento dei fori. Adesso, si ruota di 90° la griglia e si continua a scrivere e a ruotare fino ad esaurimento del messaggio. Se il messaggio è più breve del

CRITTOGRAFIA: IL PASSATO

numero totale di caselle, si possono riempire le caselle restanti con delle X; se, invece, il messaggio è più lungo si può ricominciare dalla posizione iniziale.

Per decifrare si scrive il messaggio sul quadrato di carta e lo si copre con la griglia, ruotandola successivamente e leggendo così il messaggio chiaro.

Il messaggio che si vuole cifrare è, per esempio, ARRIVANO I NOSTRI con una griglia quadrata di ordine 4, come si vede dalla fig.1.

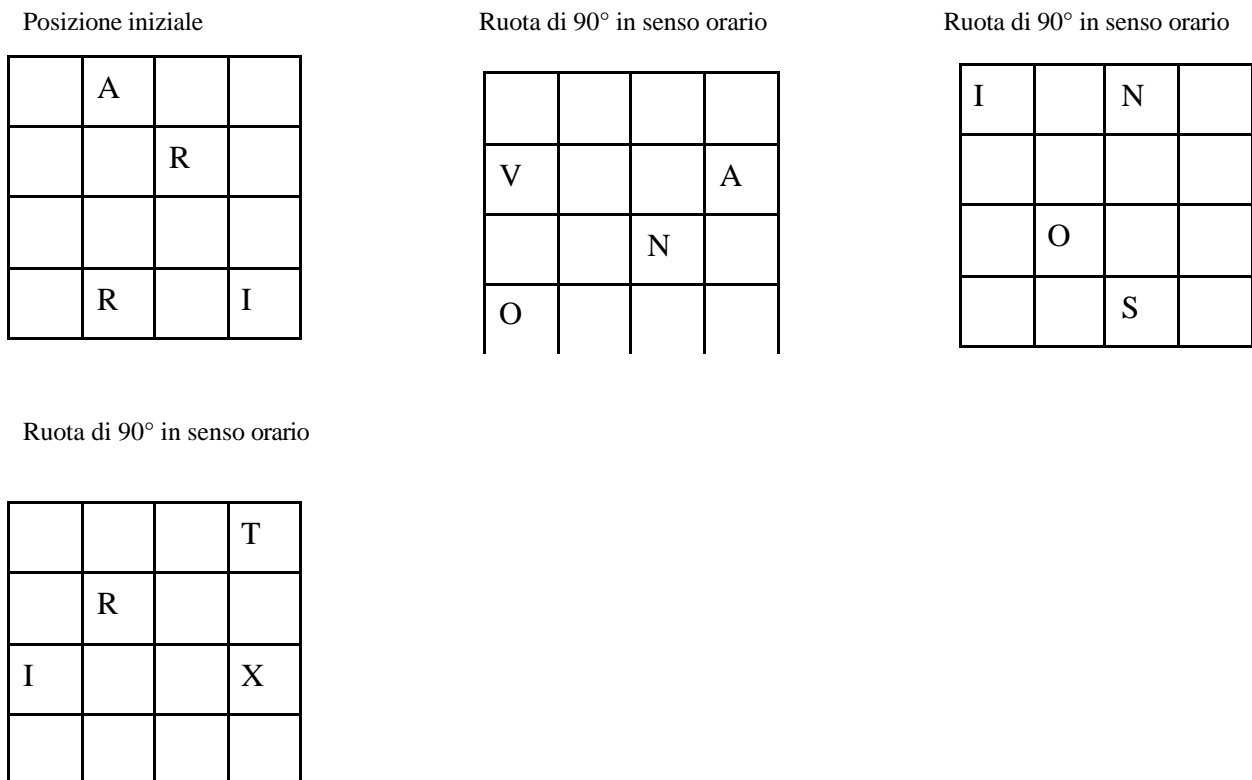


Fig.1 – Esempio di griglia quadrata di ordine 4.

Le griglie indefinite, invece, sono griglie rettangolari ad altezza fissa e a larghezza indeterminata. I fori sono disposti in modo del tutto casuale per un numero di colonne sufficiente per la lunghezza massima di un messaggio. Il numero di fori per colonna deve essere costante.

CRITTOGRAFIA: IL PASSATO

Per cifrare un messaggio si scrivono i caratteri in verticale, colonna per colonna, fino alla fine; il messaggio cifrato scaturisce dalla lettura dei caratteri riga per riga.

Per decifrare si scrive il messaggio cifrato per righe fino alla colonna n-ima; il numero di colonne si ricava in modo estremamente semplice dividendo la lunghezza del messaggio per il numero di fori per colonna.

Le griglie indefinite hanno un grado di sicurezza superiore a quelle quadrate essendo maggiore il numero delle possibili combinazioni.

Supponiamo di dover trasmettere il messaggio in chiaro: ELETTROTECNICA VITA MIA.

La griglia la fissiamo di altezza 6 con tre fori per colonna; è chiaro che il numero di colonne è pari a 7 (21 caratteri diviso tre), come da fig.2:

	T		C				
E	T			C	I		
		O	N		T	M	
L				A	A		
E		T	I			I	
	R	E		V		A	

Fig.2 – Esempio di griglia indefinita.

Il cifrato risulta essere: **TCETCIONTMLAAETIIREVA.**

Il cifrario Atbash

Il codice scriba Atbash, utilizzato per cifrare il libro Biblico di Geremia, è un primo esempio di cifratura per sostituzione. Il nome di questo cifrario deriva dal fatto che la prima lettera

CRITTOGRAFIA: IL PASSATO

dell'alfabeto ebraico (Aleph) viene cifrata con l'ultima lettera (Taw), la seconda (Beth) con la penultima (Shin). Pertanto, un codice per sostituzione, in generale, sostituisce una lettera dell'alfabeto con un'altra lettera secondo una regola fissa ed è per questo che tali cifrari sono chiamati monoalfabetici. Per il moderno alfabeto la regola viene riassunta con la seguente tabella di cifratura:

chiaro: 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

cifrato: z y x w v u t s r q p o n m l k j i h g f e d c b a

Come esempio di messaggio si consideri: Il libro biblico di Geremia, che diventa:

Ro oryil yryoxl wr Tvivnrz.

Il caso più generale di codice monoalfabetico è quello che prevede di usare come tabella di cifratura una arbitraria permutazione dell'alfabeto. In ogni caso, questo tipo di cifra è sicura solo per messaggi molto corti. Infatti, più i messaggi sono lunghi, cioè hanno più parole da trasmettere più, vedremo, sarà facile riuscire a trovare la tabella di cifratura stabilita².

La scacchiera di Polibio

Il più antico codice poligrafico (sostituzione di tipo multiplo) e monoalfabetico è molto probabilmente la *scacchiera di Polibio*. Lo storico greco Polibio (~ 200 – 118 a.C.), nelle sue Storie (Libro X) descrive un cifrario che attribuisce ai suoi contemporanei Cleoxeno e Democleito. L'idea è di cifrare una lettera dell'alfabeto con una coppia di numeri compresi fra 1 e 5, secondo la descrizione di una scacchiera 5x5. Il messaggio, che poteva essere qualsiasi e di qualsiasi lunghezza, era trasmesso con due gruppi di cinque torce. Una scacchiera per l'alfabeto moderno (mettendo insieme nella stessa casella i due caratteri meno utilizzati: k e q) è la seguente:

² Vedere il capitolo relativo alla crittanalisi.

CRITTOGRAFIA: IL PASSATO

#	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	kq	l	m	n	o
4	p	r	s	t	u
5	v	w	x	y	z

Se la disposizione delle lettere nella tabella non segue l'ordine alfabetico cresce la difficoltà di trovare la chiave che, in questo caso, ovviamente è la tabella stessa.

Esempio: domani verifica

143533111342451115422421241311.

La scacchiera di Polibio ha alcune importanti caratteristiche, e cioè la riduzione del numero di caratteri utilizzati nel messaggio cifrato (solo numeri dall'1 al 5), la conversione in numeri e la riduzione di un simbolo in due parti che possono essere utilizzati separatamente. La sua importanza nella storia della crittografia sta nell'essere alla base di altri codici di cifratura come il Playfair Cipher o il cifrario campale germanico usato nella prima guerra mondiale.

Il cifrario di cesare

Svetonio nella "Vita dei dodici Cesari" racconta che Giulio Cesare usava per le sue corrispondenze riservate un codice a sostituzione mediante trasposizione di lettera: ciascuna lettera era sostituita con quella ottenuta spostandola di un certo numero di posti (circolarmente) nella sequenza alfabetica. In origine il fattore di trasposizione era 3, ma poiché l'alfabeto internazionale è composto da 26 lettere sono possibili 26 codici di Cesare diversi.

Facciamo un esempio con un fattore di trasposizione pari a 3 per il messaggio in chiaro: tanti auguri.

CRITTOGRAFIA: IL PASSATO

La cifra è: **wdqwl dxjxul**.

Il cifrario di Augusto

Lo scrittore Robert Graves, biografo dell'imperatore Claudio, sostiene che Augusto e sua moglie Livia usavano un cifrario basato sul testo greco dell'Iliade. Il testo chiaro ed un brano dell'Iliade erano scritti in parallelo; ogni lettera del chiaro era confrontata con la corrispondente dell'Iliade, si calcolava la somma fra i numeri corrispondenti dei due caratteri in parallelo e la sequenza dei numeri così calcolati costituiva il messaggio cifrato. Nel caso in cui la somma supera 26, la lettera corrispondente viene determinata circolarmente utilizzando il procedimento della somma nella Aritmetica Modulare.

Il testo in chiaro che si vuole cifrare è: `il cifrario di agosto`.

Il brano segreto da utilizzare come chiave sono i primi versi dell'Inferno di Dante Alighieri.

Chiaro: `ilcifrariodiaugusto`

Chiave: `nelmezzodelcammini`

Cifra: `wqovkragmtplbhtdgxx`.

Si tratta di un cifrario polialfabetico che precorre di 1500 anni la tavola di Vigenere. I cifrari polialfabetici si differenziano da quelli monoalfabetici in quanto un certo carattere del testo chiaro non viene sempre cifrato con lo stesso carattere, ma con caratteri diversi in base alla parola segreta o brano da concordare.

In questo modo la sicurezza del codice aumenta in modo significativo; infatti non è più così semplice individuare le lettere del messaggio in base alla loro frequenza caratteristica di ogni lingua.

Pur essendo mediamente più sicuri dei monoalfabetici anche questi cifrari sono comunque attaccabili purché si abbia un testo cifrato sufficientemente lungo.

CRITTOGRAFIA: IL PASSATO

Sostituzione di blocchi di bit

I cifrari di sostituzione classici, monoalfabetici e polialfabetici, consistono nella sostituzione di una lettera con un'altra secondo una certa regola. Nella crittografia contemporanea, data la possibilità di utilizzare veloci e potenti computer, si preferisce la sostituzione per blocchi di bit.

E' noto che in ogni computer qualunque carattere è rappresentato con un codice ASCII a 7 o 8 bit e Unicode a 16 bit. Per cifrare un testo di caratteri si stabilisce una regola per sostituire un blocco di bit (0 o 1) del testo in chiaro con un altro diverso blocco ottenendo il testo criptato. E', altresì, ovvio che il livello di sicurezza resta sempre basso alla stregua di un codice monoalfabetico; pertanto, per aumentare il livello di sicurezza, occorre comporre in successione sostituzioni e altre trasformazioni.

Codici medievali e il disco cifrante di L.B.Alberti

Nel medioevo i cifrari sono soprattutto monografici: nomi e frasi convenzionali sono sostituiti da simboli speciali.

Un altro noto cifrario basato su macchinario fu il disco cifrante dovuto al famoso architetto Leon Battista Alberti. Il disco cifrante era composto da due dischi concentrici, uno esterno fisso con 24 caselle contenenti 20 lettere latine maiuscole (inclusa la Z, con U = V ed escluse H J K W Y) ed i numeri 1 2 3 4 per il testo in chiaro; ed uno interno mobile, con le 24 lettere latine minuscole per il testo cifrato. Le 20 lettere maiuscole erano messe in ordine alfabetico, mentre le 24 minuscole erano in disordine, ciò costituisce un passo avanti rispetto al codice di Cesare. Fissata una lettera maiuscola come indice si doveva spostare il disco mobile interno e scrivere, come prima lettera del crittogramma, la lettera minuscola corrispondente; quindi, cifrare alcune parole con la lista risultante. I quattro numeri servivano da caratteri nulli. Quando si decideva di cambiare la lista cifrante, si scriveva la nuova lettera chiave in maiuscolo. Quindi si portava quella lettera ad affacciare l'indice ed in questa nuova posizione si cifravano le altre parole secondo la nuova lista. Per aumentare la sicurezza l'Alberti suggeriva di usare uno dei quattro numeri per segnalare il cambio di alfabeto.

CRITTOGRAFIA: IL PASSATO**Le cifre di G.B. Bellaso**

Giovanni Battista Bellaso nacque a Brescia e pubblicò tra il 1553 e il 1564 tre opere di crittologia contenenti alcuni cifrari polialfabetici di notevole interesse.

Lo scopo è quello di ricavare diversi alfabeti disordinati da una parola chiave. Le lettere della parola segreta vengono scritte all'inizio a sinistra e intercalate su due righe. Le altre lettere dell'alfabeto vengono scritte di seguito sempre su due righe.

Prendiamo come esempio la seguente parola segreta: NICOLA, si ottiene il primo alfabeto derivato (alfabeto latino di 20 lettere con V = U, senza Z e con la X):

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

Il secondo alfabeto si ottiene spostando circolarmente la seconda riga:

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

e così via fino ad ottenere 5 alfabeti; ognuno di questi sarà identificato da un gruppo di quattro lettere, come nella tabella sottostante.

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

Adesso, è necessario utilizzare una frase segreta, per esempio: AUTOMA; le lettere di questo ultimo servono a selezionare l'alfabeto da usare.

Volendo, quindi, cifrare la frase "Soldati partono domenica" si ha:

CRITTOGRAFIA: IL PASSATO

verme ³ :	A	U	T
chiaro:	SOLDATI	PARTONO	DOMANI
cifrato:	HCBAMX	FEHNBTB	ACTDUX

Le cifre di Bellaso sono più deboli di quella dell'Alberti perché usano alfabeti invertiti e non del tutto arbitrari, mentre il cambio di lista non è segreto. Il Bellaso, comunque, sembra essere il primo crittologo moderno ad usare versetti o parole chiave come chiavi di cifratura; un uso poi diventato di moda a partire dal cifrario di Vigenere.

Le cifre di G.B. Porta

Giovanni Battista Porta (o Della porta) pubblicò nel 1563 a Napoli un trattato di crittografia “*De Furtivis literarum notis - vulgo de ziferis*” molto vasto e di ottimo livello. Tra le cifre proposte da Porta è nota soprattutto la *tavola* che non è certo tra le migliori di quelle presenti nel trattato e che è più debole di quella dell'Alberti e del Bellaso.

La tavola del Porta è molto simile a quella del Bellaso, ma usa 11 alfabeti invece di 5 ed usa il verme letterale, che ha il grave inconveniente di produrre un periodo di ciframento relativamente corto, perché comprende tante lettere quante ne ha il verme nel quale le liste cifranti si susseguono nello stesso ordine. Su questo fatto si basa la decrittazione del sistema.

In realtà il Porta consiglia di usare 11 alfabeti involuttori arbitrari, ma dà, come esempio la tavola con l'alfabeto base regolare: sotto questa sola forma la sua cifra è stata poi da tutti divulgata. Seguendo le indicazioni del Porta si scriverà la parola, o verme, lettera per lettera sotto ciascuna lettera del testo chiaro, ripetendola quante volte occorre: la cifratura si farà usando per ciascuna

³ Il verme è la frase segreta che si deve utilizzare. Vedremo che più è lunga meglio è.

CRITTOGRAFIA: IL PASSATO

lettera del testo chiaro la lista individuata dalla corrispondente lettera chiave, come nella tavola del Bellaso.

Il cifrario di Vigenere

Blaise de Vigenere pubblicò nel 1586 un trattato di codici cifrati dove proponeva un codice che ebbe una grande fama per la sua semplicità per vari secoli. Tale fama fu immeritata in quanto il cifrario era molto più debole di altri cifrari polialfabetici come quello del disco dell'Alberti o delle cifre del Bellaso. Vedremo nel capitolo della crittanalisi vari metodi di rottura del cifrario.

In ogni modo, dal cifrario di Vigenere deriva il cifrario di Vernam che è stato considerato l'algoritmo teoricamente perfetto.

Il metodo è in sostanza una generalizzazione del codice di Cesare, con la differenza che le lettere da cifrare non sono spostate dello stesso numero di posti, ma di un numero di posti variabile, determinato da una parola chiave (verme) che come al solito deve essere nascosta e conosciuta solamente dal mittente e dal destinatario. Tale parola deve essere scritta carattere per carattere sotto il testo da cifrare e quindi deve essere ripetuta fino al raggiungimento del testo in chiaro.

Il testo cifrato si ottiene spostando la lettera chiara di un numero fisso di caratteri pari al numero della lettera corrispondente del verme. In concreto si fa una somma aritmetica ricordando che si parte dalla $A = 0$. Sempre secondo lo studio delle aritmetiche finite, se si supera l'ultima lettera (Z) si ricomincia dall'inizio dell'alfabeto (A).

Come esempio, utilizziamo la frase in chiaro: ARRIVA NATALE, con il verme: PADRE.

Testo in chiaro: ARRIVANATALE

Verme: PADREPADREPA

Testo cifrato: PRUZZPNDKEAE

Il vantaggio rispetto ai codici monoalfabetici è che la stessa lettera del testo chiaro non ha sempre la stessa cifra. Questo rende più difficile la decrittazione, anche se non di tanto.

CRITTOGRAFIA: IL PASSATO

Chi riceve il messaggio deve fare l'operazione inversa, cioè sottrarre invece che sommare.

Il cilindro di Jefferson

Thomas Jefferson (1743 – 1826), Presidente degli Stati Uniti d'America dal 1801 al 1804 e uno degli autori della Dichiarazione d'Indipendenza inventò un codice semplice ma ancora oggi abbastanza sicuro. Molto stranamente non lo mise mai in uso e fu dimenticato fino al 1922, anno in cui l'esercito statunitense lo riscoprì e lo utilizzò fino agli anni '50.

Il codice di Jefferson è un metodo di cifratura meccanico basato su un cilindro lungo 15 cm e largo 4, montato su un asse e sezionato in 25 dischi uguali. Sull'esterno di ciascuna ruota sono scritte le 26 lettere dell'alfabeto equidistanti l'una dall'altra. L'ordine in cui sono disposte le varie lettere varia da ruota a ruota.

Il messaggio in chiaro deve essere cifrato a blocchi di 36 lettere ciascuno, se l'ultimo blocco ha meno lettere si completa con delle X. La chiave di cifratura è un numero che va da 1 a 25.

Supponiamo di dover trasmettere un messaggio in chiaro e la chiave sia il numero 6. In una riga qualsiasi componiamo il messaggio, togliendo ovviamente gli spazi, come fatto spesso fino ad ora. Il crittogramma corrispondente andrà letto sulla sesta riga sopra di quella che contiene il blocco in chiaro.

La decifratura avviene con il procedimento inverso; si compone il messaggio cifrato e si legge il testo in chiaro sei righe sotto.

Il più importante metodo di macchine cifranti, basate su cilindri e dischi rotanti intorno ad un asse, è la Macchina Enigma utilizzata dai tedeschi durante la Seconda Guerra mondiale.

Anche il cilindro di Jefferson ha il difetto di avere solo 25 chiavi e il crittogramma può essere risolto se si riesce ad avere il cilindro.

Playfair cipher

CRITTOGRAFIA: IL PASSATO

Il Playfair cipher è stato inventato dal fisico inglese Sir Charles Wheatstone (1802 – 1875), ma il suo nome deriva da Lyon Playfair, barone di St.Andrews, che lo mostrò ad una cena nel 1854 all'allora ministro degli esteri Lord Palmerston.

Il Cipher fu utilizzato dall'esercito britannico solo a partire dalla guerra Boera.

Il Playfair Cipher è una forma di cifrario poligrafico ed è il primo metodo di cifratura a bigrammi. Si usa una matrice di 25 lettere che viene riempita nelle prime caselle con la parola chiave, eliminando le eventuali lettere ripetute, ed è completata con le rimanenti lettere in ordine alfabetico. La W è omessa e se necessaria potrà essere cifrata con due V di seguito.

Una volta determinata la matrice, la cifratura si ottiene seguendo le regole:

1. Il testo in chiaro deve essere diviso in bigrammi di due lettere consecutive.
2. Le due lettere si cercano nel quadrato e sono sostituite con le altre secondo queste altre regole:
 - a. se le due lettere chiare si trovano su una stessa riga, si prendono le due lettere che le seguono a destra; se una delle due lettere chiare si trova sulla quinta colonna a destra, si prenderà la prima lettera a sinistra della stessa linea;
 - b. se le due lettere chiare sono sulla stessa colonna, si prendono le due lettere sottostanti; se una lettera è nell'ultima linea, si prenderà la lettera che sta nella prima linea della stessa colonna;
 - c. se le due lettere sono in colonne e linee diverse, si prendono le due che costituiscono un rettangolo con esse, cominciando da quella che si trova in linea (sulla riga) con la prima lettera del bigramma chiaro;
 - d. qualora il bigramma chiaro presenti due lettere uguali si cercherà di eliminare questo raddoppio, oppure di romperlo inserendo una lettera rara (k, w, x, y).

Facciamo l'esempio di voler trasmettere la frase in chiaro: ELETTROTECNICA CHE PASSIONE, con la parola chiave: EVOLUZIONE.

Si costruisce il quadrato 5x5: E V O L U

CRITTOGRAFIA: IL PASSATO

Z	I	N	A	B
C	D	F	G	H
J	K	M	P	Q
R	S	T	X	Y

Poi, dividiamo la frase in digrammi: EL ET TR OT EC NI CA CH EP AS SI ON E, quindi seguendo le regole succitate si ha: VU OR SX NO ZJ NA GZ DC LJ IX VD NFE.

Anche questo metodo di cifratura ha un difetto: le lettere più frequenti si trovano nelle righe in alto, mentre quelle rare si trovano nell'ultima riga. Questo fatto permette di ricostruire facilmente il quadrato e quindi di riuscire a decifrare il messaggio.

Il cifrario bifido di Delastelle

Il cifrario bifido di Delastelle, uno tra i massimi crittologi francesi del XIX secolo, è un altro cifrario poligrafico che utilizza una scacchiera 5x5. Il metodo si articola in tre passi:

1. Il messaggio in chiaro è spezzato in blocchi di cinque caratteri ciascuno; se l'ultimo blocco non è esattamente di cinque, gli ultimi posti sono riempiti di X.
2. Ogni lettera del blocco è cifrata con due cifre e cioè con l'indice di riga e l'indice di colonna, che sono scritte in verticale sotto la lettera del testo in chiaro.
3. Le cifre sono ora riscritte in orizzontale, riga dopo riga, ottenendo un messaggio con un numero di cifre doppio dell'originale. A questo punto ogni coppia di numeri viene ritrasformata in lettera sempre secondo la matrice di partenza. Ne risulta il messaggio cifrato da trasmettere.

La matrice può essere semplice e formata dall'alfabeto ordinato senza la W, che può sempre essere sostituita da due V, oppure può contenere, come nel cifrario di Playfair, una parola chiave.

Consideriamo la stessa parola chiave del Playfair e quindi la stessa disposizione delle lettere nella scacchiera:

1	2	3	4	5
---	---	---	---	---

CRITTOGRAFIA: IL PASSATO

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

La frase da trasmettere è: Necessaria una interrogazione.

N E C E S S A R I A U N A I N T E R R O G A Z I O N E X X X

2 1 3 1 5 5 2 5 2 2 1 2 2 2 2 5 1 5 5 1 3 2 2 2 1 2 1 5 5 5

3 1 1 1 2 2 4 1 2 4 5 3 4 2 3 3 1 1 1 3 4 4 1 2 3 3 1 4 4 4

Pertanto dal terzo passo, si ha:

21 31 53 11 12 52 52 22 41 24 12 22 25 34 23 51 55 13 11 13 32 22 14 41 23

Z C T E V S S I J A V I B G N R Y O E O D I L J N

21 55 53 14 44

Z Y T L P

Il Delastelle propose anche un cifrario trifido, cioè tridimensionale come un cubo di lato 3. In questo caso, si utilizzano 27 celle con un carattere di controllo. In questo caso ad ogni lettera corrisponde una terna di numeri.

Dal secolo XIX alla Prima Grande Guerra

Dalla metà del XIX secolo la crittografia assume un ruolo fondamentale per trasmettere messaggi di tipo militare che con l'invenzione e l'avvento della radio venivano emessi via etere e, quindi, esposti all'intercettazione del nemico molto più di una volta. I cifrari diventano sempre più essenziali e sofisticati in tutti gli stati tranne che in Italia dove solo dopo l'entrata in guerra nel 1915 si iniziò con molto ritardo a porvi rimedio.

CRITTOGRAFIA: IL PASSATO

Durante la Prima Guerra Mondiale, furono usati: il cifrario bifido di Delastelle, la cifra campale germanica e il Playfair cipher.

Il cifrario perfetto di Vernam

Come già detto, un cifrario si basa su un algoritmo che fornisce le regole di cifratura e di decifratura, e su una chiave che rende il risultato della cifratura dipendente dalla chiave stessa. Se la chiave è corta il livello di sicurezza è basso e il testo cifrato è facilmente decifrato con un "brute force".

Si può verificare che la sicurezza di un cifrario dipende dalla lunghezza della chiave; se questa fosse di lunghezza infinita o lunga quanto il messaggio, il livello di sicurezza sarebbe ottimale. E' questa l'idea di G.S. Vernam, nel 1916, per il cifrario che porta il suo nome, nel quale viene generata una chiave del tutto casuale, lunga quanto il testo in chiaro e poi sommata, come nel cifrario di Vigenere, allo stesso in modo da comporre il testo cifrato.

Claude Shannon, padre della teoria dell'informazione e delle telecomunicazioni, ha dimostrato nel 1949 che ogni cifrario teoricamente sicuro è un cifrario di Vernam e viceversa. Infatti, se la chiave è totalmente casuale e lunga quanto il messaggio in chiaro, allora il testo cifrato non contiene alcuna informazione sul testo in chiaro ed è del tutto sicuro nei confronti degli attacchi della crittanalisi statistica. Per avere una sicurezza assoluta non si dovrebbe mai usare la stessa chiave per più di una volta; se si utilizza più volte la stessa chiave, essa risulterebbe più breve della somma di tutti i messaggi ed il cifrario non può essere considerato più perfetto.

La chiave, però, deve essere nota sia al mittente che al ricevente. Trovare un canale sicuro per trasmettere la chiave è molto difficile. Potrebbe incontrarsi ogni tanto e generare una chiave lunghissima per poi spezzarla a pezzettini lunghi quanto i messaggi, fino ad esaurimento. Questi limiti rendono difficilmente utilizzabile questo metodo.

Si potrebbe semplificare il metodo generando una chiave pseudo-casuale secondo delle regole note. In questo modo però il cifrario non è più sicuro perché la chiave non è più lunga come il messaggio. Questi cifrari, detti pseudoperfetti, possono essere forzati dalla crittanalisi lineare.

CRITTOGRAFIA: IL PASSATO

Nonostante queste difficoltà, il cifrario di Vernam è stato effettivamente usato dai servizi segreti dell'Est durante la guerra fredda e per il telefono rosso tra Washington e Mosca. Un cifrario di Vernam è stato trovato nelle tasche del Che Guevara dopo la sua uccisione nel 1967.

La Prima Grande Guerra

Come detto, l'importanza della crittografia crebbe enormemente durante la I Guerra Mondiale. I francesi furono i primi a rendersi conto della situazione e disponevano di un efficiente ufficio cifra presso il quartiere generale dell'esercito già prima dello scoppio della guerra. E fin dall'ottobre 1914, i crittanalisti francesi erano in grado di decifrare i messaggi radio tedeschi. Il miglior crittanalista francese era un professore di paleontologia, Georges Painvin, che riuscì a decrittare la cifra campale germanica nel 1918.

Anche gli Austriaci erano altrettanto preparati, tanto da riuscire a decrittare i messaggi russi che per la verità erano solo in parte criptati.

Negli altri paesi veri e propri uffici cifra furono organizzati solo dopo l'entrata in guerra.

Assolutamente impreparati erano soprattutto i Russi che all'inizio della guerra non si preoccupavano neanche di cifrare i loro messaggi radio, come avvenne durante la battaglia di Tannenberg nell'agosto 1914 quando persino gli ordini operativi venivano trasmessi in chiaro; un formidabile regalo ai Tedeschi che intercettavano tutto.

I Tedeschi comunque riuscirono a decrittare i messaggi russi anche dopo che questi ultimi iniziarono a cifrare le loro comunicazioni radio; qualche successo lo ottennero anche nei confronti dei Francesi; il principale crittanalista tedesco fu il prof. Deubner.

In Inghilterra Sir Alfred Ewing organizzò la cosiddetta *room 40* dal numero della sua stanza negli uffici dell'Ammiraglio, ed ottenne grandi soddisfazioni nella decrittazione dei messaggi radio della marina tedesca. Il più importante fu sicuramente il "telegramma Zimmermann" con il quale i tedeschi offrivano ai messicani il loro appoggio contro gli Stati Uniti. Fu la lettura di tale messaggio decrittato al Congresso degli Stati Uniti che portò all'entrata in Guerra degli USA nel 1917.

CRITTOGRAFIA: IL PASSATO

Negli Stati Uniti non esisteva un ufficio cifra federale, ma una fondazione privata di Chicago fu promossa come tale. In tale fondazione lavorava colui che diverrà il più noto crittologo USA, William Friedmann.

Come già detto gli italiani erano del tutto impreparati in tale campo, tanto da doversi appoggiare ai francesi e solo dopo parecchio tempo sotto la guida di Luigi Sacco si ebbe un ufficio cifra autonomo.

In definitiva, la prima guerra mondiale ebbe il compito di mostrare a tutti gli Stati la necessità della crittografia, che fu utilizzata in modo massiccio nella Seconda Guerra Mondiale.

La II Guerra Mondiale

Se ne parla poco nei libri di scuola, ma la crittografia ha svolto un ruolo di primissimo piano per la vittoria degli alleati. La superiorità degli alleati in questo campo fu schiacciante fin dai primi anni di guerra.

I tedeschi avevano una fiducia cieca nella macchina Enigma, considerata inattaccabile. In realtà prima ancora della guerra e prima che Hitler arrivasse al potere, nel 1932 l'ufficio cifra polacco era riuscito a forzare l'Enigma. Durante la guerra gli inglesi forzavano ripetutamente i messaggi cifrati prima con l'enigma e poi, dal 1941, con la macchina Lorenz, più sofisticata della precedente.

Non è assolutamente facile sapere quali vittorie alleate avevano alla base tale superiorità criptografica. Però, sicuramente la Battaglia di Capo Matapan e lo Sbarco in Normandia sono due esempi conclamati di tale superiorità.

Il primo caso purtroppo riguarda la distruzione della flotta italiana nel marzo 1941, dovuta al fatto che gli inglesi erano riusciti a decriptare alcuni messaggi criptati della Marina Tedesca nei quali veniva fornita, appunto, la posizione esatta della flotta italiana.

Come noto, gli alleati mandarono falsi messaggi relativi allo sbarco delle loro truppe a Calais; i tedeschi caddero nel trabocchetto e mandarono le loro truppe migliori in quella zona. Gli alleati seppero del loro riuscito inganno decriptando, a loro volta, alcuni messaggi tedeschi criptati con

CRITTOGRAFIA: IL PASSATO

la macchina Lorenz. In questo modo riuscirono ad avere una resistenza quasi nulla nel loro effettivo sbarco in Normandia.

Gli Americani fin dal 1940, quindi un anno prima di Pearl Harbour, avevano realizzato una macchina, chiamata Magic, che era in grado di decriptare i messaggi giapponesi cifrati con la macchina Purple. Ci sarebbe da chiedersi come mai gli Americani non impedirono l'attacco a Pearl Harbour. La risposta viene da un noto scrittore americano, Gore Vidal, che insieme ad alcuni storici, sostiene che gli Americani sapevano dell'attacco ma non lo impedirono. In questo modo l'opinione pubblica americana, che era restia ad un intervento armato, fu tanto scossa da tale attacco a tradimento dei Giapponesi che non impedì più la propria entrata in guerra. Vi è, tuttavia, una teoria più prudente e, per certi versi, più accettabile per la quale gli Americani sapevano di un attacco giapponese ma non sapevano dove sarebbe avvenuto. Sta di fatto che a Pearl Harbour erano dislocate solo alcune vecchie navi di nessuna importanza per la guerra e nessuna portaerei. Non solo, ma alla fine della guerra il gen. Marshall ammise che, in numerosi casi di poca importanza, anche al costo di perdite umane, gli alleati dovettero fingere di non conoscere i messaggi cifrati nemici. In tale modo i tedeschi e i giapponesi continuavano a non sapere che i loro messaggi erano sistematicamente decriptati. Non sapremo mai ufficialmente, se l'attacco di Pearl Harbour può essere annoverato fra questi casi, dato che perirono in quella occasione 3000 cittadini americani.

Sappiamo sicuramente che la Battaglia di Midway e la morte dell'Ammiraglio Yamamoto sono due episodi che mostrano come gli Americani erano a conoscenza perfettamente delle mosse nemiche:

- **Battaglia delle Midway:** l'ammiraglio Isoroku Yamamoto, comandante supremo della flotta giapponese, nel maggio 1942 aveva preparato un piano per attaccare a sorpresa le isole Midway a est delle Haway, determinato com'era a infliggere una serie di duri colpi iniziali agli USA prima che la superiorità economica-industriale americana avesse il sopravvento. Ma grazie a Magic gli Americani intercettarono i piani di Yamamoto e l'Ammiraglio Nimitz, comandante della flotta USA, fu in grado di preparare la battaglia conoscendo già fin nei dettagli i piani del nemico; fece inoltre trasmettere falsi piani

CRITTOGRAFIA: IL PASSATO

americani usando un cifrario che sapeva essere stato forzato dai giapponesi. L'effetto sorpresa si trasformò in un boomerang e la vittoria USA alle Midway fu quindi in buona parte dovuta alla superiorità crittologica.

- **Morte dell'Amm. Yamamoto:** il 14 aprile 1943 fu decrittato un messaggio che diceva che l'ammiraglio Yamamoto avrebbe visitato l'isola di Bougainville il 18 e specificava persino le ore di partenza e di arrivo e il tipo di aerei usati. L'ammiraglio Nimitz subito informato, dopo aver sentito il Presidente Roosevelt, organizzò una squadra di aerei P-38 che il 18 puntualmente intercettò e abbatté l'aereo di Yamamoto; i giapponesi persero così il loro uomo più prezioso. La morte di Yamamoto fu peraltro presentata come dovuta a un incidente e solo dopo molti anni furono rivelati i dettagli dell'episodio.

In Italia, il gen. Sacco era riuscito a costruire una macchina molto complessa che inspiegabilmente fu distrutta e non venne più ricostruita. Uno strano episodio che ben si inserisce nella situazione disastrosa in cui verteva l'Italia durante la guerra.

Un successo sia pur temporaneo e di natura più spionistica che crittanalitica, lo si ebbe nel 1941 quando il servizio segreto italiano riuscì a trafugare dall'ambasciata americana a Roma il cifrario "Black". Grazie a questa impresa italiani e tedeschi riuscirono per qualche tempo a decrittare i messaggi americani nel Nord Africa; e sembra che molti dei successi di Rommel fossero dovuti a queste intercettazioni; quando nel 1942 gli alleati scoprirono che i loro messaggi venivano forzati, il cifrario "Black" fu abbandonato e sostituito con la ben più sicura macchina M-138. E, che sia stato un caso o no, finirono anche i successi di Rommel in Africa.

La macchina ENIGMA

Nella prima metà del secolo scorso iniziarono a fiorire per criptare messaggi le macchine cifranti a rotori. La più conosciuta macchina cifrante di questo tipo è l'Enigma che fu inventata a Berlino nel 1918 da Arthur Scherbius ed adottata dalla marina e dall'esercito tedesco fino alla seconda guerra mondiale, quando gli alleati riuscirono a scassarla ripetutamente.

CRITTOGRAFIA: IL PASSATO

Tale macchina applicava ripetutamente sostituzioni e trasposizioni dei singoli caratteri di un messaggio. Ogni sostituzione era ottenuta con l'uso di un insieme di connessioni elettriche che collegavano una coppia di contatti: ogni contatto corrisponde ad una lettera e ciascuna connessione era interpretabile come la trasformazione di una lettera in chiaro nella corrispondente lettera cifrata. Le connessioni erano collocate all'interno del rotore. Nel corso degli anni sono stati costruiti 10 tipi di rotori (I.VIII, Beta, Gamma), ciascuno con la propria specifica mappa di sostituzione. I rotori si muovevano con un modo odometro: ogni volta che una lettera è stata cifrata uno o più rotori ruotano di un ventesimo di giro. Il meccanismo è il seguente: il rotore 1 scatta sempre; ogni volta che ha eseguito un giro completo scatta anche il rotore 2; e così via per tutti i rotori.

L'Enigma è una macchina simmetrica, nel senso che se la lettera A è cifrata con la I in una certa posizione del testo, allora nella stessa posizione la I sarà cifrata con la A. La stessa macchina serve quindi per cifrare e decifrare; una grossa comodità operativa che è però anche una debolezza crittografica.

La macchina ha al suo interno un certo numero di rotori (nella prima versione erano 3) collegati elettricamente e liberi di ruotare; quando l'operatore preme un tasto p.es. la A un segnale elettrico passa da rotore a rotore fino al rotore finale detto il *riflettore* e quindi torna indietro fino a mostrare una lettera illuminata che è il carattere cifrato. Non esiste possibilità di stampa, dunque l'operatore deve copiare a mano, carattere per carattere il messaggio cifrato da trasmettere.

La chiave dell'Enigma è la disposizione iniziale dei rotori; questa chiave veniva cambiata ogni 24 ore secondo una regola prefissata; in definitiva la vera chiave segreta era questa regola. Anche i collegamenti interni dei rotori sono segreti.

Inoltre i tre (o più) rotori possono essere scambiati tra di loro, e quindi vi sono $n!$ ($3! = 6$ nella Enigma originale) disposizioni possibili, cosa che aumenta il numero di posizioni iniziali possibili. Era anche consigliato di tenere una scorta di rotori con cablaggi diversi, in modo da poter aumentare ancora il numero di combinazioni possibili.

I tedeschi erano convinti che l'Enigma fosse inattaccabile, ma questa fiducia era assai mal riposta. Già nei primi anni '30 un gruppo di matematici polacchi guidato da Marian Rejewski era riuscito

CRITTOGRAFIA: IL PASSATO

a ricostruire la struttura dei rotori e a deciptarne i messaggi, grazie anche al fatto di poter avere sotto mano un prototipo della macchina. Come noto, anche il servizio crittografico inglese al quale partecipava il Alan Turing riuscì a sua volta a forzare l'Enigma sin dall'inizio della guerra, sfruttando le debolezze intrinseche di questa macchina e alcune ingenuità dei cifratori tedeschi.