LICEO SCIENTIFICO CLASSICO STATALE
"**ISAAC NEWTON**"
Via Paleologi, 22 - 10034 CHIVASSO

PERCORSO CULTURALE PER L'ESAME DI STATO

RICCARDO ZANOTTO

CLASSE 5 E

Riccardo Zanotto

CODICI SEGRETI

L'evoluzione della crittografia: dalle guerre persiane ai moderni sistemi di sicurezza informatica

2014 - 2015

Indice

Introduzione

Da quando l'uomo ha cominciato a parlare e ad organizzarsi, c'è sempre stata anche la necessità di nascondere le proprie comunicazioni da orecchie indiscrete. In particolare contemporaneamente alla nascita della scrittura nei regni egizi e mesopotamici è nata anche una prima forma di crittografia; quest'arte è però stata sfruttata appieno da greci e romani che hanno inventato diversi metodi di comunicazione segreta. Il motore principale che ha favorito lo sviluppo della crittografia è stato infatti quello della guerra, dove è essenziale la segretezza delle comunicazioni e delle informazioni, il tenere all'oscuro il nemico delle proprie intenzioni per poter fare attacchi a sorpresa, ma avendo la possibilità di coordinarsi scambiando messaggi comprensibili solo ai propri alleati.
La parola "crittografia" ha un'etimologia molto semplice: dal greco "κρυπτός", nascosto, e "γραφία", scrittura; è dunque in generale il metodo usato per non far capire agli altri, tranne al destinatario, il contenuto di un messaggio. Ad essere precisi però ci sono diversi modi per nascondere il significato di un messaggio. Quello più semplice, ma ormai impossibile da attuare, è quello di occultare fisicamente il supporto su cui viene impresso il testo, e in questo caso si parla di *steganografia* (dal greco "στεγανός", coperto): ad esempio una scritta sul cranio rasato di un uomo, a cui vengono fatti ricrescere i capelli, o al giorno d'oggi nei bit poco importanti di una foto o di una traccia audio. La *crittografia* vera e propria si occupa di alterare il messaggio in modo da rendere difficile risalire al testo in chiaro, qualora il messaggio cadesse in mano al nemico. Gli elementi necessari sono questi: una chiave su cui si sono accordati mittente e destinatario, che va tenuta segreta, e un algoritmo, ovvero un modo di trasformare un testo chiaro in un testo segreto tramite la chiave e viceversa, che può anche essere pubblico. Gli algoritmi sono principalmente di due tipi diversi: la *trasposizione* che cambia di posto le lettere all'interno di un messaggio, in modo simile ad un anagramma, ed è efficace in quanto permette un numero molto elevato di chiavi; la *sostituzione* che cambia elementi del testo lasciandone invariata la posizione. La sostituzione può riguardare le parole, quindi ad esempio "sottomarino" viene cambiato in "pesce", e allora si parla di un *codice*; oppure, ed è il metodo più usato, riguarda le singole lettere, alle quali è associato un altro simbolo, ma mantengono invariata la posizione (per esempio "abc" diventa "123" se si associa ad ogni lettera la sua posizione nell'alfabeto).
Si noti infine come un'intera lingua sia un codice: ad ogni concetto associa un suono e una stringa di simboli, il cui significato viene compreso solo da chi parla quella lingua, ovvero conosce quel codice; per questo nella decifrazione dei geroglifici sono stati usati dei metodi propri della crittoanalisi, e nella seconda guerra mondiale gli Americani hanno usato il dialetto Navajo per comunicazioni segrete.

Figura 1.1: La suddivisione delle scritture segrete

In contrapposizione alla crittografia, ovvero l'arte di nascondere i messaggi, si è sviluppata la crittoanalisi, che nel corso dei secoli ha inventato tecniche sempre nuove e più avanzate per poter riportare in chiaro il significato di un messaggio criptato. Questa continua sfida tra creatori di codici e decifratori di enigmi è stata sempre presente nei secoli e ha portato a grandi passi avanti su entrambi i fronti; per comprendere certi codici ci sono voluti anche centinaia di anni, ma il primo a farlo aveva sotto controllo le comunicazioni di tutti. Per questo soprattutto in tempi di guerre gli Stati hanno investito molto sulla crittografia e sulla crittoanalisi, e in tutte le guerre degli ultimi duecento anni queste hanno avuto un ruolo fondamentale se non decisivo.
In questa breve trattazione sulla storia della crittografia si cercherà dunque di evidenziare questa continua rincorsa, analizzandone gli strumenti usati e l'impatto sulla società civile.

Il mondo antico: la nascita della crittografia

Sparta: la steganografia e la trasposizione

Come è già stato accennato, le scritture segrete hanno un'origine antichissima, e abbiamo anche una testimonianza scritta grazie a Erodoto; in questa prima fase prevaleva la steganografia, ovvero il nascondere fisicamente il messaggio. Infatti nelle sue *Storie* narra due episodi in particolare: il primo ha come protagonista Istieo, tiranno di Mileto, che voleva incoraggiare il generale Aristagora a ribellarsi al re persiano, e per non far intercettare il messaggio alle spie persiane fa rasare il cranio di un messaggero, vi scrive il messaggio e dopo che i capelli erano ricresciuti questi raggiunge il generale senza sospetti e gli spiega come leggere il messaggio. Il secondo riguarda Demarato, spartano esiliato in Persia, che vuole avvertire i suoi compatrioti del progetto d'invasione di Serse; allora raschia la cera da una tavoletta, scrive il messaggio sul legno e versa sopra nuova cera in modo che sembri una tavoletta vuota, che inviata a Sparta non desti sospetti tra i Persiani; giunta a destinazione suscitò molti sospetti, ma Gorgo, la moglie di Leonida, intuì che dovevano grattare via la cera; avvertiti dell'imminente invasione, i Greci costruirono una flotta e attirarono le navi persiane nella stretta baia di Salamina, vincendo la battaglia.
Nei secoli si sono sviluppati diversi metodi di steganografia, che però sono poi stati soppiantati -o almeno affiancati- dalla crittografia, perché basta una perquisizione approfondita per scoprire il messaggio in chiaro. Ad esempio i molti tipi di inchiostri invisibili (ad esempio il succo di limone) che si anneriscono con il calore sono stati presenti in tutte le epoche storiche, in diverse varianti, dai libri di Plinio il Vecchio ai film di James Bond. Inoltre con l'era digitale si è sfruttata la possibilità di inserire in alcuni punti di tracce audio delle sequenze di bit contenenti un messaggio che non sono percepibili attraverso un ascolto normale, oppure la riduzione di un testo con un carattere molto piccolo, tale da essere racchiuso nel puntino di una "i" normale.
Come si può intuire, già dall'antichità il motore della crittografia è stato il conflitto armato, dunque non ci si deve stupire se gli spartani siano stati pionieri anche nell'inventare una tecnica di trasposizione, aiutati da uno strumento, la scitale; questo era un bastone con un diametro fissato attorno al quale si arrotolava una striscia di pelle e si scriveva il messaggio in orizzontale, in modo che quando si srotolava la striscia si ottenesse una sequenza senza significato.
Conoscendo però l'algoritmo di cifratura, non è molto difficile risalire al testo in chiaro: le chiavi possibili, i diametri della scitale, sono al massimo pari alla lunghez-

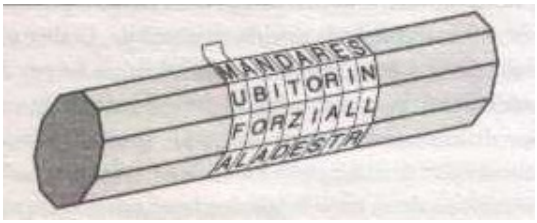


Figura 2.1: Una scitale spartana

za del messaggio dunque la decrittazione per tentativi non impiega molto tempo, anche perché bastano le prime lettere per accorgersi se si ha un messaggio sensato o meno. Si noti infine come con una scitale di diametro 2 si ottenga un'altra classica trasposizione detta "a inferriata", che consiste nello scrivere il messaggio su due o più righe, cambiando riga ad ogni carattere.

Tuttavia se si abbandonano questi algoritmi, si vede che la trasposizione offre un nu-

T A P S Z O E I F R I T
R S O I I N A N E R A A $\longrightarrow$ TAPSZOEIFRITRSOIINANERAA

Figura 2.2: Trasposizione a inferriata

mero enorme di chiavi per messaggi abbastanza lunghi: infatti ogni anagramma produce un testo criptato valido, e il numero di anagrammi cresce più che esponenzialmente. Un messaggio di n lettere ha circa $n! = n \cdot (n-1) \cdots 2 \cdot 1$ anagrammi; "prendiamo ad esempio questa frase" ha esattamente $\frac{29!}{3! \cdot 2! \cdot 5! \cdot 2! \cdot 2! \cdot 2! \cdot 2! \cdot 2! \cdot 3!} =$ 31.979.752.581.523.806.259.200.000 anagrammi possibili (32 milioni di miliardi di miliardi); se ognuno dei sei miliardi di abitanti della Terra avesse un computer con 4GHz di processore e immaginiamo di poter controllare una permutazione in un clock, ci metteremmo 15 giorni per decrittare un messaggio di 4 parole, senza contare che probabilmente ci sono anche altre permutazioni valide.

Il problema nella messa in pratica di questo sistema è che la chiave è assai complicata (deve descrivere in che posizione finisce ogni lettera) e dunque la sua distribuzione potrebbe rivelarsi molto problematica logisticamente, senza contare che potrebbe venire facilmente intercettata ed usata per decriptare i messaggi.

Roma: il cifrario di Cesare

Se in Grecia è nata la trasposizione, a Roma è nata la sostituzione, che avrà una vita molto più lunga data la facilità con cui si possono trasmettere le chiavi. Uno degli utilizzatori più assidui della crittografia fu il grande generale Giulio Cesare, che ne descrive alcuni esempi nel *De Bello Gallico*; tuttavia a Cesare è associato il cifrario descritto da Svetonio nel *De Vita Caesarum* e ancora oggi spesso usato da molti ragazzi per svago, che viene descritto brevemente in questo passo:

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.

Questo significa semplicemente che per cifrare occorre sostituire ogni lettera nel messaggio con quella tre posti più avanti nell'alfabeto, quindi la **a** diventa **D** e così via; l'operazione inversa è molto semplice, basta tornare indietro di tre lettere; in gergo, questo vuol dire che l' "alfabeto cifrante" è l'alfabeto ordinario spostato a destra di tre posti. Osserviamo poi che essendoci 26 lettere nell'alfabeto, sono

Alfabeto chiaro	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z	
Alfabeto cifrante	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C	

Testo chiaro	v	e	n	i		v	i	d	i		v	i	c	i	
Testo cifrato	B	H	Q	N		B	N	G	N		B	N	F	N	

Figura 2.3: Esempio di cifratura di un testo con il metodo di Cesare

possibili 25 cifrari "di Cesare", ciascuno corrispondente ad uno spostamento della A di $2, 3, 4, \ldots, 25$ posizioni (ovviamente uno shift di 26 posizioni equivale a nessuno spostamento, quindi l'alfabeto cifrante è lo stesso dell'alfabeto in chiaro). In ogni caso, se una spia intercettasse un messaggio sospettando che sia stato criptato con un cifrario di Cesare, avrebbe da provare solo 25 chiavi diverse.
Possiamo anche formalizzare il cifrario di Cesare attraverso l'aritmetica modulare e poi generalizzarlo a quello che si chiama un "cifrario affine". Infatti se abbiamo un alfabeto di n caratteri, e ad ognuno associamo una posizione, ovvero un numero da 1 a n, e l'alfabeto cifrante è spostato di k posizioni, si può descrivere una funzione di cifratura semplicemente come

$$C(x) \equiv x + k \pmod{n}$$

Per decifrare, basta semplicemente invertire la funzione, e qua è facile perché è una somma: $x \equiv C(x) - k \pmod{n}$, quindi se chiamiamo $D(x)$ la funzione per decrittare abbiamo

$$D(x) \equiv x - k \pmod{n}$$

Dunque rifacendoci alla figura 2.3 abbiamo $n = 21, k = 3$ e quindi alla lettera **v** corrisponde il numero 20; allora $C(20) \equiv 20 + 3 \equiv 2 \pmod{21}$ e il 2 corrisponde alla **B**; d'altra parte per decifrare il carattere **H**, che è il numero 8 nell'alfabeto, devo togliere 3, ovvero $D(8) \equiv 8 - 3 \equiv 5 \pmod{21}$ e la quinta lettera è la **e**.

La sostituzione monoalfabetica

Questo breve excursus nell'aritmetica modulare può sembrare banale se applicato solo al cifrario di Cesare, ma rivela la sua vera utilità se pensiamo anche a moltiplicare, creando una mappa affine; consideriamo ora una funzione del tipo

$$C(x) \equiv a \cdot x + b \pmod{n}$$

Vediamo che il numero di chiavi è aumentato molto, perché abbiamo due parametri, ciascuno dei quali può assumere n valori, dunque in totale abbiamo n^2 chiavi possibili, che per un alfabeto di 26 lettere sono 656, già più difficili da provare a mano, ma è fattibile con un computer, o con abbastanza tempo.
Tuttavia non è sicuro che tutti i valori diano luogo ad una cifratura valida; ad esempio se $a = 0$, tutti i valori vengono criptati come b, ed è impossibile risalire al messaggio originale; ma anche se $a = 2, n = 6$ abbiamo che $C(1) \equiv 2 + b \equiv 8 + b \equiv C(4) \pmod 6$ ovvero la prima e la quarta lettera sono cifrate nello stesso modo. Ci serve dunque che la funzione sia invertibile, ovvero che i numeri $ax + b$ siano (modulo n) una permutazione dei numeri $1, 2, \ldots, n$. Questo accade se e solo se $\gcd(a, n) = 1$ come sappiamo dall'aritmetica modulare (vedi teorema 7): in questo caso infatti esiste un intero a^{-1} tale che $a \cdot a^{-1} \equiv 1 \pmod n$; ma allora possiamo costruire una funzione di decrittazione

$$D(x) \equiv a^{-1}(x - b) \pmod n$$

A questo punto le chiavi possibili di un cifrario affine sono $n \cdot \varphi(n)$; nel caso $n = 26$ abbiamo che il numero di chiavi è $26 \cdot 12 = 312$. Possiamo però aumentarlo se prendiamo n primo in modo che $\varphi(n) = n - 1$ che è il massimo possibile; ad esempio, se all'alfabeto inglese aggiungessimo lo spazio, il punto e la virgola, avremmo $n = 29$ a cui corrispondono $29 \cdot 28 = 812$ chiavi.
Dopo il cifrario affine, nei secoli si è sviluppata anche l'idea di poter prendere come alfabeto cifrante una qualunque permutazione dell'alfabeto, non necessariamente derivante da una funzione matematica. Questa operazione infatti fa esplodere il numero di chiavi a $n!$ dove n è la lunghezza dell'alfabeto. L'utilizzo di una chiave

Alfabeto chiaro	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z	
Alfabeto cifrante	G	I	U	L	O	C	E	S	A	R	T	V	Z	B	D	F	H	M	N	P	Q	

Figura 2.4: Alfabeto cifrante a partire da una parola chiave

completamente casuale è assai scomodo, però ci sono alcuni metodi per generarne di abbastanza disordinate, ma con un algoritmo facile; si sceglie infatti una parola o una frase, ad esempio "Giulio Cesare" e si eliminano le lettere ripetute ottenendo GIULOCESAR, che sarà l'inizio dell'alfabeto cifrante, mentre il resto sarà in ordine alfabetico, partendo dall'ultima lettera della chiave e mettendo le lettere non ancora inserite. Questo metodo permette di generare molte chiavi diverse piuttosto semplicemente; ad esempio si può partire dalla data ("sei giugno"), così non c'è bisogno di distribuire le chiavi con il rischio che vengano intercettate, e se ne ha una nuova ogni giorno.
Inoltre l'architetto italiano Leon Battista Alberti ha inventato dei dischi rotanti con due corone, una delle quali mobili; quella esterna, fissa, aveva l'alfabeto in chiaro, quella interna l'alfabeto cifrante composto da una sequenza casuale di lettere. Allora mittente e destinatario dovevano condividere lo stesso disco e stabilire una chiave, corrispondente al numero di rotazioni della corona interna; per criptare bastava cercare sulla ruota esterna e leggere il carattere su quella interna, per decriptare al contrario cercare il carattere sulla ruota interna e leggere quello sulla ruota esterna.
Infine un ultimo esempio, oggi frequente su internet (http://www.rot13.com/index.php),

Figura 2.5: Disco cifrante di Leon Battista Alberti

è il ROT13, molto semplice perché prevede la stessa sostituzione per criptare e decriptare: si crea infatti un elenco di 13 coppie di lettere (A con N, e così via) e l'operazione di (de)codifica consiste nello scambiare le lettere all'interno delle coppie; ovvero, come dice il nome, di "ROTate by 13".

Tutte queste varianti più o meno sofisticate del cifrario di Cesare hanno in co-

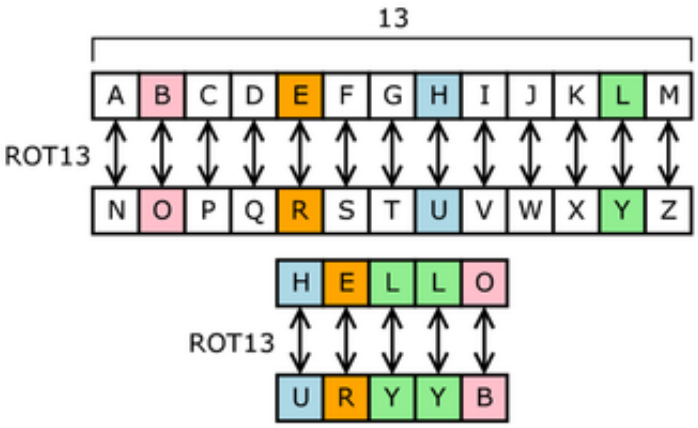


Figura 2.6: Schema di funzionamento del ROT13

mune una cosa: ad ogni lettera ne associano una sola e viceversa per decriptare ogni lettera ha un'unica inversa. Ma allora in un certo senso le lettere conservano la propria "identità": ad esempio in italiano dopo una q c'è sempre una u, quindi dopo il simbolo che cifra q nel crittogramma ci sarà sempre il simbolo che cifra u. E saranno proprietà simili a far crollare la crittografia monoalfabetica.

L'analisi delle frequenze

Il primo attacco al cifrario di Cesare giunse dai teologi arabi, e con la sua diffusione avrebbe segnato la fine della segretezza per le sostituzioni monoalfabetiche. Infatti alla morte di Maometto i primi califfi -Abu Bakr, Umar e Othman- ordinarono le

rivelazioni del profeta nei 114 capitoli che formano il Corano; col passare del tempo la cultura islamica si è sviluppata molto nelle arti e nelle scienze (come si può notare dai molti termini oggi presenti: algebra, zenith e molti altri), e nell'amministrazione pubblica si arrivò all'uso della sostituzione monoalfabetica, a volte anche con alfabeti simbolici; nell'815 venne fondata la biblioteca di Baghdad e grazie alla carta, inventata dai cinesi, e ai molti copisti si poté avere una grande diffusione della cultura. Tuttavia gli arabi sono anche gli inventori della crittoanalisi, che si è sviluppata su un terreno fertile nel quale erano diffuse conoscenze di matematica, statistica e linguistica; ma l'idea fondamentale arrivò dalle scuole di teologia: qua infatti si applicavano raffinati metodi linguistici al Corano per stabilire la cronologia dei capitoli, in particolare il conteggio di certe parole, ritenute più o meno recenti; ma alcuni studiosi arrivarono addirittura al livello delle lettere osservando che lettere come la "a" e la "g" erano le più usate.
Questa intuizione -che le lettere hanno un'identità data dalla frequenza- venne sfruttata dallo studioso al-Kindi, soprannominato "il filosofo degli arabi" poiché scrisse numerosi trattati di varie discipline, principalmente astronomia, matematica, medicina, linguistica e musica. In un manoscritto ritrovato solo nel 1987 e intitolato *Sulla decifrazione dei messaggi criptati*, oltre ampie disquisizioni sulla statistica e sulla sintassi araba, egli espone in due brevi paragrafi il rivoluzionario procedimento crittoanalitico dell'analisi delle frequenze

> *Un modo di svelare un messaggio crittato, se conosciamo la lingua dell'originale, consiste nel trovare un diverso testo in chiaro nella stessa lingua, abbastanza lungo da poterne calcolare la frequenza di ciascuna lettera. Chiamiamo "prima" quella che compare più spesso, "seconda" la successiva, e così via fino all 'esaurimento di tutte le lettere del campione di testo in chiaro.*
> *Esaminiamo poi il testo in cifra che vogliamo interpretare, ordinando in base alla frequenza anche i suoi simboli. Troviamo il simbolo più comune, rimpiazziamolo con la "prima" lettera dell'esempio in chiaro; il simbolo che lo segue per frequenze sia rimpiazzato dalla "seconda" lettera dell'esempio in chiaro, e così via fino ad aver preso in considerazione tutti i simboli che volevamo svelare.*

Il primo paragrafo si concentra su un testo -meglio se sono più testi- in chiaro appartenente alla stessa lingua del messaggio cifrato, grazie al quale si può stabilire la frequenza media delle lettere in quella lingua; oggi con l'aiuto dei computer e grazie ai moltissimi testi digitalizzati è possibile ottenere dei grafici piuttosto precisi, come ad esempio quello nella figura 2.7, preso da Wikipedia. Occorre poi contare i simboli del crittogramma e fare una tabella delle frequenze relativa al testo cifrato, e infine confrontare i valori: molto probabilmente, se il crittogramma è abbastanza lungo, l'ordine delle frequenze è lo stesso. Tuttavia il metodo di al-Kindi non si può applicare meccanicamente, in quanto brevi testi hanno una diversa frequenza relativa delle lettere; ad esempio, se viene cifrata per sostituzione la frase seguente, le possibilità di riuscita saranno minime: "Da Zanzibar allo Zambia allo Zaire la scarsezza di ozono spinge le zebre a zigzagare bizzarramente", anche perché la "z" è una delle lettere meno frequenti in italiano. In generale i testi sotto le cento lettere

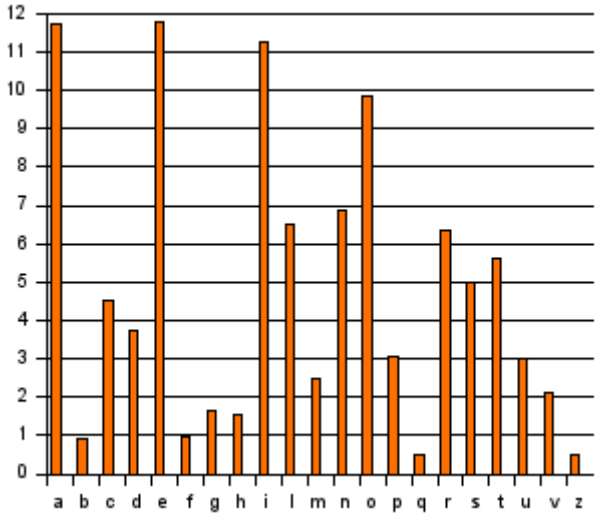


Figura 2.7: Frequenza delle lettere in italiano

sono più difficili da crittoanalizzare, ma esistono esempi di testi lunghi con frequenze comunque falsate: nel 1969 lo scrittore francese Georeges Perec portò a termine *La disparition*, un romanzo di 200 pagine senza parole contententi la lettera "e" - la lettera più comune in francese; questo romanzo venne anche tradotto in inglese da Gilbert Adair con il titolo *A void*, mantenendo questa peculiare caratteristica, e rimanendo scorrevole.
In ogni caso questo è uno strumento molto utile per un crittoanalista esperto, che deve avere molta dimestichezza con la lingua: in italiano le cinque lettere più frequenti sono E, A, I, O, N e dunque è molto probabile che le prime lettere del testo cifrato corrispondano, anche se non in ordine, a queste. Inoltre si possono sfruttare altre caratteristiche della lingua, come il fatto che le vocali non si ripetono, e le consonanti ripetute più frequenti sono NN, RR, LL; vi sono poi insiemi fissati di certe lettere, come QU, oppure la grande frequenza dell'articolo IL.
Con un po' di tentativi si può riuscire a ricostruire una parte del testo cifrato e a questo punto le parole mancanti possono essere indovinate come nei cruciverba, oppure si può tentare di ricostruire la chiave, se è stata costruita come in figura 2.4.
I crittografi, quando si resero conto che i cifrari monoalfabetici erano stati violati, cercarono di introdurre alcune accortezze, che non fecero altro che rallentare di poco la definitiva sconfitta dei cifrari di Cesare nelle comunicazioni segrete degli Stati. Ad esempio uno stratagemma adottato fu quello di associare ogni lettera a un numero da 1 a 100, e nel criptare il messaggio si inserivano a caso i numeri a cui non era associata alcuna lettera per variare i rapporti di frequenza; oppure si partiva da un testo in chiaro sgrammaticato ma comprensibile, anche questo per variare le frequenze.
Nel XVI secolo ormai i crittoanalisti più esperti erano in grado di decifrare ogni messaggio; caso esemplare è quello della Spagna di Filippo II, i cui messaggi venivano facilmente letti dal grande matematico François Viète, definito dagli spagnoli un "arcidiavolo in combutta con il Maligno"; ma anche in Vaticano decifravano i messaggi spagnoli senza interventi diabolici, per cui prestarono poca attenzione all'accusa.

The Gold-Bug

Plot

This short story by Edgar Allan Poe is set on Sullivan's Island, South Carolina and it has three main characters: the protagonist William Legrand, his friend the unnamed first person narrator, and Legrand's African-American servant Jupiter.
One day Legrand and Jupiter find a strange bug on the beach: it shines with golden shades and it is very heavy, so Jupiter thinks that the bug is made of pure gold.
In the evening the narrator pays a visit to his friend, who tells him of the bug, which unfortunately he lent to someone; but Legrand draws it on a piece of paper and shows it to his friend who says that it looks like a skull. Legrand inspects again his drawing and puts it away, thinking of it all the rest of the evening.
One month later Jupiter visits the narrator and tells him to come to the Island because his master is ill. When he arrives, Legrand tells them that they are going on an expedition into the forest. There they find a tree, which Legrand orders Jupiter to climb with the gold-bug in his hand; up the tree he finds a skull and Legrand tells him to drop the bug through the left eye. From where it falls, he determines the spot where they will begin to dig.
The narrator thinks that Legrand has gone completely mad, but then they find a big tresaure buried by a pirate, which they estimate to be a million and a half dollars worth. Once they have brought the tresaure back to Legrand's house, he explains how he found it.
The piece of paper on which he had drawn the bug was actually hiding a secret message from the pirate Captain Kidd, in fact there was a young goat - a kid. Heating the scroll Legrand found a sequence of symbols and numbers, which he decoded.

Analysis

53‡‡†305))6;4826)4‡.)4‡);806*;48†8¶60))85;;]8*;:‡*8†83(88)5*†;*
*46(;88*96*?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8¶8*;4069285);)6†8)4‡‡;1(‡9*
*;48081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;*

This is the message Legrand got from Kidd's scroll; apparently it has no meaning, but actually it is crypted with a simple substitution cipher, which is easily broken by a skilled cryptanalist as Legrand. First of all, he makes sure that the language of the ciphertext is English by noting the pun Kidd-kid. Then the basic idea is that in

English there are letters used most, like 'e' and 'I', as well as short words like 'the' or 'an'.
Here is the graphic Legrand obtained by counting how many times every symbol appeared, in contrast with the average frequency of letters in the English language.
From these and after some tries, carefully described in the story, one can say that

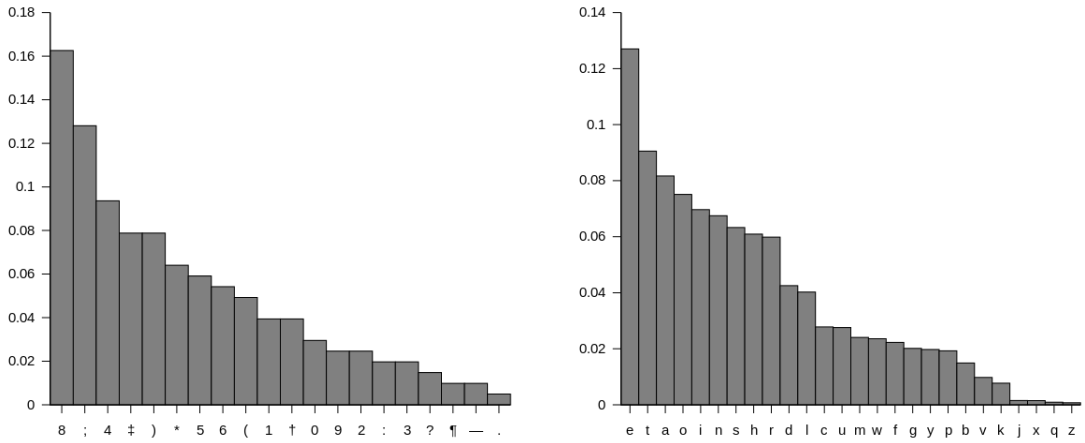


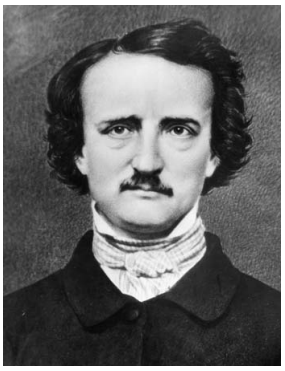
Figura 3.1: Graphic of frequencies

8 is **e** and **;** is **t**, and get more and more letters. In the end, the decoded message is
«*A good glass in the bishop's hostel in the devil's seat*
twenty-one degrees and thirteen minutes northeast and by north
main branch seventh limb east side shoot from the left eye of the death's-head
a bee line from the tree through the shot fifty feet out».
Now Legrand has to deal with the meaning, which may be a code, in fact "bishop's hostel" and "devil's seat" are quite obscure. But asking to the old people on the island, he found the "Bessop's castle", which is a big rock; there he found a ledge that looked like a chair, the "devil's seat". Then he watched through a telescope (the glass) in the direction described in the scroll and he found a skull on a very high tree, which is the one Jupiter climbed and from which he let the bug fall (shoot)

Edgar Allan Poe

Edgar Allan Poe was an American writer, poet and literary critic, considered part of the American Romantic Movement. Best known for his tales of mystery and the macabre, Poe was one of the first American writers in the style of the short story, and is generally considered the inventor of the detective fiction genre. He is further credited with contributing to the emerging genre of science fiction. He was the first well-known American writer to try to earn a living through writing alone, resulting in a financially difficult life and career.

Life



Born in Boston on January 19, 1809, Poe was the second child of two actors. His father abandoned the family in 1810, and his mother died the following year. Thus orphaned, the child was taken in by John and Frances Allan, from which he took his second name. Although they never formally adopted him, Poe stayed with them until young adulthood. Tension developed later as John Allan and Edgar repeatedly clashed over gambilng debts and the cost of secondary education; in fact Poe attended the University of Virginia for one semester but left due to lack of money. Poe quarreled with Allan over the funds for his education and enlisted in the Army in 1827 under an assumed name. It was at this time his publishing career began, although humbly, with an anonymous collection of poems, *Tamerlane and Other Poems* (1827), credited only to "a Bostonian". With the death of Frances Allan in 1829, Poe and Allan reached a temporary rapprochement. Later failing as an officer's cadet at West Point and declaring a firm wish to be a poet and writer, Poe parted with John Allan, who disinherited him.

Poe switched his focus to prose and spent the next several years working for literary journals and periodicals, becoming known for his own style of literary criticism. His work forced him to move among several cities, including Baltimore, Philadelphia, and New York City. In Baltimore in 1835, he married Virginia Clemm, his 13-year-old cousin. In January 1845 Poe published his poem, *The Raven*, which brought him to instant success. His wife died of tuberculosis two years after its publication, and on October 7, 1849, also Poe died, the cause of death unknown.

Themes and style

Poe's best known fiction works are Gothic, a genre he followed to appease the public taste. His most recurring themes deal with questions of death, including its physical signs, the effects of decomposition, concerns of premature burial, the reanimation of the dead, and mourning.

Beyond horror, Poe also wrote satires, humor tales, and hoaxes. For comic effect, he used irony and ludicrous extravagance, often in an attempt to liberate the reader from cultural conformity. *Metzengerstein*, the first story that Poe is known to have published, and his first foray into horror, was originally intended as a burlesque satirizing the popular genre. Poe also reinvented science fiction, responding in his writing to emerging technologies such as hot air balloons in *The Balloon-Hoax*. In general, Poe wrote much of his work using themes aimed specifically at mass-market tastes. To that end, his fiction often included elements of popular pseudosciences such as phrenology and physiognomy.

Poe's writing reflects his literary theories, which he presented in his criticism and also in essays such as *The Poetic Principle*. He disliked didacticism and allegory, though

he believed that meaning in literature should be an undercurrent just beneath the surface. Works with obvious meanings, he wrote, cease to be art. He believed that work of quality should be brief and focus on a specific single effect. To that end, he believed that the writer should carefully calculate every sentiment and idea.
In the essay *The Philosophy of Composition* Poe describes his method in writing *The Raven*, theorizing the genre of the short story, which focuses on a brief span of time and on a circumscribed setting conveyed through the atmosphere described by the writer; the plot is often simple and focuses on a particular episode, and it developes according to a regular pattern: an introduction, the key-note which arises the reader's interest, the ascending climax and the conclusion (which can re-establish the initial conditions, or bring a change, or it can be open leaving the conflicts unresolved).

Criptography

Poe had a keen interest in cryptography. He had placed a notice of his abilities in the Philadelphia paper Alexander's Weekly (Express) Messenger, inviting submissions of ciphers, which he proceeded to solve. In July 1841, Poe had published an essay called *A Few Words on Secret Writing* in Graham's Magazine. Capitalizing on public interest in the topic, he wrote *The Gold-Bug* incorporating ciphers as an essential part of the story. Poe's success with cryptography relied not so much on his deep knowledge of that field (his method was limited to the simple substitution cryptogram), as on his knowledge of the magazine and newspaper culture. His keen analytical abilities, which were so evident in his detective stories, allowed him to see that the general public was largely ignorant of the methods by which a simple substitution cryptogram can be solved, and he used this to his advantage. The sensation Poe created with his cryptography stunts played a major role in popularizing cryptograms in newspapers and magazines.
Poe had an influence on cryptography beyond increasing public interest during his lifetime. William Friedman, America's foremost cryptologist, was heavily influenced by Poe. Friedman's initial interest in cryptography came from reading *The Gold-Bug* as a child, an interest he later put to use in deciphering Japan's PURPLE code during World War II.

Dal Medioevo all'Ottocento

La congiura di Babington

L'8 febbraio del 1587 a Londra fu decapitata Maria Stuarda, regina di Scozia, condannata per alto tradimento; nell'agosto dell'anno prima erano stati crudelmente trucidati sette gentlemen inglesi accusati di aver organizzato una congiura per liberare Maria, prigioniera di Elisabetta, e rovesciare la monarchia inglese. Tutte queste morti, necessarie per mantenere l'ordine pubblico in Inghilterra, furono possibili grazie alla debolezza del cifrario adottato da Maria Stuarda e il capo dei congiurati, Anthony Babington.
Ricostruiamo brevemente i fatti e la situazione della Gran Bretagna nel XVI secolo. Nel 1542 l'esercito inglese di Enrico VIII sbaragliò le truppe scozzesi nella battaglia di Solway Moss, ed era a un passo dall'occupare il regno di Giacomo V; questi si ammalò gravemente e morì una settimana dopo la nascita della figlia, Maria, che a nove mesi venne incoronata regina di Scozia nel 1542. Allora Enrico VIII cambiò tattica: cessò le ostilità e chiese il fidanzamento di Maria con il proprio figlio Edoardo; ma gli scozzesi optarono per un accordo matrimoniale con Francesco, Delfino di Francia. Ripresero dunque gli attacchi, proseguiti anche dal figlio Edoardo VI, e dopo un pesante massacro nel 1547 fu deciso di portare Maria in Francia, dove conobbe Francesco; compiuti i sedici anni si sposarono, ma Francesco si ammalò e nel 1560 morì lasciando Maria vedova, che dunque tornò in Scozia.
Nel frattempo il suo paese natale era cambiato di molto, e in particolare molti sudditi si erano convertiti al protestantesimo, mentre lei era rimasta cattolica; dopo una serie di sfortunati matrimoni, da cui ebbe come unico figlio Giacomo, Maria venne imprigionata e obbligata ad abdicare dai nobili protestanti; evasa, radunò un esercito con cui tentò di tornare sul trono, ma fallì e la via di fuga più sicura era l'Inghilterra governata dalla cugina Elisabetta.
In realtà venne arrestata, accusata per l'assassinio di suo marito, ma soprattutto per motivi politici e dinastici: i cattolici inglesi la consideravano la vera regina, in quanto imparentata con Enrico VIII mentre Elisabetta era la figlia avuta nella relazione illegittima con Anna Bolena; passò dunque tutti i suoi anni in Inghilterra reclusa in castelli e ville ben sorvegliati. Non poteva ricevere né inviare posta (tentò inutilmente di comunicare con il figlio, che però la disprezzava essendo stato allevato dai cattolici); tuttavia nel 1586 le fu recapitato un pacco di lettere da Gilbert Gifford, un cattolico che si era offerto di contrabbandare le missive dall'ambasciata francese alla residenza di Chartley Hall. Il metodo era assai ingegnoso: le lettere erano avvolte in una pergamena e rinchiuse in un tappo vuoto per le botti, che poi

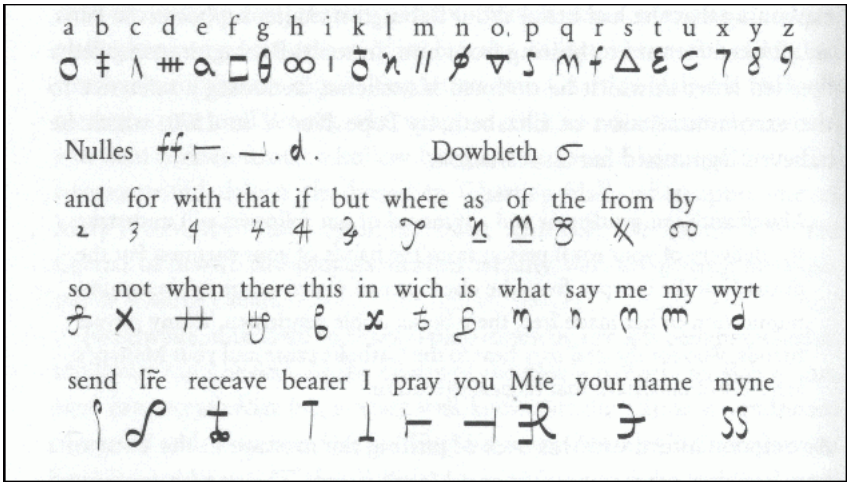


Figura 4.1: Il nomenclatore usato da Maria e Babington

venivano portate alla residenza dove un fedele servitore di Maria controllava i tappi; lo stesso metodo serviva per far uscire le lettere della prigioniera.
Intanto il sopracitato Babington, un gentiluomo ben noto in città, stava tramando per liberare la regina scozzese, anche se lei ne era all'oscuro. Questi aveva un profondo odio antiprotestante, legato soprattutto all'esecuzione del bisnonno perché sospettato di aver preso parte ad una sommossa cattolica. In pochi mesi egli e sei congiurati misero a punto un piano per liberare Maria e uccidere Elisabetta; occorreva però che la regina scozzese ne fosse informata, e quindi Babington descrisse in dettaglio il proprio piano in una lettera, che poi cifrò per avere una maggiore sicurezza, usando un nomenclatore (vedi figura 4.1), ovvero una sostituzione monoalfabetica unita ad un codice - cioè la sostituzione di intere parole con un simbolo; un estratto della lettera decriptata è il seguente:

> *Myself with ten gentlemen and a hundred of our followers will undertake the delivery of your royal person from the hands of your enemies. For the dispatch of the usurper, from the obedience of whom we are by the excommunication of her made free, there be six noble gentlemen, all my private friends, who for the zeal they bear to the Catholic cause and your Majesty's service will undertake that tragical execution.*

Maria e Babington erano più che sicuri sia del canale di comunicazione che del cifrario, ma si sbagliavano su entrambi, e questo firmò la loro condanna a morte. Infatti Gifford era una spia inglese che faceva il doppiogioco: si era infatti messo a disposizione del segretario di Stato, Sir Francis Walsingham, sapendo che l'essere cattolico gli avrebbe permesso di infiltrarsi tra i nemici di Elisabetta. Così ogni messaggio da o per Maria veniva letto dai collaboratori di Walsingham; quando si trovò il messaggio cifrato, venne immediatamente passato a Thomas Phelippes, capo dell'ufficio cifre inglese e uno dei più abili crittoanalisti europei, maestro dell'analisi delle frequenze. Dopo molti tentativi, nei quali a poco a poco accantonava le nulle, e dopo aver decifrato il resto era facile intuire il significato delle parole in codice. Già con la prima lettera Walsingham aveva materiale sufficiente per arrestare Babington, ma puntava molto più in alto: sperava nell'approvazione scritta di Maria, per

poter accusare anche lei; Elisabetta era infatti riluttante ad uccidere la cugina senza prove più che evidenti. Dopo pochi giorni arrivò la risposta, a cui Phelippes -abile anche nel simulare le calligrafie- aggiunse la richiesta di conoscere i nomi dei sei congiurati. L'eccessiva fiducia nel cifrario spinse Babington a rispondere, e quindi si poté procedere all'arresto dei complottisti; questo mostra che l'uso di una cifratura debole è peggio del non cifrare, perché ogni cosa viene scritta esplicitamente e si può essere ingannati da falsi crittogrammi aggiunti dagli intercettatori.
In conclusione, il 15 ottobre 1586 si aprì il processo contro Maria Stuarda, che come difesa disse di non sapere niente della congiura di Babington; ma questa difesa non poteva reggere, dato che le lettere erano state decriptate, e venne inevitabilmente condannata a morte. L'8 febbraio 1587 Maria regina di Scozia fu decapitata a Fotheringhay.

Le chiffre indéchiffrable

Per secoli la sostituzione monoalfabetica aveva garantito la sicurezza; ma la morte di Maria Stuarda e molti altri episodi mostravano che ormai i crittoanalisti più esperti potevano leggere qualunque crittogramma. Occorreva dunque inventare un nuovo metodo di cifratura, e questo spettava ai crittografi, che negli ultimi mille anni avevano smesso di innovare le scritture segrete. L'origine di una nuova tecni-

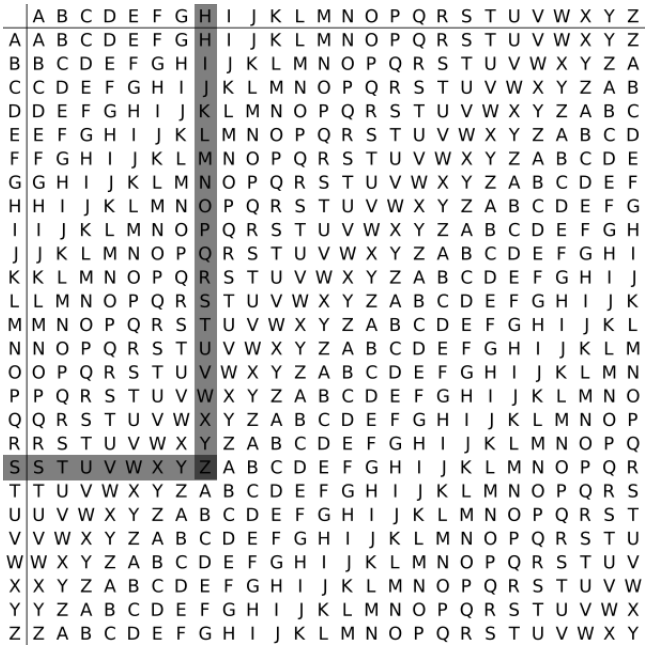


Figura 4.2: Il quadrato di Vigenère

ca, la sostituzione polialfabetica, può essere ricondotta all'architetto fiorentino Leon Battista Alberti. Egli infatti scrisse un trattato di crittografia nel quale esponeva un nuovo tipo di cifratura: suggeriva di scegliere non uno ma due o più alfabeti cifranti e di usarli alternativamente per criptare il messaggio. Questo aveva un vantaggio indubbio: la stessa lettera poteva essere cifrata in più modi diversi, e viceversa una

Parola chiave:	M	O	N	T	E	M	O	N	T	E	M	O	N	T	E	M	O	N	T	E	M	O	N
Testo chiaro:	s	p	o	s	t	a	r	e	t	r	u	p	p	e	s	u	c	i	m	a	e	s	t
Testo cifrato:	E	D	B	L	X	M	F	R	M	V	G	D	C	X	W	G	Q	V	F	E	Q	G	G

Figura 4.3: Esempio di cifratura di un testo con il cifrario di Vigènere

stessa lettera nel crittogramma poteva corrispondere a più lettere nel messaggio in chiaro. Tuttavia la sua idea fu appena abbozzata, e venne portata a compimento da un diplomatico francese da cui questa nuova tecnica prende il nome: Blaise de Vigenère.
Il quadrato di Vigenère è composto da 26 alfabeti cifranti di Cesare, spostati di uno in uno; ogni lettera poteva essere criptata in 26 modi diversi e per decriptare era necessario conoscere la riga usata per ogni singola posizione: per cifrare infatti si prendeva la colonna della lettera in chiaro, e la riga dell'alfabeto cifrante scelto, così che nell'incrocio si trovava la lettere criptata; viceversa per decodificare occorre prendere la riga dell'alfabeto cifrante, prendere la lettera e vedere a cosa corrisponde nella riga del testo in chiaro. Un possibile metodo per cifrare era passare all'alfabeto cifrante successivo per ogni lettera; ad esempio per cifrare **hai** all'interno di un messaggio, supponendo come in figura 4.2 che l'alfabeto cifrante per **h** sia "**S**" (si indica un alfabeto con la lettera a cui corrisponde la **a**), si dovrebbe scrivere **Z**, poi passare all'alfabeto **T** e quindi cifrare **a** con **T**, e infine cifrare la **i** con l'alfabeto **U**, cioè **C**, ottenendo la stringa **ZTC**.
In realtà non si è usato spesso il metodo di passare da un alfabeto al successivo (al crittoanalista sarebbe bastato provare le 26 possibili partenze), ma si sono adoperate delle parole chiave, le cui lettere corrispondono alle righe con cui cifrare. Ad esempio (figura 4.3) per criptare il messaggio **spostare truppe su cima est** con la chiave **MONTE**, per prima cosa si scrive la chiave più volte di seguito sopra al messaggio in chiaro, in modo che le lettere siano allineate in verticale a coppie; per cifrare la prima lettera, nel nostro caso una **s**, controlliamo qual è la lettera della chiave corrispondente e usiamo quell'alfabeto cifrante, che è quello indicato da **M** nella tredicesima riga del quadrato, e l'intersezione tra riga **s** e colonna **M** è **E**; passiamo alla seconda lettera, **p**, che va cifrata con l'alfabeto **O**, ovvero diventa una **D** che si trova all'incrocio; e così per tutte le lettere del messaggio. Come si può facilmente notare, su crittogrammi di questo tipo l'analisi delle frequenze è inconcludente, poiché ad esempio la **G** è la lettera che appare più spesso, ma due volte corrisponde alla **u**, una alla **s** e un'altra ancora alla **t**; viceversa le due **p** consecutive vengono cifrate come **DC**. Oltre a questa formidabile resistenza, la cifratura di Vigenère ammette un numero enorme di chiavi (qualunque parola o stringa di lettere), per cui è impossibile controllare tutte le chiavi.
Questa grande scoperta venne pubblicata dal crittografo francese con il suo *Traicté des Chiffres* nel 1586, lo stesso anno in cui Phelippes violò il cifrario di Maria Stuarda, che probabilmente se avesse potuto usare questo nuovo sistema si sarebbe salvata la vita.
Tuttavia questo metodo non venne ben accolto negli ambienti militari, in quanto troppo complicato e lento, mentre occorreva rapidità. Una possibile alternativa venne offerta dalla cosiddetta sostituzione omofonica, che consisteva nell'assegnare ad

ogni lettera un insieme di numeri compresi tra 0 e 99, in base alle frequenze: più una lettera veniva usata, più numeri le corrispondevano; così ogni numero aveva una frequenza di circa l'1% e non si ottenevano informazioni utili con l'analisi delle frequenze; tuttavia lo svantaggio era che ad ogni numero corrispondeva una sola lettera, e quindi in un certo senso le "identità" delle lettere venivano mantenute: ad esempio, in italiano la q è rara, quindi avrà un solo simbolo, ed è sempre seguita dalla u, che ha circa 3 simboli a disposizione, e quindi se si riescono a trovare delle ripetizioni si può procedere alla decifrazione.

Babbage e Kasiski decrittano Vigenère

Una delle figure scientifiche più straordinarie del XIX secolo fu il britannico Charles Babbage, oggi noto principalmente per aver progettato un precursore degli elaboratori elettronici. Fu uno scienziato estremamente poliedrico: capì per primo che la larghezza degli anelli nei tronchi degli alberi dipende dal clima dell'anno precedente, propose il sistema postale a tariffa unica, progettò diverse "macchine delle differenze" per correggere molti calcoli in tavole di navigazione, e soprattutto -per quanto ci riguarda- trovò il punto debole della cifratura di Vigenère.
Appassionato di crittoanalisi fin da piccolo (dice che era in grado di decifrare i messaggi degli altri ragazzi guardando poche parole), si guadagnò la fama di esperto nella società londinese; la più grande sfida che potesse affrontare era quella della sostituzione polialfabetica, portata all'attenzione di tutti da un articolo di un inglese che credeva di averla inventata per primo.

La cifratura di Vigenère sembrava inattaccabile, poiché immune all'analisi delle

Parola chiave:	S	O	L	E	S	O	L	E	S	O	L	E	S	O	L	E	S	O	L	E	S	O	L
Testo chiaro:	n	o	n	v	e	d	o	n	o	n	s	e	n	t	o	n	o	n	p	a	r	l	o
Testo cifrato:	F	C	Y	Z	W	R	Z	R	G	B	D	I	F	H	Z	R	G	B	A	E	J	Z	Z

Figura 4.4: Ripetizione di una stringa criptata con Vigenère

frequenze; ma aveva un'altra debolezza, più nascosta, che si osservava soprattutto in testi lunghi: se la parola chiave è lunga n lettere, allora una parola con meno lettere ha solo n modi possibili di essere cifrata; questo è utile, perché ci sono parole corte come "non" che vengono usate molto di frequente, quindi appaiono più di una volta con la stessa cifratura. Possiamo osservare che se due stringhe uguali del testo in chiaro sono ad una distanza multipla di n, allora verranno cifrate con la stessa sequenza; ad esempio nella figura 4.4 la ripetizione **RGB** deriva dal fatto che i due **non** sono a distanza 8, che è multiplo di 4; questa ripetizione è inevitabile, ed è questo il punto di partenza dell'attacco di Babbage.
Il primo passo nell'analisi di un crittogramma è cercare tutte le ripetizioni di stringhe lunghe 3-4-5 caratteri, e annotare la distanza relativa; questo ci fornisce molte informazioni sulla lunghezza della chiave: se la ripetizione è "autentica" e non casuale, vuol dire che la distanza è un multiplo della lunghezza della chiave, ovvero che la lunghezza della chiave è un divisore della distanza. Compilando una tabella simile a quella di figura 4.5 le cui colonne corrispondono alla lunghezza della chiave e le cui righe sono le stringhe, e segnando le celle in cui la lunghezza è un divisore

Vigenere Repeat Distance Repeated Sequence	Spacing	Possible length of key (or factors) 02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
MVO	156	x	x	x		x						x	x							
BDF	264	x	x	x		x		x			x	x								
NDK	198	x	x			x			x		x							x		
KPT	18	x	x			x			x									x		
KPT	156	x	x	x		x						x	x							
HRV	18	x	x			x			x									x		
HRV	138	x	x			x														
HRV	54	x	x			x			x									x		
HRV	12	x	x	x		x						x								
HCB	84	x	x	x		x	x					x		x						
RVS	18	x	x			x			x									x		
IFC	60	x	x	x	x	x				x		x			x					x
BWX	12	x	x	x		x						x								
DYM	42	x	x			x	x							x						
WBB	36	x	x	x		x			x			x						x		
BBQ	36	x	x	x		x			x			x						x		
RVV	54	x	x			x			x									x		
VVN	54	x	x			x			x									x		
VNH	54	x	x			x			x									x		
NHI	54	x	x			x			x									x		
WBBQ	36	x	x	x		x			x			x						x		
HRVV	54	x	x			x			x									x		
RVVN	54	x	x			x			x									x		
VVNH	54	x	x			x			x									x		
VNHI	54	x	x			x			x									x		
HRVVN	54	x	x			x			x									x		
RVVNH	54	x	x			x			x									x		
VVNHI	54	x	x			x			x									x		

Figura 4.5: Tabella delle possibili lunghezze della chiave

della distanza della stringa ripetuta sulla riga, si può facilmente congetturare la lunghezza della chiave (che nell'esempio è di 6 caratteri). Trovata la lunghezza n della chiave, questa sarà composta dalle lettere per ora sconosciute $L_1L_2 \dots L_n$; la prima lettera del testo in chiaro sarà dunque cifrata con L_1, la seconda con L_2 e così via. Ma la lettera alla posizione $n+1$ sarà cifrata di nuovo con L_1, così come quella in posizione $2n+1$ e tutte le successive a distanza n. Questo vuol dire che la cifratura polialfabeltica è l'unione di n distinte cifrature monoalfabetiche; ma conoscendo n, possiamo applicare l'analisi delle frequenze ad ogni singola parte del crittogramma considerando solo le lettere in posizione $an+b$ con b fissato (pari a $0, 1, \dots, n-1$). Si può dunque creare un'ipotesi di una o più chiavi confrontando ciascuno degli n grafici delle frequenze con quello della lingua originale, come si faceva per decifrare la sostituzione monoalfabetica. Probabilmente la chiave è una parola o una frase di senso compiuto, quindi è ancora più facile indovinarla. Una volta ottenuta la chiave, basta leggere il cifrario come se si fosse il destinatario legittimo.
Questa straordinaria scoperta avvenne circa nel 1854, ma rimase sconosciuta perché Babbage non la pubblicò mai; probabilmente ciò è dovuto al fatto che era appena scoppiata la guerra di Crimea e questa conoscenza dava un grosso vantaggio agli inglesi sui russi, dunque il controspionaggio britannico potrebbe aver imposto il silenzio allo scienziato.
Nel frattempo però il metodo di Babbage era stato scoperto da un ufficiale prussiano in pensione, Friedrich Wilhelm Kasiski, che lo pubblicò nel 1863, e per questo il procedimento crittoanalitico appena descritto prese il nome di "test di Kasiski". Con il tempo si è riusciti anche a dare una descrizione matematico-algoritmica del metodo di decifrazione e per questo oggi sono possibili dei programmi che decriptano cifrature polialfabetiche quasi in automatico.
L'unica possibilità di salvezza del cifrario di Vigenère è quella di avere una chiave molto lunga, possibilmente quanto il messaggio; ma anche questo non garantirebbe

la sicurezza, infatti un crittoanalista potrebbe sostituire parole molto comuni come "che" o "non", le quali darebbero parti di chiave, che se fosse una frase sensata potrebbe essere completata, e con molta pazienza questo lavoro di passare da chiave a testo in chiaro potrebbe essere completato. Serve dunque una serie di caratteri random: un sistema del genere è matematicamente indecifrabile, poiché da ogni messaggio cifrato possiamo ottenere ogni messaggio in chiaro con la chiave giusta, ma non essendocene una preferibile (ad esempio una parola esistente), tutte le decodifiche sono ugualmente valide, e ugualmente inutili. Tuttavia la chiave dovrebbe essere usata una sola volta, altrimenti si può nuovamente effettuare un confronto tra i testi cifrati inserendo parole comuni; vi è dunque l'enorme problema pratico di distribuire molte chiavi casuali a molte persone (i cosiddetti blocchi monouso), e per cui non è mai stata impiegata efficacemente.

Le guerre mondiali

Macchine che codificano

Alla fine dell'Ottocento l'elettricità era piuttosto diffusa, e veniva sfruttata soprattutto per il telegrafo, un sistema di comunicazione che permetteva l'invio di segnali elettrici a distanza attraverso dei fili; occorreva però trasformare i messaggi in un linguaggio che la macchina capisse. Fra le diverse proposte si impose un sistema di linee e punti ideato dal fisico statunitense Samuel F.B. Morse; questo sistema era una semplice sostituzione: ad ogni lettera corrisponde un insieme (da 3 a 5) di punti e linee; occorre precisare che il Morse non è un cifrario, ma solo un alfabeto alternativo perché punta ad essere comprensibile a più persone possibili. L'apparecchio inventato da Morse era costituito da un pulsante, che stabiliva il contatto elettrico; l'apparato ricevente era costituito da un elettromagnete che quando percorso da corrente magnetizzava un blocco di ferro, che attirava una parte mobile emettendo un "tac" peculiare, la cui lunghezza simboleggiava un punto o una linea. L'avvento del telegrafo diffuse anche tra la gente comune l'interesse per la crittografia: infatti per trasmettere un messaggio si doveva ricorrere a un telegrafista, che leggeva il messaggio e se fosse stato in chiaro sarebbe potuto venire a conoscenza di informazioni personali; inoltre, essendo un segnale elettrico trasmesso attraverso dei fili, una spia poteva agganciarsi ad un filo e intercettare tutte le comunicazioni. Per questo tutti iniziarono a cifrare le proprie comunicazioni più segrete contro i ficcanaso, e alcuni scrittori sfruttarono questo interesse nei loro racconti, come Poe, Conan Doyle e Verne.
A inizio Novecento il fisico italiano Guglielmo Marconi fece degli esperimenti sui circuiti elettrici e le onde elettromagnetiche, inventando la radio: si poteva quin-

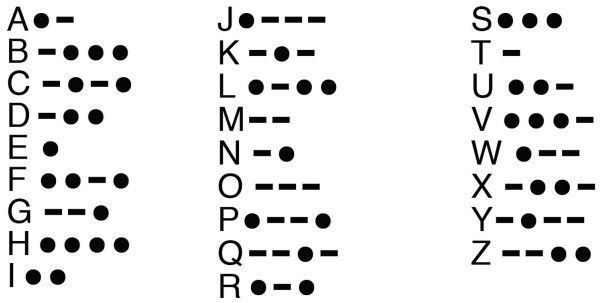
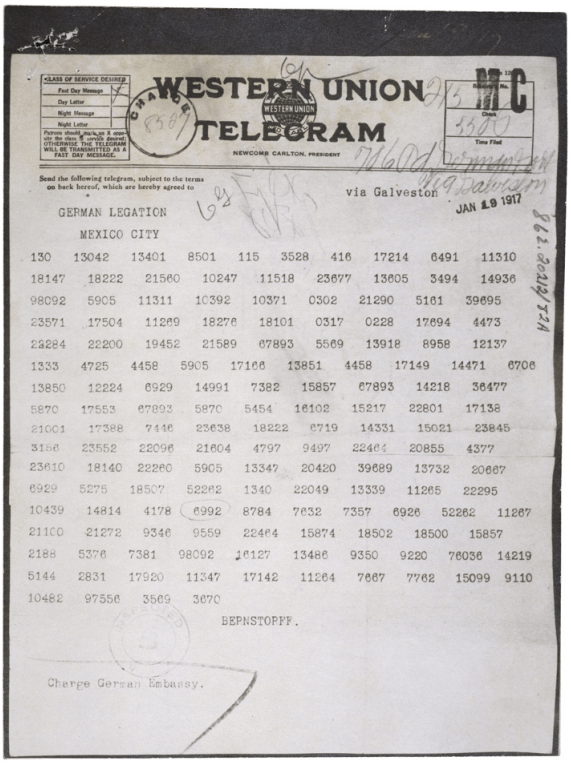


Figura 5.1: Tabella di conversione Morse

di inviare un messaggio in qualunque parte del mondo senza bisogno di fili come dimostrò nel 1901 captando un messaggio inviato dall'Inghilterra in Canada. Questo diede moltissimi vantaggi ai militari, soprattutto agli ammiragli che potevano rimanere in costante contatto con la propri flotta; d'altra parte la natura stessa dei segnali elettromagnetici rende inevitabile l'intercettazione di ogni messaggio da parte dei nemici, e dunque era necessario criptare ogni messaggio con un nuovo sistema affidabile. Questa sete di cifrature impenetrabili non venne soddisfatta e il periodo della prima guerra mondiale fu segnato da una serie di pesanti sconfitte dei crittografi da parte dei crittoanalisti.
Si vede dunque come l'avanzamento della tecnologia faccia progredire anche la crittografia e la crittoanalisi: a partire dal disco di Alberti, passando per le macchine delle differenze di Babbage, si arriverà poi a Enigma e Colossus, per giungere infine ai nostri moderni computer.

Il telegramma Zimmermann

Allo scoppiare della prima guerra mondiale i crittoanalisti più abili d'Europa furono i francesi, primato che mantennero durante tutta la guerra; questo era dovuto alla pesante sconfitta del 1871 nella guerra franco-prussiana, poiché il timore nei confronti della Germania spinse i francesi a cercare di scoprire le mosse future dei tedeschi. Molto importante fu il trattato di Kerckhoffs *La Cryptographie Militaire*, che portò alla creazione di un "Bureau du Chiffre" predisposto in parte alla rottura di nuovi codici, e in parte al lavoro di routine di decifrazione dei messaggi di cui si sapeva fare la crittoanalisi; svilupparono anche l'analisi del traffico: creando delle stazioni con un'antenna direzionabile si poteva scoprire il punto d'origine di una trasmissione, anche senza decifrare il messaggio stesso, ed inoltre impararono anche a riconoscere gli operatori in base alle lunghezze di linee, punti e pause.
Al contrario, i tedeschi entrarono in guerra senza un vero e proprio servizio crittoanalitico e crittografico, di cui non sentivano la necessità all'inizio per eccessiva fiducia in loro stessi e nella guerra lampo, in seguito perché non riuscivano ad intercettare i messaggi nemici che usavano le linee telegrafiche sul proprio territorio. Viceversa, gli alleati avevano sotto controllo sia le trasmissioni radio tedesche, che quelle telegrafiche. Vi sono un paio di episodi che mostrano l'inadeguatezza dei crittografi tedeschi.
Quello più importante, in quanto probabilmente è stato fondamentale per decidere le sorti del conflitto, riguarda la guerra sottomarina. I tedeschi infatti all'inizio della guerra volevano forzare il blocco navale inglese e separare la Francia dalla Gran Bretagna; tuttavia il 7 maggio 1915 un U-boot tedesco affondò il piroscafo *Lusitania* causando la morte di 1198 civili, di cui 128 statunitensi, motivo per cui il presidente Wilson impose che i sottomarini dovessero emergere prima di attaccare per evitare altre stragi, ma riducendo il potenziale di attacco. La Germania accettò il compromesso e nel 1916 era stato nominato come nuovo ministro degli Esteri un uomo con fama di grande negoziatore, Arthur Zimmermann, notizia che venne accolta con grande euforia negli Stati Uniti.
Nel gennaio 1917 ci fu una riunione, a cui partecipò anche Zimmermann, nella



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
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTOPFF.

Charge German Embassy.

Figura 5.2: Il telegramma Zimmermann cifrato

quale si decise di iniziare una guerra sottomarina indiscriminata, che in breve tempo avrebbe ridotto la Gran Bretagna alla fame; era però fondamentale ritardare il più possibile l'entrata in guerra degli Stati Uniti, e per questo si decise di offrire un'alleanza al Messico che avrebbe dovuto impegnare gli Stati Uniti sul loro fronte meridionale; inoltre il presidente messicano avrebbe anche dovuto persuadere il Giappone ad attaccare lungo la costa pacifica. La proposta venne riassunta in un telegramma, da cifrare (vedi figura 5.2) ed inviare all'ambasciatore a Washington che l'avrebbe inoltrato all'ambasciatore messicano, proposto qua di seguito

> *Abbiamo intenzione di cominciare il primo di febbraio una guerra sottomarina illimitata. Tenteremo però di far rimanere neutrali gli Stati Uniti d'America. Nel caso non riuscissimo, facciamo una proposta di alleanza al Messico sulle seguenti basi: condurre la guerra comunemente, siglare la pace comunemente, un generoso supporto finanziario e l'accettazione da parte nostra della riconquista messicana dei territori perduti del Texas, del Nuovo Messico e dell'Arizona. La discussione dei dettagli viene lasciata a voi. Informerete il Presidente di cui sopra nella maniera più segreta, non appena si profili la certezza della guerra contro gli Stati Uniti d'America, aggiungerete suggerimenti su vostra iniziativa, inviterete il Giappone ad un'adesione immediata ed allo stesso tempo farete da mediatore tra il Giappone e voi stessi. Per favore richiami l'attenzione del Presidente sul fatto che l'utilizzo illimitato dei nostri sottomarini ci offre la prospettiva di costringere l'Inghilterra a siglare la pace in pochi mesi. Firmato, Zimmermann.*

Il telegramma venne ovviamente intercettato dagli inglesi, che lo passarono alla Stanza 40 (l'ufficio cifre della Marina) e la sua decifrazione venne affidata a Motgomery e de Grey; non fu un lavoro semplice perché l'algoritmo combinava la codifica e la cifratura, ma sfruttando l'analisi su telegrammi precedenti in qualche ora riuscirono a comprendere alcune parole. In pochi giorni capirono a grandi linee il progetto tedesco, e portarono il telegramma in parte decifrato all'ammiraglio Hall, che però non lo diffuse e chiese solo di completare il lavoro. I suoi timori erano infatti molteplici: intanto il telegramma era stato trasmesso sulla linea protetta dagli Stati Uniti; inoltre i tedeschi avrebbero compreso che il loro codice era stato violato e l'avrebbero cambiato, privando gli inglesi di una fonte di informazioni; infine l'offensiva tedesca sarebbe scattata comunque, e in poche settimane probabilmente Wilson sarebbe comunque entrato in guerra.
Tuttavia il 3 febbraio il presidente americano annunciò al Congresso la neutralità degli Stati Uniti; questo spinse Hall ad usare il telegramma Zimmermann, poiché nel frattempo era riuscito ad ottenere la versione messicana e poté convincere tutti che l'operazione di spionaggio fosse avvenuta in Messico e non intercettando e decifrando il messaggio in Inghilterra. A fine febbraio il governo americano divulgò il telegramma, e quasi subito il ministro tedesco se ne assunse la paternità; perciò il 6 aprile 1917 gli Stati Uniti entrarono in guerra, compensando il cedimento della Russia e portando il conflitto verso la fine.

La macchina Enigma

Nel 1923 l'ingegnere tedesco Arthur Scherbius brevettò una macchina progettata per facilitare le comunicazioni segrete, portando l'elettromeccanica nel mondo della crittografia per la prima volta; la macchina, chiamata Enigma, sarebbe passata alla storia come uno dei più temibili sistemi crittografici. L'idea fondamentale non è per nulla innovativa e riprende il disco di Alberti, ma la componente elettrica rende impossibile l'analisi classica a mano; per questo nella decifrazione entreranno in gioco altri congegni meccanici, riproduzioni della macchina stessa, e anche quello che può essere considerato il primo computer della storia.
Immaginiamo ora di smontare una macchina Enigma nei suoi componenti più sempli-

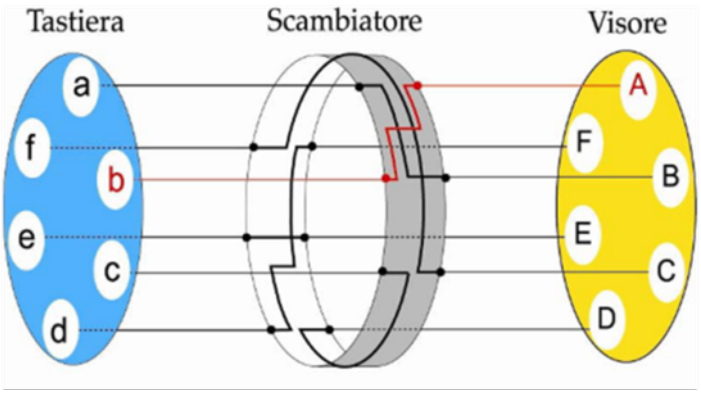


Figura 5.3: I tre elementi fondamentali di Enigma

ci; le parti principali sono tre: una tastiera, del tutto simile a quella di una macchina da scrivere, un pannello luminoso che indica quale lettera inserire nel crittogramma, e uno scambiatore. Lo scambiatore è un disco di gomma percorso da una complessa rete di fili: ogni lettera della tastiera è collegata ad un ingresso dello scambiatore, e ogni uscita è collegata ad una lampadina; il circuito interno determina in pratica l'alfabeto cifrante.
L'idea successiva è quella di far ruotare lo scambiatore ad ogni pressione di una lettera, in modo da cambiare ogni volta l'alfabeto cifrante in maniera simile ad un cifrario polialfabetico; i crittoanalisti sapevano decifrare questo tipo di codice, per cui Scherbius aggiunse un secondo scambiatore, anch'esso rotante in modo simile al contachilometri di una macchina: dopo un giro completo di un rotore, il secondo ruotava di una posizione, poi il primo faceva di nuovo un giro completo e così via; per avere una sicurezza ancora maggiore inserì anche un terzo rotore, che girava anch'esso come un contachilometri (a questo punto era una sorta di unità-decine-centinaia, solo che ogni "cifra" aveva 26 valori diversi) portando così il numero di alfabeti cifranti a $26 \cdot 26 \cdot 26 = 17576$. Il passaggio da un alfabeto all'altro avveniva automaticamente grazie ai congegni meccanici e dunque la cifratura avveniva molto rapidamente.

Per velocizzare anche la lettura l'inventore aggiunse un riflessore: anch'esso un

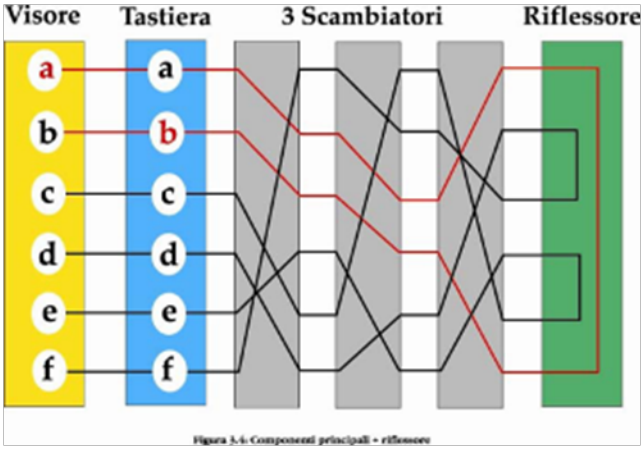


Figura 5.4: Schema semplificato di una macchina Enigma con tre rotori e il riflessore

disco di gomma con circuiti interni intrecciati, ma che riemergevano dallo stesso lato; in questo modo il segnale elettrico riattraversava i rotori, ma con un percorso differente. Ad esempio, in figura 5.4 la pressione del tasto **b** invia un impulso elettrico che giunge fino alla lampadina **A**; osservando com'è costruita la macchina ci accorgiamo che, mantenendo lo stesso assetto, la pressione del tasto **a** manda un impulso che percorre il circuito al contrario, finendo sulla lampadina **B**: dunque il processo di decifrazione è identico a quello di cifratura; l'unica cosa importante è l'assetto iniziale dei rotori, che doveva essere distribuito, ma nella seconda guerra mondiale si usava una chiave al giorno, quindi bastava un foglio contenente le chiavi di tutto il mese.
Tuttavia 17576 era ancora un numero abbastanza basso di chiavi, soprattutto se si considerava che probabilmente alcune macchine sarebbero state catturate; immagi-

nando di controllare un assetto al minuto, per verificarli tutti ci sarebbero volute un paio di settimane; ma impiegando una decina di operatori solo per questo compito, si riusciva a scoprire la chiave nell'arco di una giornata, e con un po' di fortuna in qualche ora.
Pertanto Schrebius decise di introdurre due nuove caratteristiche: intanto rese i rotori removibili ed interscambiabili, aumentando il numero delle possibili disposizioni; inoltre inserì un pannello a prese multiple tra la tastiera ed il primo rotore, che permetteva di inserire alcuni cavi per scambiare alcune lettere (ad esempio scambiando A e C, l'impulso dovuto alla pressione di **b** avrebbe seguito il percorso descritto, salvo poi uscito dal rotore in corrispondenza di **A** finire sul visore in **C**).
Siamo ora in grado di calcolare il numero di possibili chiavi di una macchina Enigma:

Figura 5.5: Una macchina Enigma con tutti i suoi elementi

Orientamento: ognuno dei tre dischi può essere ruotato in 26 modi possibili, quindi si hanno $26^3 = 17576$ possibili combinazioni di orientamenti

Posizione: potendo scegliere tra n rotori ho $M = n(n-1)(n-2)$ possibili configurazioni, che con $n = 3$ dà $M = 6$, e con $n' = 5$ (usato durante la guerra) dà $M' = 60$

Pannello: avendo a disposizione n cavi, il numero di possibili scelte di coppie è $M = \dfrac{26!}{(26-2n)! \cdot n! \cdot 2^n}$; il progetto originale prevedeva $n = 6$, ovvero $M = 100.391.791.500$, ma nelle fasi più avanzate della guerra si passò a $n' = 10$ ovvero $M' = 150.738.274.937.250$

Il numero totale di chiavi possibili è dato dal prodotto dei tre numeri, e in un caso si ottiene circa 10 milioni di miliardi, nell'altro 158 miliardi di miliardi. Questo rende un attacco bruteforce assolutamente impensabile e inattuabile. Come si può notare, il contributo maggiore arriva dal pannello; tuttavia se ci fosse solo questo, si avrebbe

una semplice sotituzione monoalfabetica, per di più solo su un insieme limitato di lettere. Combinando quindi il gran numero di chiavi di una cifratura debole con il ristretto numero di chiavi delle cifratura forte dei rotori, si ottiene un congegno che crea crittogrammi impossibili da risolvere.
Così pensava l'inventore, e anche i tedeschi che comprarono da lui il brevetto: non volevano ripetere l'esperienza della Grande guerra, tanto più che negli anni Venti gli inglesi resero noti i propri attacchi crittoanalitici alla Germania. Scherbius modificò i circuiti dei rotori, per evitare che i privati che avevano acquistato la sua macchina ricostruissero nei dettagli il funzionamento di quella ad uso militare; a partire dal 1925 e per i due decenni successivi le forze armate della Germania acquistarono circa 30.000 esemplari di macchine Enigma, che per un periodo sembrò portare al trionfo le armate naziste, ma poi fu una delle cause della loro sconfitta.

Far breccia in Enigma: Rejewski

I primi a tentare di violare la cifratura Enigma, con qualche successo, furono i polacchi già ben prima della guerra; infatti la Polonia, nonostante la riconquista dell'indipendenza, non poteva permettersi di rilassarsi e aveva sempre il timore di un'aggressione straniera, mentre le altre potenze alleate ritenevano il proprio predominio indiscusso. Affamati di notizie riservate, si munirono di un ufficio cifre, il Biuro Szyfròw; poiché Enigma era un congegno elettromeccanico, ritennero più opportuno affidare il compito a persone dell'area tecnico-scientifica, il più brillante delle quali si rivelò essere il matematico Marian Rejewski.
Per una prima fase tuttavia è servito un lavoro di intelligence nel senso classico del termine: le spie francesi riuscirono ad entrare in contatto con Hans-Tilo Schmidt, un tedesco insoddisfatto della propria patria che lavorava come impiegato nella *Chiffrierstelle*, la sala comandi della rete Enigma; nel 1931 vendette due manuali d'uso che permisero di ricostruire la versione militare della macchina, e avrebbe fornito per qualche anno le tabelle mensili con le chiavi. Tuttavia il Bureau du Chiffre era impreparato ad affrontare la decriptazione di Enigma, anche avendo a disposizione la macchina fisica, e dunque consegnarono tutto il proprio materiale ai polacchi, con cui avevano stretto un'alleanza.

Per la sua analisi Rejewski sfruttò un'indicazione che secondo i tedeschi avrebbe reso più sicuro il codice: per inviare un messaggio si impostava la macchina seguendo la chiave giornaliera, ma poi si sceglieva un nuovo orientamento dei rotori, da comunicare all'inizio del messaggio, che dopo sarebbe stato cifrato con il nuovo assetto; ad esempio, se la chiave giornaliera prevedeva l'orientamento ABC, e il mittente decideva come chiave di messaggio l'orientamento DEF, avrebbe dovuto mettere i rotori in posizione ABC, criptare la stringa **defdef** in poniamo **FHEKUJ**, poi spostare i rotori in posizione DEF e criptare il resto del messaggio; il destinatario avrebbe letto la stringa con la chiave di messaggio usando la chiave giornaliera, e poi il contenuto

vero e proprio muovendo i rotori secondo le intenzioni del mittente. In questo modo si riduceva drasticamente la quantità di testo cifrato con una stessa chiave, a prima vista complicando il lavoro dei crittoanalisti.
Tuttavia in questo modo Rejewski conosceva la struttura delle prime sei lettere di ogni messaggio: la prima e la quarta lettera erano cifrature della stessa lettera, così come la seconda e la quinta, la terza e la sesta; dunque queste coppie di lettere sono strettamente legate dall'assetto iniziale di Enigma. Ogni giorno riceveva moltissimi messaggi intercettati, e procedeva a costruire una tabella in questo modo: supponiamo di avere il messaggio **LOKRGM**, questo vuol dire che **L** e **R** sono cifrature della stessa lettera, solo con i rotori in tre posizioni più avanti; nella prima riga della tabella venivano inserite le prime lettere, nella seconda le quarte, in modo che ad esempio sotto la **L** ci fosse la **R**. Dopo un numero sufficiente di messaggi, poteva avere la tabella completa, ad esempio come in figura.
Procedeva ora a cercare delle concatenazioni: partendo da una lettera, legge quella

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

Figura 5.6: Tabella di Rejewski

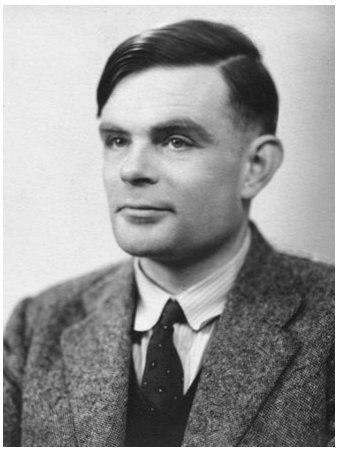
sottostante, che poi va a cercare nella prima riga e così via fino a tornare alla lettera di partenza; ad esempio alla **A** della prima riga è abbinata la **F** della seconda, poi sotto la **F** della prima riga c'è la **W** e infine alla **W** è associata la **A**. Trovati tutti i cicli nella tabella, e contando il numero di collegamenti, si accorse che cambiava ogni giorno, ovvero dipendeva fortemente dall'assetto iniziale.
La vera scoperta però fu che la struttura dipendeva solo dai rotori e non dal pannello a prese multiple, poiché era solamente un "doppio scambio"; vediamo di capire perché: se chiamiamo 1 la funzione che cifra la prima lettera, e 4 quella che cifra la quarta, abbiamo che ci sono quattro lettere a, b, c, d per cui vale $1(a) = G, 1(b) = S, 1(c) = H, 1(d) = X$, e in particolare sono le inverse ovvero $a = 1(G)$ e simili; inoltre la tabella dice che $4(a) = O, 4(b) = T, 4(c) = G, 4(d) = S$; supponiamo ora di scambiare G, S, e questa modifica rimane invariata sia cifrando la prima che la quarta lettera, e dunque $1'(a) = S, 1'(b) = G, 1'(c) = H, 1'(d) = X$ e $4'(a) = O, 4'(b) = T, 4'(c) = S, 4'(d) = G$; provando allora a rifare la tabella avremo che S sta sotto H e G sta sotto X, ma d'altra parte anche O e T si sono invertite portando dunque ai cicli $H \to S \to O$ e $X \to G \to T$.
Questo significa che il numero e la lunghezza dei cicli è come un'impronta digitale dell'orientamento dei rotori, per i quali ci sono "solo" $6 \cdot 17.576 = 107.456$; avendo a disposizione repliche di Enigma, Rejewski e i suoi collaboratori si divisero il compito di controllare tutti gli assetti e stilare un catalogo della struttura di ogni assetto; per completare l'opera ci volle quasi un anno, ma a quel punto bastava compilare la tabella per le tre lettere della chiave e controllare nel registro quale fosse l'assetto giornaliero.
Ricavare la configurazione del pannello a questo punto era abbastanza semplice, anche se lungo da fare a mano, perché ad esempio andava controllato che le prime tre lettere di ogni messaggio fossero uguali alle seconde tre partendo dall'ipotesi che non ci fossero collegamenti e andando a tentativi, oppure confrontando le permutazioni

dei rotori con quelle delle tabelle.
In seguito i tedeschi apportarono alcune modifiche, e gli elenchi stilati diventarono inutilizzabili; a questo punto Rejewski decise di automatizzare il processo e realizzò un congegno in grado di controllare automaticamente i 17.576 orientamenti fino a trovare una corrispondenza con i dati forniti; questa macchina consisteva in una versione modificata di Enigma e venne chiamata "bomba", probabilmente in riferimento al ticchettio di quando passava da una configurazione all'altra; poiché i rotori potevano essere posizionati in 6 modi, furono necessarie sei macchine per controllare tutti i possibili casi.
Tuttavia nel 1938 Rejewski dovette arrendersi ai crittografi tedeschi: aggiunsero altri due rotori, portando a 60 il numero di sequenze possibili e dunque di bombe necessarie, e diedero in dotazione ad ogni macchina dieci cavetti, in modo che il pannello scambiasse venti lettere. Nel frattempo Hitler sembrava progettare un'invasione della Polonia; il capo del Biuro allora decise di informare Francia e Gran Bretagna dei propri progressi per non disperderli nel caso di attacco, e fornì delle copie della macchina Enigma e delle bombe ai capi dello spionaggio inglese e francese che in questo modo poterono proseguire l'opera di decifrazione avendo anche a disposizione più risorse economiche.

Alan Turing a Bletchley Park

L'esperienza polacca aveva mostrato che Enigma non era inviolabile, e che per decifrarla occorrevano matematici anziché linguisti; furono dunque reclutati giovani studenti e laureati a Oxford e Cambridge, e riuniti nella sede della Government Code and Cypher School che sostituiva la Stanza 40; questa si trovava a Bletchley Park, che in tempo di guerra ospitò settemila operatori, suddivisi in varie "capanne" a seconda del compito.
In breve tempo gli inglesi padroneggiarono il metodo di analisi elaborato da Rejewski, e grazie alle maggiori risorse economiche e umane molto spesso riuscivano a ottenere la chiave giornaliera per poter poi decifrare i messaggi del resto della giornata; ad esempio, durante la Battaglia d'Inghilterra i crittoanalisti riuscivano spesso a comunicare il luogo e il momento delle incursioni tedesche e fornivano continuamente informazioni sullo stato della Luftwaffe, l'aviazione tedesca.
Riuscendo a decifrare già buona parte dei messaggi, ci si concentrò sul trovare un metodo alternativo e più rapido, e che avrebbe funzionato anche in altre circostanze: veniva infatti sfruttato il fatto che la chiave di messaggio fosse ripetuta per due volte di seguito, e che spesso fosse banale come EEE, o ripetuta per molti messaggi dello stesso operatore (magari le iniziali della fidanzata, da cui il soprannome di *cillies*). Inoltre alcune procedure di sicurezza dei tedeschi abbassavano il numero totale di chiavi, ad esempio il fatto che lo stesso rotore non potesse trovarsi nella stessa posizione per due giorni di fila, o che una lettera non fosse collegata nel pannello alle due adiacenti. In seguito alle continue modifiche di Enigma servivano dunque continue innovazioni da parte dei crittoanalisti.
Uno dei personaggi più rilevanti per la decifrazione di Enigma fu il matematico Alan Turing. Nato a Londra nel 1912, fu iscritto alla Sherborne School a quattordici anni,

dove instaurò una profonda amicizia con Christopher Morcom; nel 1930 l'amico morì di tubercolosi e Turing si dedicò solo agli studi.
Nel 1931 entrò al King's College dove incontrò tra gli altri Bertrand Russel; nel 1937 pubblicò il suo lavoro teorico più importante, "On Computable Numbers", nel quale descrisse anche una macchina immaginaria che potesse svolgere un certo algoritmo, e poi l'unione di queste macchine, oggi chiamata macchina di Turing, che sarebbe stata in grado di rispondere a qualunque domanda razionale; con l'ausilio di questo strumento teorico dimostrò che a priori non si poteva conoscere se una proposizione era indecidibile o meno, portando avanti il lavoro di Gödel del 1931. Era diventato professore a Cambridge e oltre ai successi accademici ne aveva anche dal punto di vista personale: grazie all'ambiente tollerante poté avere un certo numero di relazioni omosessuali senza timori. Il 4 settembre 1939, il giorno successivo all'entrata in guerra della Gran Bretagna, venne reclutato a Bletchley Park; era incaricato di escogitare una crittoanalisi alternativa di Enigma che non sfruttasse la ripetizione delle chiavi.



Studiando i crittogrammi già decifrati notò che in buona parte possedevano una struttura piuttosto rigida, e pensò che il contenuto di quelli nuovi si potesse inferire da quello vecchio; per esempio verso le sei del mattino i tedeschi inviavano bollettini meteorologici criptati, che quasi sicuramente contenevano la parola "wetter" (tempo atmosferico in tedesco) verso l'inizio, per di più in posizioni quasi fissate. Frammenti di testo chiaro di questo genere venivano chiamati *cribs*; Turing cercò dunque di sfruttare questi *cribs* per dedurre l'assetto di Enigma per quel messaggio, ovvero quali disposizioni di rotori e cavetti trasformasse la stringa cifrata nella parola in chiaro.
Come per Rejewski, si doveva cercare una caratteristica che dipendesse solamente dalla disposizione dei rotori, per i quali si sarebbero potute controllare meccanicamente le $60 \cdot 17.576 = 1.054.560$ disposizioni possibili; Turing cercò dunque delle concatenazioni tra un *crib* e il relativo messaggio cifrato, ovvero dei cicli di lettere, sapendo che Enigma è simmetrica, quindi gli elementi di una coppia sono interscambiabili; in particolare nella figura 5.7 possiamo notare che in posizione 2 e 3 **t** è cifrata come **N** e **S** quindi abbiamo il ciclo NTS; similmente ci sono i cicli AWCNT e ATLK, riassunti nel diagramma in figura. L'individuazione della corrispondenza probabile tra *crib* e testo chiaro era facilitata anche dal fatto che Enigma non poteva cifrare una lettera con se stessa; dunque per trovare la giusta posizione basta far scorrere il testo chiaro sul testo cifrato fino ad un punto nel quale non ci siano corrispondenze di lettere uguali.

Queste concatenazioni apparentemente casuali in realtà servono per ricavare l'assetto dei rotori, avendo a disposizione un numero sufficiente di repliche di Enigma; infatti Turing immagina di mettere in serie dei rotori, spostati secondo il numero indicato dal diagramma: oltre ad automatizzare il processo di verifica, questo ha l'effetto di annullare il pannello a prese multiple. Se infatti due lettere a, b fossero scambiate, quando il segnale elettrico (per esempio dopo aver premuto una lettera

Testo cifrato:	W	S	N	P	N	L	K	L	S	T	C	S
Crib in chiaro:	a	t	t	a	c	k	a	t	d	a	w	n
Posizione relativa:	1	2	3	4	5	6	7	8	9	10	11	12

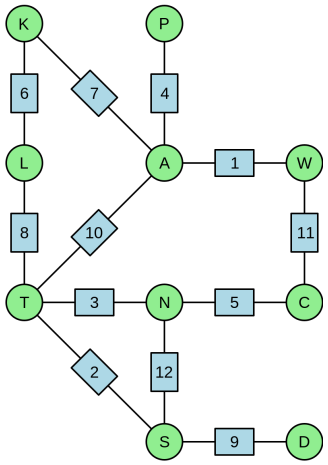


Figura 5.7: Concatenazione di un crib

c) esce dai rotori in corrispondenza di b, dopo il pannello è in corrispondenza di a; schiacciando ora a su di una macchina con lo stesso pannello, questa entra nei rotori come b: i pannelli si escludono a vicenda e basta dunque collegare i blocchi di 3 rotori più riflessore.
Creando dunque un percorso chiuso e inserendo una lampadina si può verificare se una certa disposizione dei rotori può criptare il crib nel modo che si è supposto semplicemente vedendo se la lampadina si accende; altrimenti basta mandare avanti di una posizione tutti i rotori contemporaneamente (mantenendo dunque le distanze relative). Se questa macchina controllasse un assetto al secondo, ci vorrebbero circa 5 ore per controllarli tutti. Dopo aver ottenuto la chiave di messaggio, si può ricavare la configurazione del pannello trascrivendo il messaggio cifrato con il pannello scollegato e poi verificare quali coppie di lettere sono scambiate, il che si può fare a mano, o anche con la semplice analisi delle frequenze, dato che il pannello è una sostituzione monoalfabetica.
Il genio di Turing non si fermò qui e ideò un metodo per trovare automaticamente anche la configurazione del pannello, sfruttando il fatto che ogni lettera può essere scambiata con al più un'altra; collegando opportunamente (vedi figura 5.8) ciascuna terna di rotori alle altre, configurazione poi migliorata con una "scheda diagonale" proposta dal collega Welchman, dando corrente ad un singolo cavo si riescono a ricavare le lettere scambiate.

La prima Bomba di Turing venne consegnata il 14 marzo 1940; era larga 2.01m, alta 1.98 metri, profonda 0.61m e conteneva l'equivalente di 36 macchine Enigma; tuttavia questa prima versione si rivelò troppo lenta (il disco più veloce si muoveva a 50.4rpm); vennero apportate alcune modifiche al progetto, ma nel frattempo i tedeschi smisero di raddoppiare le chiavi e ci fu un crollo di decifrazioni; fortunatamente la seconda macchina giunse l'8 agosto e si ricominciò a decifrare Enigma. In pochi mesi il governo inglese fece costruire altre Bombe, che erano in grado di trovare una chiave nel giro di un'ora, anche se spesso le macchine lavoravano su *crib* falsi, perché non era facile trovarli.
L'osso più duro per gli uffici crittografici Alleati fu la versione di Enigma per la Marina tedesca: possedevano 4 slot per i rotori e potevano sceglierli da un insieme

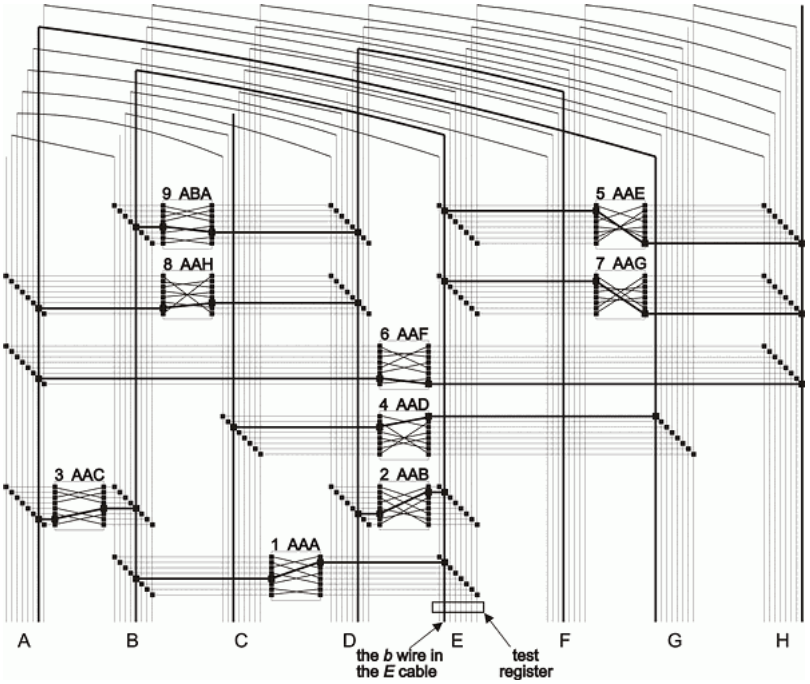


Figura 5.8: Schema dei collegamenti di una Bomba con 8 lettere

di 8; inoltre il riflessore poteva assumere 26 orientamenti diversi; infine gli operatori prestavano più attenzione ai *cribs* e avevano ideato una procedura d'invio della chiave di messaggio più affidabile. A questo punto gli Alleati diedero fondo a tutte le proprie risorse: gli inglesi mandavano la RAF a effettuare bombardamenti mirati, in modo da sapere che i messaggi contenevano ad esempio il luogo dell'attacco; inoltre si puntò molto sulle azioni di spionaggio per rubare i cifrari; infine i progetti delle bombe furono mandati agli Americani, che costruirono delle macchine con quattro rotori, il più veloce dei quali faceva 1725 giri al minuto (per una semplice macchina a 3 rotori, bastavano 50 secondi per scoprire la chiave).
Ma alla fine questi sforzi furono ripagati dall'enorme quantità di materiale decifrato, designato come dossier Ultra, che comprendeva anche le decifrazioni dell'altra macchina tedesca, Lorenz, e quella giapponese Purple; tra i successi dovuti a Ultra ricordiamo:

Battaglia d'Inghilterra La RAF era a conoscenza degli obiettivi tedeschi, e del numero di aerei abbattuti e quelli messi in servizio nella Luftwaffe

Battaglia di capo Matapan La disfatta nella battaglia navale del 1941 è in gran parte dovuta al fatto che la Marina inglese conosceva la posizione esatta delle navi italiane

Operazione Barbarossa Gli inglesi erano a conoscenza del progetto tedesco di invadere l'URSS, ma questi ultimi non ci credettero

Battaglia dell'Atlantico Dal 1942 gli Alleati riuscirono a leggere i messaggi di Enigma navale e quindi poterono evitare gli U-boot e affondare le navi tedesche di rifornimento

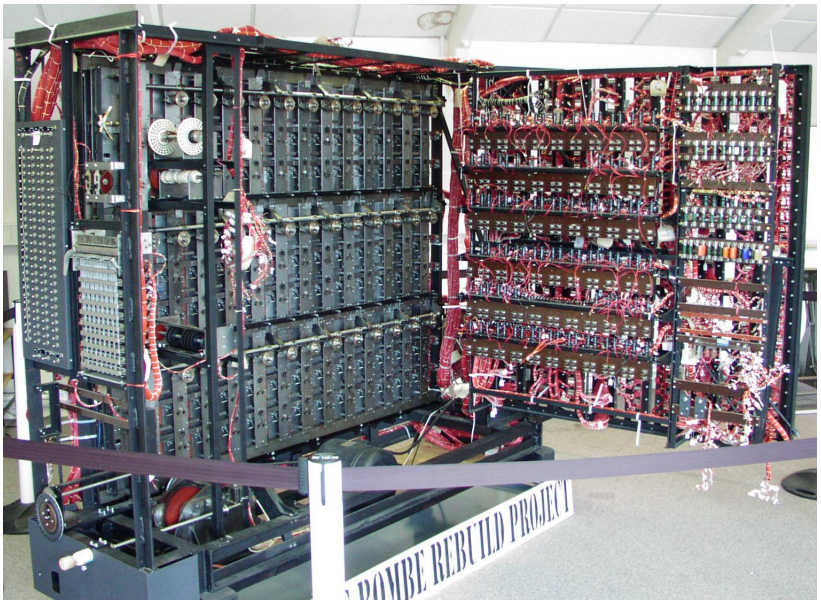


Figura 5.9: Ricostruzione moderna di una Bomba

Battaglia del Mar dei Coralli Decifrando i codici giapponesi, gli americani iniziarono a vincere sul fronte pacifico, poi anche nella battaglia delle Midway

Invasione della Sicilia Gli Alleati conoscevano i punti in cui c'era una maggiore concentrazione di soldati tedeschi

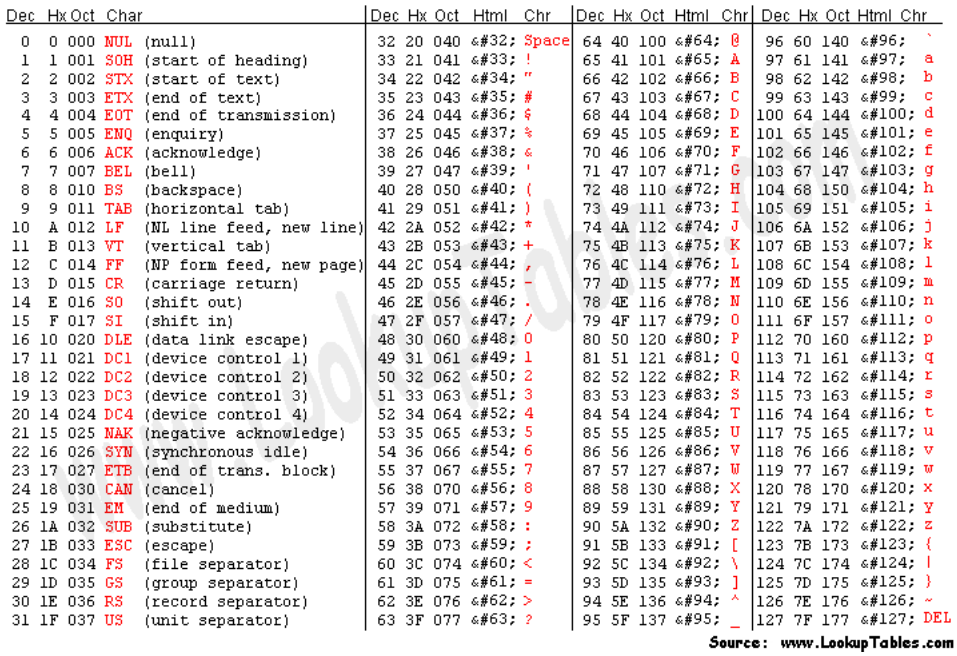
Operazione Overlord Lo sbarco in Normandia non era stato previsto dai tedeschi, e anche alcuni giorni dopo pensavano che fosse solo un diversivo

Come punto a sfavore degli inglesi ricordiamo il trattamento riservato a Turing, dopo che ha permesso di vincere la guerra. Nel 1952, denunciando di aver subito un furto, rivelò ingenuamente alla polizia di avere una relazione con un altro uomo; per questo venne arrestato, accusato di "atti gravemente contrari alla pubblica decenza"; i giornali seguirono il processo, contribuendo ad umiliarlo pubblicamente. Venne estromesso da tutte le collaborazioni con il governo, e anche dalle ricerche sui calcolatori elettronici; fu costretto a frequentare uno psichiatra e subire trattamenti ormonali che lo resero obeso (quando per tutta la vita era stato un grande maratoneta). Cadde dunque in una profonda depressione, e il 7 giugno 1954 entrò nella sua camera con una mela che aveva inzuppato in una soluzione di cianuro; morì così a 42 anni una delle più grandi menti del Novecento.

L'era digitale

L'avvento del sistema binario

Durante la seconda guerra mondiale a Bletchley Park non c'erano solo le Bombe di Turing, ma anche Colossus, un elaboratore progettato da un altro matematico, Max Newman, per decifrare la macchina Lorenz; questa era più complicata di Enigma e la sua crittoanalisi richiedeva lo svolgimento di molte operazioni diverse. Colossus era dotato di valvole elettroniche, che lo rendevano più veloce, e soprattutto era programmabile. Come tutti gli altri apparecchi di Bletchley Park fu distrutto insieme al suo progetto dopo la guerra, e dunque la storia ufficiale ha considerato ENIAC, realizzato nel 1945, il primo computer della storia.
La guerra tra crittografi e crittoanalisti da questo punto in avanti si sposta sull'informatica; i computer infatti hanno solo componenti elettroniche, e questo permette una grandissima potenza e velocità, inimmaginabile con componenti meccaniche. Un altra differenza sostanziale con le cifrature meccanizzate, è che il computer lavora solo con stringhe di numeri, e più precisamente con 0 e 1, che vengono chiamati bit (da **bi**nary digi**t**, cifra binaria); queste sequenze di 0 e 1 non sono nient'altro che l'indicazione "passa corrente" o "non passa corrente", ma grazie a circuiti molto elaborati oggi con un computer possiamo fare quasi ogni operazione.
Ovviamente siamo abituati al fatto che i computer "conoscano" le lettere; questo avviene grazie ad una codifica, molto simile a quella Morse, che trasforma ogni lettera (e i numeri e alcumi simboli) in una sequenza di 8 bit chiamata byte; la tabella di conversione usata e ormai onnipresente è chiamata ASCII e permette la comunicazione tra utente e computer attraverso i $2^8 = 256$ simboli che fornisce. Per comodità gli informatici hanno affiancato al sistema binario il sistema esadecimale; poiché $16 = 2^4$, ogni stringa binaria di lunghezza 4 si traduce in un "numero" esadecimale, che per i numeri da 10 a 15 ha adottato le lettere A... F; in questo modo ogni byte può essere espresso come un numero esadecimale di due cifre; ad esempio, secondo la tabella 6.1 il carattere Z ha il valore $90_{10} = 01011010_2 = 5A_{16}$.
Con il codice binario si possono effettuare delle semplici cifrature per sostituzione e per trasposizione; ad esempio per cifrare il carattere $S = 1010011$ si può procedere in due modi: o si scambiano i bit di due posti adiacenti, generando la stringa 0101101 che corrisponde al carattere −; oppure occorre una chiave, ad esempio $D = 1000100$, che viene sommata effettuando uno XOR bit per bit (ovvero restituisce 0 se i due addendi sono uguali, 1 se sono diversi) ottenendo $S \oplus D = 0010111$.
Nel corso degli anni Sessanta i calcolatori diventarono sempre più potenti e meno costosi, e dunque molto più frequenti anche per uso privato; in particolare molte



Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Figura 6.1: La tabella di conversione ASCII

aziende cominciarono ad usarli, e adottarono sistemi crittografici all'interno, che però non erano standardizzati e occorreva dunque mettersi d'accordo su quale metodo di cifratura usare. Nel 1973 il National Bureau of Standards invitò ufficialmente ad avanzare proposte per un sistema crittografico; un buon candidato fu il sistema Lucifer della IBM, ostacolato però dalla National Security Agency che volle ridurre il numero delle chiavi ad una grandezza sufficiente per la sicurezza privata ma abbastanza bassa per permettere a quest'ultima di curiosare nelle comunicazioni di tutti i privati; nel 1976 la cifratura Lucifer con chiavi a 56 bit fu adottata ufficialmente con il nome di DES.
Il problema però era sempre lo stesso: la distribuzione delle chiavi; le banche americane adottarono il sistema di corrieri affidabili che percorrevano il paese con borse dalle serrature sofisticatissime per consegnare di persona le chiavi informatiche. Ovviamente ci si accorse ben presto che questa pratica aveva dei costi proibitivi, soprattutto per le aziende private; allora già a partire dal dopoguerra tutti sognavano un'alternativa alla distribuzione delle chiavi, che divenne come un Santo Graal della crittografia: alcuni ne sostenevano l'inesistenza, altri la cercavano disperatamente.

Crittografia a chiave pubblica: Diffie e Hellman

Whitfield Diffie è uno dei crittografi più vulcanici del suo tempo; è nato nel 1944 e ha vissuto per gran parte della sua infanzia a New York. Fin da bambino era affascinato dalla matematica e la sua passione lo portò a laurearsi al MIT nel 1965; all'inizio degli anni Settanta era diventato uno dei pochi autentici esperti indipendenti nel campo della sicurezza dei dati informatici. Era particolarmente interessato al problema

della distribuzione delle chiavi, e divenne la sua principale occupazione; la sua visione del futuro era di un mondo inter-connesso, come lasciava intravedere la creazione di ARPAnet, che nel 1982 generò Internet. La domanda che si pose Diffie fu come potevano due estranei scambiarsi messaggi in segreto su Internet, o che una persona volesse acquistare un prodotto.
La risposta giunse dall'incontro con un altro crittografo, Martin Hellman, anche lui alla presa con il problema delle chiavi: se due persone devono comunicare in segreto, dovrebbero già condividere un altro segreto, la chiave. Tuttavia una storiella antica faceva traballare questa convinzione: in un paese di ladri, qualunque cosa esca dalla casa di un abitante viene rubata, anche se è addosso alla persona; allora due amici Alice e Bob si chiedono come mandarsi un anello senza che venga rubato. Una strada è che Bob lo chiuda in una cassaforte, e vi metta un lucchetto; ma Alice per aprirlo dovrebbe avere la chiave, e Bob non può inviarla; di nuovo non sembra esserci via d'uscita. Ma immaginiamo che Bob invii la cassaforte chiusa con il proprio lucchetto ad Alice, e che questa aggiunga il proprio lucchetto, rispedendolo indietro a Bob; questi con la propria chiave toglie il lucchetto e manda la cassaforte con solo un lucchetto ad Alice, che finalmente può togliere il proprio lucchetto e ricevere l'anello da Bob.
Questo sembra risolvere il problema delle chiavi: Bob cifra con la propria chiave, Alice ricritta, Bob toglie la propria cifratura e infine Alice ottiene il messaggio in chiaro. Tuttavia c'è un grave ostacolo: solitamente le cifrature più sicure non sono simmetriche, ovvero l'ultima cifratura aggiunta è anche la prima da togliere, al contrario di quanto avviene con i lucchetti di Alice e Bob. L'idea di Diffie e Hellman fu quella di cercare tra varie funzioni matematiche per le quali non importasse l'ordine di inversione, ma che d'altra parte fossero molto difficili da invertire; la scelta fu di concentrarsi sull'aritmetica modulare ed in particolare sulle funzioni esponenziali.
Se consideriamo infatti la funzione $3^x \pmod 7$, è molto semplice calcolarne i valori dato un valore di x, ma se si conosce il valore della funzione l'unico modo per ottenere la x è provare tutti i possibili valori; finché i numeri sono piccoli si può invertire per tentativi, ma quando i numeri aumentano di grandezza il processo diventa lunghissimo anche per un computer. Questa è l'intuizione che portò Hellman a sviluppare il primo prototipo di crittografia a chiave pubblica; è molto semplice descriverlo in pochi passaggi.

- Alice e Bob si accordano su un numero primo p e un numero y, che possono essere pubblici; ad esempio $y = 7, p = 11$
- Alice sceglie un numero a ad esempio 3, Bob un numero b ad esempio 6, da tenere segreti
- Entrambi inseriscono il proprio numero casuale nella funzione $y^x \pmod p$
- Alice ottiene α (nell'esempio 2) e lo dice a Bob; Bob ottiene β (nell'esempio 4) e lo dice ad Alice
- Alice calcola $\beta^A \pmod p$, ottenendo 9; Bob calcola $\alpha^B \pmod p$, ottenendo 9

Il risultato è che a questo punto Alice e Bob hanno uno stesso numero senza averlo deciso insieme (ricordiamo che A, B sono casuali), infatti $\beta^A \equiv (y^B)^A \equiv y^{AB} \pmod{p}$ e simmetricamente anche $\alpha^B \equiv (y^A)^B \equiv y^{AB} \pmod{p}$; inoltre non si sono scambiati informazioni sensibili che compromettono la sicurezza della chiave: l'unico modo che un'eventuale intercettatore, che chiamiamo Eva, può avere di scoprire la chiave è quello di ottenere A o B, ma può farlo solo invertendo la funzione $y^x \pmod{p}$, ma impiega troppo tempo.
D'altra parte Diffie ebbe un'intuizione geniale per un sistema a chiavi asimmetriche: classicamente la stessa chiave veniva usata sia per cifrare che per decifrare; tuttavia quello che aveva immaginato era una coppia di chiavi, una per cifrare e pubblica, l'altra per decifrare e segreta. Quello che Alice avrebbe dovuto fare per mandare un messaggio a Bob non sarebbe stato nient'altro che prendere la chiave pubblica di Bob e cifrare il messaggio; a questo punto nemmeno Alice era in grado di decifrare il proprio messaggio, e l'unico che potesse farlo era Bob con la propria chiave segreta. Il grande vantaggio rispetto allo scambio di Hellman è appunto che non c'è alcun procedimento macchinoso: per mandare un messaggio ad Alice basta cercare la sua chiave su un elenco come quello del telefono; ovviamente non c'è nemmeno più bisogno di accordarsi su alcunché.

L'algoritmo RSA

Nel 1976 con i loro articoli Diffie e Hellman avevano rivoluzionato la crittografia mostrando come fosse possibile un sistema crittografico senza che mittente e destinatario si accordassero sulla chiave; l'articolo e l'idea di Diffie suscitarono l'interesse in particolare di due giovani studenti del MIT, Ron Rivest e Leonard Adleman; Rivest era un informatico ed era pieno di idee, Adleman era un matematico rigoroso e paziente. In breve ai due si unì anche Adi Shamir, un altro specialista di computer capace di una grande concentrazione; quest'ultimo e Rivest proponevano sempre nuove idee per una funzione asimmetrica, mentre Adleman cercava i punti deboli e testava se potessero funzionare; per un anno tutte le idee non portarono a nulla, ma nell'aprile del 1977 Rivest ebbe l'intuizione vincente. Scrisse di fretta l'articolo, elencando gli autori in ordine alfabetico; Adleman mise alla prova questa nuova idea, e l'unica critica che trovò fu l'ordine degli autori: pensava di non meritare l'importanza di essere nominato per primo. In questo modo il sistema inventato dal trio non si sarebbe chiamato ARS, ma RSA; e sarebbe diventato la cifratura più influente della crittografia moderna.
Analizziamo ora come funziona l'algoritmo, rimandando la spiegazione prettamente matematico-informatica al capitolo successivo

- Alice sceglie due numeri primi p, q casuali e molto grandi
- Alice moltiplica i due primi ottenendo $n = p \cdot q$
- Alice sceglie un intero d coprimo con $\varphi(n) = (p-1)(q-1)$
- Alice calcola e, l'inverso di d modulo $(p-1)(q-1)$

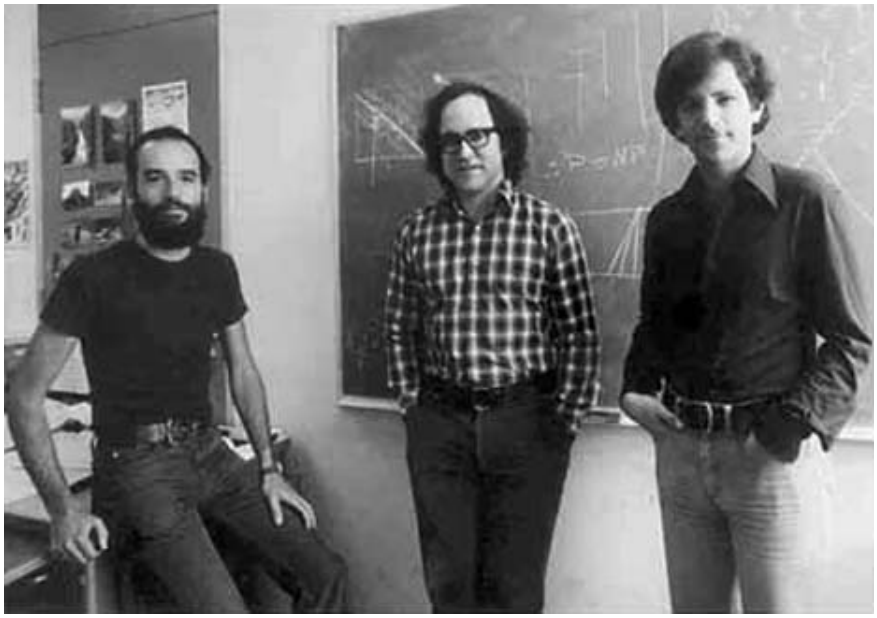


Figura 6.2: Adi Shamir, Ronald Rivest, Leonard Adleman

- La chiave pubblica di Alice sarà la coppia (e, n)
- Se Bob vuole inviare ad Alice un messaggio, prima lo converte in un numero M più piccolo di n; se ciò non fosse possibile, spezza il messaggio originale in più parti
- Bob calcola il numero $C \equiv M^e \pmod{n}$, che invia ad Alice
- Alice, ricevendo il messaggio C, calcola il numero $M' \equiv C^d \pmod{n}$
- Poiché $C \equiv M^d \pmod{n}$, allora $M' \equiv M^{d \cdot e} \equiv M \pmod{n}$ per il teorema 9 di Euler-Fermat

Facciamo un esempio di questo metodo, riprendendo quello di Rivest:
Scegliamo $p = 47, q = 59$ e dunque $n = 47 \cdot 59 = 2773$; inoltre $\varphi(2773) = 46 \cdot 58 = 2668$. Scegliamo infine $d = 157$, da cui calcoliamo $e = 17$, infatti $d \cdot e = 2669$. Scegliamo ora di codificare ogni lettera con una coppia di numeri, in modo che spazio=00, A=01, B=02,... Z=26. Raggruppiamo poi le lettere a coppie e osserviamo che il massimo numero ottenibile è 2625, che è minore di 2773.
Allora il messaggio `ITS ALL GREEK TO ME` si trasforma nella sequenza di numeri `0920 1900 0112 1200 0718 0505 1100 2015 0013 0500`.
Il primo blocco è $M = 920$; allora $C \equiv M^{17} \equiv 920^{17} \equiv 948 \pmod{2773}$.
Il messaggio criptato è dunque `0948 2342 1084 1444 2663 2390 0778 0774 0219 1655`.
Verifichiamo poi ad esempio che $778^{157} \equiv 1100 \pmod{2773}$, ovvero che la decodifica funziona.
Osserviamo inoltre come sia immediato aggiungere anche una "firma" digitale: quando Bob vuole mandare un messaggio ad Alice autenticandosi, usa anche la propria funzione di cifratura. Chiamiamo $C(x)$ la funzione di cifratura e $D(x)$ la funzione

di decifrazione, con i pedici per i rispettivi utenti, e M il messaggio; Bob allora manda ad Alice $S = D_B(C_A(M))$, che calcola $M' = D_A(C_B(S))$; ma allora $M' = D_A(C_B(D_B(C_A(M)))) = D_A(C_A(M)) = M$ e quindi Alice può leggere il messaggio ed è sicura che è stato inviato d Bob, perché solo lui conosce la funzione D_B.
La grande forza di RSA è dunque quella di essere piuttosto semplice (qualunque computer riesce a fare queste operazioni in pochissimo tempo), ma allo stato delle conoscenze attuali inviolabile. Qualunque tentativo di attacco è equivalente a fattorizzare n, ma i metodi che si conoscono finora sono troppo lenti per fattorizzare un numero abbastanza grande; il migliore è il General Number Field Sieve, che ha permesso di fattorizzare una chiave RSA lunga 232 cifre (768 bit) nel 2009, con un costo equivalente a 2000 anni su un processore da 2.2 GHz. Ormai però quasi tutte le chiavi RSA sono lunghe 1024 bit, ovvero 309 cifre, ed è quasi impossibile la loro fattorizzazione; d'altra parte è piuttosto agevole generare numeri primi anche grandi, quindi non ci sarà mai penuria di chiavi.
Il solo punto debole di questa cifratura è dunque che in futuro si scoprano metodi di molto più efficienti per fattorizzare numeri interi, usando ad esempio computer quantistici, per i quali esiste già un algoritmo veloce inventato da Shor.

Un futuro quantistico

L'ultima frontiera della crittoanalisi, dopo gli elaboratori elettronici, potrebbe essere quella dei computer quantistici, oggi ipotizzati solo a livello teorico, che però avrebbero un'enorme potenza di calcolo, inimmaginabile con i computer classici. Questo deriva dalla struttura stessa della materia, che a livelli microscopici ha comportamenti assai bizzarri, descritti nell'ultimo secolo.
La caratteristica più peculiare delle particelle elementari, come ad esempio un elettrone, è la *sovrapposizione di stati*: le particelle sono eccitazioni di campi fondamentali presenti in tutto l'Universo, che interagiscono tra loro e soprattutto con se stessi; per avvicinare la descrizione matematica al nostro "senso comune" potremmo definire un elettrone come un'onda di probabilità che interagisce con l'ambiente e con se stessa; questa è l'unica spiegazione possibile per l'esperimento della doppia fenditura.
Inoltre gli elettroni hanno una proprietà fondamentale chiamata "spin", che ha le dimensioni di un momento angolare e quindi può essere associata ad una sorta di rotazione dell'elettrone; questo spin può essere misurato secondo una direzione specifica, si è verificato che nell'atto della misura questo si allinea con la direzione scelta e il verso è casuale. Tuttavia fino alla misura l'elettrone ha tutti gli spin possibili, esattamente come è in tutti i luoghi possibili; è solo l'interazione con la misura o con l'ambiente circostante in generale che determina il collasso dell'onda ad un preciso valore.
La sovrapposizione può anche riguardare oggetti macroscopici: è il caso dell'esperimento mentale chiamato "gatto di Schrödinger"; immaginiamo di mettere un gatto in una scatola, in cui c'è una fiala di cianuro che viene aperta solo se un neutrone di un atomo radiattivo decade. Da quando chiudiamo la scatola, il neutrone entra in una sovrapposizione di stati, e quindi anche il gatto: possiamo dire che è sia vivo

che morto contemporaneamente.
Questa possibilità di avere infiniti valori contemporaneamente è la chiave per velocizzare i calcoli: un computer classico che dovesse fare una certa operazione su 100 numeri, li testa in sequenza; un computer quantistico potrebbe farlo con un solo tentativo. Prendiamo infatti degli elettroni e stabiliamo una direzione di misura; il loro spin può assumere solo due valori, e dunque un elettrone può essere usato come cifra binaria, chiamata *qubit*; misurandoli avremmo una certa sequenza determinata, come se fosse una variabile di un computer classico; ma se non li misuriamo, ogni qubit sarà in una sovrapposizione di stati e dunque avendo ad esempio 7 qubit, questi rappresentano simultaneamente 127 numeri, e facendo una data operazione, è come se stessimo provando 127 variabili insieme.
In questo modo potrebbe essere possibile raggiungere una velocità inaudita per certe operazioni, ed in particolare nel 1994 Peter Shor inventò un algoritmo per computer quantistici in grado di fattorizzare un numero in tempo polinomiale nel numero di cifre, come i test di primalità classici; questo potrebbe compromettere la sicurezza di RSA, e sarebbe dunque necessario un nuovo metodo di cifratura.
Gli stessi computer quantistici potrebbero però fornire finalmente una cifratura assolutamente inviolabile, sulla base del principio di indeterminazione di Heisenberg; quest'ultimo afferma, in una versione da lui stesso ideata, che "non possiamo conoscere il presente in tutti i suoi dettagli". Prendiamo ad esempio i fotoni, che hanno una caratteristica fondamentale chiamata polarizzazione, ovvero la direzione di vibrazione del campo elettrico; per semplicità supponiamo che ci siano solo quattro valori possibili, verticale $\uparrow$, orizzontale $\rightarrow$, diagonale destra $\nearrow$, diagonale sinistra $\searrow$. L'unico modo per determinare la polarizzazione di questi elettroni è farli passare attraverso un apposito filtro; tuttavia, se il filtro è posto in orizzontale, tutti i fotoni orizzontali lo attraversano e tutti quelli verticali vengono respinti; il bizzarro mondo quantistico però prevede che metà dei fotoni diagonali verranno respinti e metà passeranno, completamente a caso. Ponendoci al di là di un filtro non possiamo sapere con certezza quale fosse la polarizzazione di un fotone che l'ha superato; questa non è un'imperfezione tecnica, ma a quanto ne sappiamo è la natura stessa che si comporta in questo modo.

Questo permette ad Alice e Bob di accordarsi su una sequenza completamente casuale, da usare poi come chiave per una cifratura a blocco monouso, e senza possibilità di intercettazione; vediamo come. Intanto supponiamo che una polarizzazione verticale $\uparrow$ significhi 1, mentre orizzontale $\rightarrow$ sia 0; analogamente $\nearrow$ corrisponda a 1, mentre $\searrow$ sia 0. Alice allora invia una sequenza casuale di bit, passando in modo altrettanto casuale da uno schema di polarizzazione di tipo + a uno di tipo $\times$; un eventuale intercettatore Eva non è a conoscenza degli schemi usati da Alice, quindi può solo andare a caso, sbagliando circa metà delle volte; anche Bob si trova in questa difficoltà, e anche lui deciderà a caso quale tipo di rivelatore usare.
A questo punto però Bob comunica ad Alice, anche in chiaro, quali schemi ha usato per ogni bit, e lei ne conferma alcuni; a questo punto Alice e Bob hanno una sequenza comune di bit, anche molto più breve di quella mandata originariamente, che può fungere da chiave casuale. Infatti, anche sapendo quali degli schemi usati da Bob siano giusti, Eva non può ricostruire la chiave: magari quando sia Bob che Alice hanno usato lo schema + lei ha usato quello $\times$, o viceversa anche se ha usato

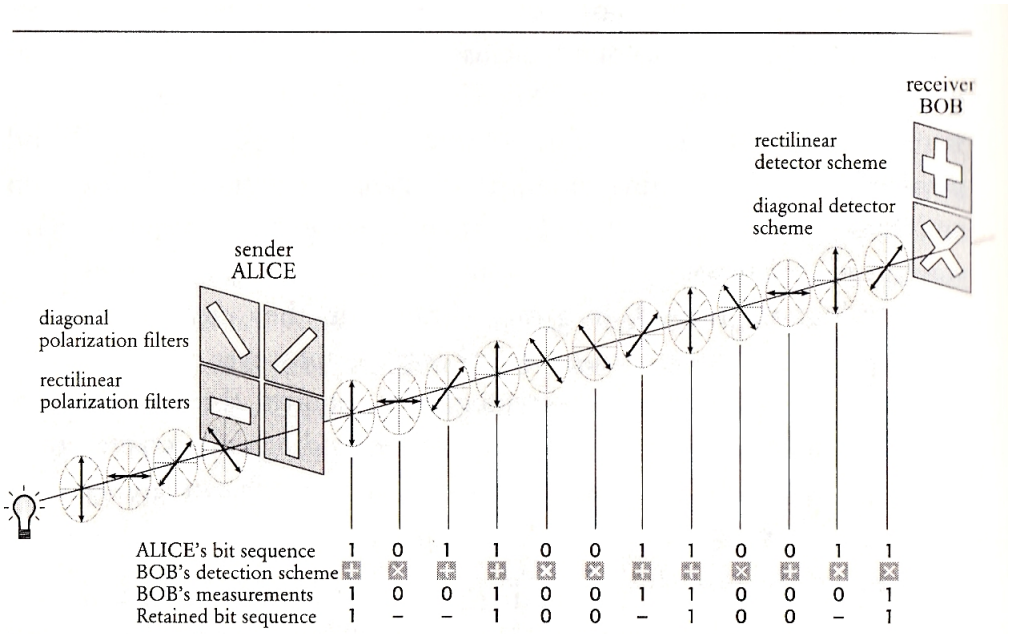


Figura 6.3: L'invio di una sequenza di bit

lo stesso di Alice, Bob ne ha usato un altro e quel bit è da scartare; la sequenza di bit di Eva è dunque inutile perché circa la metà delle cifre sono state misurate con lo schema sbagliato, quindi è ugualmente probabile che siano uno 0 o un 1.
Per fare un esempio più semplice, è come se Alice stesse mandando delle carte da gioco coperte a Bob, ma quando si gira questa carta si possa guardare solo il valore o il seme; allora Alice prima di inviare una carta, decide se guardare il seme o il valore e prende nota di cosa osserva. Supponiamo che abbia determinato che la carta è di picche; quando la carta arriva a Eva, questa decide di guardarne il numero, che è ad esempio quattro; quando la carta giunge infine a Bob, questi decide di misurare il seme e vede che è picche; poi Alice manda un'altra carta e vede che il suo valore è il 10, Eva anche guarda il valore e vede 10, mentre Bob osserva il seme che è quadri. Poi Alice e Bob si telefonano; Bob dice di aver guardato entrambe le volte il seme, Alice gli dice che ha guardato prima il seme e poi il valore. Allora i due amici hanno in comune il dato della carta di picche; estraendo tante carte, riescono ad avere una sequenza abbastanza lunga di dati comuni, dei quali per metà Eva non sa nulla.
La domanda a questo punto è solo più una: verrà realizzata prima la crittografia quantistica, decretando la vittoria finale della riservatezza, oppure i computer quantistici, creando un periodo senza alcuna possibilità di privacy fino all'avvento del nuovo tipo di crittografia?
Allo stato attuale, sembra ad uno stadio più avanzato la crittografia quantistica; nel 2007 infatti un gruppo di ricercatori di Los Alamos è riuscito ad inviare una chiave con questo metodo attraverso una fibra ottica a 148km di distanza. Questo probabilmente segna la fine della lotta millenaria tra crittografi e crittoanalisti, con la sconfitta di questi ultimi - almeno finché la meccanica quantistica non sarà sorpassata da una nuova teoria.

Teoria dei Numeri

Aritmetica modulare

Quando guardiamo un orologio digitale e vediamo scritto 16, istintivamente diciamo che sono le quattro del pomeriggio, ovvero stiamo affermando l'uguaglianza $16 = 4$; analogamente se è sabato e diciamo dopodomani è lunedì questo equivale a dire $6 + 2 = 1$ (se assegniamo al lunedì il valore 1, alla domenica il 7, etc). Queste uguaglianze sembrano assurde, perché 16 è più grande di 4; ma in realtà riflettono solo l'andamento ciclico delle ore e dei giorni della settimana, e diventano uguaglianze formalmente valide in certe strutture definite apposta, che permettono di fare operazioni molto più interessanti che leggere le ore.
Consideriamo l'anello degli interi $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$; questo è dotato di molte proprietà interessanti, molte delle quali si riconducono ad un fatto apparentemente semplicissimo, tant'è che viene insegnato alle elementari: la divisione euclidea, o con resto.

Teorema 1. *Dati due interi a, b con $b \neq 0$, esistono e sono unici due interi q, r tali che $a = qb + r$ con $0 \leq r < |b|$*

Dimostrazione. Consideriamo l'insieme $S := \{k \in \mathbb{Z} : \exists x \in \mathbb{Z} : k = x\,|b|\,, k \leq a\}$ ovvero l'insieme dei multipli di $|b|$ minori o uguali di a. Dato che $b \neq 0$ allora $|b| \geq 1$ quindi $|a||b| \geq |a|$, ovvero $-|a||b| \leq -|a| \leq a$ quindi S non è vuoto; però un insieme di interi limitato superiormente ha un massimo per l'assioma di buon ordinamento; sia allora $h|b| = \max(S) \leq a$. Dunque $a = h|b| + r$ con $r \geq 0$; d'altra parte $(h + 1)|b| > a$ (se fosse più piccolo, allora starebbe in S e sarebbe lui il massimo) cioè $h|b| + |b| > a = h|b| + r$ da cui $r < |b|$. Prendendo $q = b \cdot \operatorname{sgn}(b)$ abbiamo proprio $a = qb + r$, e sono stati scelti in maniera univoca (il massimo è uno solo). □

Possiamo ora fissare un intero n e per ogni altro intero considerare il suo resto nella divisione per n, che esiste ed è unico; diciamo allora che due interi a, b sono in relazione se hanno lo stesso resto; in alternativa diciamo che

Definizione 1. *Due interi a, b sono congrui modulo n, scritto come $a \equiv b \pmod{n}$, se e solo se $n \mid a - b$*

Questa relazione di congruenze è una relazione di equivalenza che partiziona $\mathbb{Z}$ in n classi di equivalenza, indicate con il loro resto nella divisione per n: $\mathbb{Z} = [0]_n \cup [1]_n \cup \dots \cup [n-1]_n$ dove $[a]_n = \{a + kn : k \in \mathbb{Z}\}$; si può verificare che $[a]_n + [b]_n = [a+b]_n$ e $[a]_n[b]_n = [ab]_n$. Allora possiamo considerare l'anello quoziente $\mathbb{Z}/n\mathbb{Z}$ degli interi modulo n, in cui valgono molte delle usuali proprietà degli interi:

Teorema 2. *Siano a, b, c, d degli interi tali che $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$; valgono le seguenti*

i) $a + c \equiv b + d \pmod{n}$

ii) $ac \equiv bd \pmod{n}$

Allora siamo in grado di capire cosa stiamo facendo quando leggiamo l'ora: guardiamo a che classe di congruenza modulo 12 appartiene, e ad esempio possiamo davvero scrivere $16 \equiv 4 \pmod{12}$. Ma se facciamo attenzione, possiamo vedere che le congruenze sono molto più forti: se oggi è mercoledì, possiamo sapere che giorno della settimana è tra 54 giorni, ovvero $3 + 54 \equiv 3 + 5 \equiv 1 \pmod{7}$, quindi lunedì; facendo la stessa cosa, vediamo che $365 \equiv 1 \pmod{7}$, quindi ogni anno sposta in avanti di un giorno ogni data.
Inoltre, possiamo anche moltiplicare (sebbene questo perda un po' di significato per giorni e ore), e saremmo anche tentati di dividere; purtroppo, come già accade negli interi, non sempre possiamo farlo: ad esempio $6 \equiv 2 \pmod{4}$ è una relazione vera, ma se dividessimo per 2 otterremmo $3 \equiv 1 \pmod{4}$ che è falsa. Andiamo ad indagare meglio; nell'esempio, se scriviamo la definizione abbiamo che $6-2 = 4k$; ma allora ci accorgiamo come dividere per 2 solo $6 - 2$ abbia poco senso: dobbiamo dividere anche 4. In generale se abbiamo $a \equiv b \pmod{n}$ e prendiamo un divisore comune d di a e n scriviamo $a = da_1, n = dn_1$ ed espandendo la congruenza $da_1 - b = dn_1 k$, da cui anche $b = db_1$, e dividendo tutto per d abbiamo $a_1 - b_1 = n_1 k$. Possiamo dunque dire che

Teorema 3. *Se $a \equiv b \pmod{n}$ e $d = \gcd(a, b, n)$ vale* $\dfrac{a}{d} \equiv \dfrac{b}{d} \left(\mod \dfrac{n}{d} \right)$

Tuttavia se consideriamo la congruenza $15 \equiv 3 \pmod{4}$, possiamo tranquillamente semplificare il fattore 3 ottenendo una relazione vera, cioè $5 \equiv 1 \pmod{4}$. Ci chiediamo allora quando si può semplificare senza toccare il modulo. Consideriamo ad esempio la generica congruenza $ka \equiv kb \pmod{n}$; per ogni h vale $hka \equiv hkb \pmod{n}$, e dunque se esistesse un h tale che $hk \equiv 1 \pmod{n}$ avremmo ricavato $a \equiv b \pmod{n}$.
Cerchiamo dunque un intero tale che $kh = 1 + ln$, cioè $hk - ln = 1$ dove k, n sono fissati mentre h, l sono variabili. Per il teorema di Bézout un tale h esiste se e solo se $\gcd(k, n) = 1$, e lo si può trovare esplicitamente con l'algoritmo di Euclide.

Teorema 4. *(Bézout) Dati tre interi a, b, c l'equazione $ax + by = c$ ha soluzione se e solo se $\gcd(a, b) \mid c$, nel qual caso ne ha infinite*

Dimostrazione. Sia $S := \{ax + by : x, y \in \mathbb{Z}\}$; S non è vuoto, quindi ha un minimo elemento positivo che chiamiamo $d = ar + bs$. Eseguiamo ora la divisione con resto $a = qd + r$; allora $r = a - qd = a(1 - qr) + b(-qs) \in S$, ma poiché $0 \leq r < d$ e d era il minimo intero positivo, $r = 0$ cioè $d \mid a$. Analogamente $d \mid b$, ovvero $d \mid \gcd(a, b)$. D'altra parte $\gcd(a, b) \mid a, b$ e quindi $\gcd(a, b) \mid ar + bs = d$. Dunque $d = \gcd(a, b)$, e se $c = de$, allora abbiamo $c = e(ar + bs) = a(er) + b(es)$. Infine osserviamo che tutte le coppie della forma $(r + \lambda \dfrac{s}{d}, s - \lambda \dfrac{r}{d})$ sono soluzioni di $ax + by = d$. □

Siamo dunque giunti alla seguente conclusione:

Teorema 5. *Sia a un intero coprimo con n; allora esiste un intero b che indichiamo con a^{-1} tale che $ab \equiv 1 \pmod{n}$.*

Teorema 6. *Siano k, a, b, n, d interi tali che $ka \equiv kb \pmod{n}$ e $\gcd(k, n) = d$; allora $a \equiv b \pmod{\frac{n}{d}}$*

Consideriamo ora l'insieme $S := \{ax + b : x = 0, 1, \ldots, n-1\}$ e ci domandiamo per quali a in S ci sono tutti i resti possibili nella divisione per n, ovvero S è quello che si chiama un sistema completo di residui $\mod n$. Dato che contiene n elementi, se sono a coppie disgiunti allora ci sono tutti. Ora, se x_1, x_2 producessero due elementi uguali, avremmo $ax_1 + b \equiv ax_2 + b \pmod{n}$ ovvero $ax_1 \equiv ax_2 \pmod{n}$, che alla luce del teorema 6 implica $x_1 \equiv x_2 \pmod{\frac{n}{\gcd(a,n)}}$; se a, n fossero coprimi, avremmo che $x_1 \equiv x_2 \pmod{n}$, ma partivamo da elementi diversi, quindi in S non ci sono elementi uguali; ma se $\gcd(a, n) > 1$ abbiamo che $x_1 - x_2$ è multiplo di un intero più piccolo di n, e allora possono essere due interi diversi modulo n. Ad esempio se $n = 6, a = 2, b = 1$ abbiamo che $x_1 \equiv x_2 \pmod{3}$ e infatti se cerchiamo di costruire S otteniamo $\{2 \cdot 1 + 1, 2 \cdot 2 + 1, 2 \cdot 3 + 1, 2 \cdot 4 + 1, 2 \cdot 5 + 1, 2 \cdot 6 + 1\} = \{3, 5, 1, 3, 5, 1\}$ e ci sono delle ripetizioni. Possiamo dunque scrivere

Teorema 7. *Fissati due interi a, b la funzione $f(x) = ax + b$ è una permutazione di $\mathbb{Z}/n\mathbb{Z}$ se e solo se $\gcd(a, n) = 1$.*

Dopo aver analizzato addizione e moltiplicazione, concentriamoci sull'elevamento a potenza.
Prendendo un intero a, e continuando a moltiplicarlo per se stesso, abbiamo la successione delle sue potenze $a^1, a^2, a^3, \ldots$; considerando i resti della divisione di questi numeri per un altro intero n, abbiamo un numero infinito di resti, che però possono essere solo i numeri da 0 a $n-1$: questo vuol dire che c'è una ripetizione; possiamo dire di più, se consideriamo le potenze da a^0 fino ad a^n: sono $n+1$ numeri, quindi per forza due devono ripetersi, ovvero deve accadere $a^x \equiv a^y \pmod{n}$, con $x \leq y \leq n$.
Restringendo la scelta agli interi coprimi con n, abbiamo che a possiede un inverso modulo n, che chiamiamo a^{-1}; moltiplicando la relazione precedente per a^{-x} otteniamo che $a^{y-x} \equiv 1 \pmod{n}$. Dunque ogni intero coprimo a n, dopo un certo numero di elevamenti a potenza torna a 1; chiamiamo $\mathrm{ord}_n(a)$ il minimo intero b tale che $a^b \equiv 1 \pmod{n}$; con la nostra semplice idea sappiamo solo dire che $\mathrm{ord}_n(a) < n$; tuttavia si può fare di meglio.
Definiamo intanto la funzione totiente di Euler $\varphi(n) := \#\{i : \gcd(i, n) = 1 | 1 \leq i \leq n\}$ la funzione che conta il numero di naturali coprimi con n e minori di questo; ad esempio $\varphi(6) = 2, \varphi(10) = 4, \varphi(11) = 10$. Si può notare facilmente che se p è primo allora $\varphi(p) = p - 1$; inoltre la funzione φ è moltiplicativa, e quindi si può ricavare la formula generale:

Teorema 8. *Dato un intero positivo n, allora vale la formula $\varphi(n) = n \cdot \prod_{p|n} \frac{p-1}{p}$*

Siamo ora pronti ad enunciare (e dimostrare) un risultato molto importante in teoria dei numeri, che è anche a fondamento dell'algoritmo RSA

Teorema 9. *(Euler-Fermat) Siano a, n due interi tali che* $\gcd(a, n) = 1$*; allora* $a^{\varphi(n)} \equiv 1 \pmod{n}$

Dimostrazione. Consideriamo l'insieme S dei numeri coprimi con n e minori di questo, che ha cardinalità $\varphi(n)$; dato che $\gcd(a, n) = 1$ allora l'insieme $aS = \{a \cdots , s \in S\}$ contiene gli stessi resti modulo n di S, per il teorema 7; dunque il prodotto degli elementi dei due insiemi dà lo stesso resto se diviso per n. Detto dunque $P = \prod_{s \in S} s$, abbiamo che $P \equiv a^{\varphi(n)} \cdot P \pmod{n}$; ma S contiene tutti elementi coprimi con n, che dunque possiedono un inverso; allora anche P possiede un inverso P^{-1} e moltiplicando per questo si ottiene la congruenza voluta □

Numeri primi

Definizione 2. *Un intero p si dice* primo *se* $p \mid a \cdot b \implies p \mid a \vee p \mid b \; \forall a, b$

Equivalentemente, un primo è un numero con soli due divisori, 1 e se stesso. I numeri primi sono i "mattoni" con cui vengono costruiti i numeri interi, come è sottolineato dal seguente teorema (detto appunto fondamentale dell'aritmetica)

Teorema 10. *Ogni intero positivo n si scrive come prodotto di primi in maniera univoca, a meno dell'ordine*

Fin dall'antichità i numeri primi sono stati molto studiati; ad esempio Eratostene descrisse un metodo, il crivello, per trovare tutti i primi da 2 a un certo numero: è un procedimento iterativo che consiste nel prendere il primo numero non cancellato che sarà primo, e cancellarne tutti i multipli; ripetendo questo processo fino al numero desiderato, si ottengono tutti i primi.
Sempre in Grecia Euclide dimostrò che i numeri primi sono infiniti, e fu il primo importante risultato ottenuto; nel 1700 Eulero dimostrò che la somma dei reciproci dei primi diverge.
Gauss inoltre congetturò che $\pi(n) \sim \dfrac{n}{\log n}$ cioè che il numero di primi fino ad un certo intero n fosse abbastanza vicino all'altra quantità per n sufficientemente grande; questo venne dimostrato poi nel 1896 ed è una delle pietre miliari nella caccia ai primi.
Nel 1837 Dirichlet aveva mostrato che in ogni progressione aritmetica vi sono infiniti primi, e che sono equamente distribuiti tra le varie classi di resto; nel 1852 fu dimostrato il postulato di Bertrand ovvero che tra ogni numero ed il suo doppio c'è un primo. Al giorno d'oggi però ancora molte proprietà dei numeri primi sono solo congetturate, tra cui le più importanti:

Congettura di Goldbach Ogni numero pari è somma di due primi

Congettura dei primi gemelli Ci sono infiniti primi p tali che $p + 2$ è ancora primo

Congettura di Bunyakowsky Ogni polinomio assume un valore primo infinite volte

Ipotesi di Riemann Ogni zero non banale della funzione $\zeta(s)$ ha parte reale pari a $\frac{1}{2}$

Inoltre, anche in seguito alla diffusione di RSA, si sono cercati algoritmi per testare la primalità di un intero e per fattorizzare un numero. Tuttavia per il primo problema si sono trovate soluzioni veloci (con un numero di operazioni richieste pari al più ad una potenza del numero di cifre), mentre per la fattorizzazione nonostante i continui miglioramenti non si è giunti ad una sostanziale velocizzazione. Le due categorie di algoritmi si basano grossomodo sugli stessi due principi.
Ricordando il teorema 9, se n è primo, ricaviamo che $a^{p-1} \equiv 1 \pmod{p}$; se un numero è primo, allora per ogni intero a minore di questo vale questa equazione; d'altra parte se n è composto, esistono degli a tali che $a^{n-1} \not\equiv 1 \pmod{n}$. Questa è l'idea del test di primalità dovuto a Fermat: fissato un intero n, si prende un intero a caso a e si verifica se $a^{n-1} \equiv 1 \pmod{n}$; in caso negativo, allora n non è primo, in caso affermativo si procede con un altro b; se dopo un numero sufficiente di tentativi il test non ha ancora fallito, allora quasi sicuramente il numero testato è primo.
L'idea per fattorizzare è invece dovuta a Lagrange e si basa sui quadrati modulo n: se p è primo, allora l'equazione $x^2 \equiv a \pmod{p}$ ha o nessuna soluzione, oppure due soluzioni $\pm b$; se n è composto allora $x^2 \equiv a \pmod{n}$ ha due soluzioni diverse b, c, cioè tali che $b \not\equiv \pm c \pmod{n}$. Ma allora sapendo che $b^2 \equiv c^2 \pmod{n}$ si ricava che $n \mid (b-c)(b+c)$, ma non divide nessuno dei due fattori; allora $\gcd(b-c, n)$ e $\gcd(b+c, n)$ sono dei fattori propri di n e sono facili da calcolare. La parte difficile è però trovare b e c, poiché anche la funzione x^2 non si inverte rapidamente.

Approccio informatico

Segnaliamo di seguito alcuni algoritmi che permettono di velocizzare la cifratura e la decifrazione nell'ambito del RSA.

Esponenziazione modulare

Come si è visto, Bob deve calcolare $M^e \pmod{n}$ per mandare il messaggio ad Alice; tuttavia l'elevamento a potenza fa crescere tantissimo il numero, e probabilmente si rischi di finire in overflow. C'è però un algoritmo che permette di mantenere bassi i numeri ad ogni passaggio ed eseguire il calcolo in $O(\log e)$ operazioni.
Occorre per prima cosa scrivere e in binario, che per il computer è facilissimo; a questo punto basta partire da M e ad ogni passaggio elevarlo al quadrato e poi ridurlo modulo n, ottenendo dunque la sequenza $M, M^2, M^4, \ldots, M^{2^k}$ con $k = \lfloor \log_2(e) \rfloor$; sapendo l'espansione binaria di e, basta moltiplicare tra loro le potenze giuste.
Ad esempio per calcolare $3^{100} \pmod{53}$ scriviamo $100 = 64 + 32 + 4 = 1100100_2$; facciamo poi la sequenza di quadrati: $3^2 \equiv 9$, $3^4 \equiv 9^2 \equiv 81 \equiv 28$, $3^8 \equiv 28^2 \equiv 42$, $3^{16} \equiv 42^2 \equiv 15$, $3^{32} \equiv 15^2 \equiv 13$, $3^{64} \equiv 13^2 \equiv 10$.
Calcoliamo infine $3^{64}3^{32}3^4 \equiv 10 \cdot 13 \cdot 28 \equiv 36$.
In pseudocodice, l'algoritmo sarebbe il seguente

```
function modular_pow(M, e, n)
    result := 1
    base := M mod n
    while e > 0
        if (e mod 2 == 1):
            result = (result * base) mod n
        e = e >> 1
        base = (base * base) mod n
    return result
```

Algoritmo di Euclide

L'algoritmo di Euclide è un modo, il più veloce, per calcolare il massimo comun divisore di due interi a e b; sfrutta la divisione con resto, che viene ripetuta fino ad ottenere un resto di 0.

1. Poniamo $x = a, y = b$
2. Facciamo la divisione euclidea $x = qy + r$
3. Se $r = 0$ allora il MCD è y; se $r > 0$ allora poniamo $x = y$ e $y = r$
4. Ripartire dal punto 2. con i nuovi valori di x, y

L'algoritmo ha fine, poiché il resto è sempre minore del dividendo, quindi la sequenza di resti è strettamente decrescente, quindi deve raggiungere 0; d'altra parte si ha la proprietà che $\gcd(a, b) = \gcd(bq + r, b) = \gcd(b, r)$, quindi quello trovato alla fine dei passaggi è effettivamente $\gcd(a, b)$. Aggiungendo un'altra ricorrenza, si possono calcolare i coefficienti nell'identità di Bézout $ax + by = \gcd(a, b)$:

```
function extended_gcd(a, b)
    s := 0;     old_s := 1
    t := 1;     old_t := 0
    r := b;     old_r := a
    while r != 0
        quotient = old_r div r
        (old_r, r) = (r, old_r - quotient * r)
        (old_s, s) = (s, old_s - quotient * s)
        (old_t, t) = (t, old_t - quotient * t)
    output ``Coefficienti: '', (old_s, old_t)
```

Test di primalità

Nella sezione precedente si è visto il test di Fermat, che è un modo per determinare se un numero è probabilmente primo; tuttavia esistono dei numeri n detti di Carmichael tali che $a^{n-1} \equiv 1 \pmod{n}$ per tutti gli a coprimi con n, ovvero il test di Fermat segnalerebbe questo n come primo.
Ci sono allora delle versioni migliorate del test di primalità di Fermat; in particolare

una delle più usate è l'algoritmo di *Miller-Rabin*. Anche questo è probabilistico, ma può essere reso deterministico assumendo vera l'ipotesi di Riemann.
Si basa sul fatto che l'equazione $x^2 \equiv 1p \pmod{p}$ ha solo le due soluzioni $x \equiv \pm 1 \pmod{p}$. Partendo da un primo p, sappiamo che $a^{p-1} \equiv 1 \pmod{p}$; se scriviamo $p-1 = 2^s \cdot d$ dall'equazione precedente otteniamo $a^{2^{s-1}d} \equiv \pm 1 \pmod{p}$, e se continuiamo ad ottenere 1 arriviamo a $a^d \equiv 1 \pmod{p}$. Dunque se p è primo deve esistere un r tale che $a^{2^r d} \equiv -1 \pmod{p}$.
Perciò per testare un n si sceglie un intero a random, si scrive $n - 1 = 2^s \cdot d$ e si controllano $a^d \mod n, a^{2d} \mod n, \ldots, a^{n-1} \mod n$ se danno resto -1:

```
WitnessLoop: repeat k times:
   a := random integer
   x := a^d mod n
   if x == 1 or x == n-1 then do next WitnessLoop
   repeat s-1 times:
      x = x^2 mod n
      if x == 1 then return composite
      if x == n-1 then do next WitnessLoop
   return composite
return probably prime
```

Il numero k indica il numero di volte che viene ripetuto il test; più volte viene effettuato, più è probabile che dia il risultato esatto. In particolare la probabilità che il test sbagli è al più dizaq 4^{-k}: ripetendo il test ad esempio 50 volte la probabilità di errore è inferiore alla probabilità di un errore hardware nel computer che faccia sbagliare un calcolo.
Dunque questo test è implementato in molti software di matematica per la sua rapidità e precisione, ed è anche usato per generare i primi che compongono le chiavi dell'algoritmo RSA.
Infine recentemente, nel 2002, un trio di informatici (le cui iniziali sono AKS) ha scoperto un test di primalità deterministico che impiega un tempo polinomiale, ed è il primo ad esserlo indipendentemente da altre condizioni. Si basa sul fatto che n è primo se e solo se la congruenza tra polinomi $(x-a)^n \equiv x^n - a \pmod{n}$ è valida per certi a; ci sono poi altri accorgimenti per ridurre il tempo di esecuzione.
Nonostante sia deterministico, non viene spesso usato perché è parecchio più lento del Miller-Rabin, che dà comunque una sicurezza piuttosto elevata; è però di notevole importanza teorica, come sottolinea il titolo dell'articolo in cui è stato descritto, *PRIMES in P*.

Bibliografia

[1] S. Singh, *Codici & segreti - La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet*, Milano, RCS Libri, 1999

[2] J. Gòmez Urgellés, *Matematici, spie e pirati informatici*, Villatuerta, RBA, 2012

[3] R.L. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Commun. ACM 21 (Febbraio 1978), pagg. 120-126

[4] S. Barbero, U. Cerruti, *Teoria dei Numeri e Crittografia*, Università di Torino, a.a. 2012-2013

[5] R. Schoof, *Four primality testing algorithms*, MSRI Publications, Vol. 44, 2008

[6] M. Spiazzi. M. Tavella, *Only Connect... New Directions - vol.2*, 3ª ed, Bologna, Zanichelli, 2013

[7] G. La Porta, *Prefazione a E.A. Poe* "Tutti i racconti del mistero, dell'incubo e del terrore", Roma, Newton Compton, 1989

[8] https://en.wikipedia.org/

[9] http://www.ellsbury.com/enigmabombe.htm

[10] http://simonsingh.net/The_Black_Chamber/index.html

[11] http://practicalcryptography.com/