

PROGETTO LAUREE SCIENTIFICHE

Facoltà di Scienze Matematiche, Fisiche e Naturali

Università degli Studi di Torino

a cura dell'Ing. Emanuele Salvador

APPUNTI DI CRITTOGRAFIA

Complementi al Modulo 3 del Laboratorio

UNA INTRODUZIONE ALL'ALGEBRA MODERNA

Dicembre 2007

"È veramente da mettere in dubbio che l'intelligenza umana possa creare un cifrario che poi l'ingegno umano non riesca a decifrare con l'applicazione necessaria"

Edgar Allan Poe

| | | |
|------------|---|----|
| 1. | <i>Introduzione</i> | 4 |
| 1.1 | Il problema dello scambio delle chiavi | 4 |
| 1.2 | Il Principio di Kerckhoffs | 5 |
| 2. | <i>Crittografia antica</i> | 5 |
| 2.1 | Scitala lacedemonica | 5 |
| 2.2 | Disco di Enea (390-360 a.C.) | 5 |
| 2.3 | Atbash | 6 |
| 2.4 | Albam | 6 |
| 2.5 | Atbah | 6 |
| 2.6 | Polibio (200 ca. -118 a.C.) | 7 |
| 2.7 | Cifratura di Cesare (II secolo d.C.) | 7 |
| 2.8 | Il Disco di Leon Battista Alberti | 8 |
| 2.9 | Tavola di Vigenère | 9 |
| 3. | <i>La crittografia dalla seconda metà del XIX secolo alla Grande Guerra</i> | 11 |
| 3.1 | Playfair cipher | 11 |
| 3.2 | Cifra campale germanica o ADFGVX | 13 |
| 4. | <i>Crittografia nella II Guerra Mondiale</i> | 15 |
| 4.1 | Enigma | 15 |
| 4.1.1 | Lo scambiatore | 16 |
| 4.1.2 | Il Riflessore | 17 |
| 4.1.3 | Calcolo del numero di chiavi possibili | 19 |
| 4.1.4 | Utilizzo | 19 |
| 5. | <i>Numeri primi</i> | 22 |
| 6. | <i>Aritmetica modulo n</i> | 24 |
| 6.1 | Il cifrario di Cesare "generalizzato" con l'aritmetica modulo n | 26 |
| 7. | <i>Funzione e Teorema di Eulero</i> | 27 |



| | | |
|-------|--|----|
| 7.1 | Un'applicazione della funzione di Eulero | 27 |
| 8. | <i>La nascita della crittografia a chiave pubblica</i> | 29 |
| 8.1 | Una scatola e due lucchetti: lo scambio di chiavi secondo Diffie, Hellman e Merkle | 30 |
| 8.2 | RSA | 33 |
| 8.2.1 | Curiosità e considerazioni | 36 |
| 8.2.2 | Numeri primi e RSA | 37 |
| 8.2.3 | Attacchi | 38 |
| 8.2.4 | La fattorizzazione | 39 |
| 9. | <i>Riferimenti Bibliografici</i> | 41 |

1. Introduzione



La *crittografia* (dal greco *kryptòs*=nascosto e *graphè*=scrittura) sta ad indicare un insieme di procedure ideate allo scopo di nascondere il significato di un messaggio riservato ad altri che non ne fossero il mittente o il destinatario.

Si hanno notizie dell'utilizzo della crittografia fin dal V sec. a.C., nello scambio di messaggi legati a questioni particolarmente delicate, in genere alla vigilia o durante conflitti militari; a partire dal 750 d.C. si sviluppa la *crittoanalisi*, lo studio dei sistemi in grado di svelare il contenuto di un messaggio segreto senza conoscere a priori la procedura utilizzata per cifrarlo. Da allora la storia delle informazioni riservate si snoda attraverso studi, successi e fallimenti di crittografi e crittoanalisti: i primi nel tentativo di creare una riservatezza inviolabile, gli altri in quello di trovarne i punti deboli.

Nella Società dell'informazione l'utilizzo della crittografia è legato al problema della sicurezza delle transazioni, particolarmente quelle economiche, attraverso la rete. Tra l'altro gli studi dei crittografi e dei crittoanalisti sono strettamente connessi all'informatica: la scienza che si occupa della rappresentazione e della elaborazione dell'informazione e del suo trattamento automatico mediante elaboratori elettronici deve il primo elaboratore elettronico (il Colossus) ai tentativi degli studiosi di Bletchey Park di decifrare le comunicazioni cifrate con il sistema Lorenz e scambiate tra Hitler e i suoi capi di stato maggiore durante il secondo conflitto mondiale. Nel corso degli anni che separano il 1943 dall'epoca attuale, la crittografia ha raggiunto notevoli livelli di sicurezza, passando attraverso scoperte rilevanti e attirando l'attenzione di molti studiosi, che concentrarono le loro abilità nella risoluzione dei problemi di fondo che rendevano i sistemi crittografici di utilizzo esclusivo di una ristretta cerchia di persone "fidate" e li esponevano gravemente a intercettazione e decifrazione.

1.1 Il problema dello scambio delle chiavi

Uno dei problemi più complessi nell'evoluzione della crittografia, era costituito dal cosiddetto "scambio delle chiavi": due parti che volessero scambiarsi messaggi crittografati, avevano ovviamente la necessità di conoscere entrambe la chiave di cifratura, che al mittente serviva per rendere il messaggio incomprensibile a terzi, e al destinatario serviva per riportare il messaggio cifrato in chiaro.

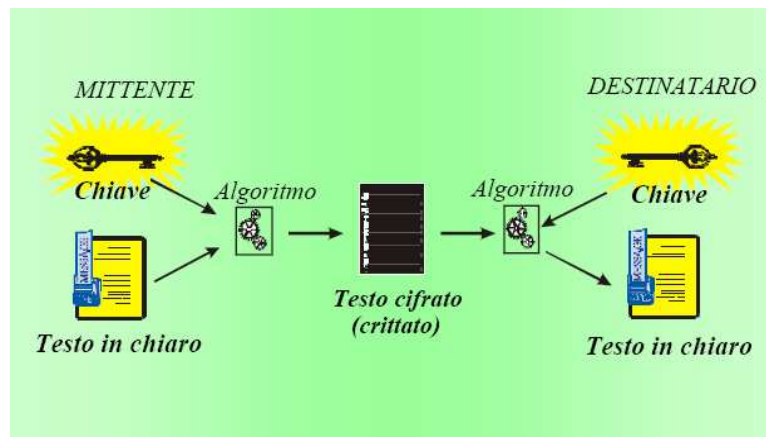


Figura 1. Il principio della Crittografia

1.2 Il Principio di Kerckhoffs

Risulterà strano, ma uno dei principi fondamentali della crittografia, utilizzato ancora nei moderni sistemi crittografici è stato individuato nel lontano 1883 dal linguista franco-olandese August Kerckhoffs nel suo celebre articolo “La cryptographie militaire” apparso nel *Journal des sciences militaires*.

Principio di Kerckhoffs:

“La sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave, in pratica si presuppone noto a priori l’algoritmo di cifratura e decifrazione”.

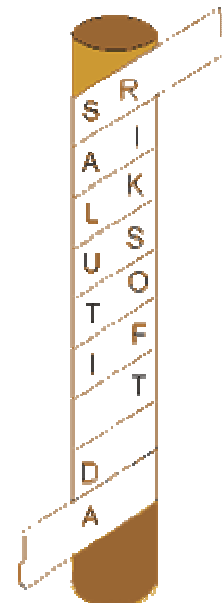
2. Crittografia antica

2.1 Scitala lacedemonica

Rappresenta una delle più antiche forme di crittografia: era già presente negli scritti di Plutarco (400 a.C.).

Consisteva in un bastone in cui si avvolgeva ad elica un nastro di cuoio (algoritmo di cifratura).

La chiave consisteva nel diametro del cilindro e la scrittura avveniva per colonne parallele all’asse del bastone lettera per lettera.



2.2 Disco di Enea (390-360 a.C.)

Tra il 390 e il 360 a.C. Enea il tattico, generale della lega arcadica, scrive il primo trattato di cifrari. Nel XXI capitolo, che tratta appunto di messaggi segreti, viene descritto un disco sulla zona esterna del quale erano contenuti 24 fori, contrassegnati dalle lettere disposte in

ordine alfabetico. Un filo, partendo da un foro centrale, si avvolgeva passando per i fori delle successive lettere del testo. Il destinatario del messaggio svolgeva il filo del disco segnando le lettere da esso indicate. Il testo si doveva poi leggere a rovescio.

2.3 Atbash

E' un metodo di cifratura ideato dal popolo ebraico: consisteva nel capovolgere l'alfabeto, con la conseguenza che la prima lettera diventava l'ultima e l'ultima la prima e così per tutte le altre lettere dell'alfabeto.

L'alfabeto chiaro e quello cifrato erano quindi rappresentati nel seguente modo:

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

Esempio

Frase da cifrare: Il sole brilla
 Frase cifrata: Ro hlov yirooz

2.4 Albam

Richiede che l'alfabeto venga diviso in due parti e che ogni lettera venga sostituita con la corrispondente dell'altra metà.

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

Esempio

Sara → Fnen

2.5 Atbah

In questo caso la sostituzione soddisfa una relazione di tipo numerico: le prime nove lettere dell'alfabeto vengono sostituite in modo tale che la somma della lettera da sostituire e della lettera sostituita risulti uguale a dieci. Per le restanti 9 lettere dell'alfabeto vale una regola simile con somma pari a 28 in decimale. Infine, per le ultime 8 lettere vale la stessa regola con somma pari a 45.

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| CHIARO | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Num | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 |
| CIFRATO | I | H | G | F | E | D | C | B | A | R | Q | P | O | N | M | L | K | J | Z | Y | X | W | V | U | T | S |



Esempio:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

La c = 3 viene sostituita con la g=7 in modo che la somma sia 10.

All'indirizzo internet <http://utenti.quipo.it/base5/combinatoria/crittografia2.htm> è possibile trovare un applet che permette di cifrare o decifrare un qualunque messaggio per mezzo dell'Atbash, dell'Albam o dell'Atbah.

2.6 Polibio (200 ca. -118 a.C.)

Nelle sue Storie (Libro X) Polibio descrive un importante metodo di cifratura. L'idea è quella di cifrare una lettera con una coppia di numeri compresi tra 1 e 5, in base ad una matrice 5x5, contenente le lettere dell'alfabeto.

Ogni lettera viene rappresentata da due numeri, guardando la riga e la colonna in cui essa si trova. Per esempio, a=11 e r=42.

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

Esempio

Attenzione agli scogli

11444415345524353415 11223224 431335223224

La sua importanza nella storia della crittografia sta nell'essere alla base di altri codici di cifratura come il **Playfair cipher** (vedi par. 3.1) o il **cifrario campale germanico** (vedi par. 3.2) usato nella prima guerra mondiale.

2.7 Cifratura di Cesare (II secolo d.C.)

Codice di sostituzione molto semplice, nel quale ogni lettera del testo veniva sostituita dalla lettera che la segue di tre posti nell'alfabeto.

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

Esempio

Testo chiaro: veni, vidi, vici

Testo cifrato: bhqn, bngn, bfn



Più in generale si dice **codice di Cesare** un codice nel quale la lettera del messaggio chiaro viene spostata di un numero fisso di posti, non necessariamente tre.

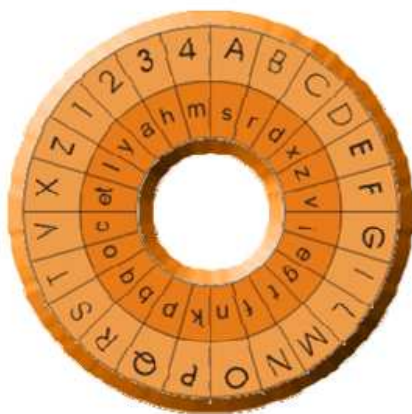
Sono possibili codici di Cesare diversi: poiché l'alfabeto internazionale è composto da 26 caratteri, sono possibili 26 alfabeti cifranti; un alfabeto (quello che comporta uno spostamento di zero posizioni) darà un cifrato uguale al messaggio chiaro iniziale.

Nel caso dei cifrari monoalfabetici, come quelli precedentemente illustrati, ad ogni lettera se ne sostituisce un'altra secondo opportune regole.

Un tale sistema è molto facile da attaccare e da violare: basta conoscere le proprietà statistiche del linguaggio con cui il testo è stato scritto, in altre parole conoscere le frequenze con le quali le lettere dell'alfabeto compaiono in un generico testo scritto nella stessa lingua del messaggio, per arrivare a trovare la corrispondenza tra le lettere del testo cifrato e quelle dell'alfabeto in chiaro.

Nel rinascimento si passò dalla sostituzione monoalfabetica a alla sostituzione polialfabetica (ad es., la Tavola di Vigenère): una cifratura per sostituzione polialfabetica si differenzia da quelle fino ad ora considerate per il fatto di utilizzare più alfabeti cifranti; con questo accorgimento il metodo dell'analisi delle frequenze perde di utilità poiché la stessa lettera nel messaggio in chiaro può essere tradotta con lettere diverse nel messaggio cifrato.

2.8 Il Disco di Leon Battista Alberti



Nel suo Trattato De Cifris (circa nel 1400), Leon Battista Alberti introdusse il primo **codice polialfabetico**.

Per tre secoli tale codice costituì il basamento dei sistemi crittografici. Inoltre, tale sistema introduce il concetto su cui si basa la macchina cifrante Enigma (vedi par. 4.1).

È un disco composto di due cerchi concentrici di rame, uno esterno fisso di diametro maggiore sul quale sono riportate le lettere dell'alfabeto in chiaro (composto di 24 caselle contenenti 20 lettere maiuscole in ordine lessicografico, escluse H, J, K, W, Y, al posto delle quali ci sono i numeri 1, 2, 3, 4) e uno interno mobile per le lettere

dell'alfabeto cifrante. Il disco interno riporta le 24 lettere minuscole in maniera disordinata (la e e la t sono collassate) ed un simbolo speciale et.

Per utilizzare questo sistema, mittente e destinatario devono avere entrambi la stessa macchinetta e aver precedentemente concordato una lettera da utilizzare come chiave di partenza. Per cifrare il messaggio, il mittente inizia ruotando il disco interno in maniera casuale; scrive quindi il testo cifrato, riportando per prima cosa la lettera sul disco piccolo

in corrispondenza della chiave concordata sul disco grande. Passa quindi ad eseguire la sostituzione del testo prelevando i caratteri sul disco più piccolo in corrispondenza dei caratteri da cifrare sul disco più grande. Terminata la prima parola, ruota di nuovo in maniera casuale il disco interno e itera la procedura di sostituzione.

In questo modo, ogni parola utilizzava un proprio alfabeto di sostituzione e con tale dispositivo ne sono a disposizione 24 (ecco perché questo sistema è classificato tra i polialfabetici). Le lettere che di volta in volta corrispondono ai numeri 1,2,3,4 non vengono usate.

Con questo tipo di sistema, la sicurezza è affidata ad una chiave di cifratura di un solo carattere: sarebbe semplicissimo decifrare il messaggio anche senza sapere che la prima lettera di ogni parola è la chiave di cifratura, basterebbe provare per ogni parola le 24 posizioni del disco.

Con questo sistema Leon Battista riusciva ad impedire l'analisi statistica basata sulla frequenza delle lettere (da lui stesso studiata).

2.9 Tavola di Vigenère

Blaise de Vigenère propose, in un trattato di cifrari pubblicato nel 1586, un codice che ebbe molta fortuna e che è ricordato con il suo nome.

La sua fama è dovuta alla semplicità del semplice codice polialfabetico. Il principale punto di forza di questo metodo è l'utilizzo non di uno ma di ben 26 alfabeti cifranti per cifrare un solo messaggio. Il metodo si può quindi considerare una generalizzazione del codice di Cesare. Tra l'altro, da tale cifrario deriva il cifrario di Vernam, considerato il cifrario teoricamente perfetto.

Invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile, determinato dalle lettere della parola chiave, da concordarsi tra mittente e destinatario. La parola è detta chiave o verme, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte.

Risulta evidente dall'esempio seguente che la stessa lettera nel testo in chiaro può essere cifrata con lettere diverse: ad esempio la "a" è stata cifrata con le lettere "s" "e" "l" "o": è dunque impossibile utilizzare un metodo di analisi delle frequenze per decrittare il messaggio (i crittoanalisti svilupparono però altre tecniche e riuscirono ad aver ragione anche della cifratura di Vigenère).

Esempio

Parola chiave: SOLE

Testo chiaro: Attacco all'alba

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | t | t | a | c | c | o | a | l | l | a | l | b | a |
| S | O | L | E | S | O | L | E | S | O | L | E | S | O |
| s | h | e | e | u | q | z | e | d | z | l | p | t | o |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|--|--|--|--|--|--|--|
| | | | | E | | | | | | L | | | | | | O | | | | | | S | | | | | | | | | | | |
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | | | | | | | | |
| b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | | | | | | | | |
| c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | | | | | | | | |
| d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | | | | | | | | |
| e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | | | | | | | | |
| f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | | | | | | | | |
| g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | | | | | | | | |
| h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | | | | | | | | |
| i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | | | | | | | | |
| j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | | | | | | | | |
| k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | | | | | | | | |
| l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | | | | | | | | |
| m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | | | | | | | | |
| n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | | | | | | | | |
| o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | | | | | | | | |
| p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | | | | | | | | |
| q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | | | | | | | | |
| r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | | | | | | | | |
| s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | | | | | | | | |
| t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | | | | | | | | |
| u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | | | | | | | | |
| v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | | | | | | | | |
| w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | | | | | | | | |
| x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | | | | | | | | |
| y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | | | | | | | | |
| z | 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 | | | | | | | | |

Figura 2. Tavola di Vigenère

Tutti i metodi crittografici fin qui analizzati erano sicuri finchè l’algoritmo stesso che li generava rimaneva segreto: la crittografia moderna si basa invece sul presupposto che il messaggio possa rimanere segreto anche se il metodo utilizzato per generarlo viene scoperto.



3. La crittografia dalla seconda metà del XIX secolo alla Grande Guerra

Dalla metà del XIX secolo l'uso della crittografia assume un ruolo determinante nella trasmissione di messaggi di carattere logistico e strategico.

Dei metodi crittografici utilizzati in questo periodo prenderemo in analisi il Playfair cipher e la cifra campale germanica o ADFGVX.

3.1 Playfair cipher

Divulgato da Lyon Playfair doveva essere utilizzato durante la guerra di Crimea ma il sistema fu effettivamente utilizzato dall'esercito britannico solamente a partire dalla guerra Boera.

Rappresenta il primo metodo di cifratura a digrammi (in altre parole, ogni lettera del testo viene crittata con gruppi di due lettere). Si usa una matrice 5x5 di 25 lettere che viene riempita nelle prime caselle con la parola chiave, abolendo le eventuali lettere ripetute, ed è completata con le rimanenti lettere nel loro ordine alfabetico.

Vediamo con una applicazione come veniva utilizzato il Playfair cipher.

Costruzione della matrice di 25 elementi:

Chiave: SEGRETI

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

Messaggio: Domani nella battaglia pensa a me

DO MA NI NE LX LA BA TX TA GL IA PE NS AM EX

Le lettere doppie sono separate per mezzo dell'inserimento di una X; inoltre, se l'ultima lettera rimane spaiata, viene a sua volta affiancata da una X.

E' possibile a questo punto che si presenti uno dei seguenti casi: lettere su righe e colonne diverse, lettere sulla stessa riga o lettere sulla stessa colonna.



Caso 1:

lettere su righe e colonne diverse

| | | | | |
|---|---|---|---|---|
| . | . | . | . | . |
| . | A | . | . | D |
| . | . | . | . | . |
| . | O | . | . | U |
| . | . | . | . | . |

Le lettere sono sostituite da quelle corrispondenti ai vertici opposti del rettangolo formato dall'incrocio di righe e colonne delle lettere del testo in chiaro.

Caso 2:

lettere sulla stessa riga

| | | | | |
|-----|---|---|---|---|
| . | . | . | . | . |
| I/J | A | B | C | D |
| . | . | . | . | . |
| . | . | . | . | . |
| . | . | . | . | . |

Le lettere sono sostituite da quelle contenute nelle celle adiacenti, alla destra delle celle contenenti le lettere del testo chiaro.

Caso 3:

lettere sulla stessa colonna

| | | | | |
|-----|---|---|---|---|
| S | . | . | . | . |
| I/J | . | . | . | . |
| F | . | . | . | . |
| N | . | . | . | . |
| V | . | . | . | . |

Le lettere sono sostituite da quelle contenute nelle celle adiacenti, sotto le celle contenenti le lettere del testo chiaro.

Il nostro messaggio viene dunque crittato come :

DO MA NI NE LX LA BA TX TA GL IA PE NS AM EX
 AU HD VF OS KY HC CB GZ ED RK AB OG VI BW DH GW

E poi raggruppato in gruppi di cinque lettere:

AUHDV FOSKY HCCBG ZEDRK ABOGV IBWDH GW



3.2 Cifra campale germanica o ADFGVX

La cifra campale germanica è un metodo di crittografia usato dall'esercito tedesco nella Grande Guerra, a partire dagli inizi del 1918, anche chiamato metodo **ADFGVX** (lettere scelte per la facilità con cui vengono trasmesse nel codice morse).

Il metodo utilizza una scacchiera 6x6 simile a quella usata nel Playfair Cipher, e nel cifrario bifido di Delastelle; si sostituiscono le lettere con gruppi di due o più lettere, le quali vengono poi sottoposte a una trasposizione per la trasmissione. Si tratta quindi di un cifrario poligrafico in cui si fa uso sia di un quadrato sia di una colonna per la trasposizione, e che necessita quindi di due chiavi per la cifratura: nel seguito chiameremo tali chiavi "chiave quadrato" e "chiave colonna".

Vediamo come sia possibile utilizzare la cifra campale germanica con un esempio concreto.

Scegliamo una chiave per il quadrato:

Chiave quadrato: DEUTSCHLAND

Si eliminano le lettere doppie dalla chiave, ottenendo: DEUTSCHLAN

Si aggiungono le rimanenti lettere dell'alfabeto in fondo alla stringa (una stringa è una serie di lettere ed eventualmente numeri, per cui si parla in generale di stringhe alfanumeriche) che si è ottenuta:

DEUTSCHLANBFGIJKMOPQRVWXYZ

Si inseriscono i numeri da 0 a 9 dopo le lettere della chiave con la seguente corrispondenza:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |

D4E5UT SC3H8L A1NB2F 6G7I9J 0KMOPQ RVWXYZ



Si inserisce la stringa alfanumerica ottenuta in un quadrato di 6x6 celle:

| | | | | | | |
|---|---|---|---|---|---|---|
| | A | D | F | G | V | X |
| A | D | 4 | E | 5 | U | T |
| D | S | C | 3 | H | 8 | L |
| F | A | 1 | N | B | 2 | F |
| G | 6 | G | 7 | I | 9 | J |
| V | 0 | K | M | O | P | Q |
| X | R | V | W | X | Y | Z |

Scegliamo un messaggio da trasmettere:

Messaggio: Questo è un segreto

Ogni lettera del messaggio è sostituita dalle lettere corrispondenti rispettivamente alla riga e alla colonna della lettera del testo chiaro:

| | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| q | u | e | s | t | o | e | u | n | s | e | g | r | e | t | o |
| VX | AV | AF | DA | AX | VG | AF | AV | FF | DA | AF | GD | XA | AF | AX | VG |

Scegliamo una chiave colonna per la trasposizione:

Chiave colonna: PANZER

A ogni lettera della chiave colonna viene assegnato un numero in base all'ordine con cui compare nell'alfabeto (se la lettera compare più volte nella chiave si prosegue la numerazione cominciando da sinistra; es.: APOLLO = 164235). La stringa alfanumerica ottenuta dal procedimento sul quadrato è riscritta in una tabella sotto la chiave colonna.

| | | | | | |
|---|---|---|---|---|---|
| P | A | N | Z | E | R |
| 4 | 1 | 3 | 6 | 2 | 5 |
| V | X | A | V | A | F |
| D | A | A | X | V | G |
| A | F | A | V | F | F |
| D | A | A | F | G | D |
| X | A | A | F | A | X |
| V | G | | | | |

Si leggono le colonne nell'ordine dato dalla chiave e si riscrivono in gruppi di cinque, ottenendo il messaggio crittato:

XAFAA GAVFG AAAAA AVDAD XVFGF DXVXV FF



4. Crittografia nella II Guerra Mondiale

Dei vari metodi di cifratura utilizzati durante la seconda guerra mondiale dalle varie nazioni belligeranti, si è scelto di parlare della macchina Enigma: essa rappresenta una delle più celebri macchine cifranti che cominciarono a diffondersi nella prima metà del XX secolo.

4.1 Enigma



Enigma era una macchina cifratrice utilizzata dal Terzo Reich negli anni precedenti e durante la Seconda Guerra Mondiale.

La macchina Enigma veniva utilizzata per "mascherare" un messaggio che un operatore telegrafico mandava ad un altro in modo che chiunque intercettasse tale messaggio non fosse in grado di sapere che cosa il messaggio stesso diceva. Quando un operatore utilizzava la macchina, egli digitava le lettere che costituivano il messaggio sulla tastiera della macchina e i meccanismi interni della stessa trasformavano quel testo in un altro apparentemente incomprensibile. La chiave di lettura era l'utilizzo della stessa macchina, opportunamente settata da parte di chi riceveva il messaggio cifrato.

Nel 1918 l'inventore Arthur Scherbius e l'amico Richard Ritter fondarono la Scherbius&Ritter, la società dalla quale avrebbe avuto origine la macchina cifratrice Enigma. Scherbius aveva studiato ingegneria elettrica ad Hannover e mise in pratica le conoscenze così acquisite progettando un dispositivo crittografico che corrispondeva ad una riproduzione elettromeccanica del disco cifrante di Leon Battista Alberti.

La macchina era costituita da diversi elementi relativamente semplici se presi singolarmente, ma che costituivano insieme un potente apparato per la produzione di scritture cifrate.

La versione base del dispositivo era costituita da tre componenti collegati tra loro con fili elettrici:

- una **tastiera** per immettere le lettere del testo in chiaro;
- un'**unità scambiatrice** che cifra la lettera trasformandola nel corrispondente elemento del crittogramma;
- un **visore** con varie lampadine che illuminandosi indicano la lettera da inserire nel testo cifrato.

In pratica l'operatore preme il tasto corrispondente ad una lettera del testo in chiaro, la macchina elabora l'impulso elettrico ricevuto e fa illuminare la lampadina corrispondente alla lettera cifrata.

In Figura 3 è rappresentato uno schema semplificato del funzionamento (con sole tre lettere) dei tre componenti principali di una macchina Enigma dal quale risulta chiaro il processo di scambio delle lettere operato dallo scambiatore.

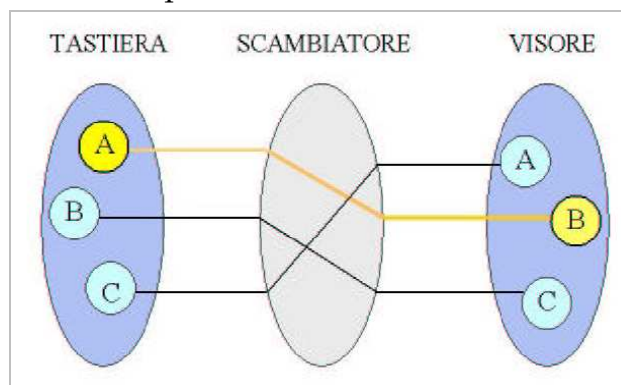


Figura 3. Schema semplificato del funzionamento di tastiera, scambiatore e visore.

4.1.1 [Lo scambiatore](#)

Lo scambiatore rappresenta la parte più importante della macchina: consiste in uno spesso disco di gomma attraversato da una fitta rete di fili provenienti dalla tastiera. Questi fili entrano nello scambiatore e dopo un percorso formato da vari gomiti emergono dalla parte opposta. Lo schema interno dello scambiatore determina in pratica un alfabeto cifrante utilizzabile per una semplice cifratura a sostituzione monoalfabetica.

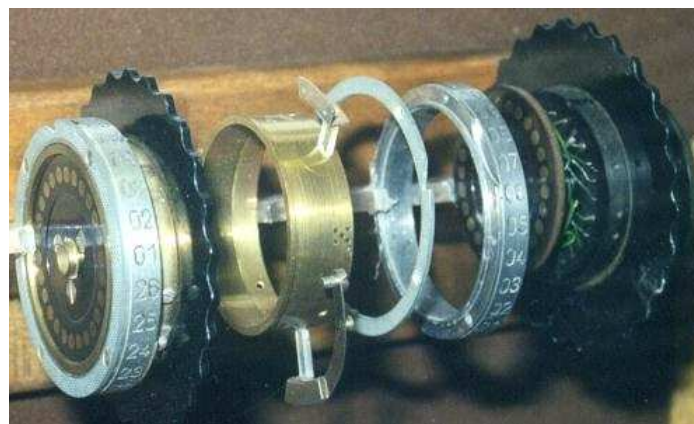


Figura 4. Schema interno di uno scambiatore

Il passo successivo dell'idea di Scherbius prevedeva di far ruotare il disco dello scambiatore di un ventiseiesimo di giro dopo la cifratura di ogni lettera, facendo sì che l'alfabeto cifrante cambiasse dopo ogni lettera trasformando la cifratura da monoalfabetica a polialfabetica.

Così com'è il meccanismo presenta ancora il problema della ripetizione che è comunemente sinonimo di cifratura debole. Per superarlo vennero introdotti un secondo e un terzo scambiatore. Il secondo compiva una rotazione parziale soltanto dopo che il primo aveva compiuto un intero giro e allo stesso modo faceva il terzo basandosi sul secondo. In questo modo la macchina di Scherbius poteva disporre di $26 \cdot 26 \cdot 26 = 17576$ procedure di sostituzione diverse.

In Figura 5 sono rappresentati in dettaglio i componenti di uno scambiatore:

- 1) Dentellature usate per posizionare il rotore;
- 2) Anello dell'alfabeto
- 3) Asse di rotazione
- 4) Gancio che blocca l'anello al nucleo (5)
- 5) Nucleo contenente i collegamenti elettrici tra contatti (6) e dischi (7)
- 6) Contatti elettrici
- 7) Dischi di contatto tra rotori successivi
- 8) Gancio per ruotare l'anello dell'alfabeto

Il diametro dello scambiatore era di circa 4 pollici (circa 10 cm); esternamente, sul lato destro erano presenti 26 contatti a molla sporgenti (*pin*, maschio), sul lato sinistro altri 26 rientranti (*pad*, femmina); internamente, era presente una corrispondenza biunivoca tra maschi e femmine data da fili elettrici. Ogni scambiatore era contrassegnato da un numero romano (I II III), ed era dotato di un anello esterno rotabile in 26 posizioni diverse.

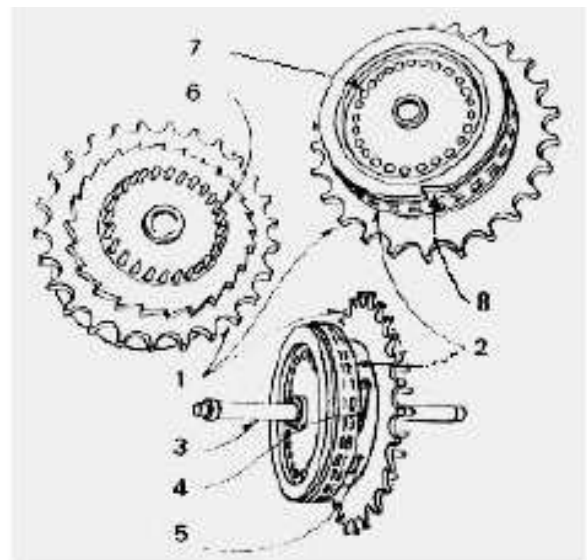


Figura 5. Dettagli di uno scambiatore

4.1.2 [Il Riflessore](#)

Un altro degli elementi del dispositivo considerato importante dallo stesso inventore era il riflesso. Esso consisteva di un disco con circuiti interni simile agli scambiatori ma che non ruotava e i fili che vi entravano riemergevano dallo stesso lato (si veda la Figura 6). Con tale elemento installato un segnale in ingresso alla macchina attraversava i tre scambiatori, poi passava al riflesso e veniva rimandato indietro passando nuovamente negli scambiatori, ma usando un percorso diverso.

In Figura 6 si vede come digitando la lettera "b" sulla tastiera, il percorso è tale da illuminare la lettera "c".

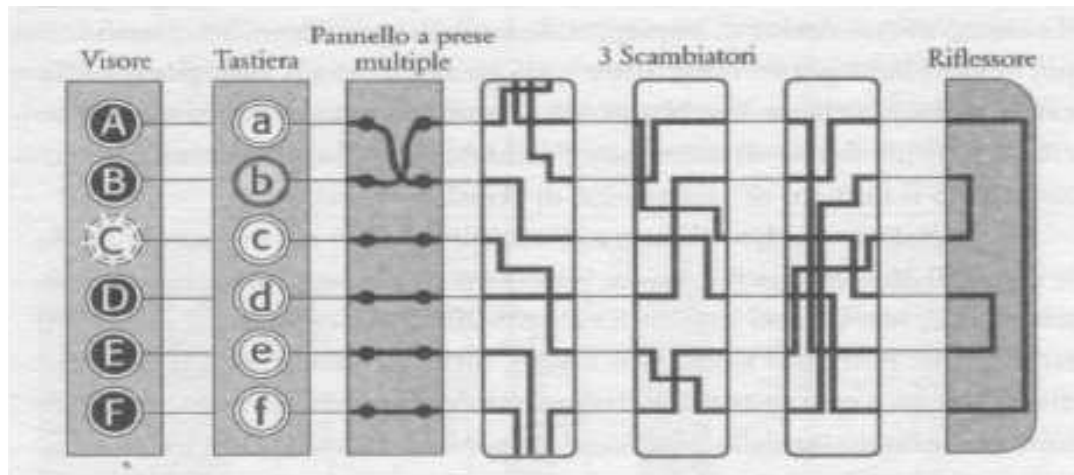


Figura 6. Schema del funzionamento di tastiera, scambiatori e visore con riflesso e pannello a prese multiple.

Per aumentare ulteriormente il numero di chiavi, i rotori disponibili vennero portati da 3 a 5. In Figura 7 è rappresentata una scatola che poteva contenere fino a sette rotori di ricambio.



Figura 7. Scatola con rotori

Venne inoltre introdotto un pannello a prese multiple (Stecker) posto tra la tastiera e il primo rotore (si vedano la Figura 6 e la Figura 8). Tale dispositivo permetteva di inserire alcuni cavi muniti di spinotti, che avevano l'effetto di scambiare due lettere prima della loro immissione nel rotore. L'operatore di Enigma aveva a disposizione sei cavi per sei coppie di lettere, mentre le altre quattordici restavano non scambiate.

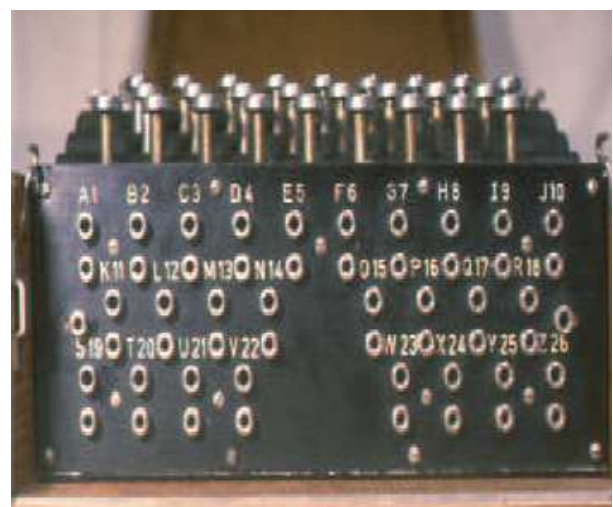


Figura 8. Pannello a prese multiple

Esempio

Collegando attraverso uno spinotto la coppia di lettere Q e R , la corrente che rappresenta la Q in entrata rappresenta poi la R in uscita. Digitando Q sulla tastiera, la sua cifratura sarà la cifratura di R . Viceversa se una qualsiasi lettera viene cifrata nella Q , il risultato finale sarà R .



Combinando insieme tutti gli elementi fin qui osservati si può calcolare il numero di chiavi che Enigma poteva impiegare.

4.1.3 Calcolo del numero di chiavi possibili

- gli scambiatori (o rotori) potevano orientarsi ognuno in 26 modi nel piano perpendicolare all'asse di rotazione, quindi tutti e tre generavano $26 \cdot 26 \cdot 26 = 17576$ combinazioni;
- all'interno dell'unità cifratrice i tre scambiatori potevano essere inseriti in diverse posizioni reciproche, così riassumibili: 123, 132, 213, 231, 312, 321. Erano quindi ammesse 6 diverse posizioni reciproche dei rotori;
- con il pannello a prese multiple i possibili abbinamenti di 12 (6×2) lettere su 26 sono moltissimi, per l'esattezza 100 miliardi 391 milioni 791 mila 500 (100.391.791.500), che si ottiene dalla formula seguente dove p rappresenta il numero di chiavi ed è pari a 6:

$$\binom{26}{2p} \cdot (2p-1) \cdot (2p-3) \cdot (2p-5) \cdot \dots \cdot 1 = \frac{26!}{(26-2p)! \cdot p! \cdot 2^p}$$

- il numero totale di chiavi si ottiene moltiplicando tra loro le suddette possibilità:

$$17576 \cdot 6 \cdot 100391791500 = 105869167644240000$$

circa 10 milioni di miliardi.

4.1.4 Utilizzo

Vediamo come veniva usata nella pratica una macchina Enigma.

Innanzitutto bisogna specificare che gli scambiatori dovevano essere posizionati con un certo assetto prima di iniziare la cifratura di un messaggio e la loro posizione costituiva una vera e propria chiave. L'insieme di tali chiavi giornaliere era contenuta in un cifrario (Figura 9) che doveva essere distribuito mensilmente a tutti gli operatori e che doveva essere, ovviamente, molto ben custodito (torna, anche in questo caso, il problema della distribuzione delle chiavi). Gli assetti giornalieri del cifrario venivano usati per tutti i messaggi di una giornata. Per cifrare un messaggio un operatore Enigma posizionava gli scambiatori secondo la chiave giornaliera, digitava il messaggio sulla tastiera della macchina e spediva via radio il risultato al destinatario. Quest'ultimo digitava il

messaggio cifrato sulla tastiera della sua macchina Enigma, sulla quale gli scambiatori erano sistemati secondo la stessa chiave giornaliera usata da chi aveva crittato il messaggio, e otteneva il messaggio in chiaro. La semplicità con cui questa operazione era realizzata era dovuta proprio all'introduzione del riflettore.

| Geheim! | | Sonder - Maschinenschlüssel BGT | | |
|---------|------------|---------------------------------|-------------------------------|---------------|
| Datum | Walzenlage | Ringstellung | Steckerverbindungen | Grundstellung |
| 31. | IV II I | F T R | HR AT IW SN UY DF GV LJ DO MX | vyj |
| 30. | III V II | Y V P | OR KI JV OE ZN NU BY YC DS GP | cqr |
| 29. | V IV I | O H R | UX JC PD BE TA XD ST BS LU FI | vhf |

Figura 9. Parte di un cifrario tedesco per macchine Enigma.

I passaggi per l'utilizzo di Enigma si possono riassumere con i seguenti punti:

1. Walzenlage: quali rotori usare e in che ordine [II I III, III V II, ecc.];
2. Ringstellung: assetto degli anelli [F T R, Y V P, ecc.];
3. Steckerverbindungen: assetto del pannello a prese multiple [es., HR AT IW SN UY DF GV LJ DO MX];
4. Grundstellung: le 3 lettere che mostravano la posizione dei rotori da usare per cifrare il messaggio [v y j]

Oltre alle chiavi contenute nei cifrari, veniva anche utilizzata una chiave di messaggio usata per regolare il nuovo assetto: tale chiave era trasmessa due volte di seguito all'inizio di ogni messaggio, con l'assetto della chiave giornaliera (fu proprio questa ripetizione della chiave di messaggio all'inizio di ogni testo trasmesso il punto di partenza che permise al matematico Marian Rejewski di far breccia nel codice Enigma).

Esempio

Cifratura

- Chiave giornaliera: QCW
- Chiave di messaggio: PGH
- Il mittente posiziona i rotori secondo la chiave giornaliera
- Digita PGH PGH sulla tastiera, ottenendo KIV BJE
- Posiziona gli scambiatori secondo la chiave di messaggio
- Scrive il messaggio

Decifratura

- Il destinatario posiziona i rotori sulla chiave giornaliera QCW
- Digita le prime sei lettere del messaggio ricevuto, ottenendo PGH PGH
- Posiziona gli scambiatori secondo la chiave di messaggio
- Digita il resto del testo cifrato sulla tastiera ottenendo il testo in chiaro





Figura 10. Macchina Enigma con visibile il pannello a prese multiple.

All'indirizzo <http://users.telenet.be/d.rijmenants/en/enigmasim.htm> è possibile scaricare un software che riproduce il funzionamento di una macchina Enigma a tre rotori in dotazione alla Wehrmacht e il modello M4 a quattro rotori in dotazione alla Kriegsmarine, entrambe utilizzate durante la Seconda Guerra Mondiale dal 1939 al 1945.

All'indirizzo <http://www.codesandciphers.org.uk/enigmafilm/emachines/enigma1.htm> è possibile utilizzare un simulatore che riproduce il funzionamento di una macchina Enigma a tre rotori in dotazione all'esercito e all'aviazione tedesca durante la seconda guerra mondiale, direttamente sul Web.

All'indirizzo <http://math.arizona.edu/~dsl/ephotos.htm> sono disponibili una serie di foto della macchina Enigma, anche con particolari dei componenti interni.

5. Numeri primi

Un intero positivo N si dice **primo** se

N è diverso da 1 ed è divisibile esattamente solo per 1 e per se stesso.

Ancora oggi il metodo più veloce per trovare *tutti* i numeri primi inferiori ad un limite L prefissato è il **crivello di Eratostene**. Tale algoritmo può essere schematizzato con i seguenti punti:

- si costruisce un elenco E degli interi compresi tra 2 e L ;
- si cancellano tutti i multipli di 2 tranne 2;
- si prende il primo numero non cancellato, che è 3, e si cancellano tutti i suoi multipli (escluso lui stesso);
- si continua così fino alla parte intera della radice quadrata di L .

I numeri superstiti sono i numeri primi compresi tra 2 e L .

Chi lo desidera può vedere il crivello in azione sul sito:

<http://britton.disted.camosun.bc.ca/sieve/jberatosapplet.htm>

Il **Teorema Fondamentale dell'Aritmetica** stabilisce che:

Ogni numero intero $\neq 0, -1, +1$ si decompone nel prodotto di numeri primi e la decomposizione è unica a meno dell'ordine e del segno dei fattori.

Dal Secondo Teorema di Euclide sui numeri primi sappiamo che:

i numeri primi formano una successione infinita.

E' da notare che la dimostrazione di Euclide della esistenza di infiniti numeri primi è *costruttiva*, fornisce cioè un metodo che consente, almeno in linea di principio, di trovare un numero primo che sia *al di fuori di qualsiasi insieme finito Q di numeri primi assegnato!*

La tecnica è la seguente:

- Sia $Q = \{q_1, q_2, q_3, \dots, q_m\}$;
- si calcola $n = q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_m + 1$;
- evidentemente n è coprimo con tutti i q_j contenuti in Q (cioè non ha fattori in comune con essi): quindi, *tutti i suoi fattori primi sono primi che non stanno in Q .*

Esempio

Supponiamo di conoscere soltanto i numeri primi 2 e 3.

Allora $Q = \{2,3\}$, $n = 2 \cdot 3 + 1 = 7$, che è primo.

Si aggiunge 7 a Q e si ottiene $Q = \{2,3,7\}$.

Al passo seguente si ha $n = 2 \cdot 3 \cdot 7 + 1 = 43$, che è primo anch'esso.

Lo aggiungo al bottino: $Q = \{2,3,7,43\}$.

Si prosegue in questo modo: $n = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1806$ che può essere scomposto in fattori primi come $1806 = 13 \cdot 139$, aggiungendo quindi due nuovi numeri all'insieme Q che diventa $Q = \{2,3,7,43,13,139\}$.

Denotiamo la successione dei primi in ordine ascendente con p_1, p_2, \dots, p_n .

Avremo allora: $p_1 = 2, p_2 = 3, p_3 = 5, \dots$

E inoltre: $p_{10} = 29, p_{100} = 541, p_{1000} = 7979, p_{10000} = 104709$

Una funzione di importanza fondamentale è $\pi(x)$:

$$\pi(x) = \text{numero dei primi minori o uguali a } x$$

Si ha quindi: $\pi(10) = 4$ perché ci sono 4 primi (2,3,5,7) minori di 10.

Alcuni valori di $\pi(x)$ sono:

$$\pi(100) = 25$$

$$\pi(1000) = 168$$

$$\pi(10000) = 1229$$

$$\pi(100000) = 9592$$

$$\pi(1000000) = 78498$$

$$\pi(10000000) = 664579$$

Nel 2000 si è arrivati (con algoritmi sofisticati ed una grande rete di computers) a 10^{22} :

$$\pi(10^{22}) = 201467286689315906290$$

Accenniamo qui soltanto al fatto che un valore approssimato di $\pi(x)$ può essere stimato per mezzo del **Teorema dei numeri primi** (dimostrato indipendentemente da Hadamard e da De la Vallée Poussin nel 1896) il quale afferma che: $\pi(x) \cong \frac{x}{\log(x)}$.

Tra le altre, una conseguenza del teorema dei numeri primi è che la probabilità che un numero x preso a caso sia primo è circa $\frac{1}{\log(x)}$.



Esempio

La probabilità che un intero casuale di 1000 cifre sia primo è circa $1/\log(10^{1000})$. Tenendo presente che nel Teorema dei numeri primi il logaritmo è in base e : $\log(10^{1000}) = 1000 \cdot \log(10) = 2302.59$. Quindi, in media, troveremo un numero primo ogni 2302 interi presi a caso.

E' possibile, dato un intero x casuale, provare velocemente che x è primo?

Naturalmente esiste un metodo ovvio (di forza bruta): dividerlo per gli interi che lo precedono. Oppure, cosa assai più intelligente, mettere in moto un crivello di Eratostene. Entrambi però richiederebbero tempi proibitivi di calcolo anche con numeri di modesta lunghezza, persino utilizzando supercomputers.

Accenniamo qui soltanto al fatto che esistono metodi per dimostrare che un intero è *probabilmente primo*, con una probabilità di errore che si può rendere piccola a piacere (tra questi ricordiamo il Test di Fermat). Esistono poi anche metodi molto più efficaci, per i quali la probabilità di errore è ancora più bassa. Il punto di forza di tutti questi metodi è che il tempo che impiegano ad eseguire il test su x è **polinomiale**, cioè è esprimibile mediante un polinomio *nel numero delle cifre di x* . Recentemente (nel 2002) tre ricercatori indiani (Agrawal, Saxena e Cayal) hanno trovato un algoritmo che è *al tempo stesso polinomiale e deterministico* per dimostrare la primalità di un numero.

Questo è un grande risultato, che ha risolto una congettura rimasta aperta per decenni. Il loro algoritmo però non è ancora utilizzato in pratica, perché è molto più lento dei test probabilistici, i quali, del resto, sono *quasi certi* per i primi di centinaia di cifre che servono attualmente in crittografia.

6. Aritmetica modulo n

Nel seguito \mathbf{N} e \mathbf{Z} denoteranno rispettivamente l'insieme dei numeri naturali $\{0,1,2,\dots\}$ e l'insieme degli interi relativi $\{\dots,-2,-1,0,+1,+2,\dots\}$.

Dati a, b in \mathbf{Z} ed $n > 1$ in \mathbf{N} , diciamo che a è *congruo a b modulo n* se a e b divisi per n danno lo stesso resto; in questo caso scriviamo $a \equiv b \pmod{n}$. La relazione di congruenza è una relazione di equivalenza.

Esempio

L'aritmetica dei moduli prende in considerazione un gruppo limitato di numeri disposti ad anello, un po' come le ore sul quadrante dell'orologio.

Consideriamo ad esempio un quadrante contenente solo 7 numeri, da 0 a 6, corrispondente al modulo 7.

Per calcolare $2 + 3$ si partirà da 2 e ci si sposterà di 3 numeri, ottenendo 5. Per calcolare $2 + 6$ si partirà da 2 e ci si sposterà di 6 numeri. In questo modo, attraversando l'intero anello,



si otterrà come risultato 1.

In pratica:

$$2 + 3 = 5 \pmod{7}$$

$$2 + 6 = 1 \pmod{7}$$

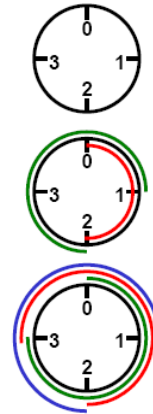
Esempio

Z_4

$$Z_4 = \{0,1,2,3\}$$

$$2+3 \pmod{4} = 1$$

$$3*3 \pmod{4} = 1$$



Ovviamente $a \equiv b \pmod{n}$ se e solo se $a = n \cdot b + k$ con k in Z .

Per indicare tutti i numeri che differiscono tra di loro per un multiplo di n si usa il nome **classe di resto modulo n** (insieme di numeri che hanno in comune il resto della divisione per n).

Tali classi sono indicate usando tale resto con una soprilineatura:

$\overline{0}$ classe di resto modulo 0: insieme dei numeri interi che divisi per n danno 0;

$\overline{1}$ classe di resto modulo 1: insieme dei numeri interi che divisi per n danno 1;

...

$\overline{n-1}$ classe di resto modulo $n-1$: insieme dei numeri interi che divisi per n danno $n-1$;

Si indica con Z_n l'insieme delle classi di resto modulo n : $Z_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

Sono valide le seguenti proprietà:

$$\overline{a} + \overline{b} = \overline{a+b} \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Esempio

Operazioni in Z_5

| | | | | | |
|---|---|---|---|---|---|
| + | 0 | 1 | 2 | 3 | 4 |
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| . | 0 | 1 | 2 | 3 | 4 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |



6.1 Il cifrario di Cesare “generalizzato” con l’aritmetica modulo n

Nel paragrafo 2.7 abbiamo parlato del cifrario di Cesare e di come fosse possibile generare messaggi cifrati per mezzo di questo metodo.

Vedremo ora come sia possibile generalizzare tale sistema di cifratura utilizzando le classi di resto, e ottenendo così una cifratura che non trasla soltanto le lettere dell’alfabeto, ma le “rimescola”.

Consideriamo l’insieme delle classi di resto modulo 26, e associamo ad ogni lettera dell’alfabeto una classe di resto modulo 26.

Fissiamo due numeri, detti **parametri di cifratura**, e otteniamo la lettera che sostituirà la lettera indicata dalla classe \bar{x} con quella individuata dalla classe \bar{y} per mezzo della formula:

$$\bar{y} = \overline{a \cdot x + b}$$

Esempio

| CHIARO | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|--------------------------------------|---|----|----|----|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| $\bar{y} = \overline{5 \cdot x + 1}$ | 6 | 11 | 16 | 21 | 0 | 5 | 10 | 15 | 20 | 25 | 4 | 9 | 14 | 19 | 24 | 3 | 8 | 13 | 18 | 23 | 2 | 7 | 12 | 17 | 22 | 1 |
| CIFRATO | F | K | P | U | Z | E | J | O | T | Y | D | I | N | S | X | C | H | M | R | W | B | G | L | Q | V | A |

Testo chiaro: veni, vidi, vici

Testo cifrato: gzst, gtut, gtpt

Risulta evidente che non tutte le scelte dei numeri a e b possono portare a una corretta cifratura e decifratura del messaggio: in particolare, è necessario che ogni lettera dell’alfabeto chiaro sia cifrata con una lettera differente, per evitare ambiguità nell’operazione di decrittazione.

Si può dimostrare che, per avere una “buona” chiave di cifratura, occorre scegliere a in modo tale che \bar{a} abbia inverso in Z_{26} .

Identità di Bézout

Se $d = MCD(a, b)$ allora esistono degli interi x e y tali che $d = a \cdot x + b \cdot y$



7. Funzione e Teorema di Eulero

La funzione di Eulero $\phi(n)$ indica il numero di elementi invertibile in Z_n , e può essere anche interpretato come il numero di interi minori di n e relativamente primi con esso.

Poiché contare le classi invertibili in Z_n è come contare i numeri tra 1 e $n-1$ che sono coprimi con n , si può affermare che:

se $n = p$ è primo, si ha $\phi(p) = p - 1$

Si ha inoltre:

se $n = p^r$ con p primo, si ha $\phi(n) = \phi(p^r) = p^{r-1} \cdot (p - 1)$

se $n = p_1^{r_1} \cdot \dots \cdot p_k^{r_k}$ con p_1, \dots, p_k primi diversi tra loro, si ha

$$\phi(n) = p_1^{r_1-1}(p_1 - 1) \cdot \dots \cdot p_k^{r_k-1}(p_k - 1)$$

La funzione di Eulero è alla base dell'importantissimo **Teorema di Eulero**:

Siano a e n due numeri interi positivi primi tra loro. Allora:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

All'indirizzo:

<http://www.math.mtu.edu/mathlab/COURSES/holt/dnt/phi1.html>

è possibile utilizzare un applet che permette di calcolare il valore della funzione di Eulero di un qualunque numero inserito dall'utente.

7.1 Un'applicazione della funzione di Eulero

Vedremo ora un'interessante applicazione del Teorema di Eulero, che permette di calcolare, dato un numero in forma di potenza, le cifre decimali del numero stesso scritto in forma posizionale.

Partiamo da un caso semplice per chiarire meglio il concetto: supponiamo di voler conoscere la cifra x che indica in numero di unità del numero 13^5 . In questo caso, una semplice calcolatrice portatile consente di ottenere il risultato 371293 e scoprire così che la cifra cercata è 3.

Vediamo come si sarebbe potuto ottenere lo stesso risultato con la funzione e il teorema di Eulero:

cercare la cifra che indica il numero di unità di 13^5 equivale a calcolare il resto della divisione per 10, ossi il numero compreso tra 0 e 9 tale che $\bar{x} = \overline{13^5}$ in Z_{10} .



- $13 \equiv 3 \pmod{10}$, in quanto il resto della divisione per 10 è uguale e pari a 3;
- $\bar{x} = \overline{13^5} = \bar{3}^5$
- per il Teorema di Eulero avremo: $a = 3$; $n = 10$; $\phi(10) = \phi(2 \cdot 5) = (2-1) \cdot (5-1) = 4$
- $3^{\phi(10)} = 3^4 \equiv 1 \pmod{10}$
(infatti: $3^4 = 81 \equiv 1 \pmod{10}$)
- $\bar{x} = \bar{3}^5 = \bar{3}^4 \cdot \bar{3} = \bar{1} \cdot \bar{3} = \bar{3}$

La cifra finale (il numero di unità) di 13^5 è quindi 3, come risultava dal calcolo diretto.

Esempio

Si vogliono calcolare le ultime due cifre decimali (decine e unità) del numero 203^{327} .

Le ultime due cifre decimali corrispondono al resto della divisione per 100.

Si procede quindi nel seguente modo:

- $203 \equiv 3 \pmod{100}$
- $\bar{x} = \overline{203^{327}} = \bar{3}^{327}$
- $a = 3$; $n = 100$; $\phi(100) = \phi(2^2 \cdot 5^2) = 2^{2-1} \cdot (2-1) \cdot 5^{2-1} \cdot (5-1) = 40$
quindi: $3^{40} \equiv 1 \pmod{100}$
- $\bar{3}^{327} = \bar{3}^{8 \cdot 40 + 7} = (\bar{3}^{40})^8 \cdot \bar{3}^7 = \bar{1} \cdot \bar{3}^7 = \overline{2187} = \bar{87}$



8. La nascita della crittografia a chiave pubblica

Tutti i metodi crittografici visti nei capitoli precedenti sono accomunati da una caratteristica: per tutti i metodi è necessario che mittente e destinatario, prima di scambiarsi un messaggio in codice, si siano accordati su quale “chiave” utilizzare per cifrare e decifrare i messaggi. Non è infatti sufficiente concordare il metodo da usare per nascondere il messaggio, ma è altresì necessario stabilire la chiave da utilizzare per applicare tale metodo.

Le chiavi da usare nei sistemi di cui abbiamo parlato nei precedenti capitoli possono essere così riassunte:

| Metodo | Chiave/i |
|--------------------------------|--|
| Scitola lacedemonica | Diametro del cilindro |
| Atbash - Albam - Atba | Alfabeto cifrante |
| Cifratura di Cesare | Numero che da di quanto viene traslato l'alfabeto chiaro |
| Disco di Leon Battista Alberti | Lettera di partenza |
| Tavola di Vigenère | Parola chiave |
| Playfair cipher | Parola chiave |
| ADFGVX | Parola chiave “quadrato” e parola chiave “colonna” |
| Enigma | Settaggio della macchina |

E' quindi possibile che la chiave sia costituita da un numero o da una o più parole; in ogni caso, due parti che vogliono scambiarsi messaggi in modo “sicuro” devono prima scambiarsi l'informazione costituita dalla chiave. E' evidente che tale chiave deve rimanere segreta se si vuole che rimanga tale anche il messaggio: nasce quindi il problema di come scambiarsi in modo sicuro la chiave, in altre parole il cosiddetto problema della distribuzione delle chiavi. Possiamo ricordare a questo proposito ciò che ha scritto Simon Singh:

“per poter condividere un segreto (tramite un messaggio crittato), due persone dovrebbero già condividere un segreto (la chiave)”.

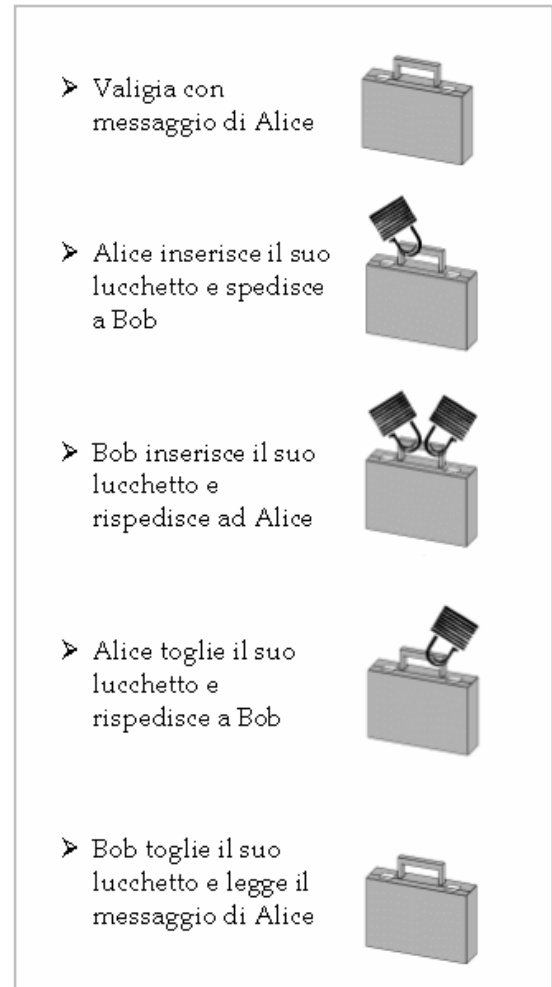
Nei prossimi capitoli vedremo come tale problema fu affrontato e risolto dopo la seconda guerra mondiale portando alla crittografia moderna a chiave pubblica.

8.1 Una scatola e due lucchetti: lo scambio di chiavi secondo Diffie, Hellman e Merkle

Il modo migliore per capire come si sia potuti arrivare a concepire e a realizzare un sistema crittografico che non necessita di uno scambio preventivo di chiavi da parte di mittente e destinatario è partire da un esempio.

Supponiamo che, per scambiarsi documenti riservati, mittente e destinatario utilizzino una scatola alla quale sia possibile applicare due lucchetti; è dunque possibile procedere nel seguente modo:

- il mittente racchiude il messaggio nella scatola e la chiude con il lucchetto del quale solo lui possiede la chiave e spedisce la scatola al destinatario;
- il destinatario riceve la scatola ma non può aprirla dato che non ha la chiave del lucchetto; applica a questo punto un altro lucchetto, del quale solo lui possiede la chiave e rimanda la scatola al mittente;
- il mittente alla ricezione della scatola toglie il lucchetto che aveva precedentemente applicato e la rispedisce al destinatario;
- la scatola che arriva al destinatario è ormai chiusa solo con il lucchetto da lui stesso applicato: egli, quindi, potrà aprirla senza problemi e leggere il messaggio in essa racchiuso, senza che nessun terzo incomodo possa averne sbirciato il contenuto.



Questa idea però non è immediatamente traducibile in un modello matematico, in quanto: svolgere il primo passaggio (mettere il primo lucchetto alla scatola) significa partire da certi dati iniziali (scatola senza lucchetti), applicare ad essi una determinata funzione matematica (primo lucchetto) e raggiungere un certo risultato (scatola con un lucchetto); svolgere il secondo passaggio (mettere il secondo lucchetto alla scatola) significa partire dai risultati del primo passaggio (scatola con un lucchetto), applicare ad essi una diversa funzione matematica (secondo lucchetto) e raggiungere un altro risultato (scatola con due lucchetti); il terzo passaggio consiste nell'inversione della funzione utilizzata nel primo passaggio (cioè nel togliere il primo lucchetto messo); il quarto, ovviamente, si realizza

invertendo la funzione applicata nel secondo passaggio. Ma in questo modo non si riottengono, in generale, i dati iniziali (scatola senza lucchetto) poiché *l'inversione della composizione di due funzioni deve avvenire in ordine contrario rispetto all'ordine di applicazione*, cioè va invertita per prima quella applicata per ultima.

Tutto ciò risulta evidente dall'esempio che segue.

Esempio

Chiave di Alice

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

Chiave di Bob

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

MESSAGGIO: ci vediamo

Cifrato da Alice: SV RGVVHYB

Ricifrato da Bob: HD YNSDOLP

Decifrato da Alice: AJ MQCJLZP

Decifrato da Bob: EI CNAIYWB

Questo problema fu affrontato e risolto negli anni '70 del secolo scorso dai ricercatori Whitfield Diffie, Martin Hellman e Ralph Merkle.

Le funzioni di cui si servirono per risolvere il problema della distribuzione delle chiavi derivano dall'aritmetica dei moduli (vedi par. 6.) dove è spesso possibile incontrare funzioni unidirezionali, tali cioè da essere "difficili" da invertire.

Dalla tabella che segue si può osservare ad esempio come la potenza cresca regolarmente, mentre nel caso dell'aritmetica dei moduli la variazione della funzione non sia regolare.

| | | | | | | | | | | |
|----------------|---|---|----|----|-----|-----|------|------|-------|-------|
| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 3^x | 3 | 9 | 27 | 81 | 243 | 729 | 2187 | 6561 | 19683 | 59049 |
| $3^x \pmod{5}$ | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 |

Inoltre, dalla tabella si evince come in aritmetica normale sia immediato, dato un valore di x , ricavare il corrispondente valore della funzione, e viceversa, dato il valore della funzione ricavare x . In aritmetica dei moduli il comportamento "imprevedibile" della funzione rende questa inversione estremamente difficile.



La funzione unidirezionale che fu scelta dai tre ricercatori era del tipo:

$$Y^x \pmod{p}$$

con p numero primo e $Y < p$.

Per capire come questo metodo consenta a mittente e destinatario di stabilire una chiave segreta senza incontrarsi faremo ricorso a tre persone immaginarie che chiameremo Alice (mittente), Bob (destinatario) e Eva (una terza persona che vuole spiare le conversazioni tra Alice e Bob).

Il metodo prevede che Alice e Bob concordino una chiave costituita dai numeri Y e p : l'aspetto affascinante del metodo è che Alice e Bob possono stabilire tali numeri "alla luce del sole", senza cioè preoccuparsi di tenerli segreti (per esempio ad Eva).

Supponiamo che Alice e Bob abbiano deciso di utilizzare: $Y = 13$ $p = 23$ e vediamo con uno schema come possono procedere per stabilire SENZA INCONTRARSI una chiave che rimarrà nota solo a loro due.

| | ALICE | BOB |
|------------------|--|---|
| <i>Passo 1</i> | Sceglie un numero, supponiamo: 8 e lo tiene <u>segreto</u> Chiameremo questo numero A | Sceglie un numero, supponiamo: 5 e lo tiene <u>segreto</u> Chiameremo questo numero B |
| <i>Passo 2</i> | Calcola: $Y^A \pmod{p}$ $13^8 \pmod{23} = 815730721 \pmod{23} = 2$ Chiameremo questo numero α | Calcola: $Y^B \pmod{p}$ $13^5 \pmod{23} = 371293 \pmod{23} = 4$ Chiameremo questo numero β |
| <i>Passo 3</i> | Alice comunica a Bob il valore di α | Bob comunica ad Alice il valore di β |
| | Lo scambio di queste informazioni può avvenire tranquillamente in chiaro, in quanto un'eventuale intercettazione da parte di Eva non potrebbe comunque consentirle di risalire alla decifratura dei messaggi. Questo perché α e β NON sono la chiave, e quindi è irrilevante che Eva ne venga a conoscenza. | |
| <i>Passo 4</i> | Calcola: $\beta^A \pmod{p}$ $4^8 \pmod{23} = 65536 \pmod{23} = 9$ | Calcola: $\alpha^B \pmod{p}$ $2^5 \pmod{23} = 32 \pmod{23} = 9$ |
| <i>La Chiave</i> | Alice e Bob hanno ottenuto lo stesso numero che rappresenterà la chiave dei loro messaggi. | |



In base a questo schema abbiamo dunque dimostrato che Alice e Bob possono concordare una chiave senza bisogno di incontrarsi e senza il timore che la chiave stessa sia intercettata da terzi: abbiamo quindi risolto il problema della distribuzione delle chiavi!

Per convincercene ulteriormente, vediamo perché ad Eva sia impossibile risalire al valore della chiave.

Poiché tutte le comunicazioni dello schema precedente tra Alice e Bob sono in chiaro, Eva potrebbe aver intercettato le seguenti informazioni:

- le comunicazioni relative alla scelta di Y e p , e quindi sapere che la funzione è del tipo:
 $13^x \pmod{23}$;
- le comunicazioni del passo 3, e quindi i valori di α e β .

Per trovare la chiave, Eva dovrebbe quindi procedere come Alice ed effettuare l'operazione $\beta^A \pmod{p}$, oppure come Bob ed effettuare l'operazione $\alpha^B \pmod{p}$. Ma Eva non conosce i valori di A o di B ! D'altronde, tentare di ricavarli invertendo la funzione non sarebbe un compito semplice, in quanto si tratta di una funzione unidirezionale.

La dimostrazione pubblica della loro scoperta fu data da Diffie, Hellman e Merkle nel giugno del 1976 alla National Computer Conference.

L'introduzione di un metodo che consente a mittente e destinatario di scambiarsi la chiave in modo "sicuro" ha costituito una vera e propria rivoluzione nel campo della crittografia; l'univo aspetto negativo del sistema Diffie - Hellman - Merkle risiede nell'introdurre una non contemporaneità tra le azioni di destinatario e mittente. Infatti, per applicare il suo "lucchetto" Bob deve attendere di ricevere il messaggio di Alice (supponiamo tramite mail), e la stessa Alice, per rimuovere il suo "lucchetto" deve attendere la risposta di Bob, e così via. Questo aspetto, che per persone che vivono in luoghi con fusi orari differenti può comportare un "ritardo" anche notevole nello scambio delle mail, rappresenta chiaramente un elemento che va contro la natura stessa della posta elettronica, che rappresenta uno dei modi più veloci di scambio delle informazioni.

Nel prossimo paragrafo vedremo come questo aspetto sia stato risolto dall'introduzione della crittografia a chiave pubblica.

8.2 RSA

Il passo avanti rispetto al metodo di scambio delle chiavi secondo Diffie-Hellman-Merkle avvenne grazie allo sforzo congiunto di tre ricercatori: Ronald Rivest, Adi Shamir e Leonard Adleman, dalle cui iniziali deriva il metodo noto come RSA.

Il pregio di questo sistema rispetto al metodo Diffie-Hellman-Merkle è che non richiede uno scambio di informazioni tra Alice e Bob per la costruzione della chiave: questo sistema fa infatti uso di due chiavi, una detta "chiave pubblica" e una chiamata "chiave privata" e utilizza un metodo di cifratura asimmetrico.

In un sistema a chiave asimmetrica la chiave usata per cifrare e quella usata per decifrare non coincidono: è possibile quindi che Alice renda pubblica la chiave da usare per cifrare un messaggio (la sua chiave pubblica) e conservi segreta la chiave da usare per decifrare il messaggio (la sua chiave privata), per essere in grado solo lei di decifrare i messaggi a lei diretti.

Il cuore della cifratura asimmetrica sviluppata da Rivest, Shamir e Adleman è una funzione unidirezionale basata sul concetto di modulo.

Il funzionamento del metodo RSA si può schematizzare con i seguenti punti:

- si scelgono due numeri primi, p e q ;
- si calcola il loro prodotto $N = p \cdot q$, chiamato *modulo* (dato che tutta l'aritmetica seguente è *modulo* N)
- si sceglie poi un numero e (chiamato *esponente pubblico*), più piccolo di N e primo rispetto a $\phi(N) = (p-1) \cdot (q-1)$, dove ϕ è la funzione di Eulero;
- si calcola il numero d (chiamato *esponente privato*) tale che $e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$

La chiave pubblica è rappresentata dalla coppia di numeri (N, e) , mentre la chiave privata è rappresentata da (N, d) .

Un messaggio m viene cifrato attraverso l'operazione $m^e \pmod{N}$, mentre il messaggio c così ottenuto viene decifrato con $c^d = m^{e \cdot d} = m^1 \pmod{N}$. Il procedimento funziona solo se la chiave e utilizzata per cifrare e la chiave d utilizzata per decifrare sono legate tra loro dalla relazione $e \cdot d \equiv 1 \pmod{N}$, e quindi quando un messaggio viene cifrato con una delle due chiavi (la chiave pubblica) può essere decifrato solo utilizzando l'altra (la chiave privata).

Vediamo in pratica come sia possibile realizzare una cifratura RSA.

Per cifrare un messaggio, questo deve essere prima di tutto trasformato in un numero o in una serie di numeri, diciamo m_1, m_2, \dots, m_k . Questa operazione può essere effettuata utilizzando, ad esempio, il codice ASCII, e trasformando il numero binario ottenuto nel corrispondente in base dieci. Per semplicità, nel prossimo esempio considereremo che il messaggio segreto che si vuole trasmettere consista di un solo numero m , senza preoccuparci del metodo utilizzato per generarlo.

Faremo inoltre nuovamente riferimento ai nostri personaggi immaginari, Alice e Bob.

Operazioni effettuate da Alice (Generazione delle Chiavi):

- 1) sceglie due numeri primi
- p
- e
- q
- :

$$p = 47 \quad q = 71$$

- 2) calcola
- $N = p \cdot q$
- :

$$N = 47 \cdot 71 = 3337$$

- 3) calcola
- $\phi(N) = (p-1) \cdot (q-1)$
- :

$$\phi(3337) = (47-1) \cdot (71-1) = 3220$$

- 4) sceglie
- e
- tale che:
- $e < N$
- e
- $MCD(e, \phi(N)) = 1$
- :

$$e = 79$$

- 5) calcola
- d
- tale che:
- $e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$

$$d = 79^{-1} \pmod{3220} = 1019$$

- 6) la chiave pubblica è:

$$(e, N) = (79, 3337)$$

- 7) la chiave privata è:

$$(d, N) = (1019, 3337)$$

Adesso Alice è libera di pubblicare la sua chiave pubblica su Internet, o su un qualsiasi altro elenco disponibile a chiunque voglia scriverle messaggi cifrati.

Supponiamo allora che Bob le voglia mandare un messaggio costituito da $m = 688$, e vediamo quale operazioni deve eseguire.

Operazioni effettuate da Bob (Cifratura):

- 1) calcola
- $c = m^e \pmod{N}$
- :

$$c = 688^{79} \pmod{3337} = 1570$$

- 2)
- c
- rappresenta il messaggio cifrato che può essere letto (decifrato) solo da chi è in possesso della chiave privata e quindi solo da Alice. Bob può quindi spedire in tutta tranquillità
- c
- senza preoccuparsi del fatto che Eva possa intercettarlo, poiché anche in quell'eventualità non sarebbe in grado di volgerlo in chiaro.

Operazioni effettuate da Alice (Decifratura):

- 1) ricevuto il messaggio Alice ricava
- m
- mediante la formula
- $m = c^d \pmod{N}$
- :

$$m = 1570^{1019} \pmod{3337} = 688$$

L'unico modo per Eva di decifrare il messaggio è di avere d e quindi di riuscire a ottenere p e q dalla fattorizzazione di N : come detto precedentemente, il processo di fattorizzazione di un numero nei suoi fattori primi è un processo molto lungo, specialmente se si ha a che fare con numeri molto grandi.

La segretezza nella comunicazioni tra Alice e Bob è quindi assicurata!



Esempio

Si scelgono due numeri primi $p=7, q=17$

si calcola $n = p \cdot q = 7 \cdot 17 = 119$

si calcola $\phi(n) = (p-1) \cdot (q-1) = 6 \cdot 16 = 96$

si sceglie $e < \phi(n)$, relativamente primo con $\phi(n)$, $e = 5$

si determina d tale che $d \cdot e \pmod{96} = 1$ e $d < 96$, $d = 77$ (infatti $77 \cdot 5 = 385 = 96 \cdot 4 + 1$)

All'indirizzo:

<http://www.math.mtu.edu/mathlab/COURSES/holt/dnt/phi4.html>

è possibile vedere in azione un programma per la codifica con RSA su una frase inserita dagli autori.

8.2.1 Curiosità e considerazioni

Samuel Wagstaff, docente di informatica all'Università dell'Indiana, è riuscito a fattorizzare un numero di 167 cifre in centomila ore di tempo computer. Il numero della prova era:

163790195580536623921741301546704495839239656848327040249837817092

396946863513212041565096492260805419718247075557971445689690738777

72973038883717449030628887379284041

Questa notizia dovrebbe far riflettere: considerando che ad oggi si scoprono ancora nuovi algoritmi matematici per decrittare sempre più velocemente e che la potenza dei calcolatori aumenta vertiginosamente di mese in mese (e non parliamo dei computers dei laboratori segreti!), sarà una buona scelta affidare dati importantissimi ad un metodo che si basa esclusivamente sulla lentezza dei calcolatori attuali?

Bisogna anche notare che una chiave da 1024 bit in un sistema a chiave pubblica, vale circa quanto una a 64 bit di un sistema a chiave simmetrica a causa del fatto che nel sistema a chiave pubblica esiste sempre un legame tra chiave privata e segreta che permette di ridurre le combinazioni necessarie per trovare il codice di accesso.

Stabilita tale corrispondenza di sicurezza tra le lunghezze delle chiavi dei due sistemi, è interessante notare quando detto alla conferenza Crypto '93 (notare che sono già passati diversi anni), da M. Wiener del Bell Northern Research, il quale ha descritto come con un milione di dollari sia realizzabile un chip speciale da 50 milioni di test al secondo che, in parallelo ad altri 57.000, può condurre un attacco con successo mediamente in 3,5 ore. Con un costo di 10 milioni di dollari il tempo si abbassa a 21 minuti, e con 100 milioni a disposizione, il codice è infranto in pochi secondi!



Fatto sta che il commercio elettronico ha già iniziato a farne uso e alcuni anni fa, il 5 Agosto 1997, il Consiglio dei Ministri Italiano ha approvato il regolamento di attuazione dell'art.15 della legge 57/97, nota anche come legge Bassanini-1, con il quale si stabilisce che l'originale di un documento può essere anche quello depositato su di un *file*. Tale documento su file ha valore probante sia sul contenuto sia sulla provenienza se corredato da firma elettronica legalmente riconosciuta.

8.2.2 Numeri primi e RSA

Da quanto esposto nei precedenti paragrafi risulta chiaro che la conoscenza di numeri primi molto "grandi" permette di effettuare cifrature RSA sempre più potenti. La ricerca di tali numeri costituisce quindi, da un po' di anni a questa parte, un vero e proprio business, e molte aziende hanno come solo scopo quello di trovarne di sempre più grandi. Nella tabella seguente sono riportati alcuni dei numeri scoperti negli ultimi anni.

| Record di primi certificati | |
|--------------------------------|-------------------------------------|
| $2^{20996011} - 1,$ | 6320430 cifre (scoperto nel 2003) |
| $2^{13466917} - 1,$ | 4053946 digits (discovered in 2001) |
| $2^{6972593} - 1,$ | 2098960 cifre (scoperto nel 1999) |
| $5359 \times 2^{5054502} + 1,$ | 1521561 cifre (scoperto nel 2003) |
| $2^{3021377} - 1,$ | 909526 cifre (scoperto nel 1998) |
| $2^{2976221} - 1,$ | 895932 cifre (scoperto nel 1997) |
| $1372930^{131072} + 1,$ | 804474 cifre (scoperto nel 2003) |
| $1176694^{131072} + 1,$ | 795695 cifre (scoperto nel 2003) |

Da molti anni accade che il più grande numero primo noto sia un primo di Mersenne. Chi volesse capovolgere la situazione, e trovare un numero primo "generico" più grande dovrà ancora una volta alzare il tiro (e di parecchio).

Il 42-esimo primo di Mersenne¹ ha "appena" 7.816.230 cifre, e sembra piccolo posto accanto al nuovo arrivato.

¹ I numeri della forma $2^n - 1$ sono detti numeri di Mersenne e sono indicati con M_n . In generale questi numeri non sono primi, nemmeno se n è primo (per esempio $M_{11}=2047=89 \cdot 23$); non si sa nemmeno se di numeri di Mersenne primi ce ne siano un numero finito o se siano infiniti.



Il più recente primo di Mersenne (il 43-esimo) è stato scoperto il 15 Dicembre 2005 da Curtis Cooper e Steven Boone :

$$2^{30402457} - 1$$

Esso rappresenta il più grande numero primo noto, con ben 9.152.052 cifre! Siamo a un passo dalla soglia dei 10 milioni di cifre, per la quale la Electronic Frontier Foundation offre 100.000 dollari.

Il premio precedente - di 50.000 dollari - è stato assegnato nel 2000 a Nayan Hajratwala il quale, partecipando alla GIMPS (Great Internet Mersenne Prime Search), trovò nel 1999 il 38-esimo primo di Mersenne (2.098.960 cifre).

8.2.3 [Attacchi](#)

Nel 1977, subito dopo il lancio del sistema di crittografia RSA, Martin Gardner pubblicò su *Scientific American* un piccolo messaggio cifrato, basato su una chiave costituita da un numero N di 129 cifre, prodotto di due numeri primi molto grandi. Il messaggio e la chiave erano stati forniti da ricercatori del MIT, che offrivano un premio in denaro a chi avesse decrittato il messaggio. A quei tempi si stimò che ci sarebbero voluti all'incirca ventimila anni per scomporre in fattori primi quel numero, con i più veloci calcolatori disponibili. Dopo di allora però ci furono importanti novità, più che sul lato della velocità dei computer, sui metodi per fattorizzare grandi numeri. Inoltre la massiccia diffusione di Internet costituì una variabile imprevista: sotto la guida di alcuni ricercatori, un esercito di 600 volontari di 20 paesi si mise all'opera e dopo non molti mesi di lavoro, nell'Aprile del 1994, la fattorizzazione fu scoperta: si trattava di due numeri, uno di 64 e uno di 65 cifre. Erano passati solo (!) 17 anni dalla pubblicazione della chiave pubblica. Solo per curiosità riportiamo qui i valori dei numeri coinvolti (i volonterosi possono provare ad eseguire il prodotto richiesto, per controllare che non ci siano errori):

$$\begin{aligned} p &= 3490529510847650949147849619903898133417764638493387843990820577 \\ q &= 32769132993266709549961988190834461413177642967992942539798288533 \\ N &= 11438162575788886766923577997614661201021829672124236256256184293570693524 \\ &\quad 5733897830597123563958705058989075147599290026879543541 \end{aligned}$$

Attualmente chiavi di 1024 bit sono considerate sufficientemente sicure.

Tempo medio di attacco:

| lunghezza chiave | tempo richiesto | tempo richiesto |
|------------------|----------------------------------|---------------------|
| (bit) | a 1 decr/ms | a 10^6 decr/ms |
| 56 | 2^{55} ms = 1142 anni | 10 ore |
| 128 | 2^{127} ms $\sim 10^{24}$ anni | $\sim 10^{18}$ anni |
| 168 | 2^{167} ms $\sim 10^{36}$ anni | $\sim 10^{30}$ anni |



8.2.4 La fattorizzazione

Discutiamo solo il problema inverso della fattorizzazione. A prima vista, sapendo che si usano numeri primi vicini a 2^{128} , si potrebbe pensare di costruirsi una tabella dei numeri che sono prodotto di due tali primi. Ma quanti sono?

In base al risultato ottenuto da Hadamard sappiamo che:

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \log(n)} = 1$$

dove $\pi(n)$ rappresenta il numero di primi minori o uguali a n

Dunque possiamo rozzamente valutare $\pi(2^{128})$ come:

$$\frac{2^{128}}{\log(2^{128})} \cong 3 \cdot 10^{36}$$

e $\pi(2^{127})$ come:

$$\frac{2^{127}}{\log(2^{127})} \cong 2 \cdot 10^{36}$$

e quindi $\pi(2^{128}) - \pi(2^{127}) \cong 10^{36}$. Stiamo cauti nella stima e diciamo che ne abbiamo almeno 10^{30} (in realtà potremmo anche dire con sicurezza 10^{35}). I prodotti di due numeri di questa forma sono allora dell'ordine di 10^{60} . Immagazzinarli in forma binaria richiede allora $2^{256} \cdot 10^{60} \cong 2^{256} \cdot 2^{199} = 2^{455}$ bit, quindi $2^{452} \cong 10^{136}$ byte. Un terabyte è circa 10^{12} byte, quindi servirebbe qualcosa come 10^{124} terabyte. Troppi anche solo da immaginare: il diametro della Galassia in metri è 10^{21} .

Più sensato è pensare di fattorizzare N , ma l'unico modo conosciuto è di dividerlo successivamente per 2, 3, e così via. E' probabile che, nel momento in cui si è ottenuta la fattorizzazione richiesta, la chiave pubblica sia cambiata da parecchi mesi, si faccia un conto approssimativo del tempo richiesto.

In matematica, RSA-2048 è il più grande dei numeri RSA (semiprimi² grandi che fanno parte del RSA Factoring Challenge), e ad esso è associato il premio più grande per la sua fattorizzazione: 200000 dollari.

RSA-2048 è un numero con 617 cifre decimali (2048 bits)!

² Un numero è detto semiprimo (anche detto biprimo o 2-quasi primo, o pq numero) è un numero naturale che è il prodotto di numeri primi (non necessariamente distinti). I primi numeri semiprimi sono: 4, 6, 9, 10, 14, 15, 21, 22, 25, 26, 33, 34, 35, 38, 39, 46, 49, 51, 55, 57, 58, 62, 65, 69, 74, 77, 82, 85, 86, 87, 91, 93, 94, 95, 106, 111, 115, 118, 119, 121, 122, 123, 129, 133, 134, 141, 142, 143, 145, 146, 155, 158, 159, 161, 166, 169, 177, 178, 183, 185, 187.



RSA-2048 =

251959084756578934940271832400483985714292821262040320277771378360436
 620207075955562640185258807844069182906412495150821892985591491761845
 028084891200728449926873928072877767359714183472702618963750149718246
 911650776133798590957000973304597488084284017974291006424586918171951
 187461215151726546322822168699875491824224336372590851418654620435767
 984233871847744479207399342365848238242811981638150106748104516603773
 060562016196762561338441436038339044149526344321901146575444541784240
 209246165157233507787077498171257724679629263863563732899121548314381
 67899885040445364023527381951378636564391212010397122822120720357

Il più grande numero RSA mai fattorizzato è composto da 200 cifre decimali (663 bits); probabilmente non si raggiungerà la fattorizzazione di RSA-2048 prima di alcuni decenni. RSA labs ritiene infatti che i computer e le memorie necessarie per fattorizzare un numero RSA siano:

| ନଫାଲ୍ | କମ୍ପ୍ୟୁଟର | ମେମୋରୀ |
|----------|---------------------|--------|
| RSA-760 | 215000 | 4 Gb |
| RSA-1024 | 342000000 | 170 Gb |
| RSA-1620 | $1.6 \cdot 10^{15}$ | 120 Tb |



9. Riferimenti Bibliografici

Testi

Simon Singh, "Codici e Segreti - La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet". BUR Saggi, Aprile 2005.

Frederick W. Winterbotham, "Ultra Secret - La macchina che decifrava i messaggi segreti dell'Asse". Mursia, 1976.

Alessandro Languasco, Alessandro Zaccagnini, "Introduzione alla Crittografia". HOEPLI Informatica, Milano, 2004.

Siti Internet

www.dia.unisa.it

www.tonymcrypt.com

www.turing.org.uk/turing

www.math.arizona.edu/~dsl/enigma.htm


www.riksoft.com/indexok.asp?Goto=critlogia.htm

www.codesandciphers.org.uk

www.icosaedro.it/crittografia/chiavi-simmetriche.html

www.matematicamente.it/storia/crittografia.htm

<http://alpha01.dm.unito.it/personalpages/cerruti/>

 *Quando numeri e figure non saranno più la chiave di tutte le creature, quando quelli che cantano o baciano sapranno più dei profondi eruditi, quando il mondo tornerà ad essere vita libera il vero mondo, quando poi luce e ombra si ricongiungeranno in un genuino chiarore, e quando in fiabe e poesie si riconosceranno le storie eterne del mondo, allora di fronte ad un'unica parola magica si dileguerà tutta la falsità”.*

Novalis, “*Enrico di Ofterdingen*”

ERRATA CORRIGE

- Pag. 11 Aggiunte le righe 28 e 29.
- Pag. 12 Modificata la matrice del Caso 1.
- Pag. 12 Modificata la matrice del Caso 3.
- Pag. 14 Riga 24 - subito dopo "cominciando da", corretto "destra" con "sinistra".
- Pag. 26 Nell'identità di Bézout, corretto $d \cdot y$ con $b \cdot y$.