

# Indice

1	Introduzione			2	
2	Crittografia classica				
	2.1	Cifrar	i simmetrici	4	
		2.1.1	Cifrari di shift	4	
		2.1.2	Cifrario affine	5	
		2.1.3	Cifrario Alberti	5	
		2.1.4	Cifrario Porta	6	
		2.1.5	Cifrario di Playfair	6	
		2.1.6	Cifrario di Hill	7	
		2.1.7	Cifrario di Vigenère	8	
		2.1.8	Cifrario di Vernam	8	

# Capitolo 1

# Introduzione

La crittografia fa parte, insieme alla crittoanalisi, della crittologia.

La crittografia è la scienza che studia tecniche e metodologie per cifrare un testo in chiaro, al fine di produrre un testo cifrato comprensibile solo ad un ricevente legittimo, il quale possiede l'informazione sufficiente (detta chiave) per decifrarlo, recuperando il testo in chiaro.

La **crittoanalisi** studia come decrittare un testo cifrato per ottenere il testo in chiaro: il verbo decrittare indica l'azione compiuta da un'entità che non possiede la chiave per recuperare, in modo legittimo, il testo in chiaro. In letteratura, suddetta entità viene indicata con il termine ascoltatore, oppure avversario o anche nemico. Lo scopo della crittografia è di produrre un messaggio cifrato m in modo che nessun avversario sia in grado di decrittarne il contenuto.

La **stegonografia** (dal greco *scrivere nascosto*), indica l'insieme delle tecniche che permettono a due (o più) entità in modo tale da occultare, agli occhi di un ascoltatore, non tanto il contenuto (come nel caso della crittografia), ma l'estistenza stessa di una comunicazione. In altre parole, è l'arte di nascondere un messaggio all'interno di un altro *messaggio contenitore*. Alcuni esempi sono:

- disposizione dei caratteri
- inchiostro invisibile
- contrassegno dei caratteri
- nascondere messaggi all'interno di bit di file multimediali
- . . .

### Proprietà di sicurezza di un messaggio

- 1. Confidenzialità
- 2. Autenticazione
- 3. Non ripudio

- 4. Integrità
- 5. **Anonimia** (canali in cui le entità comunicanti devono poter nascondere la loro identità)

# Capitolo 2

# Crittografia classica

## 2.1 Cifrari simmetrici

Con crittografia simmetrica, o crittografia a chiave privata, si intende una tecnica di cifratura che consiste nel cifrare un testo in chiaro dove la chiave di crittazione è la stessa chiave di decrittazione. Non è previsto uno scambio di chiavi, dunque le due parti devono esserne già in possesso.

Possiamo dividere i cifrari simmetrici in due categorie:

- Cifrari a flusso: trasformano pochi bit alla volta (un singolo bit, o un byte); si rivelano adatti quando si deve proteggere singoli dati generati uno dopo l'altro. Al flusso di dati in input in input corrisponde un flusso di chiavi
- Cifrari a blocchi: trasformano blocchi di più bit (64, 128, o più); si rivelano adatti quando si devono proteggere intere strutture dati

Si può fare una distinzione tra due tecniche per la cifratura del testo in chiaro:

- Sostituzione: i valori in chiaro vengono sostituiti con altri simboli
- Trasposizione: vengono scambiate le posizioni dei valori in chiaro

Queste tecniche possono essere combinate tra loro, a patto che siano reversibili.

## 2.1.1 Cifrari di shift

Sono una generalizzazione del  $cifrario\ di\ Cesare$ , senza fissare a 3 lo spostamento delle lettere.

Con questo approccio, lo schema di cifratura deve avere uno spazio delle chiavi non vulnerabile ad un attacco di *forza bruta*; tuttavia, questa è una condizione necessaria ma non sufficiente!

Anziché semplicemente shiftare le lettere, si potrebbe effettuare una permutazione casuale delle lettere dell'alfabeto; la chiave, diventa dunque una stringa di 26 lettere.

## Plain: abcdefghijklmnopqrstuvwxyz

Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN ← chiave

Con un alfabeto di 26 lettere, ci sono 26! possibili chiavi.

Potremmo aver pensato di aver ottenuto un adeguato livello di sicurezza, ma le caratteristiche del linguaggio naturale rendono possibili attacchi alternativi, come ad esempio la frequenza dei caratteri (che non cambia tra testo in chiaro e cifrato).

Alcune contromisure sono:

- usare più simboli per cifrare i caratteri più frequenti, in modo da abbassare la frequenza
- aggiungere simboli meno frequenti nel testo in chiaro, in modo da non compromettere il significato
- usare parole in codice oltre ai simboli dell'alfabeto

### 2.1.2 Cifrario affine

Sono un caso particolare di cifrario a sostituzione monoalfabetico. Per trovare la sostituzione si usa un'espressione, detta **affine**:

$$c_i = E(p_i) = (k_1p_i + k_2)mod26$$

 $\rightarrow$  la chiave è quindi data da **due costanti**.

La decrittazione avviene invece secondo la formula:

$$p_i = D(c_i) = (c_i - k_2) \cdot k_1^{-1}$$

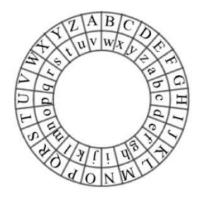
 $\operatorname{con} k_1^{-1}$ inteso come l'inverso modulo 26 di  $k_1,$ ovvero quel numero x che soddisfa l'equazione:

$$(k_1 \cdot x) mod 26 = 1$$

Affinché questo sia possibile è necessario che  $k_1$  e 26 siano primi tra loro.

## 2.1.3 Cifrario Alberti

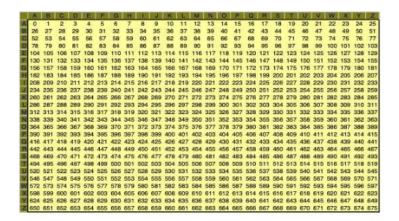
Fu il primo meccanismo che usò più alfabeti cifranti che si sostituiscono durante la cifratura. Utilizza un apparecchio composto da due dischi concentrici, rotanti in maniera indipendente, contenenti un alfabeto ordinato per il testo in chiaro, ed uno disordinato per il testo cifrato.



Si sceglie una lettera come chiave, la si fa corrispondere alla A del disco esterno, e per ogni lettera cifrata si muove in senso orario il disco interno.

## 2.1.4 Cifrario Porta

È un cifrario che si occupa di cifrare i **digrammi**, ovvero coppie di lettere. Ad ogni digramma viene assegnato un numero; la chiave è data da una permutazione arbitraria di numeri del cifrato e lettere su righe e colonne.



## 2.1.5 Cifrario di Playfair

È una tecnica di cifratura simmetrica manuale basata su un **cifrario monoal-fabetico a due lettere** (vengono cifrate due lettere alla volta). L'analisi delle frequenze può ancora essere intrapresa, ma invece che 26 monografi esistono 600 possibili digrafi! È dunque molto più difficile.

Il cifrario Playfair si basa sull'uso di una matrice  $5 \times 5$  contenente una parola chiave; la tabella viene costruita inserendo le lettere della parola chiave senza lettere duplicate, per poi riempire gli spazi rimanenti con le lettere non utilizzate dell'alfabeto (in ordine).

Essendo disponibili 25 spazi, una lettera viene esclusa (di norma la Q o la W, oppure facendo collassare la I e la J nello stesso spazio). La chiave può essere scritta nelle celle della tabella seguendo una *logica arbitraria*: la chiave è dunque **l'ordine di riempimento** della parola chiave nella tabella, oltre che la parola stessa.

La cifratura avviene separando le lettere del testo in chiaro in digrafi ed applicando a ciasuno di essi quattro regole:

- 1. se entrambe le lettere sono uguali, si aggiunge una X (o una lettera poco comune) tra di loro e poi si ripete il procedimento
- 2. se le lettere appaiono nella stessa riga, vengono codificate con quelle alla propria destra
- 3. se le lettere appaiono nella stessa colonna, vengono codificate con quelle immediatamente sotto
- 4. altrimenti, si identifica un rettangolo che ha le due lettere come vertici opposti; le lettere vengono codificate con quella sulla stessa riga in corrispondenza dell'altra colonna

Per decifrare, si usano regole inverse a queste.

### 2.1.6 Cifrario di Hill

Un cifrario a **sostituzione polialfabetica** basato sull'algebra lineare.

- In *primis*, viene fatto corrispondere ad ogni lettera un numero  $(A=0,B=1,\dots)$
- $\bullet\,$  Viene fissato un blocco di n lettere, considerate come uno spazio vettoriale di dimensione n
- Il vettore ottenuto viene moltiplicato per una matrice M di dimensione  $n \times n$  in modulo 26
- ullet Segue che m lettere in chiaro vengono sostituite con altrettante lettere cifrate secondo m equazioni lineari

La chiave è data dalla matrice M; deve essere casuale a patto che sia invertibile in  $\mathbb{Z}_2$ 6 affinché la decrittazione sia possibile.

Ad esempio, il messaggio TUO verrebbe cifrato con la chiave YYPRZWIZJ come:

$$\begin{pmatrix} 24 & 24 & 15 \\ 17 & 25 & 22 \\ 08 & 25 & 09 \end{pmatrix} \times \begin{pmatrix} 19 \\ 20 \\ 14 \end{pmatrix} = \begin{pmatrix} 1146 \\ 1131 \\ 778 \end{pmatrix} (mod 26) \equiv \begin{pmatrix} 02 \\ 13 \\ 24 \end{pmatrix}$$

## 2.1.7 Cifrario di Vigenère

È un il più semplice tra i cifrari **polialfabetici**, è considerabile come una **generalizzazione del cifrario di Cesare**: invece di spostare sempre dello stesso numero di posti la lettera da cifrare, essa viene spostata di un numero di posti variabile, ma ripetuto, determinato attraverso una **parola chiave**.

Rispetto ai cifrari monoalfabetici, si ha il vantaggio di avere n alfabeti cifranti (n lunghezza della chiave). La debolezza consiste che si tratta di n cifrari di Cesare, motivo per cui è possibile, a partire dalle ripetizioni, stimare la lunghezza della chiave per poi analizzare le frequenze in ognuno degli alfabeti cifranti.

## 2.1.8 Cifrario di Vernam

È un cifrario di Vigenère a cui viene imposto che la chiave abbia la stessa lunghezza del messaggio da cifrare.

Questo metodo è potenzialmente *unconditionally secure* (ossia sicuro indipendentemente dal tempo e risorse), ma ha il problema di necessitare di una chiave casuale (già di per sé difficile siccome le chiavi sono pseudo-casuali) ed eventualmente di grandi dimensioni.