Crittologia Classica

Return

Indice

Introduzione

Si possono utilizzare **codici** o **cifrari** per proteggere le informazioni. I codici associano ad ogni simbolo di partenza un altro simbolo. I cifrari operano su un testo mediante l'utilizzo di chiavi.

Cifrari Classici

Sostituzione monoalfabetica

Si effettua una sola operazione di sostituzione fra i simboli di un alfabeto di partenza e uno di arrivo tramite una chiave. Nel caso del cidrario di cesare la chiave è un numero che indica lo spostamento di ogni lettera dell'alfabeto. Ad esempio, con chiave 3:

```
A -> D
B -> E
...
```

Dato un alfabeto di n simboli il numero di trasformazioni possibili è $n!$ quindi debole.

Se il linguaggio di partenza è noto, si può utilizzare un attacco statistico basato sulla frequenza delle lettere del linguaggio.

Ci sono diversi accorgimenti per rendere più difficile l'attacco:

- si eliminano spazi e punteggiatura
- si introducono caratteri non significativi (nulle)
- si impiega un alfabeto più ampio nel testo cifrato
- si sostituiscono più simboli con uno solo (ad esempio "TH" -> "X")

Oggi viene applicate a blocchi di minimo 8 caratteri (a cui corrispondono, considerando ASCII, 64bit). Questo previene l'attacco statistico in quando è impossibile analizzare 2^64 dati.

Sostituzione di diagrammi: Cifrario di Playfair

Il **cifrario di Playfair** si basa sull'uso di una matrice 5x5 contenente una parola eliminando le duplicate e riempiendo gli spazi vuoti con le lettere rimanenti dell'alfabeto (J == I). Ad esempio, con la parola chiave "CIFRARIO":

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

Per cifrare una frase si dividono le lettere in coppie. Se una lettera è ripetuta, si inserisce una "X" tra le due lettere. Se la coppia è formata da due lettere della stessa riga, si sostituiscono con le lettere a destra. Se sono nella stessa colonna, si sostituiscono con le lettere sotto. Altrimenti, si formano un rettangolo e si sostituiscono con le lettere agli angoli opposti.

Ad esempio, per cifrare "Ciao mamma guarda come mi diverto" si ottiene:

```
ci ao ma mm ag ua rd ac om em id iv er to

IFCGNRLYLYGNZGFECHMTFBCWMAPE
```

Per decifrare, si applica la stessa regola ma in senso inverso.

Trasposizione di colonne

La **trasposizione di colonne** è un cifrario che non modifica i simboli ma la loro posizione. Si scrive il testo in righe paddando con X e si leggono le colonne in un certo ordine. Ad esempio, con la chiave "31425":

```
1 2 3 4 5
C I A O M
M A M A G
U A R D A
C O M E M
I A M C O
D I V E R
T O X X X
```

Si ottiene:

```
AMRMMV CMUCIDT OADECE IAAOAIO MGAMOR
```

Sostituzione polialfabetica: Cifrario di Vigenère

L'obiettivo della sostituzione polialfabetica è quello di rendere quiprobabile l'occorrenza di ogni lettera. Si utilizza una matrice 26x26 in cui ogni riga è una rotazione dell'alfabeto.

```
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
...
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
```

Per cifrare, si sceglie una chiave "CIFRARIO", il testo da cifrare "CIAO MAMMA", si prende la righa della tabella che inizia con la prima lettera della chiave e la colonna della tabella che inizia con la prima lettera del testo e si ottiene la prima lettera del messaggio cifrato. Si prosegue con la seconda lettera della chiave e del testo e così via.

Per rendere più sicuro il cifrario si utilizzano chiavi lunghe e casuali, in modo da non riuscire a sapere la lunghezza della chiave che renderebbe motlo facile l'attacco statistico, diventano n cifrari di cesare.

Cifrario Vernam One-Time Pad

È un cifrario polialfabetico, dove si trasformano i simboli della chiave e della frase usando la codifica Baudot. Nella tabella si incrociano riga e colonna per ogni simbolo e si ottiene il gruppo di bit corrispondente. In questo algoritmo per aumentare la sicurezza si fa uso di una chiave lunga quanto il testo. La chiave è monouso e casuale rendendo inutile l'attacco statistico.

Questo cifrario non può essere violato con attacchi passivi. Però serve un canale sicuro e disponibile per la chiave, che però vorrebbe dire che si può trasmettere il messaggio sullo stesso canale e non la chiave.

Definizioni di sicurezza

Sicurezza dei cifrari

Un cifrario è detto **perfetto** o **assolutamente sicuro** se dopo avere intercettato un testo cifrato, l'intetezza a posteriori sul testo in chiaro corrisponde a quella a priori. In altre parole, non si riesce a risalire al testo in chiaro. Un cifrario è detto **sicuro** se dato un testo cifrato C, trovare il testo in chiaro è impossibile per chi non conosce la chiave. Un cifrario è detto **computazionalmente sicuro** se calcolare il testo in chiaro da C è possibile ma richiede una potenza di elaborazione tale da non essere realizzabile in tempi ragionevoli.

Confusione e diffusione

Il testo cifrato deve dipendere in modo complesso dalla chiave e dal testo in chiaro. Bisogna creare confusione effettuando sostituzione. Le infomrazioni contenute nel testo in chiaro devono essere diffuse nel testo cifrato in modo che la modifica di un solo simbolo del testo in chiaro modifichi più simboli del testo cifrato. Questo si ottiene con la trasposizione.

Cifrari composti

Shannon ha introdotto il **cifrario composto** che alterna stadi di sostituzione a stadi di permutazione. Effettuando più passaggi si aumenta confusione e diffusione.

Crittologia classica e sicurezza al giorno d'oggi

Oggi l'unico cifrario considerato al di sopra della sicurezza perfetta è il cifrario **one time pad**.