Contents

1 Crittografia Simmetrica **1**
1.0.0.1 Definizione di Cifrario 1
1.0.0.2 Crittoanalisi 2
1.0.0.3 Esempi di cifrari 2

1 Crittografia Simmetrica

Se parliamo di crittografia Simmetrica, stiamo considerando uno schema in cui sono presenti almeno 2 agenti (Bob, Alice) che devono scambiare un messaggio in maniera sicura senza che un terzo (che potrebbe avere intenzioni malevole) possa capire il messaggio. Il modello quindi prevede una funzione di cifrazione (Enc) e una funzione di decifrazione (Dec), una chiave condivisa (k) e due tipi di messaggio, x detto messaggio in chiaro (plaintext) e y detto messaggio cifrato (ciphertext) ; la funzione di criptazione è determinata da un algoritmo che pubblicamente conosciuto, quello che invece rende sicuro l'utilizzo della cifratura simmetrica è la segretezza e lunghezza della chiave.

1.0.0.1 Definizione di Cifrario Un cifrario, o schema di cifratura, è defito su una tripletta composta da (K,P,C) usata nelle funzioni di (Gen,Enc,Dec) definite con questi domini:

$$Gen : Z^+ \rightarrow Kfunzionegeneratricedichiavi \tag{1}$$
$$Enc : P \times K \rightarrow Cfunzionedicifratura \tag{2}$$
$$Dec : C \times K \rightarrow Pfunzionedidecifratura \tag{3}$$
$$x \in P, y \in C, k \in K \tag{4}$$
$$y = Enc(k, x) \tag{5}$$
$$x = Dec(k, y) \tag{6}$$

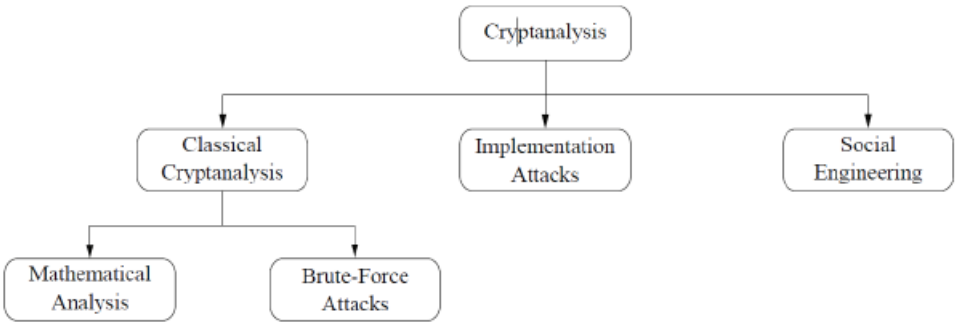
Proprieta di cifratura La cifratura deve anche rispettare le seguenti proprieta:

Correttezza : $\forall p \in P \wedge k \in K, \exists Dec(k, Enc(k, p)) = p$

Sicurezza : Un cifrario simmetrico è sicuro $\iff \forall (p, c), p \in P \wedge c \in C \Rightarrow$

- dato c ciphertext, è "difficile" determinare p plaintext senza conoscere la chiave k, e viceversa
- è "difficile" determinare k chiave, ammenoche non sia stata già usata una volta

Esempio : Sostituzione monoalfabetca Vediamo quindi un tipo di cifratura a sostituzione, dove la chiave è la permutazione dell' alfabeto. L' algoritmo prevede la sostituzione delle lettere della parola con le corrispondenti dell' alfabeto shiftato, e per decriptare si usa l' algoritmo al contrario. Le chiavi quindi possono essere circa 26! cioè circa $4 \cdot 10^26$, quindi tentare un attacco a forza bruta non è possibile, ma è possibile applicare tecniche di Crittoanalisi analizzando alcune proprietà che riguardano i linguaggi come : la frequenza delle lettere, la generalizzazione delle coppie e triple di lettere, la frequenza delle parole corte se sono identificati i separatori.



1.0.0.2 Crittoanalisi

Complessità dell'attacco Viene definito da:

Complessità dei Dati: Numero previsto di unità dei dati in ingresso richiesti.

Complessità di Storage: Numero previsto delle unità di storage richiesti.

Complessità di Elaborazione: Numero previsto di operazioni richiesti per processare i dati in input o/e per riempire la memoria con dati.

Tipi di attacco Si possono classificare in:

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack (CPA)

Se un metodo è sicuro contro i CPA, allora è sicuro anche contro gli altri.

Principi di Kerchoff

Massima di Kerckhoffs Un sistema crittografico dovrebbe rimanere sicuro anche se tutto del sistema, tranne la chiave, è di pubblico dominio.

Massima di Shannon Il nemico conosce il sistema.

Massima di Bruce Schneier Meno e più semplici sono i segreti da custodire per garantire la sicurezza del sistema, più facile sarà mantenerne la sicurezza.

Consigli per mantenera la sicurezza facile

- Le chiavi sono piccoli segreti.
- Conservare piccoli segreti è più facile che conservare grandi segreti.
- Sostituire piccoli segreti, una volta eventualmente compromessi, è più facile (ed economico) che sostituire grandi segreti.

1.0.0.3 Esempi di cifrari

Cifrario di cesare Siano PT, CT e K elementi dell'anello Z_{26}.

- **Cifratura (Encryption):**
$$y = x + k \mod 26$$
- **Decifratura (Decryption):**
$$x = y - k \mod 26$$
- **Esempio:**
  - Testo in chiaro (Plaintext, x): "`ATTACK`" $\Rightarrow$
$$x = (0, 19, 19, 0, 2, 10)$$

- Chiave (k):
$$k = 17$$
- Testo cifrato (Ciphertext, y):
$$y = (0+17, 19+17, 19+17, 0+17, 2+17, 10+17) \mod 26 = (17, 10, 10, 17, 19, 1)$$
- Risultato: "`RKKRTB`"

Cifrario Affine Definizione
Siano $a, b, x, y \in Z_{26}$.

- **Cifratura (Encryption):**
$$y = a \cdot x + b \mod 26$$
- **Decifratura (Decryption):**
$$x = a^{-1} \cdot (y - b) \mod 26$$
- La chiave è $k = (a, b)$, con $\gcd(a, 26) = 1$
- **Esempio:**
  - Testo in chiaro (Plaintext): "`ATTACK`" $\Rightarrow (0, 19, 19, 0, 2, 10)$
  - Chiave $k = (9, 13)$
  - Cifratura:
$$y = (9 \cdot x + 13) \mod 26$$
$$y = (13, 2, 2, 13, 5, 25)$$
  - Testo cifrato (Ciphertext): "`NCCNFZ`"

Calcolo dello spazio delle chiavi
Lo spazio delle chiavi si calcola come:
$$\text{Spazio delle chiavi} = N_a \cdot N_b$$
Dove:

- N_a è il numero di valori possibili di a tali che $\gcd(a, 26) = 1$.
  In questo caso: $N_a = 12$
- N_b è il numero dei possibili valori di shift b in Z_{26}.
  Quindi: $N_b = 26$

Pertanto, lo spazio delle chiavi è:
$$12 \cdot 26 = 312$$