Crittografia simmetrica

INTRODUZIONE

Crittografia

- La **crittografia** si occupa dei metodi per rendere un messaggio non comprensibile a persone non autorizzate a leggerlo.
- Utilizzata dappertutto!

PROPRIETÀ

- **Segretezza**: le informazioni sono leggibili e comprensibili solo da chi ne ha i diritti.
- **Autenticazione**: verificare e accertare l'identità di un utente
- **Integrità**: Le informazioni non sono modificabili da persone non autorizzate.

PROPRIETÀ

Alcuni schemi di cifratura garantiscono solo confidenzialità, altri **confidenzialità**, **integrità** ed **eventualmente** autenticazione.

PRIMA DI CONTINUARE…

CIFRATURA E CODIFICA???

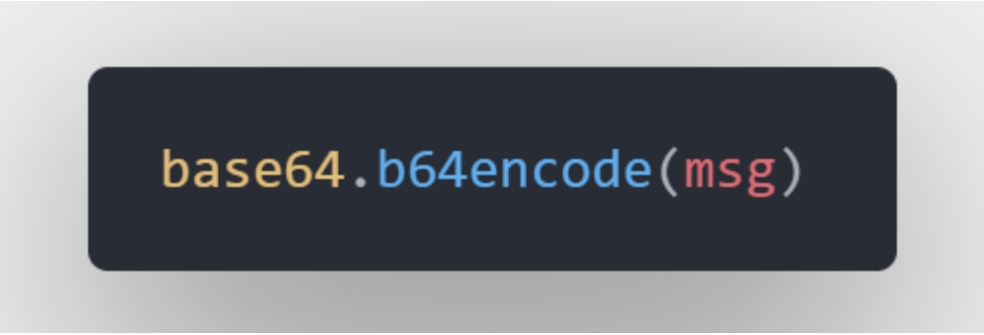
CIFRATURA

Serie di operazioni per rendere un messaggio incomprensibile.
(solo se fatta bene)

CODIFICA

Modo di rappresentare un informazione. (eg. base64, base32, rot13)
NON NASCONDE IL MESSAGGIO

CIFRATURA O CODIFICA?



CIFRATURA O CODIFICA?

```
AES.new(key, AES.MODE_ECB).encrypt(msg)
```

CIFRATURA O CODIFICA?

```
sha256(msg)
```

PRIMA DI CONTINUARE...

Crypto 02, Crypto03, **Base Party**

PRINCIPIO DI KERCKHOFFS

Bisogna assumere che il «**nemico**» riesca a **recuperare l'algoritmo** cifrante: la sicurezza quindi deve stare nella segretezza della chiave, non nella segretezza dell'algoritmo.

NO ALLA SECURITY THROUGH OBSCURITY

Cifrario perfetto

- Cifrario dove la chiave di cifratura è lunga quanto il testo e non è riutilizzabile. Chiamato anche **OTP (One Time Pad,** 'taccuino monouso'
- Non viene utilizzato perché
  - La chiave deve essere in qualche modo trasmessa alla persona interessata in **MODO SICURO!!!**
  - **La chiave deve essere generata in modo completamente causale**

PRIMA DI CONTINUARE...

Crypto 06, Crypto 05, Crypto 06?

Abcon (utilizzare https://dcode.fr/)

ATTENZIONE!

Molti dei cifrari usati oggi sono **sicuri.** Il problema è come vengono usati...

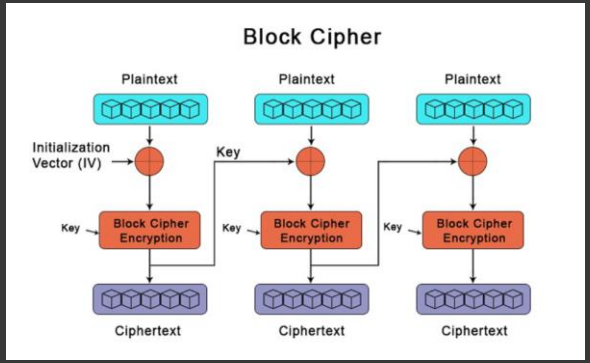
ATTENZIONE!

D'ora in poi si parlerà di **plaintext** e **ciphertext**

- **Plaintext = testo in chiaro**
- **Ciphertext = testo cifrato**

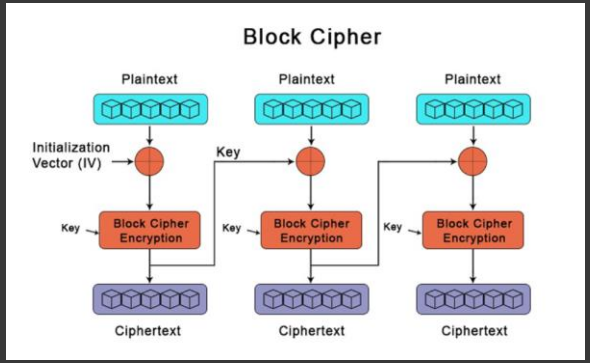
TIPI DI CIFRARI

- I cifrari simmetrici possono essere suddivisi in base al loro tipo di funzionamento:
  - **Stream ciphers:** il plaintext viene cifrato «bit by bit» (eg. RC4, Salsa20)
  - **Block ciphers:** il plaintext viene cifrato n bit per volta (eg. DES, AES, Blowfish)



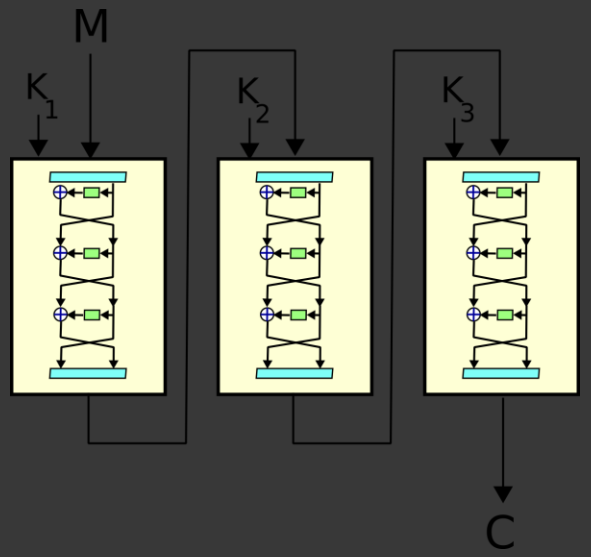
DES

- **DES (Data Encryption Standard)** è stato uno dei primi cifrari a chiave simmetrica
- **Lunghezza chiave:** 56 bit
- È un cifrario a blocchi, dove essi sono lunghi 64 bit ciascuno
- **È stato bucato quindi non viene utilizzato più**



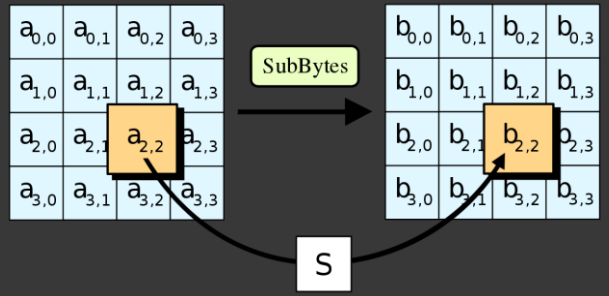
3DES

- **«Upgrade» di 3DES**
- **3 chiavi da 56 bit ciascuna**
- Da dicembre 2023 è deprecato (il suo uso è sconsigliato)



AES

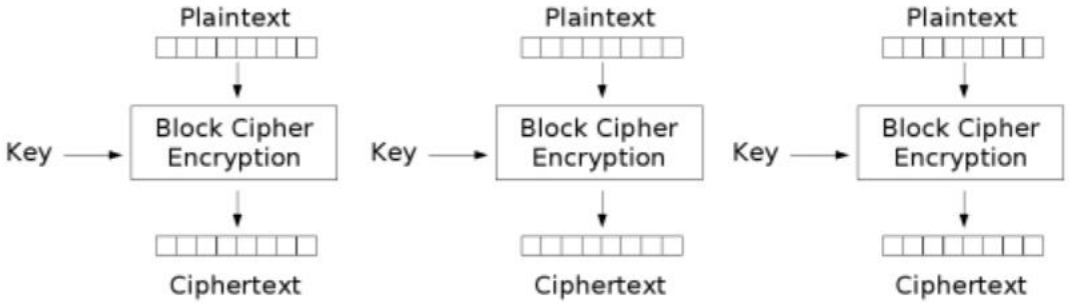
- **AES (Advanced Encryption Standard)**
- **Lunghezza chiave: 128, 192, 256 bit**
- Cifrario a blocchi, lunghi 128 bit ciascuno
- Attualmente è uno dei cifrari a blocchi più sicuri
- Estremamente veloce e facile da implementare



MODES OF OPERATION

Serie di procedimenti precisi comuni in tutti i cifrari a blocchi

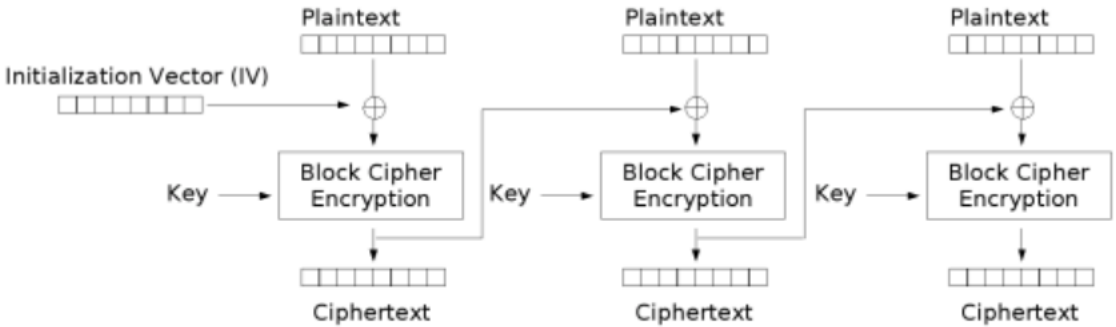
ECB (ELETRONIC CODE BOOK)



Electronic Codebook (ECB) mode encryption

Non garantisce l'integrità
Blocchi di plaintext uguali -> blocchi di ciphertext uguali

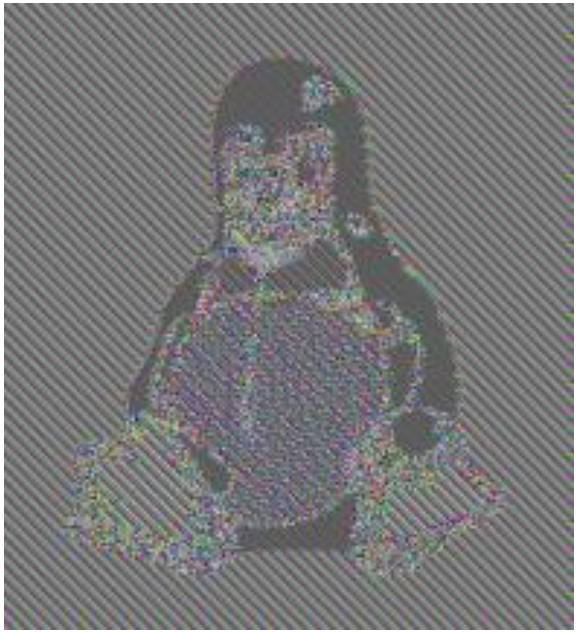
CBC (Cipher Block Chaining)



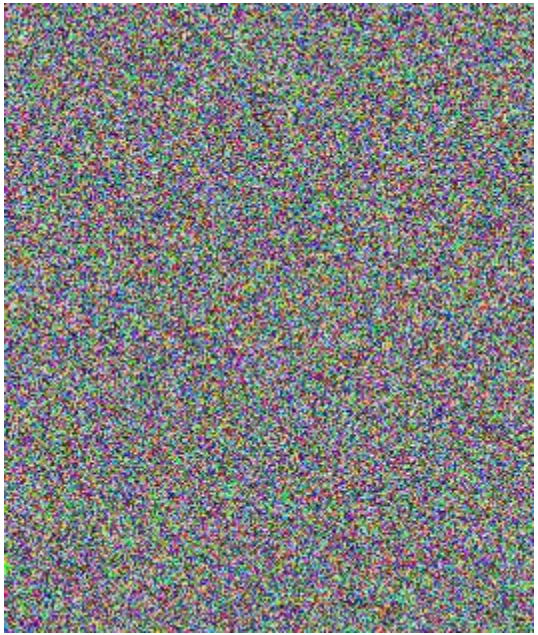
Cipher Block Chaining (CBC) mode encryption

L'IV non deve essere riutilizzato
Il valore dell'IV non deve essere prevedibile
Se hai controllo dell'IV puoi fare «robe»

UTILIZZANDO ECB...



UTILIZZANDO CBC...



Siamo vicini alla fine....

Piccolo accenno a...

PRIMA DI TERMINARE...

Risolvere «La memoria di Bob», «Flip my words»

Potete provare a risolvere queste a casa

- «A weird trip to Delphi»
- «Modes Diff»

E chi si sente forte, può risolvere

- **Berserker (iv prediction)**
- **Baby AES**
- **Private IV (key == iv)**

FINE

Salvatore Abello, 5IB

salvatore.abello2005@gmail.com
https://github.com/salvatore-abello