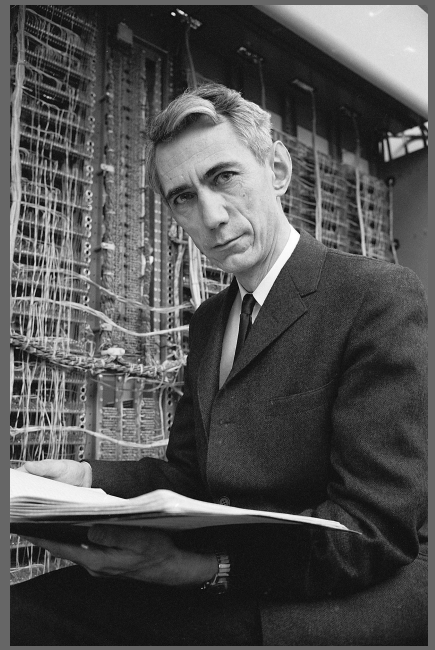
ICMC USP
SÃO CARLOS

GANESH

Criptografia moderna e One Time Pad

Criptografia Moderna

- Teoria da Informação
  - Claude Shannon
- Utilização de computadores



Motivação

- Ataques baseados somente no *ciphertext*
  - Padrões na encriptação
  - Ataques estatísticos
    - Carta do PCC

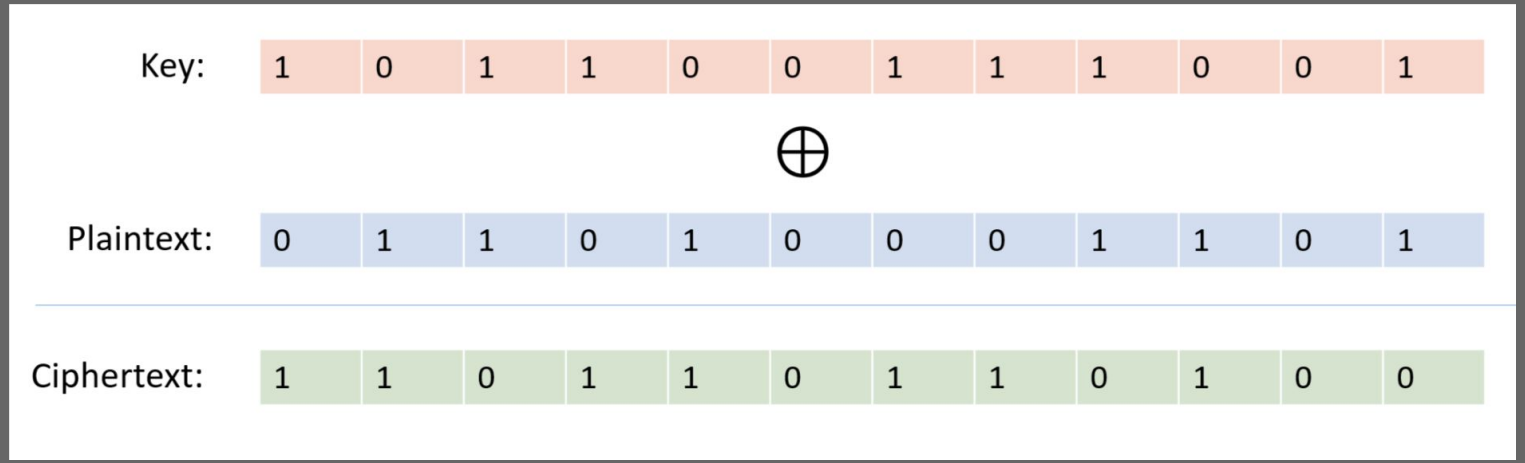
One-Time pad

- Algoritmo criptográfico
- Chave única, t.q. |k| ≥ |m|
  - *Perfect secrecy*
  - Chave randômica

One-Time pad

- Encriptação:
  - $E(k,m) = m \oplus k = c$
- Decriptação:
  - $D(k,c) = c \oplus k = m$
- E(k,m) e D(k,c) são determinísticos
  - XOR

One-Time pad


Key: 1 0 1 1 0 0 1 1 1 0 0 1
⊕
Plaintext: 0 1 1 0 1 0 0 0 1 1 0 1
Ciphertext: 1 1 0 1 1 0 1 1 0 1 0 0

One-Time pad

- Seguro porém impraticável na maioria dos casos
  - Chaves muito grandes
  - Solução: Stream-Ciphers

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br