

CRITTOGRAFIA

lezione di martedì
20 ottobre

16:15

DES



Principi di Shannon [x resistenza agli attacchi di CRYPTO ANALYSIS STATISTICA]

1) Differenze

~~incorrect~~ tutti i caratteri del testo in chiaro si devono spostare nel ciphertext -

ogni carattere del ciphertext deve dipendere da tutti i caratteri del testo in chiaro

2) Confusione

combinare testo in chiaro e chiave in modo complesso,
per non permettere al crittanalista di
separare le due componenti enclavando il ciphertext

[1972]

NBS National Bureau of Standards

(\hookrightarrow NIST : National Institute for Security and Technology)

{
1973}

- sicurezza basata nelle regole MA della chiffratura e non sul processo di cifratura e decifratura (\rightarrow pubblico)
- dispositivo efficiente in software e hardware

IBM: proporre Lucifer



NSA shielded le proposte
ha introdotto alcune variazioni

128 → 56 bit chiave
variazioni nella S-box

1977 DES accettato e reso pubblicamente disponibili
(licenza d'uso gratuita)
DATA ENCRYPTION STANDARD



rimane fino al 1999 DES
accettato solo per scopi militari
conquistò 3 DES

2005

3DES → consigliato

2005 → AES

Advanced Encryption Standard

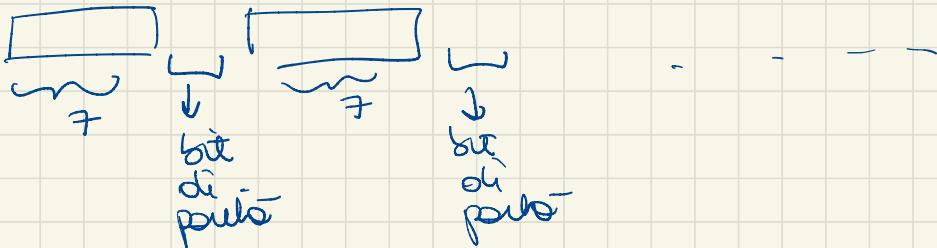
Cifrazione a blocchi di 64 bit

DES

chiave segreta di 64 bit

56 comuni

+ 8 bit di parità



$r = 16$ fasi in cui si ripetono le stesse operazioni

Attacchi' al DES

- ① architetture supportive progettate per difendere il DES
- ② calcolo distribuito su più macchine

SPADE DES

RSA

1997

\$ 10¹⁰

5 mesi

"strong cryptography makes the world a safer place"
↳ 25% delle porte chiuse

1998

39 giorni 85%

"Many hands make light work"

Attacchi esaurienti

2^{56}

- 64 duei deboli

$\hookrightarrow 2^{56} \rightarrow 2^{55}$

$$C(m, k) = c$$

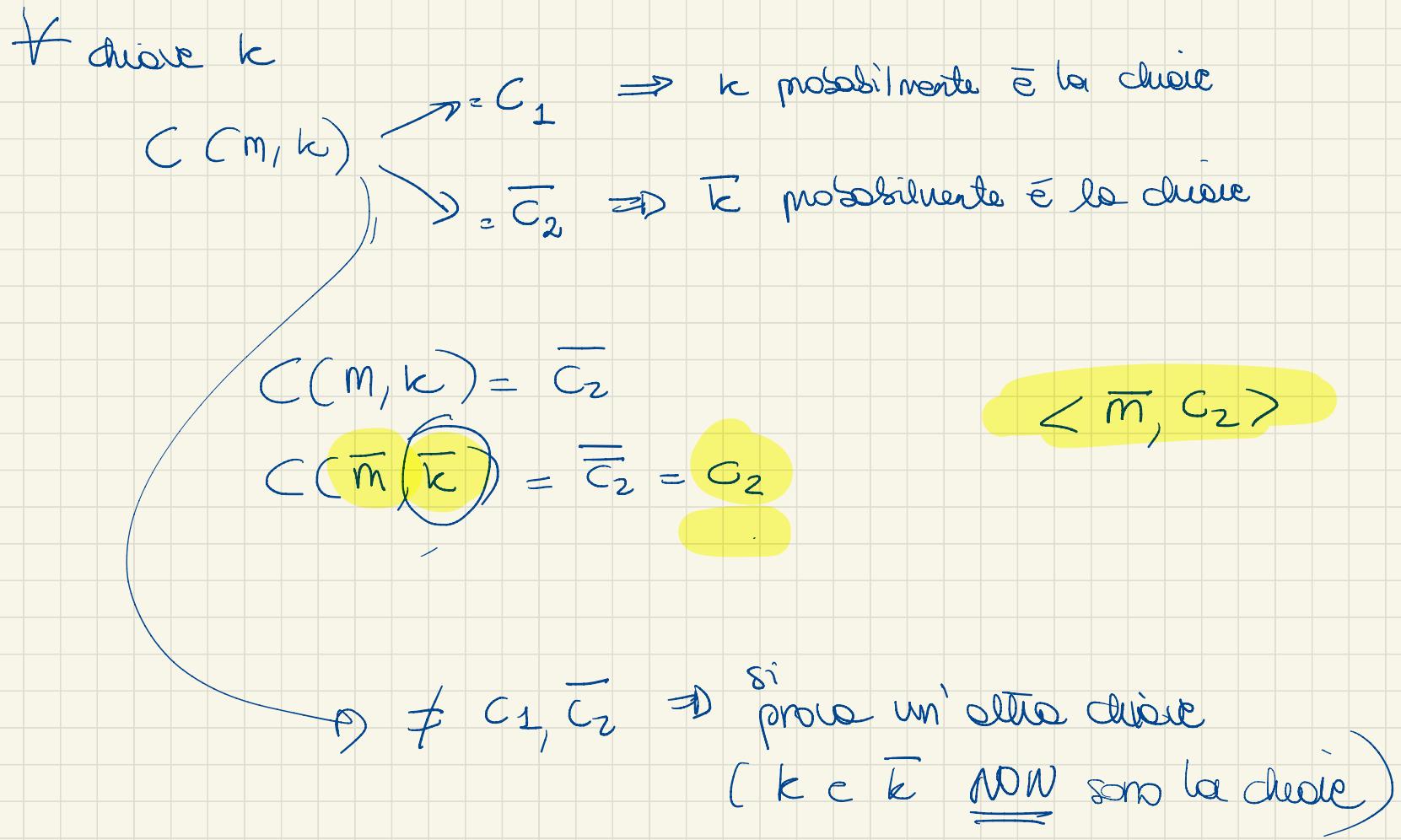
$$C(\bar{m}, \bar{k}) = \bar{c}$$

CHosen PLAIN TEXT

il crittosolida si procura copie

$\langle m, c_1 \rangle$

$\langle \bar{m}, c_2 \rangle$



Ciphertext distinguishability

1990

Rihom Shorier

chosen plain text

2^{47} copie $\langle m, c \rangle$

↓ scelti dal cibsonisti

costo complessivo
attacco

2 55.1

$r=16$

Ciphertext distinguishability 1993

Metzger

2^{43} copie $\langle m, c \rangle$

known plain text