CRITTOGRAFIA: raccolta di esercizi d'esame (cifrari perfetti).

Esercizio 1

Sia M il numero di matricola del candidato. Si converta M in una sequenza binaria B trasformando ordinatamente in binario ogni cifra decimale di M, prendendo per ciascuna di esse i tre bit meno significativi e concatenando tali gruppi di tre bit.

1. **Indicare** la sequenza B, **proporre** una chiave K di 18 bit ottenuta lanciando idealmente una moneta e **trasformare** B mediante One-Time Pad utilizzando K.
2. **Spiegare** se il cifrario può ritenersi sicuro per messaggi binari di lunghezza multipla di 18 utilizzando come chiave una ripetizione di K per il numero di volte necessario.

↳ problema: $m \oplus k = c \quad m' \oplus k = c'$

$c \oplus c' = (m \oplus k) \oplus (m' \oplus k) = m \oplus m'$

↳ può dare informazioni

Esercizio 2

In un cifrario A esistono un messaggio m e un crittogramma c tali che: Prob(M = m) = p < 1/4, Prob(M = m| C = c) = 1- p. **Spiegare** se A può essere un cifrario perfetto e le conseguenze per un crittoanalista per la coppia (m,c) indicata.

↓ NO infatti

$P(M=m \mid C=c) = 1-p > \frac{3}{4}$ e $P(M=m) < \frac{1}{4}$

acquisisce conoscenza osservando il crittogramma in transito

Esercizio 3

Spiegare con precisione matematica e proprietà di linguaggio perché il cifrario One-Time Pad su messaggi di n bit non può essere ritenuto perfetto se la chiave non è scelta perfettamente a caso.

non è qui detto che $\{M=m\}$ e $\{C=c\}$ siano eventi indipendenti (proprietà cruciale per dimostrare che OTP è perfetto)

Esercizio 4

Nel codice One-Time Pad si sostituisca l'operatore XOR con OR, o con ¬XOR (cioè XOR negato). Spiegare, per i due casi, se il protocollo funziona con le stesse proprietà del codice originale.

OR: NO, la cifratura non è iniettiva, dal crittogramma si ricavano molte informazioni sulla chiave e sul messaggio.

¬XOR: SI

Esercizio 5

Qual è lo svantaggio principale del cifrario One-Time Pad?

generazione e scambio della chiave

Esercizio 6

Nel cifrario One-Time Pad si consideri una coppia arbitraria messaggio/crittogramma *m, c* di *n* bit. **Spiegare** quanto vale la probabilità *P(M=m, C=c)* (**NOTA**: questa è la probabilità dell'intersezione degli eventi, non la probabilità condizionale).

Se la chiave è scelta perfettamente a caso $\{M=m\}$ e $\{C=c\}$ sono eventi indipendenti, inoltre $P(C=c) = \frac{1}{2^n}$.

Dunque:

$P(M=m, C=c) = P(M=m) \cdot P(C=c) = \frac{1}{2^n} P(M=m)$