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.

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.

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.

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.

Esercizio 5
Qual è lo svantaggio principale del cifrario One-Time Pad?

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).