CRITTOGRAFIA: raccolta di esercizi d'esame (complessità e randomizzazione).

Esercizio 1
Un sistema crittografico impiega chiavi private di 46 bit. Per decifrare un messaggio m data la chiave, un programma in assembler impiega un ciclo di 128 istruzioni ripetuto in media tante volte quanti sono i bit che costituiscono m. Impiegando un calcolatore che esegue un'operazione assembler in un tempo medio di 10 n s, indicare in ordine di grandezza quanti anni sarebbero necessari in media per condurre un attacco esaustivo sulle chiavi per un messaggio m di 1000 bit. **Indicare** i calcoli eseguiti.

Esercizio 2
Si vuole generare una sequenza di bit pseudocasuali utilizzando il generatore BBS basato sulla legge:

$$x(i) = x(i-1)^2 \bmod n, \quad b(i) = 1 \Leftrightarrow x(m-i) \text{ è dispari.}$$

1. **Scegliere** n = 11 * 23 e verificare che 11 e 23 soddisfino i requisiti richiesti dal generatore BBS.
2. Sia M il proprio numero di matricola. Porre y = M mod 100 e $x(0) = y^2 \bmod n$, e **indicare** una sequenza di 10 bit generati, **riportando i calcoli eseguiti**.
3. **Discutere** se il generatore può considerarsi crittograficamente sicuro.

Esercizio 3
Sia C una sequenza ottenuta rappresentando in binario ciascuna delle due cifre centrali del numero di matricola del candidato, prendendo per ciascuna di esse i tre bit meno significativi, concatenando questi due gruppi di bit e aggiungendo 1 in testa.
1. Eseguire l'operazione: $37^C \bmod 100$ per esponenziazioni successive **indicando i calcoli eseguiti**.
2. **Spiegare perché** tale metodo di calcolo è considerato efficiente.

Esercizio 4
Applicando l'algoritmo di Miller e Rabin, individuare un numero *N* primo di tre cifre decimali con probabilità di errore minore di 1/50, spiegando il procedimento eseguito.

Esercizio 5
Illustrare con quale metodo si generano numeri primi grandi in crittografia e **spiegare** perché tale metodo è considerato efficiente.