

Quiz #2

Please print your name:

Problem 1. Eve intercepts the ciphertext $c = (1101\ 0100\ 1100)_2$. It is known that a stream cipher with PRG $x_{n+1} \equiv 5x_n + 7 \pmod{16}$ was used for encryption.

Eve also knows that the plaintext begins with $m = (1111\ 01\dots)_2$. Help her crack the ciphertext!