Quiz #2

MATH 481/581 — Cryptography
Friday, Feb 3

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 $m = (1111\ 01...)_2$. Help her crack the ciphertext!

Solution. Since $c = m \oplus \text{PRG}$, we learn that the initial piece of the keystream is $\text{PRG} = m \oplus c = (1111\ 01...)_2 \oplus (1101\ 01...)_2 = (0010\ 00...)_2$. Since each x_n is 4 bits, we conclude that $x_1 = (0010)_2 = 2$.

Because the PRG is predictable, we can now recreate the entire keystream! Using $x_{n+1} \equiv 5x_n + 7 \pmod{16}$, we find $x_2 = 1$, $x_3 = 12$, ... In other words, $\text{PRG} = 2, 1, 12, ... = (0010\ 0001\ 1100\ ...)_2$.

Hence, Eve can decrypt the ciphertext and obtain $m = c \oplus \text{PRG} = (1101\ 0100\ 1100)_2 \oplus (0010\ 0001\ 1100)_2 = (1111\ 0101\ 0000)_2$. □

Armin Straub
straub@southalabama.edu