Introdução à Criptografia – Lista II

Ex. 1 — (Ainda cifra de fluxo) Um gerador pseudoaleatório funciona da seguinte maneira: dados parâmetros a, b, n, e uma semente $s < n$,

$$\begin{aligned} x_0 &= s \\ x_i &= ax_{i-1} + b \pmod{n} \end{aligned}$$

Mostre que este tipo de gerador não é seguro.

Ex. 2 — O modo CBC tolera erros no texto cifrado. Mostre que se há um erro em um bloco c_j, somente dois blocos serão decriptados incorretamente (indique quais).

Ex. 3 — Seja $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ uma função pseudoaleatórea. Argumente que F deve ser de mão única.

Ex. 4 — Seja $F : \mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_3$ definida como

$$F_K(x) = Kx \pmod{3}.$$

- F é uma cifra de bloco, de acordo com a definição dada nas notas de aula? Porque sim, ou porque não?
- F_1 é permutação?