Introdução à Criptografia – Lista III

Ex. 1 — Considere a seguinte S-box para quatro bits:

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ F & 2 & 1 & 4 & 3 & D & E & B & C & B & A & 9 & 8 & 7 & 6 & 5 \end{bmatrix}$$

a) Mostre três relações lineares entre os bits de entrada e saída; as variáveis aleatórias associadas a estas relações devem ter cada uma um viés diferente das outras;

b) Se criássemos uma cifra de 16 bits somente com dois passos, sendo cada um composto por quatro cópias paralelas desta S-box, sem passo de permutação, diga teoricamente quais bits da chave seriam facilmente identificados por criptanálise linear.

Ex. 2 — Consulte a tabela de aproximação linear nas notas de aula e determine

a) $\Pr[X_1 \oplus X_2 \oplus X_3 = Y_1 \oplus Y_4]$

b) $\Pr[X_2 = Y_2]$

c) $\Pr[X = Y]$

Ex. 3 — A respeito da tabela de aproximação linear nas notas de aula:

a) Porque a primeira coluna e a primeira linha estão zeradas, exceto pela posição $(0, 0)$? Isso é uma propriedade específica desta S-box ou é algo que deva ser verdade sempre?

b) Porque a soma de qualquer linha ou coluna é sempre $+8$ ou -8?

Ex. 4 — Suponha que alguém tenha proposto um ataque criptanalítico teórico a uma cifra de bloco. O bloco da cifra tem 80 bits e a chave, 128 bits. O ataque proposto funcionaria com 2^{100} operações em 2^{110} pares de mensagem e texto encriptado. Aponte um problema com este ataque.