Introdução à Criptografia – Lista I

Ex. 1 — [Stinson] Suponha que o one-time pad foi usado para encriptar m e m', resultando em c e c' respectivamente. Sabendo que a mesma chave foi usada (de forma contrária ao que se recomenda quando usamos o one-time pad), mostre que

$$m \oplus m' = c \oplus c'.$$

Diga também o que pode acontecer de errado (como um atacante poderia usar este fato, e em que elel conseguiria?)

Ex. 2 — Considere o criptossistema a seguir (uma variante do one-time pad):
Construção 1 (Criptossistema furado)**.**

- $\mathsf{Gen}(1^n)$ seleciona uniformemente uma sequência de bits em $\{0,1\}^n$;
- $\mathsf{Enc}(m,k)$ funciona da seguinte maneira: a mensagem m é dividida em blocos $m_0, m_1, \cdots, m_m$ de n bits. Cada bloco é encriptado separadamente, sendo que $c_i = m_i \oplus k$;
- $\mathsf{Dec}(c,k)$ é semelhante a Enc, mas permutando c e m. ♦

a) Prove que o criptossistema funciona corretamente (ou seja, para todos k e m, $\mathsf{Dec}(\mathsf{Enc}(m,k),k) = m$).

b) Prove que o criptossistema não é seguro de acordo com nenhuma das definições dadas em aula (contra texto cifrado conhecido, texto claro conhecido, etc).

Ex. 3 — Dê uma demonstração rigorosa de que o gerador pseudoaleatório Blum-Blum-Shub é seguro (a descrição deste gerador está no Capítulo 4 das notas de aula).

Ex. 4 — Informe-se e estude o que se chama de *Cifra de Vigenère*.

a) Descreva a cifra formalmente (dê a descrição de $\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}$).

b) Prove que esta cifra tem sigilo perfeito para encriptação de um único caracter

c) Para quantos caracteres a cifra tem sigilo perfeito?

Ex. 5 — Seja G um gerador pseudoaleatório de bits com fator de expansão $l(n) > 2n$. Quais dos seguintes também são geradores pseudoaleatórios?

a) $G'(s) = G(aa)$, onde a é a primeira metade da sequencia s.

b) $G'(s) = G(ba)$, onde $a = s_0 s_1 s_2 \ldots s_{n/2}$ e $b = s_{n/2+1} \ldots s_n$.

c) $G'(s) = G(0)$ concatenado com $G(s)$