Introdução à Criptografia – Lista I

Ex. 1 — É possível construir uma rede de Feistel usando códigos autenticadores de mensagens no "core" da rede (na função f)? Sugira um esquema de escalonamento de chaves.

Ex. 2 — Mostre como generalizar o protocolo Diffie-Hellman de distribuição de chaves para um número arbitrário de participantes. Qual é o custo com- putacional da sua construção, comparado com o do Diffie-Hellman para dois participantes?

Ex. 3 — Usarmos o esquema de assinatura ElGamal, com a notação usada nas notas de aula (Construção 10.14, Cap. 10). Suponha que tenhamos usado

$$p = 31847$$
$$g = 5$$
$$h = 25703$$

Suponha também que as duas assinaturas abaixo tenham sido produzidas com esta chave secreta:

$$m = 8990, \sigma = (23972, 31396)$$
$$m = 31415, \sigma = (23972, 20481)$$

Sem resolver log discreto, mostre o elemento aleatório y usado nas assinaturas e a chave secreta x.

Ex. 4 — Suponha que em uma licitação todos tenham que fazer a oferta de preço usando o protocolo de comprometimento de Pedersen: se meu preço é k, publico o comprometimento

$$c = g^k h^r \pmod{p},$$

onde g, h, p são parâmetros conhecidos e r é gerado aleatoriamente por mim na hora de produzir o comprometimento.
Eu argumento que este esquema não funciona. Se um concorrente quiser bater meu preço, ele pode enviar

$$c' = c \cdot X \pmod{p},$$

onde X é o comprometimento com -100. Isto resultará no comprometimento com $k - 100$, e ele estará em vantagem. Comente: meu argumento está correto? Se não, diga porque. Se sim, há como consertar o esquema?

Ex. 5 — Refaça o exercício anterior, mas usando comprometimento com log discreto (não Pedersen).

Ex. 6 — Mostre como jogar par-ou-ímpar por telefone, de maneira segura.

Ex. 7 — Escolha problemas em NP e construa para eles sistemas de prova interativa.