Introdução à Criptografia – Lista IV

Ex. 1 — No RSA, porque o expoente para encriptação (e) deve ser co-primo com $\phi(n)$?

Ex. 2 — Porque todo criptossistema de chave pública deve necessariamente ter segurança CPA?

Ex. 3 — Mostre como implementar o esquema de assinaturas de Lamport usando logaritmo discreto.

Ex. 4 — Mostre como implementar o esquema de assinaturas de Lamport usando uma função de mão única qualquer. No entanto, o esquema deve usar a função uma única vez (não pode calcular $f(x)$ para mais de um valor x);

Ex. 5 — Considere o criptossistema RSA com módulo n. Um inteiro $1 < m < n-1$ é chamado de *ponto fixo* se $\mathsf{Enc}_e(m) = m$, ou seja, se sua encriptação é igual a ele mesmo. Mostre que se m é ponto fixo, $n - m$ também é.