CIn–UFPE
Introdução à Criptografia Moderna (Graduação)
Fundamentos da Criptografia Moderna (Pós-Graduação)
2009.1
Lista de Exercícios 1
Entrega: 5ª feira, 19/03/2009

Exercício 1 (Katz & Lindell (2007), 1.4 (2,0)) Numa tentativa de evitar o ataque de Kasiski sobre a cifra de Vigenère, a seguinte modificação foi proposta. Dado o período t da cifra, o purotexto é quebrado em blocos de tamanho t. Lembre-se que dentro de cada bloco, a cifra de Vigenère funciona encriptando o i-ésimo caracter com a i-ésima chave (usando a cifra de deslocamento). Suponha que as chaves sejam $k_1, \ldots, k_t$, então isso significa que o i-ésimo caracter em cada bloco é encriptado adicionando a ele k_i módulo 26. A modificação proposta é encriptar o i-ésimo caracter no j-ésimo bloco adicionando $k_i + j$ módulo 26.

(a) Mostre que a decriptação funciona como desejado.

(b) Descreva o efeito da modificação acima sobre o ataque de Kasiski.

(c) Elabore uma forma alternativa de determinar o período para esse esquema.

Exercício 2 (Katz & Lindell (2007), 2.3 (2,0)) Quando se usa o bloco-de-uso-único (cifra de Vernam) com a chave $k = 0^\ell$, segue que $\mathsf{Enc}_k(m) = k \oplus m = m$ e a mensagem é enviada em aberto! Por isso foi sugerido como melhorar o bloco-de-uso-único simplesmente encriptando com uma chave $k \neq 0^\ell$ (i.e., fazendo com que o algoritmo Ger de geração de chaves escolha k uniforme e aleatoriamente do conjunto de chaves *não-zero* de comprimento ℓ). Isso é de fato um melhoramento? Em particular, esse esquema modificado tem sigilo perfeito? Prove sua resposta. Se sua resposta for positiva, explique por que o bloco-de-uso-único não é descrito dessa maneira. Se sua resposta for negativa, mostre como reconciliar isso com o fato de que encriptar com 0^ℓ não modifica o purotexto.

Exercício 3 (Katz & Lindell (2007), 2.3 (2,0)) Suponha que se exija somente que um esquema de encriptação $(\mathsf{Ger}, \mathsf{Enc}, \mathsf{Dec})$ sobre um espaço de mensagem $\mathcal{M}$ satisfaz o seguinte: para toda $m \in \mathcal{M}$, a probabilidade de que $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$ seja no mínimo 2^{-t}. (Essa probabilidade é tomada sobre a escolha de k assim como qualquer aleatoriedade que possa ser usada durante a encriptação ou decriptação.) Mostre que o sigilo perfeito pode ser atingido com $|\mathcal{K}| < |\mathcal{M}|$ quando $t \geq 1$. Dê um limitante inferior no tamanho necessário de $\mathcal{K}$.

Exercício 4 (Stinson (2006), 2.11 (2,0)) Prove que um criptossistema tem sigilo perfeito se e somente se $H(P|C) = H(P)$. (Obs.: P e C são variáveis aleatórias associadas aos conjuntos de purotextos e cifrotextos, respectivamente.)

Exercício 5 (Stinson (2006), 2.12 (2,0)) Prove que em qualquer criptossistema $H(K|C) \geq H(P|C)$. (Obs.: Intuitivamente, isso quer dizer que, dado um cifrotexto, a incerteza do adversário sobre a chave é no mínimo tão grande quanto a incerteza sobre o purotexto.)