CIn-UFPE
Introdução à Criptografia Moderna (Graduação)
Fundamentos da Criptografia Moderna (Pós-Graduação)
2009.1

Lista de Exercícios 2

Entrega: 5ª feira, 26/03/2009

Exercício 1 (Katz & Lindell (2007), 3.2 (2,0)) O melhor algoritmo conhecido hoje em dia para encontrar fatores primos de um número de n -bits roda em tempo $2^{c \cdot n^{\frac{1}{3}} (\log n)^{\frac{2}{3}}}$. Assumindo a disponibilidade de computadores com processadores de 4GHz, e $c = 1$ (e que as unidades da expressão dada sejam ciclos do clock do processador), dê uma estimativa do tamanho de números que não podem ser fatorados pelos próximos 100 anos.

Exercício 2 (Katz & Lindell (2007), 3.3 (2,0)) Prove que a Definição 3.8 (segurança em relação a encriptações indistinguíveis na presença de um abelhudo) se Π puder encriptar mensagens de comprimentos arbitrários e o adversário **não** estiver restrito a dar como saída mensagens de igual comprimento no experimento $\text{ChPriv}_{\mathcal{A}, \Pi}^{\text{abe}}$.

Dica: Seja $q(n)$ um limitante superior polinomial no comprimento do cifrotexto quando Π é usado para encriptar um único bit. Então considere um adversário que produz $m_0 \in \{0, 1\}$ e $m_1 \in \{0, 1\}^{q(n)+2}$ aleatória.

Exercício 3 (Katz & Lindell (2007), 3.4 (2,0)) Suponha que $\Pi = (\text{Ger}, \text{Enc}, \text{Dec})$ seja tal que para $k \in \{0, 1\}^n$, o algoritmo Enc_k seja definido somente para mensagens de comprimento no máximo $\ell(n)$ (para algum polinômio ℓ). Construa um esquema satisfazendo a Definição 3.8 (segurança em relação a encriptações indistinguíveis na presença de um abelhudo) mesmo quando o adversário **não** estiver restrito a produzir como saída mensagens de mesmo comprimento no experimento $\text{ChPriv}_{\mathcal{A}, \Pi}^{\text{abe}}$.

Exercício 4 (Katz & Lindell (2007), 3.6 (2,0)) Seja G um gerador pseudoaleatório tal que $|G(s)| \geq 2 \cdot |s|$.

- (a) Defina $G'(s) \stackrel{\text{def}}{=} G(s0^{|s|})$. Esse G' será necessariamente um gerador pseudoaleatório? Justifique.
- (b) Defina $G'(s) \stackrel{\text{def}}{=} G(s_1 \cdots s_{n/2})$, onde $s = s_1 \cdots s_n$. Esse G' será necessariamente um gerador pseudoaleatório? Justifique.

Exercício 5 (Katz & Lindell (2007), 3.10 (2,0)) Seja G um gerador pseudoaleatório e defina $G'(s)$ como sendo a saída de G truncada para n bits (onde $|s| = n$). Prove que a função $F_k(x) = G'(k) \oplus x$ não é pseudoaleatória.