CIn–UFPE
Introdução à Criptografia Moderna (Graduação)
Fundamentos da Criptografia Moderna (Pós-Graduação)
2009.1
Lista de Exercícios 9
Entrega: 3ª feira, 02/06/2009

**Exercício 1 (Katz & Lindell (2007), 10.1 (2,0))** Suponha que se tenha à disposição um esquema de encriptação de chave-pública para mensagens de um único bit. Mostre que, dada a chave pública $cp$ e um cifrotexto $c$ computado via $c \leftarrow \mathsf{Enc}_{cp}(m)$, é possível para um adversário de recursos ilimitados determinar $m$ com probabilidade $1$. Isso mostra que encriptação de chave-pública perfeitamente-secreta é impossível.

**Exercício 2 (Katz & Lindell (2007), 10.3 (2,0))** Mostre que para qualquer esquema de encriptação de chave pública seguro contra ataque de purotexto-escolhido, o tamanho do cifrotexto após e encriptar um único bit é superlogarítmico no parâmetro de segurança. Ou seja, para $(cp, cs) \leftarrow \mathsf{Ger}(1^n)$, deve ser o caso que $|\mathsf{Enc}_{cp}(b)| = \omega(\log n)$ para qualquer $b \in \{0,1\}$. (**Dica:** Se não for o caso, o conjunto de possíveis cifrotextos é apenas polinomial no tamanho.)

**Exercício 3 (Katz & Lindell (2007), 10.7 (2,0))** Fixe $N$, e assuma que existe um adversário $\mathcal{A}$ que roda em tempo $t$ para o qual

$$\Pr[\mathcal{A}([x^e \bmod N]) = x] = 0,01,$$

onde a probabilidade é tomada sobre a escolha aleatória de $x \leftarrow \mathbb{Z}_N^*$. Mostre que é possível construir um adversário $\mathcal{A}'$ para o qual

$$\Pr[\mathcal{A}'([x^e \bmod N]) = x] = 0,99.$$

O tempo de execução $t'$ de $\mathcal{A}'$ deve satisfazer $t' = \mathsf{poly}(\| N \|, t)$. (**Dica:** Use o fato de que $y^{1/e} \cdot r = (y \cdot r^e)^{1/e} \bmod N$.)

**Exercício 4 (Katz & Lindell (2007), 10.8 (2,0))** O expoente público $e$ no RSA pode ser escolhido arbitrariamente, desde que $\mathrm{mdc}(e, \phi(N)) = 1$. Escolhas comuns de $e$ incluem $e = 3$ e $e = 2^{16} + 1$. Explique por que tais valores de $e$ são preferíveis a um valor aleatório do mesmo comprimento. (**Dica:** Veja o algoritmo para exponenciação modular no Apêndice B.2.3 do livro de Katz & Lindell.)

**Exercício 5 (Boneh (2009) (2,0))** Vamos explorar por que no RSA cada participante tem que estar associado a um módulo diferente $N = pq$. Suponha que tentemos usar o mesmo módulo $N = pq$ para todos os participantes. Cada participante é associado a um expoente público $e_i$ e um expoente privado $d_i$ tal que $e_i \cdot d_i = 1 \bmod \phi(N)$. À primeira vista isso parece funcionar bem: para encriptar uma mensagem para Bob, Alice computa $c = m^{e_{Bob}}$ e envia $c$ a Bob. Um abelhudo Abel, não sabendo o valor $d_{Bob}$ parece ser incapaz de decriptar $c$. Vamos mostrar que usando $e_{Abel}$ e $d_{Abel}$ Abel pode facilmente decriptar $c$.

a. Mostre que, dados $e_{Abel}$ e $d_{Abel}$, Abel pode obter um múltiplo de $\phi(N)$.

b. Mostre que, dado um inteiro $K$ que é um múltiplo de $\phi(N)$, Abel pode fatorar o módulo $N$. Deduza que Abel pode decriptar qualquer cifrotexto RSA encriptado usando o módulo $N$ que seria para Alice ou Bob.

   (**Dica:** Considere a seqüência $g^K, g^{K/2}, g^{K/4}, \ldots, g^{K/\tau(K)} \bmod N$ onde $g$ é aleatório em $\mathbb{Z}_N$ e $\tau(N)$ é a maior potência de $2$ que divide $K$. Use o elemento mais à esquerda nessa seqüência que não é igual a $\pm 1 \bmod N$.)