CIn–UFPE
Introdução à Criptografia Moderna (Graduação)
Fundamentos da Criptografia Moderna (Pós-Graduação)
2009.1
Lista de Exercícios 3
Entrega: 5ª feira, 02/04/2009

Exercício 1 (Katz & Lindell (2007), 3.14 (2,5)) Seja F uma permutação pseudo-aleatória, e defina um esquema de encriptação $(\mathsf{Ger}, \mathsf{Enc}, \mathsf{Dec})$ da seguinte forma: Sobre a entrada $m \in \{0,1\}^{n/2}$ e $k \in \{0,1\}^n$, o algoritmo Enc escolhe uma cadeia aleatória $r \leftarrow \{0,1\}^{n/2}$ de comprimento $n/2$ e computa $c := F_k(r \parallel m)$.

Mostre como decriptar, e prove que esse esquema é seguro contra ataques de purotexto-escolhido para mensagens de comprimento $n/2$. Quais são as vantagens e desvantagens dessa construção em relação à Construção 3.24 do livro-texto?

Exercício 2 (2,5) Suponha que se implemente encriptação no modo CBC com um vetor inicial VI aleatório, mas ao invés de escolher VI aleatoriamente, VI é implementado como um contador. (Obs.: note que não se trata de usar o modo CTR!) Ou seja, a mensagem de número i é encriptada usando i como vetor inicial. O sistema resultante é semanticamente seguro sob ataques de purotexto-escolhido (isto é, quando a chave secreta é usada para encriptar múltiplas mensagens)? Justifique sua resposta.

Exercício 3 (2,5) Suponha que o usuário A esteja enviando pacotes em regime de broadcast a n destinatários $B_1, \ldots, B_n$. Assuma que privacidade não seja importante, mas que integridade o seja. Em outras palavras, a cada um dos $B_1, \ldots, B_n$ deve ser assegurado que os pacotes que estão recebendo foram de fato enviados por A. O usuário A decide usar um esquema de código de autenticação de mensagens (MAC).

(a) Suponha que o usuário A e os destinatários $B_1, \ldots, B_n$ compartilham uma chave secreta k. O usuário A acrescenta uma etiqueta a todo pacote que ele envia usando k. Cada usuário B_i pode então verificar o MAC. Usando no máximo duas sentenças, explique por que esquema é inseguro, a saber, mostre que o usuário B_1 não tem garantia de que os pacotes que ele está recebendo são de fato provenientes de A.

(b) Suponha que o usuário A tenha um conjunto $S = \{k_1, \ldots, k_m\}$ de m chaves secretas. Cada usuário B_i tem algum subconjunto $S_i \subseteq S$ das chaves. Quando A transmite um pacote ele adiciona m etiquetas MAC's usando cada uma das suas m chaves. Quando o usuário B_i recebe um pacote ele

o aceita como válido somente se todas as etiquetas MAC correspondentes a chaves em S_i forem válidas. Que propriedade deveriam satisfazer os conjuntos $S_1, \ldots, S_n$ de modo que o ataque do item (a) não se aplique? Estamos assumindo que todos os usuários $B_1, \ldots, B_n$ estejam suficientemente distanciados uns dos outros de modo que eles não possam combinar nada.

(c) Mostre que quando $n = 10$ (i.e. dez destinatários) o emissor em broadcast A só precisa adicionar 5 etiquetas MAC a todo pacote para satisfazer a condição da parte (b). Descreva os conjuntos $S_1, \ldots, S_{10} \subseteq \{k_1, \ldots, k_5\}$ que você usaria.

Exercício 4 (Katz & Lindell (2007), 3.20 (2,5)) Para uma função $g : \{0,1\}^n \to \{0,1\}^n$, suponha que $g^{\$}(\cdot)$ seja um oráculo que, sobre a entrada 1^n, escolhe $r \leftarrow \{0,1\}^n$ uniforme e aleatoriamente e retorna $(r, g(r))$. Dizemos que uma função chaveada F é uma **função fracamente pseudoaleatória** se para todo algoritmo de tempo polinomial probabilístido D, existe uma função desprezível despr tal que:

$$\left|\Pr[D^{F_k^{\$}(\cdot)}(1^n) = 1] - \Pr[D^{f^{\$}(\cdot)}(1^n) = 1]\right| \leq \mathsf{despr}(n),$$

onde $k \leftarrow \{0,1\}^n$ e $f \leftarrow \mathsf{Func}_n$ são escolhidas uniforme e aleatoriamente.

(a) Prove que se F for pseudoaleatória então ela também é fracamente pseudoaleatória.

(b) Seja F' uma função pseudoleatória, e defina:

$$F_k(x) = \begin{cases} F'_k(x) & \text{se } x \text{ for par} \\ F'_k(x+1) & \text{se } x \text{ for ímpar} \end{cases}$$

Prove que F é fracamente pseudoaleatória mas *não* é pseudoaleatória.

(c) Um esquema de encriptação implementado em modo contador e que usa uma função fracamente pseudoaleatória F é necessariamente seguro contra ataques de purotexto-escolhido? Será que ele necessariamente tem encriptações indistingüíveis na presença de um abelhudo? Justifique suas respostas.

(d) Construa um esquema de encriptação seguro contra ataques de purotexto-escolhido baseado numa função fracamente pseudoaleatória.