CIn–UFPE
Introdução à Criptografia Moderna (Graduação)
Fundamentos da Criptografia Moderna (Pós-Graduação)
2009.1
Lista de Exercícios 4
Entrega: 2ª feira, 13/04/2009

Exercício 1 (Katz & Lindell (2007), 4.1 (2,0)) Digamos que $\Pi = (\mathsf{Ger}, \mathsf{Mac}, \mathsf{Vrf})$ seja um MAC seguro, e para toda $k \in \{0,1\}^n$ o algoritmo gerador de etiquetas Mac_k sempre produza etiquetas de comprimento $t(n)$. Prove que t tem que ser super-logarítmica ou, equivalentemente, que se $t(n) = \mathcal{O}(\log n)$ então Π não pode ser um MAC seguro.

> **Dica**: Considere a probabilidade de se adivinhar aleatoriamente uma etiqueta válida.

Exercício 2 (Katz & Lindell (2007), 4.2 (2,0)) Considere o seguinte esquema de código de autenticação de mensagens de comprimento fixo para mensagens de comprimento $\ell(n) = 2n - 2$ usando uma função pseudoaleatória F: Sobre a mensagem $m_0 \parallel m_1$ (com $|m_0| = |m_1| = n-1$) e chave $k \in \{0,1\}^n$, o algoritmo Mac produz $t = F_k(0 \parallel m_0) \parallel F_k(1 \parallel m_1)$. O algoritmo Vrf é definido da maneira natural. Será que $(\mathsf{Ger}, \mathsf{Mac}, \mathsf{Vrf})$ é existencialmente inforjável sob um ataque de mensagem-escolhida? Prove sua resposta.

Exercício 3 (Katz & Lindell (2007), 4.3 (2,0)) Seja F uma função pseudoaleatória. Mostre que o seguinte MAC para mensagens de comprimento $2n$ é inseguro: A chave compartilhada é uma $k \in \{0,1\}^n$ aleatória. Para autenticar uma mensagem $m_1 \parallel m_2$ com $|m_1| = |m_2| = n$, compute a etiqueta $\langle F_k(m_1), F_k(F_k(m_2))\rangle$.

Exercício 4 (Katz & Lindell (2007), 4.4 (2,0)) Seja F uma função pseudoaleatória. Mostre que cada um dos seguintes esquemas de código de autenticação de mensagens é inseguro. (Em cada caso a chave compartilhada é uma $k \in \{0,1\}^n$ aleatória.):

(a) Para autenticar uma mensagem $m = m_1 \parallel \cdots \parallel m_\ell$, onde $m_i \in \{0,1\}^n$, compute $t := F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$.

(b) Para autenticar uma mensagem $m = m_1 \parallel \cdots \parallel m_\ell$, onde $m_i \in \{0,1\}^n$, escolha $r \leftarrow \{0,1\}^n$ aleatoriamente, compute $t := F_k(r) \oplus F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$, e envie $\langle r, t\rangle$.

(c) Para autenticar uma mensagem $m = m_1 \parallel \cdots \parallel m_\ell$, onde $m_i \in \{0,1\}^{n/2}$, escolha $r \leftarrow \{0,1\}^n$ aleatoriamente, compute

$$t := F_k(r) \oplus F_k(\langle 1 \rangle \parallel m_1) \oplus \cdots \oplus F_k(\langle \ell \rangle \parallel m_\ell)$$

(onde $\langle i \rangle$ é uma codificação de $n/2$-bits do inteiro i), e envie $\langle r, t \rangle$.

Exercício 5 (2,0) Fortalecendo funções de dispersão e MACs.

(a) Suponha que nos são dadas duas funções de dispersão $H_1, H_2 : \{0,1\}^* \to \{0,1\}^n$ (por exemplo, SHA1 e MD5) e nos é informado que ambas são resistentes à colisão. Claro, não podemos confiar totalmente nessas informações. Nosso objetivo é construir uma função de dispersão $H_{12} : \{0,1\}^* \to \{0,1\}^m$ que seja resistente à colisão assumindo que *pelo menos* uma das duas H_1, H_2 seja resistente à colisão. Dê a melhor construção que você possa dar para H_{12} e prove que um adversário que encontre uma colisão para sua H_{12} pode ser usado para encontrar colisões para ambas H_1 e H_2 (isso deverá provar a resistência à colisão de H_{12} assumindo que uma das duas é resistente à colisão). Note que uma construção simples para H_{12} serve, desde que você prove a segurança no sentido acima.

(b) As mesmas questões da parte (a) para códigos de autenticação de mensagens (MACs). Prove que um forjador existencial sob um ataque de mensagem escolhida na sua Mac_{12} dá um forjador existencial sob um ataque de mensagem escolhida para ambas Mac_1 e Mac_2. Novamente, uma construção simples é aceitável, desde que você prove a segurança. A prova de segurança aqui é um pouco mais complicada que na parte (a). É preciso garantir que sua prova defina explicitamente como o forjador da Mac_1 (ou Mac_2) funciona, dado o forjador da Mac_{12}.