CIn–UFPE
Introdução à Criptografia Moderna (Graduação)
Fundamentos da Criptografia Moderna (Pós-Graduação)
2009.1
Lista de Exercícios 5
Entrega: 5ª feira, 23/04/2009

Exercício 1 (Katz & Lindell (2007), 4.9 (2,0)) Prove que as seguintes modificações do CBC-MAC não levam a MAC de comprimento-fixo seguro:

(a) Modifique o CBC-MAC de modo que um VI aleatório é usado a cada vez que uma etiqueta é computada (e o VI é produzido como saída juntamente com t_ℓ). Ou seja, $t_0 \leftarrow \{0,1\}^n$ é escolhida aleatoria e uniformemente ao invés de ser fixada como 0^n, e a etiqueta é t_0, t_ℓ.

(b) Modifique o CBC-MAC de modo que todos os blocos $t_1, \ldots, t_\ell$ são dados como saída (ao invés de apenas t_ℓ).

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), 4.11 (2,0)) Seja (Ger_1, H_1) e (Ger_2, H_2) sejam duas funções de dispersão. Defina (Ger, H) de modo que Ger rode Ger_1 e Ger_2 para obter as chaves s_1 e s_2, respectivamente. E aí defina $H^{s_1,s_2}(x) = H_1^{s_1}(x) \parallel H_2^{s_2}(x)$.

(a) Prove que se pelo menos um dos dois (Ger_1, H_1) ou (Ger_2, H_2) for resistente à colisão, então (Ger, H) é resistente à colisão.

(b) Determine se uma afirmação análoga se verifica para a resistência à segunda pré-imagem para a resistência à pré-imagem, respectivamente. Prove sua resposta em cada caso.

Exercício 4 (Katz & Lindell (2007), 4.17 (2,0)) Antes que HMAC fosse inventado, era bastante comum se definir um MAC por $\mathsf{Mac}_k(m) = H^s(k \parallel m)$ onde H é uma função de dispersão resistente à colisão. Mostre que esse não é um MAC seguro quando H é construído através da transformada de Merkle–Damgård.

Exercício 5 (Katz & Lindell (2007), 5.6 e 5.7 (2,0)) Mostre que a cifra DES tem a propriedade de que $DES_k(x) = \overline{DES_{\overline{k}}(\overline{x})}$ para toda chave k e toda entrada x (onde $\overline{z}$ denota o complemento bit-a-bit de z). Essa é chamada de *propriedade da complementaridade* da DES.

Use essa propriedade para mostrar como é possível encontrar a chave secreta na DES (com probabilidade 1) em tempo 2^{55}. (**Dica:** Use um ataque de purotexto-escolhido com dois purotextos cuidadosamente escolhidos.)