

Segunda lista de exercícios

Professor: Nicollas Mocelin Sdroievski

Essa lista de exercícios aborda os assuntos da segunda parte da disciplina de Tópicos em Algoritmos - Fundamentos da Criptografia. Esta lista pode ser realizada por grupos de até três alunos, e deve ser entregue (em formato manuscrito ou formatada com L^AT_EX) por um dos membros até às 23:59 do dia 27/10. A entrega pode ser feita por e-mail (*nmsdroievski@ufpr.br*) ou presencialmente durante o horário de aula.

Exercícios para entrega

Todos os exercícios possuem o mesmo peso para fins de avaliação.

1. Seja $F : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ uma função pseudoaleatória (chaveada). Neste exercício, vamos mostrar que nenhum adversário probabilístico polinomial $\mathcal{A}$ consegue encontrar dois valores x e y tal que $F_k(x) = F_k(y)$ com probabilidade não-negligenciável.

- (a) Seja $\mathcal{A}$ um algoritmo de tempo polinomial $q(n)$ tal que $\mathcal{A}^{\mathcal{O}(\cdot)}(1^n) = 1$ se e somente se $\mathcal{A}$ encontra uma colisão na função $\mathcal{O} : \{0, 1\}^n \rightarrow \{0, 1\}^n$. Usando o Lema A.15 do livro, argumente que, se $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ é uma função aleatória, então: ¹

$$\Pr [\mathcal{A}^{f(\cdot)}(1^n) = 1] \leq \frac{q(n)^2}{2^{n+1}}.$$

- (b) Usando o fato de que F é pseudoaleatória, conclua que existe uma função negligenciável negl tal que

$$\Pr [\mathcal{A}^{F_k(\cdot)}(1^n) = 1] \leq \text{negl}(n).$$

2. Prove que o modo de operação CTR não é CCA-seguro.
3. **(Exercício 4.1 do livro, adaptado)** Considere um MAC $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ tal que, para uma chave $k \in \{0, 1\}^n$, Mac_k sempre tem como saída uma tag de tamanho $c \cdot \log_2 n$, onde c é uma constante. Prove que Π não pode ser um MAC seguro. ²
4. Considere uma variação de segurança CCA (que chamamos de segurança CCA-1) em que o adversário $\mathcal{A}$ só pode fazer consultas ao oráculo de decifragem **antes** de enviar um par de mensagens para o desafiante. Chamaremos este experimento de $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{cca-1}}(n)$. Neste exercício, vamos provar que a Construção 3.30, além de CPA-segura, ainda é CCA-1-segura.
 - (a) Seja $\tilde{\Pi}$ uma versão da cifra da construção 3.30 onde se usa uma função aleatória no lugar da função pseudoaleatória F . Fixe um adversário probabilístico polinomial $\mathcal{A}$ e considere o experimento $\text{PrivK}_{\mathcal{A}, \tilde{\Pi}}^{\text{cca-1}}(n)$. Defina $r^* \in \{0, 1\}^n$ como a string aleatória utilizada pelo desafiante para cifrar a mensagem de desafio m_b . Por fim, defina o evento Ruim como a união de dois eventos Repete e Repete', definidos a seguir:

¹Dica: como f é aleatória, a única maneira que $\mathcal{A}$ pode tentar extrair informação de f é através de consultas. Qual o máximo de consultas que $\mathcal{A}$ consegue realizar?

²Dica: Considere a probabilidade de adivinhar aleatoriamente uma tag válida.

- Repete é o evento de que, no experimento $\text{PrivK}_{A,\Pi}^{\text{cca-1}}(n)$, o desafiante usa r^* como string aleatória para cifrar alguma mensagem consultada por $\mathcal{A}$, antes ou depois de $\mathcal{A}$ receber o texto cifrado de desafio do desafiante. Esse é o mesmo evento considerado na demonstração da aula 10.
- Repete' é o evento de que, no experimento $\text{PrivK}_{A,\Pi}^{\text{cca-1}}(n)$, o adversário envia para o desafiante alguma consulta de decifragem do tipo $\langle r^*, \cdot \rangle$ **antes** de receber o texto cifrado de desafio do desafiante.

Prove que $\Pr[\text{Ruim}] \leq \frac{q(n)}{2^{n-1}}$ e que $\Pr[\text{PrivK}_{A,\Pi}^{\text{cca-1}}(n) \mid \overline{\text{Ruim}}] = 1/2$, onde $q(n)$ é um limite para o número de consultas de cifragem/decifragem que $\mathcal{A}$ realiza. Conclua então que

$$\Pr \left[\text{PrivK}_{A,\Pi}^{\text{cca-1}}(n) = 1 \right] \leq \frac{1}{2} + \frac{q(n)}{2^{n-1}}.$$

- (b) Usando o fato de que F é uma função pseudoaleatória, prove que existe uma função negligenciável negl tal que:

$$\left| \Pr \left[\text{PrivK}_{A,\Pi}^{\text{cca-1}}(n) = 1 \right] - \Pr \left[\text{PrivK}_{A,\Pi}^{\text{cca-1}}(n) = 1 \right] \right| \leq \text{negl}(n).$$

Conclua então que a Construção 3.30 é CCA-1-segura.

5. **(Exercício 5.3 do livro, adaptado)** Seja (Gen, H) uma função hash resistente à colisões, e defina $(\text{Gen}, \hat{H})$ como $\hat{H}^s(x) \doteq H^s(H^s(x))$. A função $(\text{Gen}, \hat{H})$ é também resistente à colisões? Justifique sua resposta.

Exercícios para pós-graduação

6. **(Exercício 2.8 do livro, adaptado).**

- (a) Modifique o experimento $\text{PrivK}_{A,\Pi}^{\text{mult}}(n)$ de maneira a capturar uma noção de indistinguibilidade para múltiplas mensagens *distintas*. Isto é, o esquema não precisa ser seguro caso a mesma mensagem seja cifrada duas ou mais vezes.
- (b) Considere a seguinte cifra simétrica $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ para espaço de mensagens $\{0, 1\}^n$ baseada em uma permutação pseudoaleatória/cifra de bloco F :
 - $\text{Gen}(1^n)$ retorna uma chave k para F .
 - $\text{Enc}_k(m) = F_k(m)$.
 - $\text{Dec}_k(c) = F_k^{-1}(c)$.

Mostre que Π respeita à sua definição de segurança do item anterior.

7. Considere um MAC $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ tal que, para parâmetro de segurança n , Gen produz uma chave k aleatória em $\{0, 1\}^n$, e Mac_k é aleatorizado, produzindo tags para mensagens de tamanho n usando n bits aleatórios. Considere ainda uma função chaveada $F : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$.

- (a) Usando F e Π , construa um novo MAC $\Pi' = (\text{Gen}', \text{Mac}', \text{Vrfy}')$ tal que Mac' é determinístico.
- (b) Prove que, se Π é um MAC seguro e F uma função pseudoaleatória, então Π' também é um MAC seguro.

Exercícios opcionais

8. Prove que o modo de operação ECB não é nem EAV-seguro.
9. Usei a cifra da construção 3.17 (que usa um gerador pseudoaleatório para obter o *pad* do one-time pad) para cifrar um inteiro de 8 bits que contém a nota de um aluno (fictício) que atingiu uma média entre 10 e 20, e este é o resultado: 10110101. Modifique este texto cifrado para refletir a nota de um aluno que foi aprovado.
10. Considere os seguintes PRGs (o mesmo com dois parâmetros de segurança diferentes): $G_n : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$ e $G_{2n} : \{0, 1\}^{2n} \rightarrow \{0, 1\}^{4n}$. Prove que $G_{2n}(G_n(\cdot))$ também é um PRG usando o método híbrido.
11. Sejam $F : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^*$ e $P : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^*$ uma função e uma permutação pseudoaleatória, respectivamente, ambas preservando o tamanho da entrada. Prove que, para qualquer distinguidor probabilístico polinomial D , existe uma função negligenciável negl tal que

$$|\Pr [D^{F_k(\cdot)}(1^n) = 1] - \Pr [D^{P_k(\cdot)}(1^n) = 1]| \leq \text{negl}(n).$$

12. Considere uma função hash (Gen, H) tal que, para uma chave $s \in \{0, 1\}^n$, o tamanho da saída de H^s é $c \cdot \log_2 n$, onde c é uma constante fixa. Prove que (Gen, H) não pode ser uma função hash resistente à colisões.
13. **Desafio.** Assuma que existe um PRG G com esticamento $\ell(n) = n + 1$. Prove, usando o método híbrido, que existe um PRG G' com esticamento $\ell'(n) = n + 2$. Modifique sua prova para mostrar que, para qualquer polinômio p , existe um PRG G_p com esticamento $p(n)$.
14. **Desafio.** Seja p um número primo e $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$. Considere a família de funções $\mathcal{H}$ composta por funções $h_{a,b} : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ parametrizadas por $a, b \in \mathbb{Z}_p$ tal que $h_{a,b}(x) = ax + b \pmod{p}$.

- (a) Prove que $\mathcal{H}$ é uma função hash (não criptográfica) 2-universal. Ou seja, prove que

$$\Pr[h_{a,b}(x_1) = y_1 \wedge h_{a,b}(x_2) = y_2] = \frac{1}{p^2},$$

onde $x_1 \neq x_2 \in \mathbb{Z}_p$ e $y_1, y_2 \in \mathbb{Z}_p$, e a probabilidade é sobre a escolha aleatória de $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$.

- (b) Seja $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ o seguinte MAC para o espaço de mensagens $\mathcal{M} = \mathbb{Z}_p$:

- **Gen** tem como saída (a, b) escolhidos de maneira aleatória em $\mathbb{Z}_p \times \mathbb{Z}_p$.
- **Mac** _{(a,b)} $(m) = h_{a,b}(m)$ para $m \in \mathbb{Z}_p$.
- **Vrfy** _{a,b} (m, t) verifica se $t = \text{Mac}_{(a,b)}(m)$, respondendo 1 caso sim e 0 caso contrário.

Considere uma variação do experimento **Mac-forge** _{$\mathcal{A}, \Pi$} (n) , que chamaremos de **Mac-forge** _{$\mathcal{A}, \Pi$} ^{1-time}, em que o adversário deve fazer apenas uma consulta m' para o desafiante antes de produzir um par (m, t) tal que $m \neq m'$ e **Vrfy** _{a,b} $(m, t) = 1$. Prove que para **todo** adversário $\mathcal{A}$ (mesmo adversários que rodam em tempo mais que polinomial):

$$\Pr[\text{Mac-forge}_{\mathcal{A}, \Pi}^{\text{1-time}} = 1] \leq \frac{1}{p}.$$