CI1355 / INFO7056: Tópicos em Algoritmos - Fundamentos da Criptografia 2026

Terceira 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 LaTeX) por um dos membros até às 23:59 do dia 03/12. A entrega pode ser feita por e-mail (*nmsdroievski[arroba]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 $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$, onde p é um número primo. Usando os resultados vistos em sala, prove que $\mathbb{Z}_p^*$ forma um grupo com a operação de multiplicação módulo p.

2. **(Exercício 10.3 do livro, adaptado)**. Descreva um ataque "Man-in-the-middle" para o protocolo de troca de chaves de Diffie-Hellman. No fim do protocolo, o adversário deve ter compartilhado uma chave k_A com Alice e uma chave k_B com Bob, potencialmente diferente de k_A, e Alice e Bob não detectam o que ocorreu.

3. Seja $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ uma cifra de chave pública que é CPA-segura com espaço de mensagens $\{0,1\}^n$ para parâmetro de segurança n. Neste exercício, vamos mostrar que "o jeito óbvio" de estender Π para mensagens de tamanho $\{0,1\}^{2n}$ é também CPA-seguro. Em particular, vamos mostrar que a cifra $\Pi' = (\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$ onde $\mathsf{Enc}'_{pk}((m_1, m_2)) = (\mathsf{Enc}_{pk}(m_1), \mathsf{Enc}_{pk}(m_2))$ e $\mathsf{Dec}'_{sk}((c_1, c_2)) = (\mathsf{Dec}_{sk}(c_1), \mathsf{Dec}_{sk}(c_2))$ é também CPA-segura.

   Para a demonstração, usaremos o método híbrido, com três experimentos híbridos baseados no experimento $\mathsf{PubK}^{\mathsf{eav}}_{\Pi',\mathcal{A}}(n)$ (lembre que uma cifra de chave pública EAV-segura é também CPA-segura) definidos a seguir:

   - E_{00} é idêntico ao experimento $\mathsf{PubK}^{\mathsf{eav}}_{\Pi',\mathcal{A}}(n)$, porém o desafiante, ao receber as mensagens de desafio $(m_{0,0}, m_{0,1})$ e $(m_{1,0}, m_{1,1})$, sempre retorna $\mathsf{Enc}'_{pk}(m_{0,0}, m_{0,1})$.
   - E_{01} é também idêntico ao experimento $\mathsf{PubK}^{\mathsf{eav}}_{\Pi',\mathcal{A}}(n)$, porém o desafiante sempre retorna $\mathsf{Enc}'_{pk}(m_{0,0}, m_{1,1})$. Isto é, o desafiante produz um texto cifrado que corresponde à primeira metade da primeira mensagem e à segunda metade da segunda mensagem.
   - E_{11} é também idêntico ao experimento $\mathsf{PubK}^{\mathsf{eav}}_{\Pi',\mathcal{A}}(n)$, porém o desafiante sempre retorna $\mathsf{Enc}'_{pk}(m_{1,0}, m_{1,1})$.

   Perceba que o experimento E_{01} não corresponde à uma situação que de fato possa ocorrer no experimento $\mathsf{PubK}^{\mathsf{eav}}_{\Pi',\mathcal{A}}(n)$. Ainda assim, nada nos impede de analisar o comportamento de $\mathcal{A}$ nessa situação (e essa análise é útil para nossa demonstração).

   (a) Defina p_{00}, p_{01} e p_{11} como a probabilidade de que o adversário $\mathcal{A}$ responda $b' = 1$ no experimento E_{00}, E_{01} e E_{11}, respectivamente.

Argumente que

$$\Pr[\mathsf{PubK}^{\mathsf{eav}}_{\Pi',\mathcal{A}}(n) = 1] = \frac{1}{2} + \frac{1}{2} \cdot (p_{11} - p_{00})$$

(b) Prove, a partir da segurança de Π, que existe uma função negligenciável negl tal que

$$|p_{01} - p_{00}| \leq \mathsf{negl}(n).$$

Dica. Apresente uma redução que transforma um adversário $\mathcal{A}$ para o qual $|p_{01} - p_{00}| = \varepsilon$ em um adversário $\mathcal{A}'$ que possui vantagem similar para quebrar a segurança de Π.

Explique, de maneira sucinta, como a sua demonstração pode ser adaptada para provar também que existe uma função negligenciável negl tal que

$$|p_{11} - p_{01}| \leq \mathsf{negl}(n).$$

(c) Argumente que Π' é CPA-segura.

Dica. Use a seguinte propriedade de diferenças modulares:

$$|a - c| = |a - b + b - c| \leq |a - b| + |b - c|.$$

4. **(Exercício 12.4 do livro, adaptado)**. Considere o seguinte experimento de segurança para assinaturas digitais: um adversário probabilístico polinomial $\mathcal{A}$ recebe uma chave pública $\langle N, e\rangle$ e uma mensagem $m \leftarrow \mathbb{Z}_N^*$ escolhida de maneira uniforme, e produz uma "assinatura" σ. O adversário vence se σ é uma assinatura válida para m. Perceba que o adversário não pode realizar nenhuma consulta de assinatura.

   Assumindo que o problema RSA é difícil, mostre que, para o esquema de assinatura RSA básico que vimos em sala obedece ao seguinte: para todo adversário probabilístico polinomial $\mathcal{A}$ existe uma função negligenciável negl tal que

$$\Pr[\mathcal{A}(\langle N, e\rangle, m) \text{ vence no experimento}] \leq \mathsf{negl}(n).$$

   Onde n é o parâmetro de segurança usado para gerar a chave $\langle N, e\rangle$ e a aleatoriedade é sobre as escolha de $\langle N, e\rangle$, m e sobre a aleatoriedade de $\mathcal{A}$.

Exercícios para pós-graduação

5. Prove o Teorema 12.4 (página 444) do livro. Em mais detalhes, prove que, caso Π seja um esquema de assinatura seguro para mensagem de tamanho ℓ e Π_H uma função hash resistente à colisões com tamanho de entrada arbitrário e tamanho de saída ℓ, então a Construção 12.3 é um esquema de assinatura seguro para mensagens de tamanho arbitrário.

   Dica. A demonstração é quase idêntica à demonstração do Teorema 5.6, que vimos na aula 16.

Exercícios opcionais

6. Considere a seguinte cifra simétrica $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ com espaço de chaves, de mensagens e de textos cifrados iguais a um grupo finito $\mathbb{G}$.

   - Gen tem como saída um elemento uniforme k de $\mathbb{G}$.
   - $\mathsf{Enc}_k(g) = kg$.
   - $\mathsf{Dec}_k(c) = k^{-1}c$.

   Prove que:

   (a) A cifra é correta, isto é, $\mathsf{Dec}_k(\mathsf{Enc}_k(g)) = g$ para todos $g, k \in \mathbb{G}$.

   (b) A cifra é perfeitamente secreta.

7. Mostre que, se a hipótese do logaritmo discreto para um algoritmo de geração de grupo $\mathcal{G}$ é verdadeira, então existe uma função unidirecional.

8. Seja $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ uma cifra de chave pública determinística com espaço de mensagens $\mathcal{M}_n$ para parâmetro de segurança n. Apresente um ataque de tempo $|\mathcal{M}_n| \cdot \mathsf{poli}(n)$ que, ao receber uma chave pública pk e um texto cifrado $c \leftarrow \mathsf{Enc}_{pk}(m)$, recupera a mensagem original m com probabilidade 1.

9. Seja $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ um esquema de assinatura com assinaturas para o qual existe uma constante c tal que o esquema sempre produz assinaturas de tamanho $c \cdot \log_2 n$ com parâmetro de segurança n. Prove que Π não é seguro.

10. **Desafio.** Neste exercício, vamos provar que o problema do logaritmo discreto é aleatoriamente auto-redutível (*random self-reducible* em inglês). Por simplicidade, fixamos um grupo $\mathbb{G}$ de ordem q e um gerador $g \in \mathbb{G}$. Mostre que se existe um algoritmo aleatorizado polinomial $\mathcal{A}$ tal que

$$\Pr[\mathcal{A}(g^x) = x] \geq \varepsilon,$$

    onde a aleatoriedade é sobre a aleatoriedade de $\mathcal{A}$ e uma escolha aleatória de $x \in \mathbb{Z}_q$, então existe um algoritmo aleatorizado polinomial $\mathcal{A}'$ tal que, para todo $x \in \mathbb{Z}_q$,

$$\Pr[\mathcal{A}'(g^x) = x] \geq \varepsilon,$$

    onde a probabilidade é **apenas** sobre a aleatoriedade de $\mathcal{A}'$.

    Adicionalmente, mostre que, se $\varepsilon \geq 1/p(n)$ para algum polinômio p (onde $n = |q|$), então é possível modificar $\mathcal{A}'$ para que ainda execute em tempo polinomial e tenha probabilidade de sucesso 0.99.

11. **Desafio.** Considere a seguinte variação da Definição 10.1 da aula 19 (sobre a segurança de protocolos de troca de chaves). No experimento, o adversário $\mathcal{A}$ recebe apenas o parâmetro de segurança 1^n e a transcrição trs da execução do protocolo Π entre Alice e Bob, e deve tentar produzir como saída a chave k que Alice e Bob geraram no fim da execução do protocolo. Dizemos que o protocolo Π é "mais ou menos seguro" se, para todo adversário $\mathcal{A}$,

existe uma função negligenciável negl tal que a probabilidade do adversário acertar a chave k é no máximo negl.

Assumindo a dificuldade da versão de **busca** do problema de Diffie-Hellman para um algoritmo de geração de grupos $\mathcal{G}$, apresente um protocolo de troca de chaves Π e uma cifra simétrica Π' tal que Π é um protocolo "mais ou menos seguro" e Π' é EAV-segura. Ainda assim, existe um adversário $\mathcal{A}$ que, ao receber como entrada a transcrição trs da execução do protocolo Π (que produz uma chave k) e um texto cifrado $c \leftarrow \mathsf{Enc}_k(m)$, consegue recuperar m com probabilidade 1.

Dica 1. Você pode assumir que é possível extrair uma chave binária de tamanho n de um elemento $g \in \mathbb{G}$ tal que $\mathbb{G}$ foi produzido a partir de $\mathcal{G}(1^n)$ (assim como fizemos em sala de aula).

Dica 2. É possível escolher Π' como uma variação do one-time pad que usa apenas uma parte da chave (por exemplo, com chaves de tamanho $2n$ e mensagens de tamanho n).

12. **Desafio.** Estenda a demonstração do exercício 3 para o caso em que uma variação de Π' é usada para cifrar/decifrar mensagens de tamanho arbitrário (porém ainda múltiplos de n).

    Dica. A demonstração é quase idêntica à do Teorema 11.6 no livro (página 383).