Henrique Tsuyoshi Yara
11796083

Prova 1

MAC0336 - Routo Terada
13 de outubro de 2021

Exercício 1

1.A.1

Resolução.
Parâmetros do *Decripto*

1. 64 é o número de bits em cada variável (i.e., cada posição de memória);
2. 12 é o número de iterações (rounds);
3. 8 é o número de bytes na chave.

1.A.2

Resolução.
Operações básicas:

1. $v \boxplus u$ é a soma dos inteiros v,u de 64 bits, resultando um valor de 64 bits (*i.e.*, soma mod 264);
2. $v \oplus u$ é o ou-exclusivo (XOR) de v,u de 64 bits, resultando um valor de 64 bits;
3. $v \gg t$ é o deslocamento circular (i.e., rotação) de t posições para a direita dos bits em v.

1.A.3

Resolução.
Algoritmo Decripto
Entrada: chave de 8 bytes, texto criptografado de 2×64 bits (A, B);
Saída: legível de 2×64 bits (A, B);

1. Calcular $2 \times 12 + 2$ subchaves $K_0, K_1, K_2, ...K_{2\times12+1}$ (* Usando o algoritmo dado *)
2. **para** $i = K_{2\times12+1}, K_{2\times12}, K_{2\times11+1}, ...K_0$:
   Achar K_i^{-1}, tal que
   $K_i \boxplus K_i^{-1} == 0$
   $\overline{K_i} \leftarrow K_i^{-1}$

3. **para** $j = 12, 11, 10, ...1$ **faça**:
   $B \leftarrow ((A \boxplus \overline{K_{2j+1}}) \gg A) \oplus A$;$A \leftarrow ((A \boxplus \overline{K_{2j}}) \gg B) \oplus B$
4. $B \leftarrow B \boxplus \overline{K_1}$;$A \leftarrow A \boxplus \overline{K_0}$
5. A saída é o valor (A, B)

1.B

Sendo (A', B') os textos ilegíveis, (A, B) os textos legíveis e $overline K_0, overline K_1, overline K_2, ...overline K$ as subchaves complementares às subchaves $K_0, K_1, K_2, ...K_{2\times12+1}$ em relação à $\boxplus$:
Provando uma iteração:

1. $B' = ((B \oplus A) \ll A) \boxplus K_{2_j+1}$
2. $B' \boxplus \overline{K_{2_j+1}} = (((B \oplus A) \ll A) \boxplus K_{2_j+1}) \boxplus \overline{K_{2_j+1}}$
3. $B' \boxplus \overline{K_{2_j+1}} = ((B \oplus A) \ll A)$
4. $(B' \boxplus \overline{K_{2_j+1}}) \gg A = ((B \oplus A) \ll A) \gg A$
5. $(B' \boxplus \overline{K_{2_j+1}}) \gg A = (B \oplus A)$
6. $((B' \boxplus \overline{K_{2_j+1}}) \gg A) \oplus A = (B \oplus A) \oplus A$
7. $((B' \boxplus \overline{K_{2_j+1}}) \gg A) \oplus A = B$

1. $A' = ((A \oplus B) \ll B) \boxplus K_{2j}$
2. $A' \boxplus \overline{K_{2j}} = (((A \oplus B) \ll B) \boxplus K_{2j}) \boxplus \overline{K_{2j}}$
3. $A' \boxplus \overline{K_{2j}} = ((A \oplus B) \ll B)$
4. $(A' \boxplus \overline{K_{2j}}) \gg B = ((A \oplus B) \ll B) \gg B$
5. $(A' \boxplus \overline{K_{2j}}) \gg B = (A \oplus B)$
6. $((A' \boxplus \overline{K_{2j}}) \gg B) \oplus B = (A \oplus B) \oplus B$
7. $((A' \boxplus \overline{K_{2j}}) \gg B) \oplus B = A$

A operação inicial antes das iterações:

1. $B' = B \boxplus K_1$

2. $(B' \boxplus \overline{K_1}) = B \boxplus K_1 \boxplus \overline{K_1})$
3. $(B' \boxplus \overline{K_1}) = B \boxplus K_1$

1. $A' = A \boxplus K_0$
2. $(A' \boxplus \overline{K_0}) = A \boxplus K_0 \boxplus \overline{K_0})$
3. $(A' \boxplus \overline{K_0}) = B \boxplus K_0$

□

2

2.1

Calcular T para $p = 7$, $S = 2$, e executar o Crip para $k = 3, x = 2$, obtendo (y, z)
Resolução.
T = 2, y = 6, z = 2

2.2

Justifique porque $k = 0$, e $k = 1$ devem ser evitados no Passo (1) do Crip.
Resolução.
$K = 0$ deve ser evitado, pois $z = xT^0$ então $z = x$ o texto vai ser enviado sem estar criptografado.
$K = 1$ deve ser evitado, pois T é público e é fácil descobrir T^{-1} e consequentemente descobrir x.

2.3

Resolução.
Algoritmo Decriptografia do Crip
Entrada (y, z) criptografados da alice

1. $y \leftarrow y^{-1}$
2. $y \leftarrow y^S$
3. $x \leftarrow z \times y$
4. A saída é o valor de x

2.4

Resolução.
Executando o algoritmo obtenho $x = 2$.

2.5

Resolução.

1. $z \times y^{-}S \mod p$
2. $xT^k \times y^{-}S \mod p$
3. $x(g^S)^k \times y^{-}S \mod p$
4. $x(g^S)^k \times (g^k)^{-}S \mod p$
5. $x(g^S)^k \times g^{-kS} \mod p$
6. $x(g^{Sk}) \times g^{-kS} \mod p$
7. $xg^{Sk} \times g^{-kS} \mod p$
8. $x \mod p$

2.6

Resolução.
Ele é mais rápido, pois ele consiste em uma exponenciação e uma inversa, enquanto a criptogrfia consiste em duas exponenciações.

2.7

Resolução.
A definição do problema que faz essa criptografia computacionalmente segura é o Problema do Logaritmo Discreto. Se esse problema fosse de fácil solução o atacante poderia descobrir o valor de k e assim descobrir o valor de T^k e descobrir x com a equação $z(T^{-}k)$.

2.8

Resolução.
A razão de existir o NONCE k no Passo 1 é que caso o atacante consiga x_1 e x_2 que foram criptografados com um mesmo k, é possível obter x_2 usando x_1 na equação:
$\frac{z_1}{z_2} = \frac{x_1}{x_2}$

2.9

2.10

Resolução.
Autenticação do Rementente de Y é o destinatário ter a certeza de quem foi que mandou a mensagem. Ela não garante a autenticação do remetente, pois qualquer um pode forjar e se passar por Beto.

2.11

Resolução.
Autenticação do Destinatário de Y é apenas a pessoa que recebeu a informação consiga ler a mensagem. Ela garante a Autenticação do Destinatário pois, a chave secreta S é conhecida apenas pela Alice.

2.12

Resolução.