Segurança da Informação – SIN

Prof. Pedro Carlos da Silva Lara
Instituto Superior de Tecnologia em Ciências da Computação de Petrópolis

Lista de Exercícios 2

1) Como é possível obter uma segurança perfeita em criptografia? (explique com suas palavras o one-time-pad)

2) Dada a entrada $(1002000008000004)_{16}$ de 64 bits no algoritmo de criptografia DES, obtenha o valor de saída na **Permutação Inicial** (*veja apêndice*).

3) Dadas as entradas $(010100)_2$, $(111001)_2$ e $(010011)_2$ de 6 bits na DES, obtenha o valor de saída na **S-Box1, S-Box2** e **S-Box3** respectivamente (*veja apêndice*).

4) Demonstre que na geração de subchaves do DES, se trocarmos o deslocamento circular para esquerda para o deslocamento circular para a direita e trocarmos o valor de L_1 para 0, as subchaves são geradas na ordem reversa (na decifragem do DES).

5) Defina efeito avalanche e efeito completude. Qual a importância na segurança de algoritmos de criptografia simétrica.

6) Considere 3 criptossistemas simétricos $E1_k(x), E2_k(x)$ e $E3_k(x)$ cuja entrada x é um bloco de 32 bits. Para cada um dos algoritmos, criptografamos dois textos legíveis:

$$x_1 = (00000000)_{16}$$

$$x_2 = (00000001)_{16}$$

Os 3 algoritmos usam 8 rodadas (*rounds*). Para estes textos planos, foram avaliados, em cada algoritmo, o número de bits diferentes em cada rodada na criptografia.

	Rodada							
Algoritmo	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
$E1_k(x)$	15	2	13	3	19	1	16	1
$E2_k(x)$	15	16	17	13	16	15	17	17
$E3_k(x)$	30	31	29	30	31	32	32	30

Número de bits diferentes em cada rodada para as entradas x_1 e x_2.

Qual algoritmo que melhor satisfaz o efeito avalanche? Por que? O algoritmo $E3_k(x)$ satisfaz o efeito avalanche?

7) Considere o algoritmo de criptografia $E_k(x)$ hipotético como segue abaixo:

Algorithm 1: Algoritmo de criptografia hipotético.

Entrada: Texto plano x de 32 bits e as chaves de rodada $\{k_1, k_2, \ldots, k_8\}$ cada uma com 32 bits
Saída: O criptograma y de 32 bits.
início
  $y \leftarrow x \oplus C$;
  para $i = 1$ **até** 8 **faça**
    $y \leftarrow y \oplus k_i$;
    $y \leftarrow y <<< 3$;
  retorna y;

Descreva o algoritmo de decriptografia $E_k^{-1}(y)$ onde C é uma constante de 32 bits dada.

8) Cite as vantagens e desvantagem dos dois modos de criptografia **ECB** (*Eletronic Code Book*) e **CBC** (*Cipher Block Chaining*).

Apêndice
DES: Permutação Inicial e S-Box (1, 2 e 3)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Permutação Inicial

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S-Box 1

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S-Box 2

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S-Box 3