Segurança da Informação – SIN

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

Lista de Exercícios 3

Questão 1) [Casa da Moeda – 2012] Na criptografia simétrica, um algoritmo utiliza uma chave para converter dados legíveis em dados sem sentido que permitem que um algoritmo (tipicamente o mesmo) utilize a mesma chave para recuperar os dados originais. Por questão de segurança, quando é necessário reutilizar as chaves simétricas em diferentes operações, deve-se usar a cifragem

a) de bloco
b) de fluxo
c) de enchimento
d) híbrida
e) invertida

Questão 2) O algoritmo de criptografia DES (*Data Encryption Standard*) projetado pela IBM e adotado como padrão do governo norte americano em 1997, foi o primeiro algoritmo de criptografia cujo o seu conhecimento se tornou público. Uma das principais críticas ao algoritmo DES encontra-se no segredo mantido no projeto das S-Boxes. Os usuários do DES não possuem qualquer garantia que não existam pontos vulneráveis nas S-Boxes. Com relação ao algoritmo DES responda as questões abaixo:

a) Qual é o tamanho do bloco de entrada (em *bits*)?
b) Quantas rodadas possui?
c) Qual é o tamanho da chave (sem os *bits* de paridade)?
d) Qual é a saída, na S-Box1 (veja apêndice), cuja a entrada é o valor $(010101)_2$?
e) Quais são as entradas cuja a saída, na S-Box1 (veja apêndice), é o valor $(0011)_2$?

Questão 3) [**Perito Criminal - PCERJ (2008)**] Analise as características dos protocolos criptográficos abaixo:

I. **PTCL01** – Derivado de um algoritmo assimétrico, é amplamente utilizado na geração de assinatura digital, sendo sua segurança baseada na dificuldade da fatoração de números grandes.

II. **PTCL02** – Derivado de um algoritmo simétrico, permite cerca de 2^{56} combinações, seu tamanho de chave de 56 bits é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na Internet.

Esses protocolos **PTCL01** e **PTCL02** são conhecidos respectivamente, por:

a) RSA e SSL.
b) MD5 e SSL.
c) RSA e SHA-1.
d) MD5 e DES.
e) RSA e DES.

Questão 4) Em outubro de 2000 o NIST (*National Institute of Standards and Technology*) anunciou o novo padrão de criptografia simétrica do governo norte-americano, o AES (*Advanced Encryption Standard*). Este algoritmo veio a substituir o DES. Considerando o algoritmo AES, aplique a operação de *SubBytes* (veja apêndice) no bloco abaixo :

2A	F7	10	B2
43	96	E7	19
1A	62	08	9B
21	18	17	70

Após a aplicação da operação de *SubBytes* obtenha o resultado da operação de *ShiftRows*.

5) Considere a chave a seguinte chave de 128 bits do algoritmo AES abaixo:

6B	74	11	09
7F	6A	E7	12
B0	00	11	03
02	09	E0	70

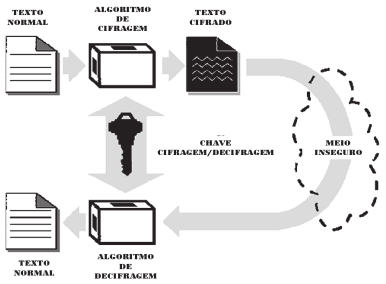
Obtenha a primeira coluna da chave de rodada 1 (Veja a tabela Rcon em anexo)

6) Que algoritmo de criptografia simétrica foi escolhido como padrão AES (Advanced Encryption Standard)?

a) RSA
b) 3DES
c) Rijndael

d) Blowfish
e) Diffie-Hellman

Questão 7) [**Perito Criminal - PCERJ (2008)**] Analise a figura abaixo, que ilustra o funcionamento de um processo criptográfico.



Assinale a alternativa em que se apresente um algoritmo que empregue o esquema acima e o nome pelo qual esse processo criptográfico é conhecido.

a) ElGamal e Criptografia de Chave Assimétrica
b) ElGamal e Criptografia de Chave Simétrica
c) AES e Criptografia de Chave Assimétrica
d) AES e Criptografia de Chave Simétrica
e) ICP (Infraestrutura de Chave Pública) e Criptografia de Chave Simétrica

8) Descreva o processo de decifragem de uma mensagem criptograda $c_1, c_2, \ldots, c_L$ usando o modo **CBC**.

9) O algoritmo de hash SHA-256 aplicado à frase "Para que o mal triunfe, basta que os bons não façam nada."produz como resultado

a) strings diferentes de tamanho variável conforme a semente aleatória utilizada.
b) uma string que permite a recuperação do texto original.
c) sempre a mesma string de tamanho fixo.
d) diferentes strings de 256 KB conforme a semente aleatória utilizada.
e) `2dd30740a31cd09b6e4a8ec08bc4b6d540084a2e` (40 dígitos hexadecimais).

Questão 10) O resumo de mensagem é produzido, de forma geral, por algoritmos que recebem qualquer comprimento de informação de entrada para produzir uma saída pseudoaleatória de largura fixa chamada digest. Uma de suas principais propriedades, chamada efeito avalanche, visa a garantir que

a) pequenas variações na informação de entrada produzam digests iguais.
b) pequenas variações na informação de entrada produzam digests diferentes.
c) grandes variações na informação de entrada produzam digests iguais.
d) grandes variações na informação de entrada produzam digests mais seguros.
e) pequenas e grandes variações na informação de entrada produzam digests iguais.

Questão 11) [**Perito Criminal Federal - PF (2002)**] Um sistema criptográfico é constituído por uma tripla $(\mathcal{M}, \mathcal{K}, \mathcal{C})$, em que $\mathcal{M}$ é o espaço das mensagens, $\mathcal{K}$ é o espaço das chaves, e $\mathcal{C}$ é o espaço dos criptogramas. Associado a esses, tem-se um algoritmo criptográfico, o qual transforma qualquer mensagem $m \in \mathcal{M}$ em um criptograma $c \in \mathcal{C}$, de forma controlada por uma chave $k \in \mathcal{K}$. Pode- se representar essa transformação por $c = E_k(m)$, que corresponde à operação de cifração, e por $m = D_k(c)$, a operação inversa, de decifração. A respeito de sistemas criptográficos em geral, julgue a seguir. os itens subseqüentes.

- Sistemas criptográficos são ditos simétricos ou de chave secreta quando a chave utilizada para cifrar é a mesma utilizada para decifrar. Sistemas assimétricos ou de chave pública utilizam chaves distintas para cifrar e decifrar. Algoritmos simétricos são geralmente mais eficientes computacionalmente que os assimétricos e por isso são preferidos para cifrar grandes massas de dados ou para operações online.
- Diz-se que um sistema criptográfico tem segredo perfeito quando, dado um criptograma c, a incerteza que se tem em relação à mensagem m que foi cifrada é a mesma que se tinha antes de conhecer o criptograma. Uma condição necessária para que um sistema criptográfico tenha segredo perfeito é que o espaço de chaves seja pelo menos tão grande quanto o espaço de mensagens, ou seja, $|\mathcal{K}|$ e $|\mathcal{M}|$.
- Uma técnica eficiente para tornar um sistema criptográfico mais forte é se utilizar um algoritmo de compressão de dados após a cifração.
- Em um determinado sistema criptográfico, para cada mensagem possível m, existe apenas um criptograma possível, c, que será o resultado da cifração de m com determinada chave k. Não obstante, mensagens distintas podem resultar em um mesmo criptograma, se utilizadas chaves distintas.

Assinale a alternativa correta para as respectivas afirmações (**V** verdadeiro e **F** falso).

a) V–V–F–F
b) V–F–V–F
c) F–F–V–F
d) F–V–F–V
e) V–V–F–V

	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

DES S-Box 1

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

AES S-Box

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

AES Rcon