Rede de Computadores

Lista de Exercícios Nº 2 - Semestre 2017.2
Prazo final para entrega: 05/04/2018
Prof.: Edmar José do Nascimento

1. Explique a diferença entre os sistemas de criptografia simétrica e assimétrica.

2. Por que se recorre a uma criptografia simétrica como o AES ao invés de se usar uma criptografia assimétrica como o RSA em todo o processo de criptografia?

3. Faça uma pesquisa e diga quais são as quantidades de bits usadas atualmente nos números p, q e n a fim de produzir as chaves pública e privada usando o algoritmo RSA. Essa quantidade de bits já foi menor? Explique.

4. Faça uma pesquisa e explique as falhas que foram descobertas na cifra de fluxo RC4 e quais foram as suas implicações na segurança de protocolos como o WEP usado em redes sem fio.

5. Por que se usa um vetor de inicialização (IV) diferente para cada sessão em um encadeamento de cifras de bloco (CBC)?

6. Qual é o papel de uma autoridade certificadora no processo de criptografia? Quais são os riscos de se usar uma chave não certificada?

7. Considere uma mensagem criptografada c de 9 bytes de comprimento, cuja representação em ASCII estendido é dada por c=`Kçz0Bzxu1` (4B 87 7A 30 42 7A 78 75 31 em hexadecimal ou 75 135 122 48 66 122 120 117 49 em decimal, assim como pode ser verificado na tabela ASCII em anexo). Sabe-se que na criptografia foi usada uma cifra de bloco, na qual blocos de 2 bits foram mapeados para blocos de 2 bits e que o texto aberto corresponde a uma mensagem escrita em língua portuguesa. De posse dessas informações:

   (a) Enumere as 24 possibilidades de mapeamento possíveis para a chave secreta.

   (b) Use a técnica de força bruta para obter a chave secreta usada na criptografia e o texto aberto (mensagem enviada por Alice para Bob).

Decimal	Binário	Hex	Referência
0	00000000	00	Null - NUL
1	00000001	01	Start of Heading - SOH
2	00000010	02	Start of Text - STX
3	00000011	03	End of Text - ETX
4	00000100	04	End of Transmission - EOT
5	00000101	05	Enquiry - ENQ
6	00000110	06	Acknowledge - ACK
7	00000111	07	Bell, rings terminal bell - BEL
8	00001000	08	BackSpace - BS
9	00001001	09	Horizontal Tab - HT
10	00001010	0A	Line Feed - LF
11	00001011	0B	Vertical Tab - VT
12	00001100	0C	Form Feed - FF
13	00001101	0D	Enter - CR
14	00001110	0E	Shift-Out - SO
15	00001111	0F	Shift-In - SI
16	00010000	10	Data Link Escape - DLE
17	00010001	11	Device Control 1 - D1
18	00010010	12	Device Control 2 - D2
19	00010011	13	Device Control 3 - D3
20	00010100	14	Device Control 4 - D4
21	00010101	15	Negative Acknowledge - NAK
22	00010110	16	Synchronous idle - SYN
23	00010111	17	End Transmission Block - ETB
24	00011000	18	Cancel line - CAN
25	00011001	19	End of Medium - EM
26	00011010	1A	Substitute - SUB
27	00011011	1B	Escape - ESC
28	00011100	1C	File Separator - FS
29	00011101	1D	Group Separator - GS
30	00011110	1E	Record Separator - RS
31	00011111	1F	Unit Separator - US
32	00100000	20	Space - SPC
33	00100001	21	!
34	00100010	22	"
35	00100011	23	#
36	00100100	24	$
37	00100101	25	%
38	00100110	26	&
39	00100111	27	'
40	00101000	28	(
41	00101001	29	)
42	00101010	2A	*
43	00101011	2B	+
44	00101100	2C	,
45	00101101	2D	-
46	00101110	2E	.
47	00101111	2F	/
48	00110000	30	0
49	00110001	31	1
50	00110010	32	2
51	00110011	33	3
52	00110100	34	4
53	00110101	35	5
54	00110110	36	6
55	00110111	37	7
56	00111000	38	8
57	00111001	39	9
58	00111010	3A	:
59	00111011	3B	;
60	00111100	3C	<
61	00111101	3D	=
62	00111110	3E	>
63	00111111	3F	?
64	01000000	40	@
65	01000001	41	A
66	01000010	42	B
67	01000011	43	C
68	01000100	44	D
69	01000101	45	E
70	01000110	46	F
71	01000111	47	G
72	01001000	48	H
73	01001001	49	I
74	01001010	4A	J
75	01001011	4B	K
76	01001100	4C	L
77	01001101	4D	M
78	01001110	4E	N
79	01001111	4F	O
80	01010000	50	P
81	01010001	51	Q
82	01010010	52	R
83	01010011	53	S
84	01010100	54	T
85	01010101	55	U
86	01010110	56	V
87	01010111	57	W
88	01011000	58	X
89	01011001	59	Y
90	01011010	5A	Z
91	01011011	5B	[
92	01011100	5C	\
93	01011101	5D	]
94	01011110	5E	^
95	01011111	5F	_
96	01100000	60	`
97	01100001	61	a
98	01100010	62	b
99	01100011	63	c
100	01100100	64	d
101	01100101	65	e
102	01100110	66	f
103	01100111	67	g
104	01101000	68	h
105	01101001	69	i
106	01101010	6A	j
107	01101011	6B	k
108	01101100	6C	l
109	01101101	6D	m
110	01101110	6E	n
111	01101111	6F	o
112	01110000	70	p
113	01110001	71	q
114	01110010	72	r
115	01110011	73	s
116	01110100	74	t
117	01110101	75	u
118	01110110	76	v
119	01110111	77	w
120	01111000	78	x

Figura 1: Tabela ASCII