EXERCÍCIOS

1. Explique resumidamente o funcionamento das ferramentas abaixo:
   a. `setoolkit`
   b. `caesar`
   c. `ccdecrypt`

2. Qual é a relação entre a frase "*O hambúrguer não pode voltar para a vaca*" e *hashes* criptográficos? Assuma que o hambúrguer foi produzido com a carne da vaca.

3. Sabendo que a expressão "AFNWJLW W KGES ME" foi criptografada utilizando a Cifra de César, informe o texto original e a chave utilizada no processo de cifragem.

4. Utilizando a Cifra de Vigenère e a chave "LISTA", decifre a mensagem "BCWLTLW".

5. Decifre o texto abaixo, sabendo que ele foi cifrado com transposição alfabética e matriz 3x9.

   `OEOÉTNEOI IUMBTAUUC MNEEIESRA`

6. Preencha a tabela abaixo respondendo o que se pede.

TEXTO CLARO	TEXTO CIFRADO	QUAL É A CHAVE?	SIMÉTRICA OU ASSIMÉTRICA?
TASHKENK	LOFLITBU		
BAKU	VLBC		
KABUL	MVCBL		
ISLAMABAD	EBCBNBMTJ		
NAIROBI			

7. Quais são as vantagens e as desvantagens da criptografia assimétrica?

8. Assinale V para as verdadeiras e F para as falsas. Justifique as falsas.

( ) Não existe geração de par de chaves no algoritmo RSA.
( ) O RSA é seguro porque, tendo o valor de *p*, não é fácil obter o valor de *q*.
( ) O RSA é o substituto do MD5.
( ) Uma mensagem não pode ser cifrada com a chave privada.
( ) Uma mensagem não pode ser cifrada com a chave pública.

9. Para o par de chaves abaixo, gerado pelo algoritmo RSA, quais eram os valores de `p` e `q`, respectivamente?

Chave pública = (7, 33)
Chave privada = (3, 33)

10. (CESPE - ABIN/2010 - Agente Técnico de Inteligência - Área de Tecnologia da Informação) O algoritmo de criptografia RSA (Rivest, Shamir e Adleman) é embasado no conceito de chave simétrica. Certo ou Errado?

11. (Adaptado de FCC - TJ-PE/2012 - Técnico Judiciário - Suporte Técnico) Sobre o algoritmo RSA, considere:

I. O algoritmo é de característica simétrica, pois se dá pela utilização de chaves públicas e privadas.
II. O algoritmo oferece as funcionalidades de criptografia e assinatura digital de mensagens pela utilização de chaves públicas e privadas.
III. Baseia-se na utilização de números primos para a geração das chaves, sendo sua segurança garantida pela dificuldade atual de fatoração de grandes números.
Está correto o que se afirma em

a) I e II, apenas.
b) I, II e III.
c) I e III, apenas.
d) II e III, apenas.
e) III, apenas.

12. (FCC - TRT 4ª Região/2006 - Técnico Judiciário - Programação) A principal desvantagem do método RSA de criptografia é

a) a insegurança gerada pela fraqueza algorítmica.
b) não ser um algoritmo de chave pública.
c) a identidade algorítmica com o AES, porém menos preciso.

d) a lentidão causada pela exigência de chaves com muitos bits (> = 1024) para manter um bom nível de segurança.
e) o fato de utilizar o modo de cifra de fluxo.

13. (NC-UFPR - ITAIPU BINACIONAL/2017 - Professor de Computação ou Informática - Suporte) O desenvolvimento da criptografia de chave pública caracterizou uma revolução, permitindo a alteração do modelo de distribuição de chaves utilizado pela criptografia simétrica. A respeito de criptografia de chave pública, considere as seguintes afirmativas:

1. Tornou a criptografia simétrica obsoleta.
2. Por definição, a chave privada é a utilizada para descriptografar os dados.
3. Permite o uso de novos modelos de distribuição de chaves quando comparada à criptografia simétrica.

Assinale a alternativa correta.

a) Somente a afirmativa 3 é verdadeira.
b) Somente as afirmativas 1 e 2 são verdadeiras.
c) Somente as afirmativas 1 e 3 são verdadeiras.
d) Somente as afirmativas 2 e 3 são verdadeiras.
e) As afirmativas 1, 2 e 3 são verdadeiras.

14. José está aprendendo sobre o algoritmo RSA. Para cifrar mensagens com este algoritmo, resolveu escolher os seguintes valores:

- p = 139;
- q = 491;
- e = 67619;
- d = 67619.

a) Quais são os valores de n e $\phi(n)$?
b) Os valores escolhidos por José são adequados? Justifique.
c) Proponha alguma alteração nos valores escolhidos por José. Justifique.

15. Quando o algoritmo RSA não é seguro?

16. Considere o par de chaves abaixo, gerado com o algoritmo RSA, e decifre a mensagem “6355 5075”

Chave pública = (4947, 7597)

Chave privada = (3, 7597)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y