Números Inteiros e Criptografia — Segunda prova (parte 1) — 25/6/2019

A prova é individual e sem consulta. Responda as questões na folha de respostas, a lápis ou a caneta. Se tiver qualquer dúvida consulte o professor. Você pode usar livremente qualquer resultado visto em sala ou em listas de exercício, mas deve escrever claramente qual é o teorema/exercício/fato sendo usado. É **proibido** o uso de celular.

JUSTIFIQUE SUAS RESPOSTAS!

Questão 1. Para esta questão, use a codificação de símbolos da tabela abaixo.

(a) (½ ponto) Em um sistema RSA, sua chave pública (para encriptação) é $e = 9899$, $n = 15163 = 59 \cdot 257$ (sendo e o expoente de encriptação e n o módulo). Qual é a sua chave privada (para descriptação)?

(b) (½ ponto) Você recebe a mensagem encriptada `5184, 12603, 6404, 8004`. Qual é a mensagem descriptada?

(c) (½ ponto) A minha chave pública é $e = 3$, $n = 33$. Me envie uma mensagem que faça sentido.

código	*símb.*
11	0
12	1
13	2
14	3
15	4
16	5
17	6
18	7
19	8
21	9
22	.
23	,
24	!

código	*símb.*
25	?
26	:
27	;
28	"
29	(
31	)
32	+
33	-
34	*
35	/
36	=
37	_
38	A

código	*símb.*
39	B
41	C
42	D
43	E
44	F
45	G
46	H
47	I
48	J
49	K
51	L
52	M
53	N

código	*símb.*
54	O
55	P
56	Q
57	R
58	S
59	T
61	U
62	V
63	W
64	X
65	Y
66	Z
67	À

código	*símb.*
68	Á
69	Â
71	Ã
72	É
73	Ê
74	Í
75	Ó
76	Ô
77	Õ
78	Ú

Questão 2. (1½ pontos) Seja $(G, *)$ um grupo, seja n um inteiro positivo e defina um subconjunto $G[n]$ de G da seguinte forma:

$$G[n] = \{g \in G \,;\, g^n = e\},$$

onde e é o elemento neutro de $(G, *)$. Mostre que se $(G, *)$ for comutativo, i.e., se $x*y = y*x$ for verdadeiro para quaisquer $x, y \in G$, então $(G[n], *)$ é um subgrupo de $(G, *)$.

Questão 3. (1½ pontos) Bob quer enviar uma mensagem m para Alice, encriptada usando RSA. Como o canal de comunicação entre eles sofre muita interferência, para evitar erros na transmissão Alice decidiu usar RSA com *duas* chaves públicas (e_0, n) e (e_1, n), sendo e_0, e_1 os expoentes para encriptação e n o módulo. Alice pediu então para Bob enviar m duas vezes, uma encriptada com (e_0, n) e a outra com (e_1, n), para que ela possa descriptar ambas e conferir se o resultado é o mesmo.

Oscar, mal intencionado, intercepta as transmissões e descobre as mensagens encriptadas x_0 e x_1, correspondentes a m encriptada com (e_0, n) e (e_1, n) respectivamente. Se $\text{mdc}(e_0, e_1) = 1$, como Oscar pode descobrir m?

Números Inteiros e Criptografia — Segunda prova (parte 2) — 27/6/2019

A prova é individual e sem consulta. Responda as questões na folha de respostas, a lápis ou a caneta. Se tiver qualquer dúvida consulte o professor. Você pode usar livremente qualquer resultado visto em sala ou em listas de exercício, mas deve escrever claramente qual é o teorema/exercício/fato sendo usado. É **proibido** o uso de celular.

JUSTIFIQUE SUAS RESPOSTAS!

Questão 4. Dado um inteiro positivo n, o número $F_n = 2^{(2^n)} + 1$ é chamado de o *n-ésimo número de Fermat*. Assim, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$ e $F_4 = 2^{16} + 1 = 65\,537$ são primos, porém esses são os únicos n para os quais sabemos que F_n é primo. Dentre outras coisas, já se sabe também que F_n é composto para $5 \leq n \leq 32$.

(a) (1 ponto) Mostre o funcionamento da execução do algoritmo com entrada F_5 e base $b = 2$ (*teste de mesa*).

(b) (1 ponto) Mostre que é impossível concluir que um dado F_n qualquer é composto usando o Teste de Miller–Rabin com base $b = 2$.

Questão 5. (2 pontos) No *Manual de Aritmérica do Mestre Sun*, escrito em aprox. 300 d.C., consta o seguinte problema:

> Temos uma certa quantidade de coisas, mas não sabemos exatamente quantas. Se contadas de três em três, sobram duas; se contadas de cinco em cinco, sobram três; se contadas de sete em sete, sobram duas. Quantas coisas temos?

Qual a menor resposta para o problema, e qual fórmula gera todas as respostas?

Questão 6. Seja n o produto de dois primos ímpares distintos.

(a) (1 ponto) Suponha que x, y sejam inteiros positivos tais que

$$x^2 \equiv y^2 \pmod{n}, \qquad x \not\equiv y \pmod{n} \qquad \text{e} \qquad x \not\equiv -y \pmod{n}.$$

Mostre que $\mathrm{mdc}(x + y, n)$ e $\mathrm{mdc}(x - y, n)$ são os dois fatores primos de n.

Dica. $x^2 - y^2 = (x + y)(x - y)$.

(b) (1 ponto) Já vimos que se um inteiro positivo a qualquer tem alguma raiz quadrada módulo n, então ele tem *quatro* raízes quadradas distintas módulo n. Suponha que você tenha um algoritmo para calcular as quatro raízes quadradas módulo n de um a qualquer dado como entrada, quando essas raízes existem. Como você pode usar esse algoritmo (e possivelmente outros auxiliares) para fatorar n?

Dica. Primeiro, escolha um inteiro positivo a que *com certeza* tem raízes quadradas módulo n. Depois mostre que pelo menos duas dentre as quatro raízes quadradas de a têm que estar na situação da letra (a).

Foi um prazer tê-los como alunos esse semestre!