Nuno José Mendonça Madaleno - 45645 - MIEI Mark: 1.7/5 (total score: 1.7/5)

		+24/1/14+
	Departamento de Matemát Criptografia	ica Faculdade de Ciências e Tecnologia — UNL 8/7/2018 Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 2 2 2 2 2 3 3 3 3 3 4 4 4 4 4	← Marque o seu número de aluno preenchendo completamente os quadrados respectivos da grelha ao lado (■) e escreva o nome completo, o número e o curso abaixo. Nome: No
	88888	Curso: Número de aluno: \(\frac{1}{3645} \) O exame é composto por 10 questões de escolha múltipla. Nas questões marque a resposta certa preenchendo completamente o quadrado respectivo (\(\brace{\pi} \)) com caneta azul ou preta, cada resposta certa vale 0,5 valores, cada resposta errada desconta 0,2 valores e marcações múltiplas anulam a questão. Se a soma das classificações das questões de escolha múltipla der um número negativo, será atribuído 0 valores como resultado final.
-0.2/0.5	sc, c só sc: n é um número primo. um número primo ín Questão 2 Os princípios de	upo $\mathbb{Z}/n\mathbb{Z}$. Pode-se definir uma multiplicação tal que \mathbb{F}_n é um corpo
0.5/0.5	só do segredo do algorith só da chave, mas não do só da complexidade da c do segredo da chave e do	encriptação.
0.5/0.5	☐ DES ☐ Vigenère	otocolos criptográficos é assimétrico? AES ElGamal
0.5/0.5	Questão 4 O Discrete Logarithm Prob Determine h, dados g, p Determine g, dados h, p	

0.5/0.5	Questão 5 No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usam números secretos a e b para calcular números A e B que são depois trocados. A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$. A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $(ab)^g \pmod{p}$. A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$. A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $A \cdot B$. Questão 6 No protocolo $ElGamal$, Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para
-0.2/0.5	enviar um ciphertext (c_1, c_2) com $c_1 \equiv g^k \pmod{p}$ e $c_2 \equiv mA^k \pmod{p}$; k uma chave ephemeral. Para recuperar a mensagem m , Alice calcula:
	Questão 7 — O algoritmo de Miller-Rabin devolve um número primo com probablidade elevada. No caso improvável do número devolvido p não ser primo, o que pode acontecer no protocolo criptográfico de $ElGamal$ que usa este número para a escolha de \mathbb{F}_p^* :
-0.2/0.5	 A encriptação torna-se lenta.
0.5/0.5	 Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se: O protocolo pode ser quebrado em tempo polinomial. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts. O protocolo pode ser quebrado em tempo exponencial. A probabilidade de um plaintext é independente do ciphertext.
0/0.5	 Questão 9 O funcionamento do RSA é baseado no seguinte: ☐ Exponenciação em F_p* é fácil e o Discrete Logarithm Problem é difícil. ☐ Mulitplicação é fácil e factorização é difícil. ☐ Mulitplicação é fácil e divisão é difícil. ☐ Exponenciação em F_p* é fácil e factorização é difícil.
-0.2/0.5	 Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente): A exponenciação é mais rápida sobre curvas elípticas do que em F_p*. A operação de "adição" é mais fácil sobre curvas elípticas do que em F_p*. A operação de "adição" é mais complicada sobre curvas elípticas do que em F_p*. A solução do DLP é mais complicada sobre curvas elípticas do que em F_p*.

Nuno Tiago Falcão Alpalhão - 46102 - LM Mark: 2.2/5 (total score: 2.2/5)

+41/1/40+

	Departamento de Matemá	tica	Faculdade de Ciências e	Tecnologia — UNL
	Criptografia	8/7/2	018	Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Nome:	imero de aluno preenchendo con grelha ao lado () e escreva ixo. Liugo falcae	iltipla. Nas questões e o quadrado respecterta vale 0,5 valores, s múltiplas anulam a escolha múltipla der
		um número negativo,	será atribuído 0 valores como r	esultado final.
	Questão 1 Considere o gr se, e só se:	rupo Z/nZ. Pode-se o	definir uma multiplicação tal	que \mathbb{F}_n é um corpo
0.0/0.F	$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	impar.	n é um número par.	
-0.2/0.5	n é um número primo.		otin n é uma potência de u	m número primo.
	Questão 2 Os princípios de satisfazer. Um princípio de K deve depender:		cípios que todos os sistemas e diz que <i>a segurança de um s</i>	•
	do segredo da chave e d	lo segredo do algorita	no.	
-0.2/0.5	só da complexidade da só do segredo do algorit só da chave, mas não do	encriptação. chmo, mas não do seg	gredo da chave.	
	Questão 3 Qual destes pr	rotocolos criptográfico	os é assimétrico?	
0.5/0.5	⊠ ElGamal		DES	
0.0,0.0	Vigenère		☐ AES	
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	congruência $g^x \equiv h \pmod p$ é	:
0.5/0.5	\square Determine g , dados h , p	e x.	\square Determine h , dados g ,	pex.
0.5/0.5	\bigotimes Determine x , dados y , h			

	Questão 5 No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usam números secretos a e b para calcular números A e B que são depois trocados.
0.5/0.5	☐ A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$. ☐ A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $A \cdot B$. ☐ A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$. ☐ A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $(ab)^g \pmod{p}$.
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para enviar um <i>ciphertext</i> (c_1, c_2) com $c_1 \equiv g^k \pmod{p}$ e $c_2 \equiv mA^k \pmod{p}$; k uma chave <i>ephemeral</i> . Para recuperar a mensagem m , Alice calcula:
0.5/0.5	
	Questão 7 — O algoritmo de Miller-Rabin devolve um número primo com probablidade elevada. No caso improvável do número devolvido p não ser primo, o que pode acontecer no protocolo criptográfico de $ElGamal$ que usa este número para a escolha de \mathbb{F}_p^* :
0.5/0.5	 □ Dois ciphertexts podem encriptar a mesma mensagem. □ A encriptação torna-se lenta. □ A quebra do protocolo é fácil.
	Duas mensagens podem ser codificadas pelo mesmo ciphertext.
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se: A probabilidade de um plaintext é independente do ciphertext.
	O protocolo pode ser quebrado em tempo exponencial.
0.5/0.5	O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.
	O protocolo pode ser quebrado em tempo polinomial.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
	\bigotimes Exponenciação em \mathbb{F}_p^* é fácil e factorização é difícil.
-0.2/0.5	Mulitplicação é fácil e divisão é difícil.
	Mulitplicação é fácil e factorização é difícil.
	Exponenciação em \mathbb{F}_p^{\bullet} é fácil e o Discrete Logarithm Problem é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
	\square A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .
-0.2/0.5	A operação de "adição" é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .
	A solução do DLP é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .
	\square A exponenciação é mais rápida sobre curvas elípticas do que em \mathbb{F}_p^* .

Patrícia Monteiro Negrão - 45703 - MIEI Mark: 2.2/5 (total score: 2.2/5)

		+81/1/20+
	Departamento de Matemá Criptografia	tica Faculdade de Ciências e Tecnologia — UNI 8/7/2018 Exame Final
	Número de aluno 0 0 0 0 0 0	← Marque o seu número de aluno preenchendo completamente os qua drados respectivos da grelha ao lado (■) e escreva o nome completo, o número e o curso abaixo.
	2 2 2 2 2 3 3 3 3 3 24 4 4 4 4	Nome: Pakiaa Lonkizo veszac
	5 6 6 6 6	Curso:LEI Número de aluno:
	7 7 7 7 7 8 8 8 8 8 8 9 9 9 9 9 9	O exame é composto por 10 questões de escolha múltipla. Nas questões marque a resposta certa preenchendo completamente o quadrado respectivo () com caneta azul ou preta, cada resposta certa vale 0,5 valores, cada resposta errada desconta 0,2 valores e marcações múltiplas anulam a questão. Se a soma das classificações das questões de escolha múltipla der um número negativo, será atribuído 0 valores como resultado final.
	Questão 1 Considere o g se, c só sc:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se definir uma multiplicação tal que \mathbb{F}_n é um corpo
-0.2/0.5		
		le Kerckhoff são princípios que todos os sistemas criptográficos devem erckhoff fundamental diz que a segurança de um sistema criptográfico
0.5/0.5	só da complexidade da só da chave, mas não do do segredo da chave e d só do segredo do algorit	o segredo do algoritmo.
	Questão 3 Qual destes pr	rotocolos criptográficos é assimétrico?
0.5/0.5	DES ElGamal	☐ Vigenère ☐ AES
	Questão 4 O Discrete Logarithm Pro-	$blem\;(DLP)$ para a congruência $g^x\equiv h\;(\operatorname{mod} p)$ é:
-0.2/0.5		e x . Determine x , dados g , $h \in p$.



	Questão 5 No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usam números secretos a e b para calcular números A e B que são depois trocados.		
	\square A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$.		
0.5/0.5	$A \in \text{calculado por } a^g \pmod{p}$, $B \text{ por } b^g \pmod{p}$ e a chave comum secreta $e \pmod{p} \pmod{p}$.		
	A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$.		
	\square A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $A \cdot B$.		
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para enviar um <i>ciphertext</i> (c_1, c_2) com $c_1 \equiv g^k \pmod{p}$ e $c_2 \equiv mA^k \pmod{p}$; k uma chave <i>ephemeral</i> . Para recuperar a mensagem m , Alice calcula:		
2 E /2 E			
0.5/0.5			
	Questão 7 — O algoritmo de Miller-Rabin devolve um número primo com probablidade elevada. No caso improvável do número devolvido p não ser primo, o que pode acontecer no protocolo criptográfico de $ElGamal$ que usa este número para a escolha de \mathbb{F}_p^* :		
	Dois ciphertexts podem encriptar a mesma mensagem.		
0.2/0.5	A encriptação torna-se lenta.		
0.2/0.5	A quebra do protocolo é fácil.		
	□ Duas mensagens podem ser codificadas pelo mesmo ciphertext.		
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:		
	A probabilidade de um plaintext é independente do ciphertext.		
0.5/0.5	O protocolo pode ser quebrado em tempo exponencial.		
J.5/U.5	O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.		
	O protocolo pode ser quebrado em tempo polinomial.		
	Questão 9 O funcionamento do RSA é baseado no seguinte:		
	\blacksquare Exponenciação em \mathbb{F}_p^* é fácil e o Discrete Logarithm Problem é difícil.		
0.2/0.5	Mulitplicação é fácil e divisão é difícil.		
0.2/0.5	Mulitplicação é fácil e factorização é difícil.		
	Exponenciação em \mathbb{F}_p^* é fácil e factorização é difícil.		
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):		
	\square A operação de "adição" é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .		
0.5/0.5	\square A exponenciação é mais rápida sobre curvas elípticas do que em \mathbb{F}_p^* .		
J.0/0.0	A solução do DLP é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .		
	\square A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .		

Paulo Guilherme Domingos Canha Moreira dos Santos - 51836 - EMP Mark: 4.3/5 (total score: 4.3/5)

			+92/1/5	58+
	Departamento de Matemát Criptografia	tica 8/7/2	Faculdade de Ciências 018	e Tecnologia — UNL Exame Final
	8 8 8 8 9 9 9 9	Nome: Jank Nome: Jank Curso: MM Curso: MM Curso: Month of the composto marque a resposta certivo () com caneta cada resposta errada o questão. Se a soma da	imero de aluno preenchendo grelha ao lado () e escretivo.	múltipla. Nas questões ente o quadrado respeca certa vale 0,5 valores, ções múltiplas anulam a de escolha múltipla der
0.5/0.5		rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se o	definir uma multiplicação	tal que \mathbb{F}_n é um corpo
	Questão 2 Os princípios d satisfazer. Um princípio de Ko deve depender:		cípios que todos os sistema diz que a segurança de un	
0.5/0.5	do segredo da chave e d só do segredo do algorit só da complexidade da d só da chave, mas não do	hmo, mas não do seg encriptação.	redo da chave.	
		otocolos criptográfico		
-0.2/0.5	DES AES		✓ ElGamal✓ Vigenère	
	Questão 4 O Discrete Logarithm Prob	blem (DLP) para a c	ongruência $g^x \equiv h \; (ext{mod} p$) é:
0.5/0.5	Determine g , dados h , p Determine x , dados g , h		Determine h , dados g Determine p , dados g	-

	Questão 5 No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usam múmeros secretos a e b para calcular números A e B que são depois trocados.
0.5/0.5	☐ A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$. ☐ A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$. ☐ A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $(ab)^g \pmod{p}$. ☐ A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $A \cdot B$.
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para enviar um <i>ciphertext</i> (c_1, c_2) com $c_1 \equiv g^k \pmod{p}$ e $c_2 \equiv mA^k \pmod{p}$; k uma chave <i>ephemeral</i> . Para recuperar a mensagem m , Alice calcula:
0.5/0.5	
	Questão 7 — O algoritmo de Miller-Rabin devolve um número primo com probablidade elevada. No caso improvável do número devolvido p não ser primo, o que pode acontecer no protocolo criptográfico de $ElGamal$ que usa este número para a escolha de \mathbb{F}_p^* :
0.5/0.5	 ☐ A quebra do protocolo é fácil. ☐ Dois ciphertexts podem encriptar a mesma mensagem. ☐ A encriptação torna-se lenta.
	Duas mensagens podem ser codificadas pelo mesmo ciphertext.
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
0.5/0.5	 O protocolo pode ser quebrado em tempo polinomial. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.
	O protocolo pode ser quebrado em tempo exponencial.
	A probabilidade de um plaintext é independente do ciphertext.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
	Mulitplicação é fácil e factorização é difícil. Mulitplicação é fácil e divisão é difícil.
0.5/0.5	Exponenciação em \mathbb{F}_p^* é fácil e o Discrete Logarithm Problem é difícil.
	Exponenciação em \mathbb{F}_p^* é fácil e factorização é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
	\square A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .
0.5/0.5	A operação de "adição" é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .
0.0/0.0	A exponenciação é mais rápida sobre curvas elípticas do que em \mathbb{F}_p^* .
	\square A solução do DLP é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .

Paulo Henrique Branco Dias - 45672 - MIEI Mark: 3.1/5 (total score: 3.1/5)

+50/1/22+

	Departamento de Matemá Criptografia	itica 8/7/	Faculdade de Ciências e Tecnologia — UNL 2018 Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 1		número de aluno preenchendo completamente os qua- a grelha ao lado () e escreva o nome completo, o aixo.
	2 2 2 2 3 3 3 3 3 3 4 4 4 4 4 4		Henrique branca Dis
	5 5 5 6 6 6 7 7 7 6 7	Curso: M. LE.J.	Número de aluno:4.5.6.7.2
	8 8 8 8 8 9 9 9 9	marque a resposta ce tivo () com caneta cada resposta errada questão. Se a soma de	por 10 questões de escolha múltipla. Nas questões rta preenchendo completamente o quadrado respecazul ou preta, cada resposta certa vale 0,5 valores, desconta 0,2 valores e marcações múltiplas anulam a as classificações das questões de escolha múltipla der será atribuído 0 valores como resultado final.
	Questão 1 Considere o gr sc, e só se:		definir uma multiplicação tal que \mathbb{F}_n é um corpo
-0.2/0.5	n é um número par. n é um número primo í		n é um número primo. n é uma potência de um número primo.
	Questão 2 Os princípios de satisfazer. Um princípio de Kodeve depender:	le <i>Kerekhof</i> f são prin erckhoff fundamental	cípios que todos os sistemas criptográficos devem l diz que a segurança de um sistema criptográfico
0.5/0.5	só da complexidade da d do segredo da chave e d só da chave, mas não do só do segredo do algorit	o segredo do algorita o segredo do algorita	no.
	Questão 3 Qual destes pr	otocolos criptográfic	os é assimétrico?
0.5/0.5	☐ Vigenère ☐ AES		ElGamal DES
	Questão 4 O Discrete Logarithm Prob	blem (DLP) para a c	eongruência $g^{m{x}} \equiv h \; (mod p) \;$ é:
0.5/0.5	Determine x , dados g , h Determine p , dados g , h		Determine h , dados g , $p \in x$. Determine g , dados h , $p \in x$.

A é calculado por a ^g (mod p), B por b ^g (mod p) e a chave comum secreta é g ^{ab} A é calculado por g ^a (mod p), B por g ^b (mod p) e a chave comum secreta é A · A · Questão 6 No protocolo ElGamal, Bob usa a chave pública da Alice A ≡ g ^a (nenviar um ciphertext (c ₁ , c ₂) com c ₁ ≡ g ^k (mod p) e c ₂ ≡ mA ^k (mod p); k uma chave Para recuperar a mensagem m, Alice calcula: □ c ₁ · (c ₂ ^a) ⁻¹ (mod p)	
 0.5/0.5 A é calculado por g^a (mod p), B por g^b (mod p) e a chave comum secreta é g^{ab} A é calculado por a^g (mod p), B por g^b (mod p) e a chave comum secreta é A · B Questão 6 No protocolo ElGamal, Bob usa a chave pública da Alice A ≡ g^a (nenvir um ciphertext (c₁, c₂) com c₁ ≡ g^k (mod p) e c₂ ≡ mA^k (mod p); k uma chave Para recuperar a mensagem m, Alice calcula: 0.5/0.5 Questão 7 O algoritmo de Miller-Rabin devolve um número primo com probablida No caso improvável do número devolvido p não ser primo, o que pode acontecer n criptográfico de ElGamal que usa este número para a escolha de F_p: Duas mensagens podem ser codificadas pelo mesmo ciphertext. A encriptação torna-se lenta. Dois ciphertexts podem encriptar a mesma mensagem. A quebra do protocolo é fácil. Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos ciphertexts. O protocolo pode ser quebrado em tempo exponencial. A probabilidade de um plaintext é independente do ciphertext. O protocolo pode ser quebrado em tempo polinomial. Questão 9 O funcionamento do RSA é baseado no seguinte: Exponenciação em F_p é fácil e o Discrete Logarithm Problem é difícil. 	am números
Questão 6 No protocolo ElGamal, Bob usa a chave pública da Alice A ≡ g ^a (n enviar um ciphertext (c ₁ , c ₂) com c ₁ ≡ g ^k (mod p) e c ₂ ≡ mA ^k (mod p); k uma chave Para recuperar a mensagem m, Alice calcula: □ c ₁ · (c ₂ ^a) ⁻¹ (mod p) □ (c ₁) ⁻¹ · (c ₂) ^a (mod p) □ (c ₁ ^a) · (c ₂) ⁻¹ (mod p) □ (c ₁ ^a) · (c ₂) ⁻¹ (mod p) Questão 7 O algoritmo de Miller-Rabin devolve um mimero primo com probablida No caso improvável do número devolvido p não ser primo, o que pode acontecer n criptográfico de ElGamal que usa este número para a escolha de F _p [*] : □ Duas mensagens podem ser codificadas pelo mesmo ciphertext. □ A encriptação torna-se lenta. □ Dois ciphertexts podem encriptar a mesma mensagem. □ A quebra do protocolo é fácil. Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só □ O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos ciphertexts. □ O protocolo pode ser quebrado em tempo exponencial. □ A probabilidade de um plaintext é independente do ciphertext. □ O protocolo pode ser quebrado em tempo polinomial. Questão 9 O funcionamento do RSA é bascado no seguinte: □ Exponenciação em F _p [*] é fácil e factorização é difícil. □ Exponenciação em F _p [*] é fácil e factorização é difícil. □ Exponenciação em F _p [*] é fácil e factorização é difícil.	\pmod{p} . \pmod{p} .
Questão 7 O algoritmo de Miller-Rabin devolve um número primo com probablida No caso improvável do número devolvido p não ser primo, o que pode acontecer n criptográfico de ElGamal que usa este número para a escolha de F _p . Duas mensagens podem ser codificadas pelo mesmo ciphertext. A encriptação torna-se lenta. Dois ciphertexts podem encriptar a mesma mensagem. A quebra do protocolo é fácil. Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos ciphertexts. O protocolo pode ser quebrado em tempo exponencial. A probabilidade de um plaintext é independente do ciphertext. O protocolo pode ser quebrado em tempo polinomial. Questão 9 O funcionamento do RSA é baseado no seguinte: Exponenciação em F _p é fácil e factorização é difícil. Exponenciação em F _p é fácil e factorização é difícil	(mod p) para
No caso improvável do número devolvido p não ser primo, o que pode acontecer n criptográfico de ElGamal que usa este número para a escolha de F*: Duas mensagens podem ser codificadas pelo mesmo ciphertext. A encriptação torna-se lenta. Dois ciphertexts podem encriptar a mesma mensagem. A quebra do protocolo é fácil. Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos ciphertexts. O protocolo pode ser quebrado em tempo exponencial. A probabilidade de um plaintext é independente do ciphertext. O protocolo pode ser quebrado em tempo polinomial. Questão 9 O funcionamento do RSA é baseado no seguinte: Exponenciação em F* é fácil e factorização é difícil.	
O/0.5 A encriptação torna-se lenta. Dois ciphertexts podem encriptar a mesma mensagem. A quebra do protocolo é fácil. Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos ciphertexts. O protocolo pode ser quebrado em tempo exponencial. A probabilidade de um plaintext é independente do ciphertext. O protocolo pode ser quebrado em tempo polinomial. Questão 9 O funcionamento do RSA é baseado no seguinte: Exponenciação em F [*] _p é fácil e o Discrete Logarithm Problem é difícil. Exponenciação em F [*] é fácil e factorização é difícil	
O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos ciphertexts. O protocolo pode ser quebrado em tempo exponencial. A probabilidade de um plaintext é independente do ciphertext. O protocolo pode ser quebrado em tempo polinomial. Questão 9 O funcionamento do RSA é baseado no seguinte: Exponenciação em F _p * é fácil e o Discrete Logarithm Problem é difícil. Exponenciação em F* é fácil e factorização é difícil.	
O protocolo pode ser quebrado em tempo exponencial. A probabilidade de um plaintext é independente do ciphertext. O protocolo pode ser quebrado em tempo polinomial. Questão 9 O funcionamento do RSA é baseado no seguinte: Exponenciação em F _p * é fácil e o Discrete Logarithm Problem é difícil. Exponenciação em F* é fácil e factorização é difícil.	
Questão 9 O funcionamento do RSA é baseado no seguinte: Exponenciação em F _p [*] é fácil e o Discrete Logarithm Problem é difícil. Exponenciação em F [*] é fácil e factorização é difícil	
Exponenciação em \mathbb{F}_p^* é fácil e o Discrete Logarithm Problem é difícil. Exponenciação em \mathbb{F}_p^* é fácil e factorização é difícil	
Mulitplicação é fácil e divisão é difícil. Mulitplicação é fácil e factorização é difícil.	
Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamen	ente):
 A operação de "adição" é mais fácil sobre curvas elípticas do que em F_p*. N solução do DLP é mais complicada sobre curvas elípticas do que em F_p*. A operação de "adição" é mais complicada sobre curvas elípticas do que em F_p*. A exponenciação é mais rápida sobre curvas elípticas do que em F_p*. 	