Francisco José Sampaio de Freitas Cardoso - 42997 - MIEI Mark: 1.5/5 (total score: 1.5/5)

			+21/1/20+
	Departamento de Matemá Criptografia	itica 8/7/2	Faculdade de Ciências e Tecnologia — UNL 2018 Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1		úmero de aluno preenchendo completamente os qua- a grelha ao lado () e escreva o nome completo, o ixo.
	2 2 2 2 3 3 3 3 3 4 4 4 4	Nome: For Calo	gue Soenjoir de Freibl
	5 5 5 5 5 6 6 6 6 6 7 7 7 7 7	Curso: .H.I.E.J	Número de aluno: 42997 por 10 questões de escolha múltipla. Nas questões
	88888	marque a resposta ce tivo () com caneta cada resposta errada e questão. Se a soma da	rta preenchendo completamente o quadrado respec- azul 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 g se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se	definir uma multiplicação tal que \mathbb{F}_n é um corpo
0.5/0.5	n é um número primo n n é um número par.	ímpar.	$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $
			cípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
0.5/0.5	só da chave, mas não d do segredo da chave e d só da complexidade da só do segredo do algorid	lo segredo do algoritr encriptação.	no.
	Questão 3 Qual destes p	rotocolos criptográfic	os é assimétrico?
0.5/0.5	☐ AES		☐ Vigenère ☐ DES
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	eongruência $g^x \equiv h \pmod p$ é:
0.5/0.5	Determine h , dados g , h Determine x , dados g , h		Determine p , dados g , $h \in x$. Determine g , dados h , $p \in x$.

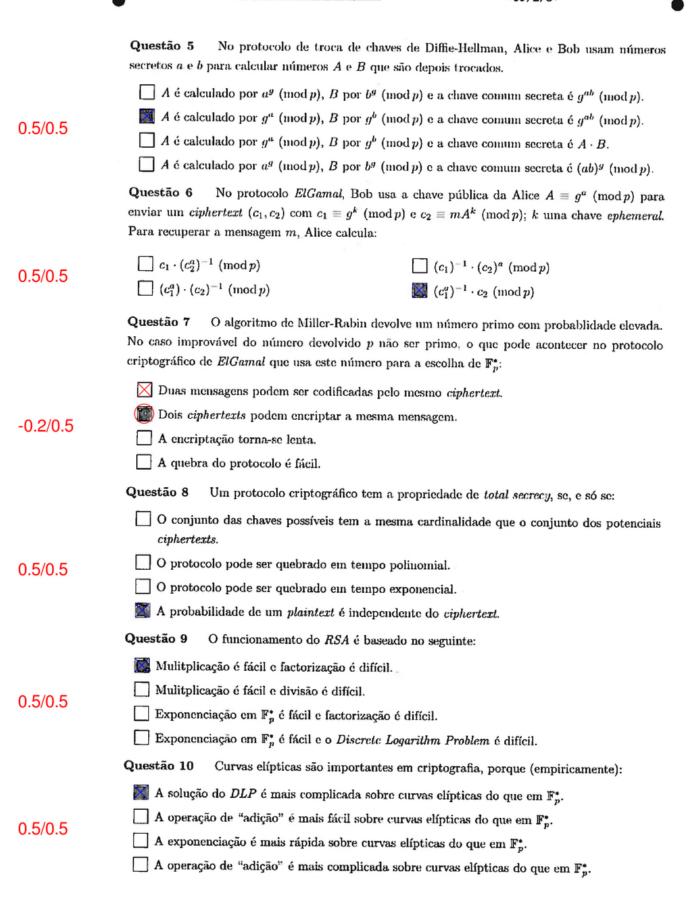
	Questão 5 No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usam números secretos a e b para calcular números A e B que são depois trocados.
-0.2/0.5	\bigcirc A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$. \bigcirc A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$. \bigcirc 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:
-0.2/0.5	
	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^* :
-0.2/0.5	A cuchra de matucale é fécil.
	 ☐ 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: O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.
0.5/0.5	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:
-0.2/0.5	 Exponenciação em F_p[*] é fácil e factorização é difícil. Mulitplicação é fácil e divisão é difícil. Mulitplicação é fácil e factorização é difícil.
	Exponenciação em \mathbb{F}_p^* é fácil e o Discrete Logarithm Problem é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
	A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* . A exponenciação é mais rápida sobre curvas elípticas do que em \mathbb{F}_p^* .
-0.2/0.5	\boxtimes A solução do DLP é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .
	\square A operação de "adição" é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .

Frederico Miguel Costa Lopes - 42764 - MIEI Mark: 3.6/5 (total score: 3.6/5)



+59/1/4+

	Departamento de Matemá	ica Faculdade de Ciências e Tecnologia		e Tecnologia — UNL
	Criptografia	8/7/2		Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 2 2 2 2 3 3 3 3 3 4 4 4 4 5 5 5 5 5 6 6 6 6 6	← Marque o seu m drados respectivos da número e o curso aba	úmero de aluno preenchendo u grelha ao lado (█) e escr	completamente os quaceva o nome completo, o
	7 7 10 7 7 8 8 8 8 8 9 9 9 9 9	marque a resposta cer tivo () com caneta cada resposta errada o questão. Sc a soma da	por 10 questões de escolha rta preenchendo completame azul ou preta, cada respost desconta 0,2 valores e marca es classificações das questões será atribuído 0 valores com	ente o quadrado respec- a certa vale 0,5 valores, ções múltiplas anulam a de escolha múltipla der
	Questão 1 Considere o gr se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se e	definir uma multiplicação	tal que \mathbb{F}_n é um corpo
	n é um número par. n é uma potência de um Questão 2 Os princípios d satisfazer. Um princípio de Ke deve depender:	le <i>Kerckhoff</i> são princ	n é um número prim n é um número prim (MO) cípios que todos os sistemas diz que a segurança de un	no. s criptográficos deven
0.5/0.5 _{wh} ~	só da complexidade da de segredo do algorito só da chave, mas não de do segredo da chave e de	hmo, mas não do seg o segredo do algoritm	ю.	
	Questão 3 Qual destes pr	rotocolos criptográfico	os é assimétrico?	
0.5/0.5	ElGamalVigenère		☐ DES ☐ AES	
	Questão 4 O Discrete Logarithm Prol	blem (DLP) para a c	ongruência $g^x\equiv h\pmod p$) é:
0.5/0.5			Determine x , dados g Determine h , dados g	



Gonçalo António Branco Pombeiro - 45296 - MIEI Mark: 0.8/5 (total score: 0.8/5)

•			+65/1/52+
	Departamento de Matemá Criptografia	tica 8/7/26	Faculdade de Ciências e Tecnologia — UNL D18 Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 1		mero de aluno preenchendo completamente os qua- grelha ao lado () e escreva o nome completo, o xo.
	2 2 2 2 2 3 3 3 3 3 3 4 4 4 4 4	Nome: Gougal	. Albino Brance
	5 5 5 6 6 6 6	Curso: MIEI	Número de aluno: 45296
	7 7 7 7 7 8 8 8 8 8 9 9 9 (1) 9	marque a resposta cer tivo () com caneta cada resposta errada d questão. Se a soma da	por 10 questões de escolha múltipla. Nas questões ta preenchendo completamente o quadrado respecazul ou preta, cada resposta certa vale 0,5 valores, lesconta 0,2 valores e marcações múltiplas anulam a s classificações das questões de escolha múltipla der será atribuído 0 valores como resultado final.
	Questão 1 Considere o g se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se o	lefinir uma multiplicação tal que \mathbb{F}_n é um corpo
-0.2/0.5	n é um número primo n é um número par.	ímpar.	n é um número primo. n n é uma potência de um número primo.
			cípios que todos os sistemas criptográficos devein diz que a segurança de um sistema criptográfico
0.5/0.5	só do segredo do algori só da chave, mas não d só da complexidade da do segredo da chave e	lo segredo do algoritm encriptação.	10.
wła		orotocolos criptográfic	.
-0.2/0.5	DES		Vigenère ElGamal
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	eongruência $g^x \equiv h \pmod p$ é:
-0.2/0.5			Determine g , dados h , $p \in x$. Determine h , dados g , $p \in x$.

	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 $(ab)^g \pmod{p}$. 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 $A \cdot B$. ☐ A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$.		
	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:		
-0.2/0.5			
	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 encriptação torna-se lenta. □ Dois ciphertexts podem encriptar a mesma mensagem. □ 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:		
0.5/0.5	A probabilidade de um plaintext é independente do ciphertext. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts. O protocolo pode ser quebrado em tempo polinomial.		
	O protocolo pode ser quebrado em tempo exponencial. Questão 9 O funcionamento do RSA é baseado no seguinte:		
-0.2/0.5	 Questão 9 O funcionamento do RSA é baseado no seguinte: 		
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):		
-0.2/0.5	☐ A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* . ☐ A operação de "adição" é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .		
	\boxtimes A solução do DLP é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .		
	A exponenciação é mais rápida sobre curvas elípticas do que em \mathbb{F}_p^* .		

Gonçalo Querido de Sousa - 45616 - MIEI Mark: 0/5 (total score: -0.5/5)



+57/1/8+

	Departamento de Matemá Criptografia	8/7/2	Faculdade de Ciências e Tecnolog 2018 Ex	ria — UNL rame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 1		número de aluno preenchendo completam a grelha ao lado () e escreva o nome aixo.	
	2 2 2 2 2 3 3 3 3 3 4 4 4 4	1	to Queido de Sousa	- 1
	5 5 5 5 6 6 6 6 7 7 7 7 7 7		Número de aluno:	
	88888	marque a resposta ce tivo () com caneta cada resposta errada questão. Se a soma de	erta preenchendo completamente o quadr azul ou preta, cada resposta certa vale desconta 0,2 valores e marcações múltipla as classificações das questões de escolha r será atribuído 0 valores como resultado	rado respec- 0,5 valores, as anulam a múltipla der
	Questão 1 Considere o gr sc, c só se:	rupo Z/nZ. Pode-se	definir uma multiplicação tal que F, c	é um corpo
0/0.5	n é um número par. n é uma potência de un	n número primo.	n é um número primo ímpar. n é um número primo.	
			cípios que todos os sistemas criptográfi l diz que <i>a segurança de um sistema cr</i>	
-0.2/Q.5 ₄ ,	só da chave, mas não do só do segredo do algorit do do segredo da chave e d só da complexidade da o	chmo, mas não do seg o segredo do algorita	gredo da chave.	
	Questão 3 Qual destes pr	rotocolos criptográfic	os é assimétrico?	
-0.2/0.5	ElGamal DES D		☐ Vigenère	
	Questão 4 O Discrete Logarithm Prob	blem (DLP) para a c	congruência $g^x\equiv h\ (\mathrm{mod} p)$ é:	
0.5/0.5			Determine p , dados g , $h \in x$. Determine x , dados g , $h \in p$.	



	Questão 5 No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usam número 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 $(ab)^g \pmod{p}$.	
0.0/0.5	\bigcirc A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$	e a chave comum secreta é g^{ab} (mod p).	
0.2/0.5	$\boxtimes A$ é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$	e a chave comum secreta é g^{ab} (mod 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:		
2/0 =		$] (c_1)^{-1} \cdot (c_2)^a \pmod{p} $	
0/0.5	$(c_1^a)^{-1} \cdot c_2 \pmod{p}$		
	Questão 7 — O algoritmo de Miller-Rabin devolve u No caso improvável do número devolvido p não ser criptográfico de $ElGamal$ que usa este número para a		
	Dois ciphertexts podem encriptar a mesma mens	sagem.	
0/0.5	A quebra do protocolo é fácil.		
J/U.3	Duas mensagens podem ser codificadas pelo mesmo ciphertext.		
	A encriptação torna-se lenta.		
	Questão 8 Um protocolo criptográfico tem a prop	oriedade de total secrecy, se, e só se:	
	A probabilidade de um plaintext é independente	e do ciphertext.	
0.2/0.5	O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.		
	O protocolo pode ser quebrado em tempo exponencial.		
	O protocolo pode ser quebrado em tempo polinomial.		
	Questão 9 O funcionamento do RSA é baseado no	o seguinte:	
	$\hfill \Box$ Exponenciação em \mathbb{F}_p^* é fácil e factorização é dif	ícil.	
0/0.5	Mulitplicação é fácil e divisão é difícil.		
5/0.5	\square Exponenciação em \mathbb{F}_p^* é fácil e o Discrete Logari	ithm Problem é difícil.	
	Mulitplicação é fácil e factorização é difícil.		
	Questão 10 Curvas elípticas são importantes em o	criptografia, porque (empiricamente):	
0.2/0.5	A solução do DLP é mais complicada sobre curv	vas elípticas do que em \mathbb{F}_p^* .	
	A operação de "adição" é mais complicada sobre	e curvas elípticas do que em \mathbb{F}_p^* .	
	A exponenciação é mais rápida sobre curvas elíp	oticas do que em \mathbb{F}_p^* .	
	A operação de "adição" é mais fácil sobre curvas	s elípticas do que em \mathbb{F}_p^* .	

Gonçalo Vagos Morais Callé de Almeida - 45353 - MIEI Mark: 4.3/5 (total score: 4.3/5)





Departamento de Matemática Criptografia Faculdade de Ciências e Tecnologia — UNL /2018 Exame Final

	Criptograna	8/1/20	018	Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 2 2 2 2 2 2 3 3 3 3 5 5 6 6 6 6 6 6 7 7 7 7 7 7 8 8 8 8 8 8 9 9 9 9 9	Curso: MIEI O exame é composto marque a resposta certivo () com caneta cada resposta errada de questão. Se a soma da	imero de aluno preenchendo e grelha ao lado () e escreta ixo. Número de aluno: Por 10 questões de escolha meta preenchendo completamenta preen	núltipla. Nas questões nte o quadrado respectorta vale 0,5 valores, ões múltiplas anulam a de escolha múltipla der
-0.2/0.5	se, e só se:	n número primo. le <i>Kerckhoff</i> são princ	definir uma multiplicação to la n é um número par. n é um número prime fipios que todos os sistemas diz que a segurança de um	o ímpar. criptográficos devem
0.5/0.5	só da complexidade da do segredo da chave e d só do segredo do algorit só da chave, mas não do	o segredo do algoritm	redo da chave.	
0.5/0.5	☐ AES ☐ Vigenère Questão 4	otocolos criptográfico	☐ DES ☐ ElGamal	
0.5/0.5	O Discrete Logarithm Pro Determine g , dados h , p Determine h , dados g , p	e x.	ongruência $g^x \equiv h \pmod{p}$ Determine x , dados g , Determine p , dados g ,	, <i>h</i> e <i>p</i> .



	Questão 5 No protocolo de troca de cha secretos a e b para calcular números A e B qu	aves de Diffie-Hellman, Alice e Bob usam números ne são depois trocados.			
0.5/0.5	\square A é calculado por $a^g \pmod{p}$, B por b^g	$(\text{mod } p)$ e a chave comum secreta é $(ab)^g \pmod{p}$.			
		\pmod{p} e a chave comum secreta é $g^{ab} \pmod{p}$.			
		\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 ElGamal, Bob u	ısa a chave pública da Alice $A \equiv g^a \pmod{p}$ para			
		$\operatorname{pd} p$) e $c_2 \equiv mA^k \pmod p$; k uma chave ephemeral.			
	Para recuperar a mensagem m , Alice calcula:	K Ak			
0.5/0.5					
0.0/0.0					
	Questão 7 O algoritmo de Miller-Rabin de	evolve um número primo com probablidade elevada.			
		não ser primo, o que pode acontecer no protocolo			
	criptográfico de ElGamal que usa este número	para a escolha de \mathbb{F}_p^* :			
	A encriptação torna-se lenta.				
0.5/0.5	Duas mensagens podem ser codificadas pelo mesmo ciphertext.				
	A quebra do protocolo é fácil.				
	Dois ciphertexts podem encriptar a mesn	na mensagem.			
	Questão 8 Um protocolo criptográfico tem	a propriedade de total secrecy, se, e só se:			
	O protocolo pode ser quebrado em tempo polinomial.				
0.5/0.5	A probabilidade de um plaintext é independente do ciphertext.				
	O protocolo pode ser quebrado em tempo exponencial.				
	O conjunto das chaves possíveis tem a n ciphertexts.	nesma cardinalidade que o conjunto dos potenciais			
	Questão 9 O funcionamento do RSA é bas	eado no seguinte:			
	Mulitplicação é fácil e divisão é difícil.				
0.5/0.5	\square Exponenciação em \mathbb{F}_p^* é fácil e o Discrete	Logarithm Problem é difícil.			
0.5/0.5	Mulitplicação é fácil e factorização é difíc	il.			
	Exponenciação em \mathbb{F}_p^* é fácil e factorização	io é difícil.			
	Questão 10 Curvas elípticas são important	es em criptografia, porque (empiricamente):			
	A exponenciação é mais rápida sobre cur	vas elípticas do que em \mathbb{F}_p^* .			
0.5/0.5	\blacksquare A solução do DLP é mais complicada sob	ore curvas elípticas do que em \mathbb{F}_p^* .			
	A operação de "adição" é mais fácil sobre	•			
	A operação de "adição" é mais complicad	a sobre curvas elípticas do que em \mathbb{F}_p^* .			