João de Sousa Falcão Henriques - 42650 - MIEI Mark: 2.9/5 (total score: 2.9/5)

•			+69/1/44+
	Departamento de Matemá Criptografia	tica 8/7/20	Faculdade de Ciências e Tecnologia — UNL 118 Exame Final
	Número de aluno 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	drados respectivos da número e o curso abai: Nome: João de Curso: MIEI	mero de aluno preenchendo completamente os quagrelha ao lado () e escreva o nome completo, o co. Sousa talcão Henriques Número de aluno: 42650
	8 8 8 8 8 9 9 9 9	tivo () com caneta cada resposta errada d questão. Se a soma da	ta preenchendo completamente o quadrado respec- azul ou preta, cada resposta certa vale 0,5 valores, esconta 0,2 valores e marcações múltiplas anulam a s classificações das questões de escolha múltipla der erá atribuído 0 valores como resultado final.
	Questão 1 Considere o g se, e só se:	grupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se o	lefinir uma multiplicação tal que \mathbb{F}_n é um corpo
0.5/0.5		ímpar. de <i>Kerckhof</i> f são princ	n é um número primo. n é um número par. nípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
0.5/0.5	só da chave, mas não d só da complexidade da do segredo da chave e só do segredo do algori	encriptação. do segredo do algoritm	10.
0.5/0.5	Questão 3 Qual destes p AES ElGamal	orotocolos criptográfic	os é assimétrico? DES Vigenère
	Questão 4 O Discrete Logarithm Pr	oblem (DLP) para a c	ongruência $g^x \equiv h \; (\operatorname{mod} p) \;$ é:
-0.2/0.5		-	Determine x , dados g , $h \in p$. Determine p , dados g , $h \in x$.
•	•	costa	

Questão 5 No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usan secretos a e b para calcular números A e B que são depois trocados.	números
	\pmod{p} .
Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a$ (me 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 a Para recuperar a mensagem m , Alice calcula:	- / -
Questão 7 — O algoritmo de Miller-Rabin devolve um número primo com probablidad. No caso improvável do número devolvido p não ser primo, o que pode acontecer no criptográfico de $ElGamal$ que usa este número para a escolha de \mathbb{F}_p^* :	
Duas mensagens podem ser codificadas pelo mesmo ciphertext. Dois ciphertexts podem encriptar a mesma mensagem. A quebra do protocolo é fácil. A encriptação torna-se lenta.	
Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se O protocolo pode ser quebrado em tempo polinomial. A probabilidade de um plaintext é independente do ciphertext. O protocolo pode ser quebrado em tempo exponencial. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos processor ciphertexts.	
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. Exponenciação em F _p [*] é fácil e factorização é difícil. Mulitplicação é fácil e divisão é difícil.	
Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamento A operação de "adição" é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .	te):
D.5/0.5 A exponenciação é mais rápida 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^* . A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .	

Luis Duarte Martins Bastos De Oliveira - 41894 - MIEI Mark: 1/5 (total score: 1/5)

	•		+28/1/6+
	Departamento de Matem Criptografia	ática 8/7/2	Faculdade de Ciências e Tecnologia — UNL 018 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 5 5 5 5 5 5	drados respectivos da número e o curso abai	monte Martine Bostos de
	6 6 6 6 7 7 7 7 7 8 8 8 8 9 9 9 9 9	marque a resposta cer tivo () com caneta cada resposta errada o 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 se classificações das questões de escolha múltipla der será atribuído 0 valores como resultado final.
	Questão 1 Considere o sc, c só sc:	grupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se	definir uma multiplicação tal que \mathbb{F}_n é um corpo
-0.2/0.5		o ímpar. s de <i>Kerckhoff</i> são princ	n é um número primo. n é um número par. rípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
0.5/0.5	do segredo da chave e só da chave, mas não só da complexidade da	do segredo do algoritm do segredo do algoritm a encriptação. rithmo, mas não do seg	io.
		protocolos criptográfico	
0.5/0.5	X ElGamal DES		☐ AES ☐ Vigenère
	Questão 4 O Discrete Logarithm Pr	roblem (DLP) para a c	ongruência $g^x \equiv h \; (\operatorname{mod} p) \; ext{\'e}$:
-0.2/0.5	\boxtimes Determine x , dados g , \rtimes Determine g , dados h ,		Determine p , dados g , h e x . Determine h , dados g , p e x .

	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.
0.5/0.5	☐ 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 $g^{ab} \pmod{p}$. ☐ 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 ElGamal, Bob usa a chave pública da Alice $A \equiv g^u \pmod{p}$ para
	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:
0/0.5	
0/0.5	
	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 <i>ElGamal</i> que usa este número para a escolha de \mathbb{F}_p^* :
	A quebra do protocolo é fácil.
0.5/0.5	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, c só se:
	 O protocolo pode ser quebrado em tempo exponencial. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais
-0.2/0.5	ciphertexts.
	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	Mulitplicação é fácil e factorização é difícil.
	☐ Mulitplicação é fácil e divisão 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):
-0.2/0.5	$X \bigcirc A$ exponenciação é mais rápida 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^* .
	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^* .

Manuel António de Melo Chinopa de Sousa Ribeiro - 47257 - MIEI Mark: 2.9/5 (total score: 2.9/5)

			+3/1/56+
	Departamento de Matemá Criptografia	itica 8/7/2	Faculdade de Ciências e Tecnologia — UNL 018 Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 2 2 2 2 2 3 3 3 3 3 3 4 4 4 4 4 5 5 5 5 5 6 6 6 6 6 7 7 7 7 8 8 8 8 8 9 9 9 9 9 9	Nome: Manual Nome: Manual Curso: M.I.E.I O exame é composto marque a resposta certivo () com caneta cada resposta errada é questão. Se a soma da	nuero de aluno preenchendo completamente os quagrelha ao lado () e escreva o nome completo, o xo. Autorio de Melo. Número de aluno:
	Questão 1 Considere o g se, e só se:	grupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se o	definir uma multiplicação tal que \mathbb{F}_n é um corpo
-0.2/0.5	n é um número primo n é um número primo.		\nearrow n é uma potência de um número primo. \nearrow n é um número par. \nearrow
			cípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
0.5/0.5	só da complexidade da só do segredo do algori só da chave, mas não d do segredo da chave e	ithmo, mas não do seg lo segredo do algoritm	ю.
	Questão 3 Qual destes p	orotocolos criptográfic	os é assimétrico?
0.5/0.5	☐ Vigenère ※ ElGamal		☐ AES ★ ☐ DES ★
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	ongruência $g^x \equiv h \pmod p$ é:
0.5/0.5	Determine h , dados g , Determine p , dados g ,	pex.	Determine g , dados h , $p \in x$. \forall 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.
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 $a^g \pmod{p}$, 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 $g^{ab} \pmod{p}$.
	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^* :
-0.2/0.5	 ☐ A encriptação torna-se lenta. ☐ A quebra do protocolo é fácil. ☐ Dois ciphertexts podem encriptar a mesma mensagem.
	 ☑ 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. □ A probabilidade de um plaintext é independente do ciphertext. □ O protocolo pode ser quebrado em tempo exponencial. □ O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
-0.2/0.5	 Exponenciação em F_p[*] é fácil e factorização é difícil. 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.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0.5/0.5	A exponenciação é mais rápida 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^* . A operação de "adição" 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^* . \vee

Manuel Maria Silva Barbas - 45384 - MIEI Mark: 1/5 (total score: 1/5)

+70/1/42+

	Departamento de Matemá	tica	Faculdade de Ciências e Tecnologia — UN		
	Criptografia	8/7/2	018	Exame Final	
	Número de aluno 0 0 0 0 0 1 1 1 1 1 1		ímero de aluno preenchend grelha ao lado () e esc ixo.		
	2 2 2 2 2 3 3 3 3	Nome: Marwel	Hapia Silva	Barbes	
	4 4 4 6 5 6 5 5 5				
	66666	Curso: MIEI	Número de alun	o: .4.5.3.8.9	
	7 7 7 7 7 8 8 8 8 8 9 9 9 9 9 9	marque a resposta cer tivo () com caneta cada resposta errada d questão. Se a soma da	por 10 questões de escolha rta preenchendo completam azul ou preta, cada respos desconta 0,2 valores e marca as classificações das questões será atribuído 0 valores con	nente o quadrado respec- ta certa vale 0,5 valores, ações múltiplas anulam a s de escolha múltipla der	
	Questão 1 Considere o g se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se o	definir uma multiplicação	tal que \mathbb{F}_n é um corpo	
0.5/0.5	📓 n é uma potência de un	m número primo.		mo împar.	
0.5/0.5	n é um número primo.		n ć um número par		
	Questão 2 Os princípios o satisfazer. Um princípio de K deve depender:		cípios que todos os sistema diz que <i>a segurança de u</i>		
	do segredo da chave e d	do segredo do algorita	no.		
0.5/0.5	só da chave, mas não d só da complexidade da	-	00.		
	só do segredo do algorithmo, mas não do segredo da chave.				
	Questão 3 Qual destes p	rotocolos criptográfico	os é assimétrico?		
0.5/0.5	☐ Vigenère		☐ AES		
0.5/0.5	DES		ElGamal		
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	congruência $g^x \equiv h \; (mod j)$	p) é:	
0 E/0 E	\square Determine x , dados g , l	h e p.	\Box Determine g , dados	$h, p \in x$.	
0.5/0.5	\square Determine h , dados g , p	9 e x.	\square Determine p , dados	$g, h \in x$.	

	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	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 $A \cdot B$. A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$.
	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:
0/0.5	
	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	 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.
-0.2/0.5	 Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se: ☐ O protocolo pode ser quebrado em tempo polinomial. ☐ O protocolo pode ser quebrado em tempo exponencial. ☐ A probabilidade de um plaintext é independente do ciphertext. ☐ O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.
-0.2/0.5	 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 o Discrete Logarithm Problem 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 (empiricamente):
-0.2/0.5	 Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente): A operação de "adição" é mais complicada sobre curvas elípticas do que em F_p*. A operação de "adição" é mais fácil sobre curvas elípticas do que em F_p*. A exponenciação é mais rápida sobre curvas elípticas do que em F_p*. A solução do DLP é mais complicada sobre curvas elípticas do que em F_p*.



+38/1/46+

	Departamento de Matemá	itica Faculdade de Ciências e Tecnologia — UNL
	Criptografia	8/7/2018 Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1	← 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.
	2 2 2 2 2 3 3 3 3 3 4 4 4 4	Nome: Marcelo Tilipe Cantinho
	5 5 5 5 5 6 6 6 6 6 7 7 7 7 7	Curso: MICI Número de aluno:43.0.99
	8 8 8 8 8 9 9 9 1	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 se:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se definir uma multiplicação tal que \mathbb{F}_n é um corpo
0.5/0.5	\square n é um número primo.	n é um número par.
0.5/0.5	n é um número primo	ímpar.
		le Kerckhoff são princípios que todos os sistemas criptográficos devem erckhoff fundamental diz que a segurança de um sistema criptográfico
-0.2/0.5	só da chave, mas não d to do segredo da chave e o só do segredo do algoria só da complexidade da	do segredo do algoritmo. chmo, mas não do segredo da chave.
	Questão 3 Qual destes p	rotocolos criptográficos é assimétrico?
-0.2/0.5	⊠ ElGamal □ DES	AES Vigenère
	Questão 4 O Discrete Logarithm Pro	$blem\;(DLP)$ para a congruência $g^x\equiv h\;(\operatorname{mod} p)$ é:
0.5/0.5	Determine g , dados h , p Determine h , dados g , p	

