Bernardo Rafael Pereira de Sousa - 45322 - MIEI Mark: 1.5/5 (total score: 1.5/5)

+10/1/42+

	Departamento de Matemát Criptografia	tica 8/7/20	Faculdade de Ciências e Tecnologia — UNL 018 Exame Final
	Número de aluno 0 0 0 0 0 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 2 2 2 2 2 2 2 2 2 2 2 2 2 2		Refort Periso de Sousa
	6 6 6 6 6 7 7 7 7 7 8 8 8 8 8 9 9 9 9	O exame é composto 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
	Questão 1 Considere o g se, e só se:		será atribuído 0 valores como resultado final. definir uma multiplicação tal que \mathbb{F}_n é um corpo
-0.2/0.5	otin n é uma potência de un $ otin n$ é um número primo.	n número primo.	$n \in um$ número par. $n \in um$ número primo ímpar.
			rípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
0.5/0.5	do segredo da chave e d só da chave, mas não de só do segredo do algorit só da complexidade da	o segredo do algoritm	о.
	Questão 3 Qual destes pr	rotocolos criptográfico	os é assimétrico?
-0.2/0.5	ElGamal AES		☐ Vigenère ☐ DES
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	ongruência $g^x \equiv h \; (mod p)$ é:
0.5/0.5	Determine x , dados g , h Determine g , dados h , p		Determine h , dados g , $p \in x$. Determine p , dados g , $h \in x$.

	Questão 5 No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usam númer 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 $A \cdot B$. ☐ 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 $g^{ab} \pmod{p}$.			
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ par 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>ephemere</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 protoco criptográfico de $ElGamal$ que usa este número para a escolha de \mathbb{F}_p^* :			
0.2/0.5	 A quebra do protocolo é fácil. ② 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: O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciai			
0.5/0.5	ciphertexts. O protocolo pode ser quebrado em tempo polimomial. A probabilidade de um plaintext é independente do ciphertext. O protocolo pode ser quebrado em tempo exponencial.			
0.2/0.5	 Questão 9 O funcionamento do RSA é baseado no seguinte: Exponenciação em F_p[*] é fácil e factorização é difícil. Mulitplicação é fácil e divisão é difícil. Exponenciação em F_p[*] é fácil e o Discrete Logarithm Problem é difícil. Mulitplicação é fácil e factorização 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^* .			
0.2/0.5	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^* . \square A exponenciação é mais rápida sobre curvas elípticas do que em \mathbb{F}_p^* .			

Bernardo da Palma Abraços Soares de Albergaria - 41931 - MIEI Mark: 1.4/5 (total score: 1.4/5)

•			+7/1/48+
	Departamento de Matemát Criptografia	tica 8/7/20	Faculdade de Ciências e Tecnologia — UNL 018 Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1		úmero de aluno preenchendo completamente os qua- grelha ao lado () e escreva o nome completo, o ixo.
	2 2 2 2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3		o Albergaria
	6 6 6 6 6 7 7 7 7 7 8 8 8 8 8 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 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 se 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	definir uma multiplicação tal que F _n é um corpo
0/0.5	n é um número primo í n é um número primo.	ínpar.	$\ \ \ \ \ \ \ \ \ \ \ \ \ $
			cípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
-0.2/0.5	só da chave, mas não de do segredo da chave e d só do segredo do algorit só da complexidade da	do segredo do algoritm	no.
	Questão 3 Qual destes pr	rotocolos criptográfico	os é assimétrico?
0.5/0.5	☐ DES		□ Vigenère□ AES
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	congruência $g^x \equiv h \pmod{p}$ é:
0/0.5	Determine p , dados g , h Determine x , dados g , h		Determine h , dados g , $p \in x$. 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.				
	\square A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$.				
-0.2/0.5	\blacksquare 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 $(ab)^g \pmod{p}$. A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$.				
	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 =					
0.5/0.5					
	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^* :				
	A encriptação torna-se lenta.				
0/0.5	Duas mensagens podem ser codificadas pelo mesmo ciphertext.				
0/0.0	A quebra do protocolo é fácil.				
	Dois ciphertexts podem encriptar a mesma mensagem.				
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:				
	O protocolo pode ser quebrado em tempo polinomial.				
-0.2/0.5	A probabilidade de um plaintext é independente 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.				
	Questão 9 O funcionamento do RSA é baseado no seguinte:				
	Exponenciação em \mathbb{F}_p^* é fácil e factorização é difícil.				
0.5/0.5	Mulitplicação é fácil e divisão é difícil.				
0.5/0.5	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):				
	\square A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .				
0.5/0.5	\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^* .				
	A exponenciação é mais rápida sobre curvas elípticas do que em \mathbb{F}_n^* .				

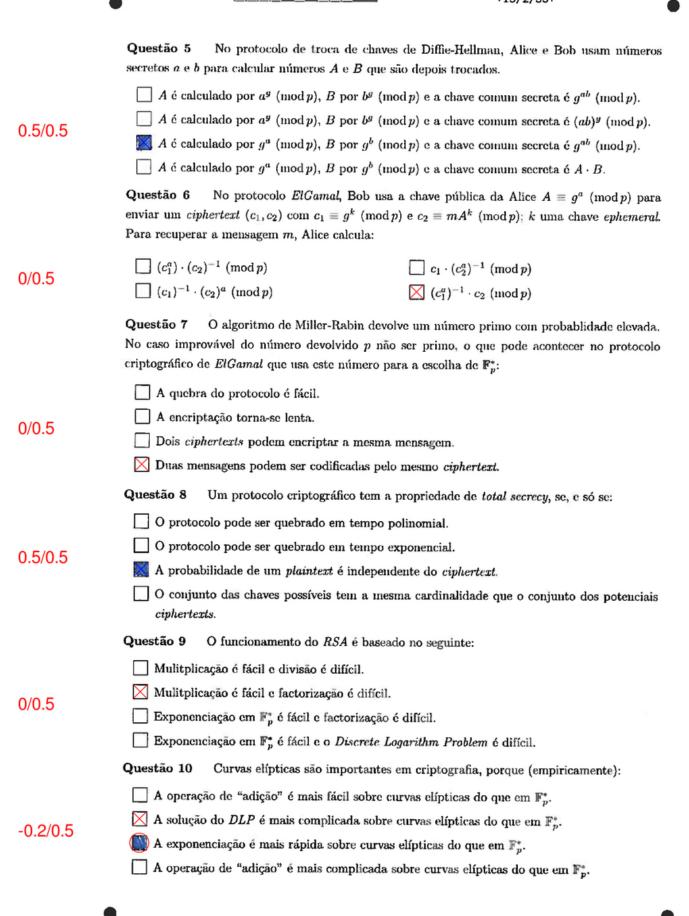
Bruno Vicente dos Santos - 44935 - MIEI Mark: 1.4/5 (total score: 1.4/5)

			+89/1/4+
	Departamento de Matemá Criptografia	tica Fa 8/7/2018	aculdade de Ciências e Tecnologia — UNI 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 4 4 4 4 5 5 5 5 5 6 6 6 6 6 7 7 7 7 7 8 8 8 8 8 9 9 9 9 9	Nome:	ro de aluno preenchendo completamente os qua cilha ao lado () e escreva o nome completo, o completo, comple
0/0.5	sc, e só se: n é um número par. n é uma potência de un Questão 2 Os princípios o	rupo Z/nZ. Pode-se defin m número primo.	nir uma multiplicação tal que F _n é um corpo n é um número primo impar. n é um número primo. os que todos os sistemas criptográficos devem a que a segurança de um sistema criptográficos
0.5/0.5	_		lo da chave.
0.5/0.5	☐ AES ☐ DES	rotocolos criptográficos é	e assimétrico? ElGamal Vigenère
0.5/0.5	Questão 4 O Discrete Logarithm Pro Determine p, dados g, h Determine g, dados h, p	nex.	gruência $g^x \equiv h \pmod p$ é: Determine h , dados g , p e x . Determine x , dados g , h e 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 $g^a \pmod{p}$, 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 $(ab)^g \pmod{p}$. A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$.
	Questão 6 No protocolo $ElGamal$, Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ 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:
-0.2/0.5	
	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^* :
0/0.5	 Duas mensagens podem ser codificadas pelo mesmo ciphertext. A encriptação torna-se lenta. A quebra do protocolo é fácil. Dois ciphertexts podem encriptar a mesma mensagem.
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
-0.2/0.5	 O protocolo pode ser quebrado em tempo polinomial. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts. A probabilidade de um plaintext é independente do ciphertext. O protocolo pode ser quebrado em tempo exponencial.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
0/0.5	 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.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
-0.2/0.5	 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*. ☐ A exponenciação é mais rápida sobre curvas elípticas do que em F_p*.
	\square A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .

Catarina Paulo de Matos - 47360 - MIEI Mark: 2.1/5 (total score: 2.1/5)

			+13/1/36+
	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 0 0 0 0 0 0 0 0 0 0 0 0 0		mero de aluno preenchendo completamente os qua- grelha ao lado () e escreva o nome completo, o so.
	2 2 2 2 2 3 3 3 3		Paulo de Matos
	5 5 5 5 6 6 6 6 6		Número de aluno:43360
	7 7 7 7 8 8 8 8 8 9 9 9 9 9	marque a resposta certivo () com caneta a cada resposta errada de questão. Se a soma das	por 10 questões de escolha múltipla. Nas questões ta preenchendo completamente o quadrado respectazul 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:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se d	lefinir uma multiplicação tal que \mathbb{F}_n é um corpo
-0.2/0.5	n é um número primo n é um número primo.		
			ípios 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 o	thmo, mas não do seg o segredo do algoritm	o.
	Questão 3 Qual destes p	rotocolos criptográfico	s é assimétrico?
0.5/0.5	☐ AES ElGamal		☐ Vigenère ☐ DES
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a co	ongruência $g^{oldsymbol{x}} \equiv h \; (\operatorname{mod} p) \; ext{\'e}$:
0.5/0.5	Determine h , dados g , g Determine g , dados h , g		Determine x , dados g , $h \in p$. Determine p , dados g , $h \in x$.



Claúdio Vicente Pascoal - 41921 - MIEI Mark: 2.3/5 (total score: 2.3/5)

0.5/0.5

Determine g, dados h, $p \in x$.

•			+79/1/24+	
	Departamento de Matemá Criptografia	tica 8/7/20	Faculdade de Ciências e T 18	ecnologia — UNL Exame Final
	Número de aluno 0 0 0 0 0 1		nero de aluno preenchendo con grelha ao lado () e escreva co.	
	2 2 2 2 2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3		Vicente Poseock	
	5 5 5 5 6 6 6 6 7 7 7 7 7	Curso: MIEI.	Número de aluno:	
	8 8 8 8 8 9 9	tivo () com caneta a cada resposta errada de questão. Se a soma das	ta preenchendo completamente azul ou preta, cada resposta co esconta 0,2 valores e marcações s classificações das questões de erá atribuído 0 valores como re	erta vale 0,5 valores s múltiplas anulam a escolha múltipla den
	Questão 1 Considere o g se, e só se:	grupo Z/nZ. Pode-se d	lefinir uma multiplicação tal	que \mathbb{F}_n é um corpo
-0.2/0.5	n é um número primo. n é um número primo		n é uma potência de un n é um número par.	m número primo.
	Questão 2 Os princípios satisfazer. Um princípio de le deve depender:		ípios que todos os sistemas c diz que <i>a segurança de um s</i>	
0.5/0.5	só da complexidade da do segredo da chave e só da chave, mas não o só do segredo do algor	do segredo do algoritm do segredo do algoritm	o.	
	Questão 3 Qual destes p	protocolos criptográfico	os é assimétrico?	
0.5/0.5	☐ Vigenère ☑ ElGamal		☐ DES ☐ AES	
	Questão 4 O Discrete Logarithm Pr	roblem (DLP) para a c	ongruência $g^x \equiv h \pmod{p}$	é:
0.5/0.5		h e x.	\square Determine x , dados g ,	h e p.

Determine h, dados g, $p \in x$.

