Diogo Santos Ferreira - 41627 - MIEI Mark: 4.5/5 (total score: 4.5/5)

		+8/1/46+
	Departamento de Matemát Criptografia	ica Faculdade de Ciências e Tecnologia — UNI 8/7/2018 Exame Final
	Número de aluno 0 0 0 0 0 1 2 1 1 1	← Marque o seu mimero 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 2 3 3 3 3 3 3 3 3 4 4 4 4 4 4	Nome: Dago Ferreiva
	5 5 5 5 5 6 6 6 6 6	Curso: HIE1 Número de aluno: 41624
	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 gr 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	n é um número primo í n é um número primo.	mpar. \square n é um número par. \square n é uma potência de um número primo.
		e Kerckhoff são princípios que todos os sistemas criptográficos devem erckhoff fundamental diz que a segurança de um sistema criptográfico
0.5/0.5	so da complexidade da d	segredo do algoritmo.
	Questão 3 Qual destes pr	otocolos criptográficos é assimétrico?
0.5/0.5	ElGamal AES	DES Vigenère
	Questão 4 O Discrete Logarithm Pro-	$blem\;(DLP)$ para a congruência $g^x\equiv h\;(ext{mod}p)\;$ é:
0.5/0.5		e x . Determine x , dados g , h e p .

	Owerting November 1	1 DIM W II
	Questão 5 No protocolo de troca de ch secretos a e b para calcular números A e B q	aves de Diffie-Hellman, Alice e Bob usam números ne são depois trocados.
0.5/0.5	\square A é calculado por $g^a \pmod{p}$, B por g^b \square A é calculado por $a^g \pmod{p}$, B por b^g	$(\text{mod } p)$ e a chave comum secreta é $(ab)^g \pmod{p}$. $(\text{mod } p)$ e a chave comum secreta é $A \cdot B$. $(\text{mod } p)$ e a chave comum secreta é $g^{ab} \pmod{p}$. $(\text{mod } p)$ e a chave comum secreta é $g^{ab} \pmod{p}$.
		usa a chave pública da Alice $A \equiv g^a \pmod p$ para $\operatorname{od} p$) e $c_2 \equiv mA^k \pmod p$; k uma chave ephemeral.
0.5/0.5		
		evolve um número primo com probablidade elevada. não ser primo, o que pode acontecer no protocolo para a escolha de \mathbb{F}_p^* :
0.5/0.5	 ☐ A quebra do protocolo é fácil. ☐ A encriptação torna-se lenta. ☐ Dois ciphertexts podem encriptar a mes 	ma mensagem.
	Duas mensagens podem ser codificadas	pelo mesmo ciphertext.
	Questão 8 Um protocolo criptográfico ten	n a propriedade de total secrecy, se, e só se:
	A probabilidade de um plaintext é indep	
0.5/0.5	 O protocolo pode ser quebrado em temp O conjunto das chaves possíveis tem a ciphertexts. 	nesma cardinalidade que o conjunto dos potenciais
	O protocolo pode ser quebrado em temp	o exponencial.
	Questão 9 O funcionamento do RSA é ba	
(ei(0		
0.5/0.5	Exponenciação em \mathbb{F}_p^* é fácil e factorizaç \mathbb{F}_p^* .	
	 Exponenciação em F_p[*] é fácil e o Discret Mulitplicação é fácil e divisão é difícil. 	с Logarunm Ртовіет е анісн.
		tes em criptografia, porque (empiricamente):
	A operação de "adição" é mais complica	
0/0 5	A solução do DLP é mais complicada so	•
0/0.5	A operação de "adição" é mais fácil sobr	
	A exponenciação é mais rápida sobre cu	rvas elípticas do que em \mathbb{F}_p^* .

Emanuel Rúben de Oliveira Leston - 48299 - MIEI Mark: 1.4/5 (total score: 1.4/5)

		Ш	

+15/1/32+

	Departamento de Matemá Criptografia	tica 8/7/20	Faculdade de Ciências e Tecnologia — UNL 18 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 co.
	2 2 2 2 2 3 3 3 3 3 3 3 3 3 3 3		1 Ruben De Cliverra Lation
	5 5 5 5 5 6 6 6 6 6 7 7 7 7 7	1	Número de aluno: 48244
	8 8 8 8 9 9 9 9	marque a resposta cert tivo () com caneta a cada resposta errada de questão. Se a soma das	por 10 questões de escolha múltipla. Nas questões la 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 Z/nZ. Pode-se d	efinir uma multiplicação tal que \mathbb{F}_n é um corpo
-0.2/0.5	n é um número primo. n é uma potência de un	m número primo.	$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $
		Name and Address of the Owner, when the Owner, which	ípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
0/0.5	 do segredo da chave e o só do segredo do algorio xó da chave, mas não d só da complexidade da 	thmo, mas não do segro o segredo do algoritmo	redo da chave.
	Questão 3 Qual destes p	rotocolos criptográfico	s é assimétrico?
0.5/0.5	☐ Vigenère ☐ ElGamal		☐ DES ☐ AES
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a co	ongruência $g^x \equiv h \pmod p$ é:
0.5/0.5			Determine x , dados g , $h \in p$. 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	\boxtimes 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 $A \cdot B$. \square A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $(ab)^g \pmod{p}$. \square
	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^* :
0.5/0.5	 □ A quebra do protocolo é fácil. □ Dois ciphertexts podem encriptar a mesma mensagem. □ Duas mensagens podem ser codificadas pelo mesmo ciphertext. □ 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 protocolo pode ser quebrado em tempo exponencial. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.
	A probabilidade de um plaintext é independente do ciphertext. Questão 9 O funcionamento do RSA é baseado no seguinte:
0/0.5	Exponenciação em \mathbb{F}_p^* é fácil e factorização é difícil. Exponenciação em \mathbb{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):
-0.2/0.5	 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*. ☐ 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*.

Filipe Miguel Pinho Santos - 45411 - MIEI Mark: 2.1/5 (total score: 2.1/5)

+90/1/2+

	Departamento de Matemá Criptografia	tica 8/7/2	Faculdade de Ciências e Tecnologia — UNL 018 Exame Final
	Número de aluno 0 0 0 0 0 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 4 4 4 5 5 5 5 5		Santos
	6 6 6 6 6 7 7 7 7 7 8 8 8 8 8 9 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
0/0.5	igcap n é um número primo n é um número par.	ímpar.	$\begin{tabular}{ll} \hline & n \ \'e \ um \ potência \ de \ um \ n\'umero \ primo. \end{tabular}$
			rípios 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 do segredo do algori do segredo da chave e d só da complexidade da	thmo, mas não do seg do segredo do algoritn	redo da chave.
	Questão 3 Qual destes p	rotocolos criptográfico	os é assimétrico?
0.5/0.5	ElGamal Uigenère		☐ DES ☐ AES
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	ongruência $g^x \equiv h \pmod p$ é:
0.5/0.5	Determine g , dados h , g Determine h , dados g , g		Determine x , dados g , $h \in p$. 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.
0.5/0.5	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 $a^g \pmod{p}$, 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 $A \cdot B$.
	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^* :
0/0.5	 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 <i>ciphertext</i> .
-0.2/0.5	 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 polinomial. 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 o Discrete Logarithm Problem é difícil. Exponenciação em 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 (empiricamente):
0.5/0.5	 A solução do DLP 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 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*.

			+4/1/54	+
	Departamento de Matemá Criptografia	ática 8/7/2	Faculdade de Ciências e 2018	Tecnologia — UNI Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 2 2 2 X 2 3 3 3 3 3 X 4 X 4 4	drados respectivos da número e o curso aba	úmero de aluno preenchendo da grelha ao lado (■) e escrevixo. DE LUNA	a o nome completo, o
	5 5 5 5 X 6 6 6 6 6 7 7 7 7 7 8 X 8 8 8 9 9 9 9 9	O exame é composto marque a resposta ce tivo () com caneta cada resposta errada questão. Se a soma de	por 10 questões de escolha m rta preenchendo completamen azul ou preta, cada resposta desconta 0,2 valores e marcaçõ as classificações das questões d será atribuído 0 valores como	uíltipla. Nas questões te o quadrado respec- certa vale 0,5 valores, ses múltiplas anulam a e escolha múltipla der
	Questão 1 Considere o g se, e só se:	grupo Z/nZ. Pode-se	definir uma multiplicação ta	d que \mathbb{F}_n é um corpo
-0.2/0.5	$\ \ \ \ \ \ \ \ \ \ \ \ \ $		n é um número primo n í uma potência de u	7
	Questão 2 Os princípios e satisfazer. Um princípio de K deve depender:		cípios que todos os sistemas e l diz que <i>a segurança de um</i> :	
-0.2/0.5	só da chave, mas não d do segredo da chave e d só da complexidade da só do segredo do algori	do segredo do algorita encriptação.	mo.	
		protocolos criptográfic	cos é assimétrico?	
-0.2/0.5 CEOTO	∑ ElGamal Vigenère		☐ DES AES	
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	congruência $g^{m{x}} \equiv h \pmod{p}$	é:
0.5/0.5	Determine p , dados g , h Determine h , dados g , g		Determine g , dados h , Determine x , dados g ,	•

CECIO

	Questão 5 No protocolo de troca de secretos a e b para calcular números A e b	e chaves de Diffie-Hellman, Alice e Bob usam números B que são depois trocados.
0.5/0.5	\nearrow A é calculado por g^a (mod p), B por A é calculado por a^g (mod p), B por A	r g^b (mod p) e a chave comum secreta é $A \cdot B$. r g^b (mod p) e a chave comum secreta é g^{ab} (mod p). r b^g (mod p) e a chave comum secreta é $(ab)^g$ (mod p).
		ob usa a chave pública da Alice $A \equiv g^a \pmod p$ para $\pmod p$ e $c_2 \equiv mA^k \pmod p$; k uma chave ephemeral. ula:
-0.2/8.5		
		in devolve um número primo com probablidade elevada. p p não ser primo, o que pode acontecer no protocolo nero para a escolha de \mathbb{F}_p^* :
(zet0 0.5/0.5	Dois <i>ciphertexts</i> podem encriptar a r Duas mensagens podem ser codificac A quebra do protocolo é fácil. A encriptação torna-se lenta.	
		tem a propriedade de total secrecy, se, e só se:
0.5/0.5	 O protocolo pode ser quebrado em te O protocolo pode ser quebrado em te A probabilidade de um plaintext é in O conjunto das chaves possíveis tem ciphertexts. 	empo polinomial.
	Questão 9 O funcionamento do RSA é	baseado no seguinte:
0.5/0.5	Mulitplicação é fácil e factorização é Mulitplicação é fácil e divisão é difíci Exponenciação em \mathbb{F}_p^* é fácil e factor Exponenciação em \mathbb{F}_p^* é fácil e o Disc	l. ização é difícil.
		rtantes em criptografia, porque (empiricamente):
CECTA -	A exponenciação é mais rápida sobre	
-0.2/0.5		licada sobre curvas elípticas do que em \mathbb{F}_p^* . a sobre curvas elípticas do que em \mathbb{F}_p^* .
	A operação de "adição" é mais fácil s	•

Francesco Lupo Elisa - 47701 - MIEI Mark: 2.1/5 (total score: 2.1/5)



+75/1/32+

	Departamento de Matemá Criptografia	tica 8/7/2	Faculdade de Ciências e Tecnolog 2018 Ex	gia — UNL same Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1		úmero de aluno preenchendo completam a grelha ao lado () e escreva o nome aixo.	
	2 2 2 2 2 3 3 3 3 3	Nome: Trance	xo Jupo Elisa	
	4 4 5 5 5 5 6 6 6 6	Curso: MIEI	Número de aluno: .477 (
	7 2 7 7 8 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. Na rta preenchendo completamente o quada azul ou preta, cada resposta certa vale desconta 0,2 valores e marcações múltiplas classificações das questões de escolha a será atribuído 0 valores como resultado	rado respec- 0,5 valores, as anulam a múltipla der
	Questão 1 Considere o g se, c só se:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se e	definir uma multiplicação tal que \mathbb{F}_n	é um corpo
-0.2/0.5		de <i>Kerckhof</i> f são princ	n é um número par. n é uma potência de um númer cípios que todos os sistemas criptográf diz que a segurança de um sistema cr	ficos devem
	deve depender: do segredo da chave e d			rprografico
0.5/0.5	só da complexidade da só do segredo do algorit só da chave, mas não de	thmo, mas não do seg		
	Questão 3 Qual destes pr	rotocolos criptográfico	os é assimétrico?	
0.5/0.5	☐ AES ☑ ElGamal		☐ DES ☐ Vigenère	
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	congruência $g^x \equiv h \pmod p$ é:	
0.5/0.5	Determine g , dados h , p Determine p , dados g , h		Determine x , dados g , $h \in p$. Determine h , dados g , $p \in x$.	

	Questão 5 No protocolo de troca de chaves secretos a e b para calcular números A e B que s	s de Diffie-Hellman, Alice e Bob usam números ão depois trocados.	
0.5/0.5	 A é calculado por a^g (mod p), B por b^g (mod p) A é calculado por g^a (mod p), B por g^b (mod p) A é calculado por a^g (mod p), B por b^g (mod p) A é calculado por g^a (mod p), B por g^b (mod p) 	od p) e a chave comum secreta é $g^{ab} \pmod{p}$. od p) e a chave comum secreta é $g^{ab} \pmod{p}$.	
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa enviar um <i>ciphertext</i> (c_1, c_2) com $c_1 \equiv g^k \pmod{p}$ Para recuperar a mensagem m , Alice calcula:	a chave pública da Alice $A \equiv g^a \pmod{p}$ para p) e $c_2 \equiv mA^k \pmod{p}$; k uma chave ephemeral.	
0/0.5	$igsqcup c_1 \cdot (c_2^a)^{-1} \pmod p$ $igsqcup (c_1^a) \cdot (c_2)^{-1} \pmod p$		
	Questão 7 — O algoritmo de Miller-Rabin devol No caso improvável do número devolvido p não criptográfico de $ElGamal$ que usa este número pa		
0/0.5	 Duas mensagens podem ser codificadas pelo A encriptação torna-se lenta. Dois ciphertexts podem encriptar a mesma e A quebra do protocolo é fácil. 		
	Questão 8 Um protocolo criptográfico tem a	propriedade de total secrecy, se, e só se:	
	O conjunto das chaves possíveis tem a mesi ciphertexts.	ma cardinalidade que o conjunto dos potenciais	
0.5/0.5	O protocolo pode ser quebrado em tempo po		
	A probabilidade de um plaintext é independente do ciphertext. O protocolo pode ser quebrado em tempo exponencial.		
	Questão 9 O funcionamento do RSA é basead		
0/0.5	 Mulitplicação é fácil e divisão é difícil. Mulitplicação é fácil e factorização é difícil. Exponenciação em F_p é fácil e o Discrete Lo. 	garithm Problem é difícil.	
	Exponenciação em \mathbb{F}_p^* é fácil e factorização é		
		em criptografia, porque (empiricamente):	
	 A operação de "adição" é mais fácil sobre cu A solução do DLP é mais complicada sobre 		
0.2/0.5	A operação de "adição" é mais complicada s		
	A exponenciação é mais rápida sobre curvas		