Miguel Henrique Rodrigues de Almeida - 45526 - MIEI Mark: 1.8/5 (total score: 1.8/5)

			+60/1/2+
	Departamento de Matemá Criptografia	tica 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  2 2 2 2 2 2  3 3 3 3 3  4 4 4 4 4  5 5 5 5  6 6 6 6 6  7 7 7 7 7  8 8 8 8 8	Nome: Miguel  Curso: MIFI  O exame é composto marque a resposta cer	Hemoique Rodigues de Almeida
0/0.5	Questão 1 Considere o g se, e só se:   \[ \text{n \circ uma potência de um} \] \[ n \circ um n\timero primo.	questão. Se a soma da um número negativo, rupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se	desconta 0,2 valores e marcações múltiplas anulam a as classificações das questões de escolha múltipla der será atribuído 0 valores como resultado final.  definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo $\square$ $n$ é um número par. $\square$ $n$ é um número primo ímpar.
			cípios que todos os sistemas criptográficos devem l diz que a segurança de um sistema criptográfico
-0.2/0.5	só do segredo do algori do segredo da chave e o só da complexidade da só da chave, mas não d	do segredo do algoritr encriptação.	mo.
0.5/0.5	Questão 3 Qual destes p  Vigenère  AES	rotocolos criptográfic	cos é assimétrico?  DES  ElGamal
	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 $h$ , dados $g$ , $g$	hex.	Determine $g$ , dados $h$ , $p \in x$ .  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.
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 $a^g \pmod{p}$ , $B$ 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 <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 $\mathbb{F}_p^*$ :
0/0.5	<ul> <li>☐ A encriptação torna-se lenta.</li> <li>☐ Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>☐ A quebra do protocolo é fácil.</li> </ul>
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
0.5/0.5	<ul> <li>O protocolo pode ser quebrado em tempo exponencial.</li> <li>A probabilidade de um plaintext é independente do ciphertext.</li> <li>O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.</li> </ul>
	O protocolo pode ser quebrado em tempo polinomial.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
0/0.5	<ul> <li>Exponenciação em F<sub>p</sub>* é fácil e factorização é difícil.</li> <li>Mulitplicação é fácil e divisão é difícil.</li> <li>Exponenciação em F<sub>p</sub>* é fácil e o Discrete Logarithm Problem é difícil.</li> <li>Mulitplicação é fácil e factorização é difícil.</li> </ul>
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0/0.5	<ul> <li>A exponenciação é mais rápida sobre curvas elípticas do que em F<sub>p</sub><sup>*</sup>.</li> <li>A solução do DLP é mais complicada sobre curvas elípticas do que em F<sub>p</sub><sup>*</sup>.</li> </ul>
	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 $\mathbb{F}_p^*$ .

Miguel Santos Araújo - 45699 - MIEI Mark: 1.8/5 (total score: 1.8/5)

•			+23/1/16+
	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		número de aluno preenchendo completamente os qua- a grelha ao lado ( ) e escreva o nome completo, o aixo.
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 5 5 5 5	Nome: Migus	Número de aluno: 45699
	6 6 6 6 7 7 7 7 7 8 8 8 8 8 8 8 9 9 9 9 10 10 10 10 10 10 10 10 10 10 10 10 10	O exame é composto marque a resposta ce tivo ( ) com caneta cada resposta errada questão. Se a soma da	por 10 questões de escolha múltipla. Nas questões erta preenchendo completamente o quadrado respectazul 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
0/0.5	n é uma potência de un n é um número par.  Questão 2 Os princípios o		n é um número primo.  n é um número primo ímpar.  cípios que todos os sistemas criptográficos devem
			l diz que a segurança de um sistema criptográfico
0.5/0.5	só da chave, mas não de só da complexidade da só do segredo do algoridado do segredo da chave e de ségredo da chave e de segredo da	encriptação. thmo, mas não do seg	gredo da chave.
	Questão 3 Qual destes pr	rotocolos criptográfic	os é assimétrico?
0.5/0.5	☐ Vigenère ☐ ElGamal		_ AES _ DES
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	congruência $g^{m{ au}} \equiv h \pmod{p}$ é:
0.5/0.5	Determine $p$ , dados $g$ , $h$ Determine $x$ , dados $g$ , $h$		Determine $h$ , dados $g$ , $p \in x$ .  Determine $g$ , dados $h$ , $p \in x$ .

	<b>Questão 5</b> 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.
0/0.5	$\boxtimes$ $A$ 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 $a^g \pmod{p}$ , $B$ por $b^g \pmod{p}$ e a chave comum secreta é $(ab)^g \pmod{p}$ . $\square$ $A$ é calculado por $a^g \pmod{p}$ , $B$ por $b^g \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$ . $\square$ $A$ 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:
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	<ul> <li>□ Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>□ A quebra do protocolo é fácil.</li> <li>☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> </ul>
	A encriptação torna-se lenta.  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.
-0.2/0.5	O protocolo pode ser quebrado em tempo exponencial.  O protocolo pode ser quebrado em tempo polinomial.
	A probabilidade de um plaintext é independente do ciphertext.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
0/0.5	<ul> <li>Mulitplicação é fácil e divisão é difícil.</li> <li>Exponenciação em F<sub>p</sub><sup>*</sup> é fácil e o Discrete Logarithm Problem é difícil.</li> <li>Mulitplicação é fácil e factorização é difícil.</li> </ul>
	Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente): $\boxtimes$ A solução do $DLP$ é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
0/0.5	A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\square$ 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 $\mathbb{F}_p^*$ .

Miguel da Silva de Brito Cordeiro - 41793 - MIEI Mark: 3.3/5 (total score: 3.3/5)

+78/1/26+

	Departamento de Matemá Criptografia	itica Faculdade de C 8/7/2018	Ciências e Tecnologia — UNL Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1	Marque o seu número de aluno predrados respectivos da grelha ao lado ( número e o curso abaixo.	) e escreva o nome completo, o
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 5 5 5 5 5	Nome: Higuel da Silve Cordeion Curso: MI EI Número	a de Brito
	6 6 6 6 6 7 7 7 7 7 8 8 8 8 8 9 9 9 9 9	O exame é composto por 10 questões de marque a resposta certa preenchendo co tivo ( ) com caneta azul ou preta, cada cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das um número negativo, será atribuído 0 val	e escolha múltipla. Nas questões mpletamente o quadrado respec- a resposta certa vale 0,5 valores, s e marcações múltiplas anulam a questões de escolha múltipla der
	Questão 1 Considere o g se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multip	
-0.2/0.5	n é um número primo. $n$ é uma potência de um	m número primo.  n é um núm	-
		le Kerckhoff são princípios que todos os erckhoff fundamental diz que a seguran	
0.5/0.5			
	Questão 3 Qual destes pr	rotocolos criptográficos é assimétrico?	
0.5/0.5	☐ DES ☐ Vigenère	ElGamal  AES	
	Questão 4 O Discrete Logarithm Pro	$blem\;(DLP)$ para a congruência $g^x\equiv h$	$n \pmod{p}$ é:
0.5/0.5			, dados $h$ , $p \in x$ . , 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.
0.5/0.5	
	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 $\mathbb{F}_p^*$ :
0/0.5	<ul> <li>Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>A encriptação torna-se lenta.</li> <li>A quebra do protocolo é fácil.</li> <li>Dois ciphertexts podem encriptar a mesma mensagem.</li> </ul>
	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 protocolo pode ser quebrado em tempo exponencial.  O protocolo pode ser quebrado em tempo polinomial.  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:
0.5/0.5	<ul> <li>Exponenciação em F<sub>p</sub>* é fácil e o Discrete Logarithm Problem é difícil.</li> <li>Mulitplicação é fácil e divisão é difícil.</li> <li>Exponenciação em F<sub>p</sub>* é fácil e factorização é difícil.</li> <li>Mulitplicação é fácil e factorização é difícil.</li> </ul>
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0/0.5	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 $\mathbb{F}_p^*$ .  A operação de "adição" é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\square$ A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

Miguel Ângelo Lage Madeira - 45139 - MIEI Mark: 1/5 (total score: 1/5)



+73/1/36+

	Departamento de Matemá Criptografia	tica 8/7/20	Faculdade de Ciências e Tecnologia — UNL 018 Exame Final
	Número de aluno  0 0 0 0 0  1 1 2 1 1		imero 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	Nome: Higgs	PÂngelo dage Madeira
	5 <b>3</b> 5 5 5 6 6 6 6 6 7 7 7 7 7	Curso: MIEI	I Número de aluno: 45139
	8 8 8 8 8 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:		definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5	$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	m número primo.	
			cípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
-0.2/0.5	do segredo da chave e d  só do segredo do algorid  só da chave, mas não d  só da complexidade da	thmo, mas não do seg o segredo do algoritm	gredo da chave. X
	Questão 3 Qual destes p	rotocolos criptográfico	os é assimétrico?
0/0.5	⊠ ElGamal □ Vigenère ∡		
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	congruência $g^x \equiv h \pmod p$ é:
0.5/0.5			Determine $x$ , dados $g$ , $h \in p$ .  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.
-0.2/0.5	
	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	<ul> <li>□ Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>□ A quebra do protocolo é fácil.</li> <li>□ A encriptação torna-se lenta.</li> </ul>
-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 exponencial.  A probabilidade de um plaintext é independente do ciphertext.  O protocolo pode ser quebrado em tempo polinomial.  O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.
0.5/0.5	<ul> <li>Questão 9 O funcionamento do RSA é baseado no seguinte:</li> <li>☐ Exponenciação em F<sub>p</sub>* é fácil e o Discrete Logarithm Problem é difícil.</li> <li>☐ Mulitplicação é fácil e factorização é difícil.</li> <li>☐ Mulitplicação é fácil e divisão é difícil.</li> <li>☐ Exponenciação em F<sub>p</sub>* é fácil e factorização é difícil.</li> </ul>
-0.2/0.5	<ul> <li>Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):</li> <li></li></ul>

Miguel Ângelo Leal Pereira - 43858 - MIEI Mark: 3.3/5 (total score: 3.3/5)

	•		+44/1/34	+
	Departamento de Mat Criptografia		Faculdade de Ciências e /2018	Tecnologia — UNI Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1		número de aluno preenchendo c da grelha ao lado ( ) e escreva	
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 4 5 5 5 5 5 5 5		just Angela Loa	
	6 6 6 6 6 7 7 7 7 7 8 8 8 8 9 9 9 9 9	O exame é composta o marque a resposta o tivo ( ) com canet cada resposta errada questão. Se a soma	Número de aluno:  no por 10 questões de escolha m certa preenchendo completament ca azul ou preta, cada resposta a desconta 0,2 valores e marcaçõe das classificações das questões de o, será atribuído 0 valores como	últipla. Nas questões te o quadrado respec- certa vale 0,5 valores, es múltiplas anulam a e escolha múltipla dcr
	Questão 1 Consider se, e só se:	e o grupo Z/nZ. Pode-s	e definir uma multiplicação ta	l que $\mathbb{F}_n$ é um corpo
0/0.5	igwedge n é uma potência $igwedge n$ é um número pr		n é um número primo $n$ é um número par.	ímpar.
			ncípios que todos os sistemas o al diz que a segurança de um s	
0.5/0.5	só da complexidad só do segredo do a	ão do segredo do algorio e da encriptação. Igorithmo, mas não do s e e do segredo do algori	egredo da chave.	
	Questão 3 Qual des	tes protocolos criptográf	icos é assimétrico?	
0.5/0.5	☐ DES ☐ AES		ElGamal Vigenère	
	Questão 4 O Discrete Logarithm	a <i>Problem (DLP</i> ) para a	congruência $g^x \equiv h \pmod p$	é:
0.5/0.5	$\Box$ Determine $g$ , dados $\Box$ Determine $h$ , dados		Determine $p$ , dados $q$ ,	

