Rafael dos Reis Ferreira da Costa - 45464 - MIEI Mark: 3.8/5 (total score: 3.8/5)

		+29/1/4+
	Departamento de Matemá Criptografia	tica Faculdade de Ciências e Tecnologia — UNL 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 5 5 5 5 5	Nome: Rafael dos Reis Ferreira da
	6 6 6 6 6 7 7 7 7 7 8 8 8 8 8	Curso: MIEI. Número de aluno: 45464  O exame é composto por 10 questões de escolha múltipla. Nas questões marque a resposta certa preenchendo completamente o quadrado respec-
	99999	tivo ( ) 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, 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	satisfazer. Um princípio de K	n é um número primo ímpar.  n número primo.  n é um número primo.  de Kerckhoff são princípios que todos os sistemas criptográficos devem ferckhoff fundamental diz que a segurança de um sistema criptográfico
0.5/0.5		lo segredo do algoritmo. thino, mas não do segredo da chave.
	Questão 3 Qual destes p	rotocolos criptográficos é assimétrico?
0.5/0.5	☐ AES ☐ DES	<ul><li>☑ ElGamal</li><li>☑ Vigenère</li></ul>
	Questão 4 O Discrete Logarithm Pro	$ablem\;(DLP)$ para a congruência $g^x\equiv h\;(\operatorname{mod} p)$ é:
0.5/0.5	Determine $p$ , dados $g$ , $h$ Determine $g$ , dados $h$ , $g$	

4

	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 $A \equiv g^a \pmod{p}$ 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>ephemera</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 protocole criptográfico de <i>ElGamal</i> que usa este número para a escolha de $\mathbb{F}_p^*$ :
0.5/0.5	<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	<ul> <li>O protocolo pode ser quebrado em tempo polinomial.</li> <li>O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.</li> </ul>
	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:
	Mulitplicação é fácil e divisão é difícil.  Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
0.5/0.5	Mulitplicação é fácil e factorização é difícil.
	$\square$ 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 complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
-0.2/0.5	$\square$ A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$lacksquare$ A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\boxtimes$ A solução do <i>DLP</i> é mais complicada sobre curvas elípticas do que em $\mathbb{F}_{p}^{*}$ .

Raquel Rodrigues Ferreira - 49847 - MIEI Mark: 2.2/5 (total score: 2.2/5)



+82/1/18+

	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		imero de aluno preenchendo completamente os qua- grelha ao lado ( ) c escreva o nome completo, o ixo.
	3 3 3 3 3 3 4 4 4 4 4 5 5 5 5 5 5 6 6 6 6 6 6	Nome: Raque	1 Rodrigues Ferreiro  Número de aluno: 49843
	7 7 7 7 8 8 8 8 8 8 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 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		definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5			n é um número primo impar.  n é uma potência de um número primo.  cípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
-0.2/0.5	só da complexidade da só do segredo do algorit do segredo da chave e d só da chave, mas não de	thmo, mas não do seg lo segredo do algoritn	uo.
-0.2/0.5	Questão 3 Qual destes proposed Vigenère  DES	rotocolos criptográfico	os é assimétrico?  AES  ElGamal
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	ongruência $g^x \equiv h \pmod p$ é:
0.5/0.5			Determine $p$ , dados $g$ , $h \in x$ .  Determine $x$ , dados $g$ , $h \in p$ .

	<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.
0.5/0.5	
	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 $\mathbb{F}_p^*$ :
-0.2/0.5	A quebra do protocolo é fácil.  A encriptação torna-se lenta.  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 secrecu se e só ser
0.5/0.5	<ul> <li>Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:</li> <li>O protocolo pode ser quebrado em tempo polinomial.</li> <li>O protocolo pode ser quebrado em tempo exponencial.</li> <li>O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.</li> </ul>
	A probabilidade de um plaintext é independente do ciphertext.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
0.5/0.5	<ul> <li>Mulitplicação é fácil e factorização 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 divisão é difícil.</li> <li>Exponenciação em F<sub>p</sub><sup>*</sup> é fácil e factorização é difícil.</li> </ul>
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0.5/0.5	<ul> <li>A operação de "adição" é mais fácil sobre curvas elípticas do que em F<sub>p</sub>*.</li> <li>A solução do DLP é mais complicada sobre curvas elípticas do que em F<sub>p</sub>*.</li> <li>A exponenciação é mais rápida sobre curvas elípticas do que em F<sub>p</sub>*.</li> <li>A operação de "adição" é mais complicada sobre curvas elípticas do que em F<sub>p</sub>*.</li> </ul>
	$\square$ A operação de "adição" é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

Ricardo Boto Semblano da Silva - 41951 - MIEI Mark: 3.3/5 (total score: 3.3/5)

+91/1/60+

	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 1 1 1 1 1 1 1 1 1	drados respectivos da número e o curso aba	imero de aluno preenchendo completamente os qua- grelha ao lado ( ) e escreva o nome completo, o ixo.
	3 3 3 3 3 4 4 4 4 5 5 5 5 5 5 6 6 6 6 6	Nome:	
	7 7 7 7 7 8 8 8 8 8 8 9 9	marque a resposta certivo ( ) com caneta cada resposta errada o questão. Se a soma da	por 10 questões de escolha múltipla. Nas questões rta preenchendo completamente o quadrado respec- azul ou preta, cada resposta certa vale 0,5 valores, lesconta 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 Z/nZ. Pode-se	definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
0.5/0.5		m número primo.	n é um número par. n é um número primo ímpar.
			cípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
0.5/0.5	só do segredo do algorido só da complexidade da do segredo da chave e do só da chave, mas não de	encriptação. lo segredo do algorita	no.
	Questão 3 Qual destes pa	rotocolos criptográfic	os é assimétrico?
0.5/0.5	☐ Vigenère ☐ AES		ElGamal  DES
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	eongruência $g^{oldsymbol{ au}}\equiv h\ (\mathrm{mod} p)$ 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 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 $g^{ab} \pmod{p}$ . $\square$ $A$ 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 $g^a \pmod{p}$ , $B$ 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 $\mathbb{F}_p^*$ :
0.2/0.5	<ul> <li>☐ A encriptação torna-se lenta.</li> <li>☑ Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>☐ A quebra do protocolo é fácil.</li> </ul>
	<ul> <li>Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>Questão 8 Um protocolo criptográfico tem a propriedade de total secrecu, se. e só se:</li> </ul>
	<ul> <li>Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:</li> <li>O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.</li> </ul>
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.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
0.5/0.5	<ul> <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><sup>*</sup> é fácil e factorização é difícil.</li> <li>Exponenciação em F<sub>p</sub><sup>*</sup> é fácil e o Discrete Logarithm Problem é difícil.</li> </ul>
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0.5/0.5	$\square$ A operação de "adição" 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 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 $\mathbb{F}_p^*$ .
	•

Ricardo João Duarte Pinheiro - 41631 - MIEI Mark: 1.4/5 (total score: 1.4/5)

•			+68/1/46	<u>;</u> +
	Departamento de Matemá Criptografia	itica 8/7/2	Faculdade de Ciências e 018	Tecnologia — UNI Exame Final
	Número de almo 0 0 0 0 0 1 1 1 1		imero de aluno preenchendo o grelha ao lado (  ) e escrevixo.	
	2 2 2 2 2 3 3 3 3 3 3 4 4 4 4 4	Nome: Rica ob	João Quarte P	linhein O
	5 5 5 5 6 6 6 6 7 7 7 7 7	Curso: HIEI	Número de aluno:	
	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 n rta preenchendo completamer azul ou preta, cada resposta desconta 0,2 valores e marcações es classificações das questões de será atribuído 0 valores como	nte o quadrado respec certa vale 0,5 valores ões múltiplas anulam a de escolha múltipla de
	Questão 1 Considere o g se, e só se:	grupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se o	definir uma multiplicação ta	al 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 $n$ é um número par.	um número primo.
	Questão 2 Os princípios satisfazer. Um princípio de F deve depender:		cípios que todos os sistemas diz que <i>a segurança de um</i>	
0/0.5	<ul> <li>do segredo da chave e</li> <li>≤ só da chave, mas não d</li> <li>só da complexidade da</li> <li>só do segredo do algori</li> </ul>	do segredo do algoritm encriptação.	ю.	**
	Questão 3 Qual destes p	protocolos criptográfico	os é assimétrico?	
0.5/0.5	ElGamal  Vigenère		☐ 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 $x$ , dados $g$ ,			

-0.2/0.5	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. $A$ 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 $g^{ab} \pmod{p}$ . $A$ 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:
0.5/0.5	
	<b>Questão 7</b> 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 quebra do protocolo é fácil.</li> <li>☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>□ A encriptação torna-se lenta.</li> <li>□ Dois ciphertexts podem encriptar a mesma mensagem.</li> </ul>
0.5/0.5	<ul> <li>Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:</li> <li>O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.</li> <li>O protocolo pode ser quebrado em tempo exponencial.</li> <li>O protocolo pode ser quebrado em tempo polinomial.</li> <li>A probabilidade de um plaintext é independente do ciphertext.</li> </ul>
0/0.5	Questão 9 — O funcionamento do $RSA$ é baseado no seguinte: $\square$ Exponenciação em $\mathbb{F}_p^*$ é fácil e o $Discrete$ $Logarithm$ $Problem$ é difícil. $\square$ Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil. $\square$ Mulitplicação é fácil e divisão é difícil. $\square$ Mulitplicação é fácil e factorização é difícil.
-0.2/0.5	<ul> <li>Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):</li> <li>A operação de "adição" é mais fácil sobre curvas elípticas do que em F<sub>p</sub>*.</li> <li>A exponenciação é mais rápida sobre curvas elípticas do que em F<sub>p</sub>*.</li> <li>A operação de "adição" é mais complicada sobre curvas elípticas do que em F<sub>p</sub>*.</li> <li>A solução do DLP é mais complicada sobre curvas elípticas do que em F<sub>p</sub>*.</li> </ul>

Ricardo Miguel Gonçalves Leitao - 47296 - MIEI Mark: 2.2/5 (total score: 2.2/5)

•			+11/1/40+
Departar Criptogra	nento de Matemática afia	Faculdade 8/7/2018	e de Ciências e Tecnologia — UNI Exame Final
	0 0 0 drados		no preenchendo completamente os quado ( ) e escreva o nome completo, o
2 2 1 3 3 ( 4 ( 5 5 (	3 3 3 4 4 4 4	1105	Gonfaluer Leitat
6 6 6 7 7 7 7 7 8 8 8 8 8 9 9 5	7 7 7 O exan 8 8 8 marque tivo ( cada re questão	ne é composto por 10 quest a resposta certa preenchen ) com caneta azul on preta sposta errada desconta 0,2 v . Se a soma das classificaçõe	ões de escolha múltipla. Nas questões do completamente o quadrado respecto, cada resposta certa vale 0,5 valores, alores e marcações múltiplas anulam a es das questões de escolha múltipla der o 0 valores como resultado final.
Questão : sc, e só se:	1 Considere o grupo Z/		nultiplicação tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5	un número par. m número primo.		número primo ímpar. na potência de um número primo.
Questão 2 satisfazer. deve depend	Um princípio de Kerckhofl	choff são princípios que too fundamental diz que a seg	los os sistemas criptográficos devem gurança de um sistema criptográfico
0.5/0.5 do seg	complexidade da encripta gredo da chave e do segred chave, mas não do segred segredo do algorithmo, m	do do algoritmo. o do algoritmo.	e.
Questão 3	Qual destes protocolo	s criptográficos é assimétr	ico?
0.5/0.5 ElGar Vigen		☐ DES ☐ AES	
Questão 4  O Discre	ete Logarithm Problem (D	LP) para a congruência $g$	$x \equiv h \pmod{p}$ é:
0.5/0.5	mine $g$ , dados $h$ , $p \in x$ .  nine $x$ , dados $g$ , $h \in p$ .	Determi	ine $p$ , dados $g$ , $h \in x$ . ine $h$ , 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 $g^a \pmod{p}$ , $B$ 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 <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	<ul> <li>A quebra do protocolo é fácil.</li> <li>□ Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>□ A encriptação torna-se lenta.</li> </ul>
	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 polinomial.
	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:
	Mulitplicação é fácil e factorização é difícil.
-0.2/0.5	Exponenciação em $\mathbb{F}_p^*$ é fácil e o Discrete Logarithm Problem é difícil.  Mulitplicação é fácil e divisão é difícil.
	Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
	$\square$ A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
0.5/0.5	$\square$ A operação de "adição" é mais fácil 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 complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .