Guilherme de Oliveira Valadas Faria - 47260 - MIEI Mark: 0.2/5 (total score: 0.2/5)

 $\square$  Determine h, dados g, p e x.

		+61/1/60+
	Departamento de Matemát Criptografia	cica Faculdade de Ciências e Tecnologia — UNL 8/7/2018 Exame Final
	Número de aluno  0 0 0 0 1 1 1 1 1 1 1 1 1 1 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.  Nome:   Fauta
	99999	Curso: MIEL Número de aluno: 47766  O exame é composto por 10 questões de escolha múltipla. Nas questões marque a resposta certa preenchendo completamente o quadrado respectivo (1) 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, 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		impar. $n$ é uma potência de um número primo. $n$ é um número primo.
		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 do segredo do algorit só da chave, mas não do só da complexidade da do segredo da chave e d	encriptação.
	Questão 3 Qual destes pr	rotocolos criptográficos é assimétrico?
-0.2/0.5	<ul><li>☑ ElGamal</li><li>☑ AES</li></ul>	☐ Vigenère ☐ DES
	Questão 4 O Discrete Logarithm Pro	$blem\;(DLP)\;  ext{para a congruência}\; g^{\mathbf{r}}\equiv h\;(\operatorname{mod} p)\;  ext{\'e} :$
-0.2/0.5	Determine p, dados g, h	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.		
0.5/0.5			
	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			
	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 $\mathbb{F}_p^{\bullet}$ :		
)/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.		
)/0.5	<ul> <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>		
	Questão 9 O funcionamento do RSA é baseado no seguinte:		
)/0.5	<ul> <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>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> </ul>		
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):		
0.2/0.5	<ul> <li>A operação de "adição" é mais fácil 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> <li>A exponenciação é mais rápida sobre curvas elípticas do que em F<sub>p</sub>*.</li> </ul>		

Heitor da Silva Cordeiro Moniz - 45809 - MIEI Mark: 2.1/5 (total score: 2.1/5)

T		1	

+80/1/22+

	Departamento de Matemá Criptografia	itica 8/7/20	Faculdade de Ciências e Tecnologia — UNL D18 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 4  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: Haiton  Nome: Haiton  Nome: Manua  Curso: MIEI  O exame é composto parque a resposta certivo ( ) com caneta a cada resposta errada dequestão. Se a soma das	nero de aluno preenchendo completamente os quagrelha ao lado (  ) e escreva o nome completo, o xo.   da Silva Condeino  Número de aluno: 45809  Dor 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 se classificações das questões de escolha múltipla der cerá atribuído 0 valores como resultado final.
	Questão 1 Considere o g se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se d	efinir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
0.5/0.5	n é um número par.  n é um potência de un  Questão 2 Os princípios e satisfazer. Um princípio de K  deve depender:	le <i>Kerckhoff</i> são princi	n é um número primo.  n é um número primo ímpar.  (pios 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 algoria só da chave, mas não d do segredo da chave e d	thmo, mas não do segro o segredo do algoritmo	).
0.5/0.5	Questão 3 Qual destes por DES ElGamal	rotocolos criptográfico	s é assimétrico?  Vigenère  AES
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a co	ngruência $g^x \equiv h \pmod{p}$ é:
0/0.5		1	Determine $x$ , dados $g$ , $h \in p$ .  Determine $h$ , dados $g$ , $p \in x$ .

	<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.
0.2/0.5	$\nearrow$ $A$ é calculado por $g^a \pmod{p}$ , $B$ por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$ . $\nearrow$ $A$ é calculado por $g^a \pmod{p}$ , $B$ por $g^b \pmod{p}$ e a chave comum secreta é $A \cdot B$ . $\nearrow$ $A$ é calculado por $a^g \pmod{p}$ , $B$ por $b^g \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$ . $\nearrow$ $A$ 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 $\mathbb{F}_p^*$ :
0/0.5	<ul> <li>□ Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>□ A encriptação torna-se lenta.</li> <li>□ A quebra do protocolo é fácil.</li> </ul>
	Duas mensagens podem ser codificadas pelo mesmo <i>ciphertext</i> .
	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	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:
	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 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 $\mathbb{F}_p^*$ .
0/0 <b>E</b>	$\square$ A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
0/0.5	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 $\mathbb{F}_p^*$ .



+67/1/48+

	Departamento de Matemá	tica Faculdade de C	liências e Tecnologia — UNL
	Criptografia	8/7/2018	Exame Final
	Número de aluno  0 0 0 0 0  1 1 1 1 1  2 2 2 2	← Marque o seu número de aluno predrados respectivos da grelha ao lado (■ número e o curso abaixo.	) e escreva o nome completo, o
	3 3 3 3 3 3 3 4 4 4 4 4 5 5 5 5 5 6 6 6 6 6 6 6 6 6 6	I.ValG	de aluno: 42526
	77777	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	mpletamente o quadrado respec- a resposta certa vale <u>0,5</u> valores, e e marcações múltiplas anulam a questões de escolha múltipla der
	Questão 1 Considere o g se, c só sc:	rupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multip	plicação tal que F <sub>n</sub> é um corpo
-0.2/0.5	n é um número primo. n é uma potência de un		nero primo ímpar. nero par.
		de Kerckhoff são princípios que todos os cerckhoff fundamental diz que a seguran	
0/0.5	só da complexidade da	thmo, mas não do segredo da chave.	
	Questão 3 Qual destes p	rotocolos criptográficos é assimétrico?	
0.5/0.5	☐ AES  ■ ElGamal	☐ Vigenère ☐ DES	
	Questão 4 O Discrete Logarithm Pro	$color (DLP)$ para a congruência $g^x \equiv b$	$h \pmod{p}$ é:
-0.2/0.5	$igstyle igstyle  ext{Determine } x,  ext{ dados } g, g$ $igstyle  ext{Determine } h,  ext{ dados } g, g$		a, dados $h$ , $p$ e $x$ . a, dados $g$ , $h$ e $x$ .

	<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.
0.5/0.5	☐ $A$ 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 $g^a \pmod{p}$ , $B$ 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 $(ab)^g \pmod{p}$ . >
	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:
-0.2/0.5	
	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 $\mathbb{F}_p^*$ :
0.5/0.5	<ul> <li>Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>A quebra do protocolo é fácil.</li> <li>Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>A encriptação torna-se lenta.</li> </ul>
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
-0.2/0.5	<ul> <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> <li>O protocolo pode ser quebrado em tempo polinomial.</li> <li>X probabilidade de um plaintext é independente do ciphertext.</li> </ul>
	Questão 9 O funcionamento do RSA é baseado no seguinte:
-0.2/0.5	<ul> <li>Mulitplicação é fácil e factorização 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> <li>Mulitplicação é fácil e divisão é difícil.</li> </ul>
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
-0.2/0.5	$\boxtimes$ 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 $\mathbb{F}_p^*$ .
	☐ A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .  ☐ A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

Hugo Daniel Cepeda Mochão - 47231 - MIEI Mark: 0.8/5 (total score: 0.8/5)

+37/1/48+

	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 1	drados respectivos da número e o curso abai	
	3 3 3 3 3		nochao
	5 5 5 5 5 6 6 6 6 6 7 <b>7</b> 7 7	O exame é composto	número de aluno: 7 2 3 1
	9 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, lesconta 0,2 valores e marcações múltiplas anulam a s classificações das questões de escolha múltipla der será atribuído 0 valores como resultado final.
	Questão 1 Considere o gr se, c só se:	rupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se o	definir uma multiplicação tal que F <sub>n</sub> é um corpo
0.5/0.5	n ć um número primo í $n$ ć um número primo.	ímpar.	n é uma potência de um número primo. $n$ é um número par.
			rípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
-0.2/0.5	só da complexidade da  só da chave, mas não do  só do segredo do algorit  do segredo da chave e d	o segredo do algoritm	redo da chave.
	Questão 3 Qual destes pr	rotocolos criptográfico	os é assimétrico?
-0.2/0.5	ElGamal  AES		<ul><li>□ Vigenère</li><li>□ DES</li></ul>
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	ongruência $g^x \equiv h \; (\operatorname{mod} p) \; \acute{\mathrm{e}}$ :
0.5/0.5	Determine $h$ , dados $g$ , $p$ Determine $x$ , dados $g$ , $h$		Determine $p$ , dados $g$ , $h \in x$ .  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.
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:
-0.2/0.5	
	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 <i>ElGamal</i> que usa este número para a escolha de $\mathbb{F}_p^*$ :
0.5/0.5	<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:
-0.2/0.5	<ul> <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:  Mulitplicação é fácil e divisão é difícil.
-0.2/0.5	<ul> <li>✓ Mulitplicação é fácil e factorização é difícil.</li> <li>☐ Exponenciação em F<sub>p</sub> é fácil e o Discrete Logarithm Problem é difícil.</li> </ul>
	$\bigoplus$ Exponenciação em $\mathbb{F}_p^*$ 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 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 $\mathbb{F}_p^*$ .
	$\boxtimes$ A solução do $DLP$ é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

Hélio Torres Aguiar - 41745 - MIEI Mark: 0/5 (total score: -0.6/5)



+95/1/52+

	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	← 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	Nome: Helio Torres Agrins
	4     4       5     5       5     6       6     6       6     6       6     6	Curso: MIEI Número de aluno: 41745
	7 7 7 7 8 8 8 8 8 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 g se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5	igwedge n é uma potência de un $igwedge n$ é um número par.	n número primo. $n \in \mathbb{R}$ n é um número primo. $n \in \mathbb{R}$ 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 complexidade da  só da chave, mas não de  do segredo da chave e d  só do segredo do algorit	o segredo do algoritmo.
	Questão 3 Qual destes pr	rotocolos criptográficos é assimétrico?
0.5/0.5	☐ DES ☐ Vigenère	☐ AES ElGamal
	Questão 4 O Discrete Logarithm Pro	$blem\;(DLP)\;  ext{para a congruência}\; g^x\equiv h\;(\operatorname{mod} p)\;  ext{\'e} :$
-0.2/0.5	Determine $p$ , dados $g$ , $h$ Determine $h$ , dados $g$ , $p$	<b>y</b> , and <b>y</b> , and <b>y</b>

	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 $g^a \pmod{p}$ , $B$ 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 $g^{ab} \pmod{p}$ .  ☐ $A$ 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:
-0.2/0.5	
	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 $\mathbb{F}_p^*$ :
-0.2/0.5	<ul> <li>Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>         ☐ A encriptação torna-se lenta.     </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:
-0.2/0.5	O protocolo pode ser quebrado em tempo exponencial.
	O protocolo pode ser quebrado em tempo polinomial.
	<ul> <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:
	Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
-0.2/0.5	Mulitplicação é fácil e divisão é difícil.
	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 complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
0.2/0.5	$\bigcirc$ A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
-0.2/0.5	$\square$ A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\nearrow$ A solução do $DLP$ é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .