José Francisco Ribeiro - 49546 - MIEI Mark: 1.2/5 (total score: 1.2/5)

+20/1/22+

	Departamento de Matemá Criptografia	tica 8/7/2	Faculdade de Ciências c Tecnologia — UNL 1018 Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 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 4 4 4 4 5 5 5 5 5		Francisco Rubino Rubino Número de aluno: 49546
	6 6 6 6 6 7 7 7 7 7 7 8 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, desconta 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, e só se:		definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
0/0.5	n é um número primo. n é um número par.		n é um número primo ímpar. n é uma potência de um número primo.
			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 do segredo do algorit  só da complexidade da e  só da chave, mas não do	hmo, mas não do seg encriptação.	redo da chave.
	Questão 3 Qual destes pr	otocolos criptográfico	os é assimétrico?
0.5/0.5	☐ DES ☐ AES		☐ Vigenère ☐ ElGamal
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	ongruência $g^{m{x}} \equiv h \pmod p$ é:
0.5/0.5			Determine $x$ , dados $g$ , $h \in p$ .  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.
0.2/0.5	
	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:
0/0.5	
	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>A encriptação torna-se lenta.</li> <li>∑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</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	<ul> <li>□ O protocolo pode ser quebrado em tempo polinomial.</li> <li>□ A probabilidade de um plaintext é independente do ciphertext.</li> <li>□ O protocolo pode ser quebrado em tempo exponencial.</li> </ul>
	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>Mulitplicação é fácil e factorização é difícil.</li> <li>Exponenciação em F<sub>p</sub>* é fácil e factorização 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 exponenciação é mais rápida 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>
	. , ,

João André Furtado Teixeira - 48047 - MIEI Mark: 0/5 (total score: -0.2/5)

+12/1/38+

	Departamento de Matemá	tica Faculdade de Ciências e Tecnologia — UNL			
	Criptografia	8/7/2018 Exame Final			
	Número de aluno	← Marque o seu número de aluno preenchendo completamente os qua-			
	0 0 👹 0 0	drados respectivos da grella ao lado ( ) e escreva o nome completo, o			
		número e o curso abaixo.			
	2 2 2 2 2	12 Robert E. A.A. T.			
	3 3 3 3	Nome: Jose Andre Eurlado Teixusa			
	44444				
	5 5 5 5	Curso: MIEI Número de aluno: 48047			
	66666	Curso: 1911 Número de aluno:			
	7777	O exame é composto por 10 questões de escolha múltipla. Nas questões			
	8 🌉 8 8 8	marque a resposta certa preenchendo completamente o quadrado respec- tivo ( ) com caneta azul ou preta, cada resposta certa vale 0,5 valores,			
	99999	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			
-0.2/0.5	n é um número primo.	$\nearrow$ $n$ é uma potência de um número primo.			
0.2, 0.0	n é um número primo í	mpar. $\square$ $n$ é um número par.			
		le Kerckhoff são princípios que todos os sistemas criptográficos devem erckhoff fundamental diz que a segurança de um sistema criptográfico			
	só do segredo do algorit	hmo, mas não do segredo da chave.			
0.0/0.5	só da complexidade da	encriptação.			
-0.2/0.5	🕡 do segredo da chave e d	do segredo da chave e do segredo do algoritmo.			
	🔀 só da chave, mas não do	🔀 só da chave, mas não do segredo do algoritmo.			
	Questão 3 Qual destes pr	otocolos criptográficos é assimétrico?			
0.0/0.5	☐ Vigenère				
(orto	->DES	AES			
	Questão 4 O Discrete Logarithm Pro-	$blem\;(DLP)$ para a congruência $g^x\equiv h\;(\mathrm{mod}p)\;$ é:			
0.5/0.5	Determine g, dados h, p	***			
	$\bigsqcup$ Determine $p$ , dados $g$ , $h$	e $x$ . 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	o depois trocados.	
0.5/0.5	☐ $A$ é calculado por $g^a$ (mod $p$ ), $B$ por $g^b$ (mod $p$ ), $B$ por $b^g$ (mod $p$ ), $B$ por $b^g$ (mod $p$ ), $B$ por $g^b$ (mod $p$ ), $B$ p	$(d p)$ e a chave comum secreta é $g^{ab} \pmod{p}$ . $(d p)$ e a chave comum secreta é $g^{ab} \pmod{p}$ .	
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a 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 e $c_2 \equiv mA^k \pmod p$ ; $k$ uma chave $ephemeral$	
-0.2/0.5		$(c_1^a)^{-1} \cdot c_2 \pmod{p}$	
	Questão 7 O algoritmo de Miller-Rabin devolv No caso improvável do número devolvido p não e criptográfico de <i>ElGamal</i> que usa este número para		
-0.2/0.5	<ul> <li>Duas mensagens podem ser codificadas pelo e</li> <li>Dois ciphertexts podem encriptar a mesma m</li> <li>A quebra do protocolo é fácil.</li> <li>A encriptação torna-se lenta.</li> </ul>		
	Questão 8 Um protocolo criptográfico tem a p	ropriedade de total secrecy, se, e só se:	
0/0.5	O protocolo pode ser quebrado em tempo exp		
0,010	<ul> <li>O protocolo pode ser quebrado em tempo pol</li> <li>O conjunto das chaves possíveis tem a mesm ciphertexts.</li> </ul>	linomial. a cardinalidade que o conjunto dos potenciais	
	Questão 9 O funcionamento do RSA é baseado	o no seguinte:	
	$\square$ Exponenciação em $\mathbb{F}_p^*$ é fácil e o Discrete Log	arithm Problem é difícil.	
0/0.5	<ul> <li>Mulitplicação é fácil e divisão é difícil.</li> <li>Exponenciação em F<sub>p</sub> é fácil e factorização é</li> </ul>	difícil.	
	Mulitplicação é fácil e factorização é difícil.		
	Questão 10 Curvas elípticas são importantes en	m criptografia, porque (empiricamente):	
	A solução do DLP é mais complicada sobre c	eurvas elípticas do que em $\mathbb{F}_p^*$ .	
0.0/0.5	A operação de "adição" é mais fácil sobre cur	rvas elípticas do que em $\mathbb{F}_p^*$ .	
-0.2/0.5	A exponenciação é mais rápida sobre curvas e	the state of the s	
	A operação de "adição" é mais complicada so	bre curvas elípticas do que em $\mathbb{F}_p^*$ .	

João Carlos Cristo Reis - 43914 - MIEI Mark: 1.7/5 (total score: 1.7/5)

+22/1/18+

	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 1 1 1 1 1 1 1 1 1 1 1 1 1 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 4 4 4 4	Nome: Sooo C	arlos Cristo Reis
	5 5 5 5 5 6 6 6 6 6 7 7 7 7 7	Curso: MIE	Número de aluno: 43914
	88888	marque a resposta cer tivo () com caneta cada resposta errada o questão. Se a soma da	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 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	igwedge n é uma potência de un $igwedge n$ é um número par.	n número primo.	$n \in \mathbb{R}$ n $n$ um número primo. $n \in \mathbb{R}$ n $n$ um número primo impar.
			cípios 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 complexidade da  só da chave, mas não de  só do segredo do algorit	encriptação. o segredo do algoritm	ю.
	Questão 3 Qual destes pr	rotocolos criptográfico	os é assimétrico?
0.5/0.5	☐ DES  ElGamal		☐ AES ☐ Vigenère
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	ongruência $g^x \equiv h \; (\operatorname{mod} p) \;$ é:
0.5/0.5			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.
	$A \in \text{calculado por } a^g \pmod{p}$ , $B \text{ por } b^g \pmod{p}$ e a chave comum secreta $ext{calculator} g^{ab} \pmod{p}$ .
0.5/0.5	$A$ é calculado por $g^a$ (mod $p$ ), $B$ por $g^b$ (mod $p$ ) e a chave comum secreta é $g^{ab}$ (mod $p$ ).
0.5/0.5	$\square$ A é calculado por $g^a$ (mod $p$ ), $B$ por $g^b$ (mod $p$ ) 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 $(ab)^g \pmod{p}$ .
	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:
	$igspace (c_1^a)^{-1} \cdot c_2 \pmod p$ $\qquad \qquad \qquad$
-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 $\mathbb{F}_p^*$ :
	A encriptação torna-se lenta.
-0.2/0.5	Duas mensagens podem ser codificadas pelo mesmo ciphertext.
-0.2/0.3	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 exponencial.
0.5/0.5	A probabilidade de um plaintext é independente do ciphertext.
0.5/0.5	O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais
	ciphertexts.
	O protocolo pode ser quebrado em tempo polinomial.
	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 factorização é difícil.
	Mulitplicação é fácil e divisão 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):
	A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
0/0.5	$\boxtimes$ 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 $\mathbb{F}_p^*$ .
	A operação de "adição" é mais complicada sobre curvas elípticas do que em F <sup>∗</sup> <sub>p</sub> .

João Daniel da Luz Mota - 47598 - MIEI Mark: 2.4/5 (total score: 2.4/5)

•			+35/1/52+
	Departamento de Matemá Criptografia	ática 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		úmero de aluno preenchendo completamente os qua- u grelha ao lado (  ) e escreva o nome completo, o ixo.
	2 2 2 2 2 3 3 3 3 3 4 4 4 4		Deniel Nota
	5 5 5 5 6 6 6 6 7 7 7 7	Curso: MIEI	Número de aluno:
	8888	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 respec- azul 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 sc, c só se:	rupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se o	definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5	n é uma potência de un n é um número primo i	ímpar.	$n \in \mathbb{R}$ n'é um número par. $n \in \mathbb{R}$ n'é um número primo.
		erckhoff fundamental	diz que a segurança de um sistema criptográfico
0.5/0.5	do segredo da chave e d  só do segredo do algorit  só da chave, mas não do  só da complexidade da	thmo, mas não do seg o segredo do algoritm	redo da chave.
	Questão 3 Qual destes pr	rotocolos criptográfico	os é assimétrico?
0/0.5	☐ DES ☐ Vigenère		☐ AES ☑ ElGamal
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a co	ongruência $g^{oldsymbol{x}} \equiv h \pmod{p}$ 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.
	$A$ é calculado por $g^a \pmod{p}$ , $B$ por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$ .
0.5/0.5	$\square$ 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 $a^g \pmod{p}$ , $B$ 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 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:
0.5/0.5	
	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 ElCarral que use este primo este primo.
	criptográfico de $ElGamal$ que usa este número para a escolha de $\mathbb{F}_p^*$ :
	A quebra do protocolo é fácil.
-0.2/0.5	Duas mensagens podem ser codificadas pelo mesmo ciphertext.
	<ul> <li>☐ Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>☐ A encriptação torna-se lenta.</li> </ul>
	O protocolo pode ser quebrado em tempo polinomial.
0.5/0.5	A probabilidade de um plaintext é independente do ciphertext.
	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:
	Exponenciação em $\mathbb{F}_p^*$ é fácil e o Discrete Logarithm Problem é difícil.
-0.2/0.5	Mulitplicação é fácil e factorização é difícil.
-0.2/0.5	Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
	Mulitplicação é fácil e divisão é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
	A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
0.5/0.5	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 operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

João Manuel Calixto Figueira - 41734 - MIEI Mark: 2.2/5 (total score: 2.2/5)



+85/1/12+

	Departamento de Matemá	Total Carlo
	Criptografia	8/7/2018 Exame Final
	Número de aluno 0 0 0 0 0	← 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: Jose Manuel Calixto Figurira
	5 5 5 5 6 6 6 6	Curso: MIEI Número de aluno: 41734
	7 7 7 7 8 8 8 8 8 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 u $igwedge n$ é um número primo	
		de Kerckhoff são princípios que todos os sistemas criptográficos devem cerckhoff fundamental diz que a segurança de um sistema criptográfico
0.5/0.5	só da chave, mas não d	thmo, mas não do segredo da chave.
	Questão 3 Qual destes p	rotocolos criptográficos é assimétrico?
0.5/0.5	☐ AES ☐ Vigenère	ElGamal  DES
	Questão 4 O Discrete Logarithm Pro	$ablem\;(DLP)\;  ext{para a congruência}\; g^x\equiv h\;(\operatorname{mod} p)\;  ext{\'e};$
0.5/0.5	Determine $p$ , dados $g$ , $f$ Determine $x$ , dados $g$ , $f$	



	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 $g^{ab} \pmod{p}$ .
	$\square$ 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:
0.0/0.5	$igstyle (c_1^a)^{-1} \cdot c_2 \pmod p$ $ \qquad $
0.2/0.5	$(c_1)^{-1} \cdot (c_2)^a \pmod{p}$ $(c_1)^{-1} \cdot (c_2)^{-1} \pmod{p}$
	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 encriptação torna-se lenta.
	A quebra do protocolo é fácil.
	Duas mensagens podem ser codificadas pelo mesmo ciphertext.
	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 exponencial.
	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.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
0.2/0.5	$\square$ 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.
	$lacksquare$ Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0.5/0.5	$\square$ 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 $\mathbb{F}_p^*$ .
	$\square$ 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 $\mathbb{F}_p^*$ .