Maria Beatriz Lourenço e Sá de Ferreira Moreira - 47797 - MIEI Mark: 2.9/5 (total score: 2.9/5)

•			+27/1/	'8 <b>+</b>
	Departamento de Matemá Criptografia	itica 8/7/2	Faculdade de Ciências o	e Tecnologia — UNI Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1		imero de aluno preenchendo grelha ao lado () e escre ixo.	
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 4 5 5 5 5 5		Beamiz Morcia	
	6 6 6 6 6 7 7 7 7 8 8 8 8 8 9 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 ta preenchendo completame azul ou preta, cada respostalesconta 0,2 valores e marcaços classificações das questões será atribuído 0 valores com	múltipla. Nas questões ente o quadrado respec- a certa vale 0,5 valores, ções múltiplas anulam a de escolha múltipla der
	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 um número primo $n$ é um número primo $n$	ímpar.	n é uma potência de $n$ é um número par.	um número primo.
	Questão 2 Os princípios o satisfazer. Um princípio de K deve depender:		cípios que todos os sistemas diz que <i>a segurança de un</i>	
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 lo segredo do algoritu	redo da chave.	
	Questão 3 Qual destes p	rotocolos criptográfico	os é assimétrico?	
0.5/0.5	☐ DES ☐ Vigenère		☐ AES  ElGamal	
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	ongruência $g^x \equiv h \pmod p$	) é:
0.5/0.5			Determine $x$ , dados $g$ Determine $h$ , dados $g$	

	<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 $g^a \pmod{p}$ , $B$ 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 $g^{ab} \pmod{p}$ . $A$ 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>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> <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>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> </ul>
	A probabilidade de um plaintext é independente do ciphertext.  Questão 9 O funcionamento do RSA é baseado no seguinte:
-0.2/0.5	<ul> <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>Mulitplicação é fácil e factorização 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 exponenciação é mais rápida sobre curvas elípticas do que em F<sub>p</sub><sup>*</sup>.</li> <li>A operação de "adição" é mais complicada 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> <li>A operação de "adição" é mais fácil sobre curvas elípticas do que em F<sub>p</sub><sup>*</sup>.</li> </ul>

Maria Bernardo Courelas Lobo da Silva - 47363 - MIEI Mark: 2.3/5 (total score: 2.3/5)

	•		+74/1/34+	
	Departamento de Mater Criptografia	mática 8/7/1	Faculdade de Ciências e Tecnologia — UNI 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 nixo.	
	2 2 2 2 2 3 3 3 3 3 3 3 4 4 4 4 5 5 5 5 5 5 5		Runardo Countian 1000 da Silva  Número de aluno: .47363.	
	6 6 6 6 6 6 7 7 7 7 8 8 8 8 8 8 9 9 9 9 9 9	O exame é composto marque a resposta co tivo () com caneta cada resposta errada questão. Se a soma d	o por 10 questões de escolha múltipla. Nas questões erta preenchendo completamente o quadrado respecta azul ou preta, cada resposta certa vale 0,5 valores, desconta 0,2 valores e marcações múltiplas anulam a las classificações das questões de escolha múltipla der a será atribuído 0 valores como resultado final.	,
	Questão 1 Considere se, e só se:	o grupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se	definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo	)
-0.2/0.5			n é um número par. n é um número primo ímpar.	
		-	ncípios que todos os sistemas criptográficos devem al diz que a segurança de um sistema criptográfico	
0.5/0.5	do segredo da chave	o do segredo do algorita e do segredo do algorita porithmo, mas não do se da encriptação.	mo.	
	Questão 3 Qual deste	s protocolos criptográfi	cos é assimétrico?	
0.5/0.5	ElGamal Uigenère		☐ DES ☐ AES	
	Questão 4 O Discrete Logarithm	Problem (DLP) para a	congruência $g^{\mathbf{r}} \equiv h \pmod{p}$ é:	
0.5/0.5	Determine $h$ , dados Determine $p$ , dados		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 número
0.5/0.5	secretos $a \in b$ para calcular números $A \in B$ que são depois trocados.  A é calculado por $g^a \pmod{p}$ , $B$ por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$ .  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 $A \cdot B$ .
	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	<ul> <li>Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <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>
	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 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:
0/0.5	<ul> <li>Exponenciação em F<sub>p</sub><sup>*</sup> 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 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	☐ A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^{\bullet}$ .  ☐ A solução do $DLP$ é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^{\bullet}$ .  ☐ A operação de "adição" é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^{\bullet}$ .  ☐ A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^{\bullet}$ .

Mauricio Daniel Flores Landos - 45511 - MIEI Mark: 1.4/5 (total score: 1.4/5)

•			+76/1/30+	
	Departamento de Matemá Criptografia	tica 8/7/20	Faculdade de Ciências e Tecr 018	nologia — UNL Exame Final
	Número de aluno  0 0 0 0 0  1 1 1 1	Nome: MIEI  Curso: MIEI  O exame é composto marque a resposta certivo ( ) com caneta cada resposta errada é questão. Se a soma da	mero de aluno preenchendo complegrelha ao lado ( ) e escreva o receiva o receiva de la completa del completa de la completa del completa de la completa de la completa de la completa de l	ola. Nas questões quadrado respectivale 0,5 valores, últiplas anulam a olha múltipla der
0/0.5	Questão 1 Considere o g se, e só se: $n \in \text{um número primo}$ $n \in \text{um número primo}$		definir uma multiplicação tal que  n é um número par.  n é uma potência de um n	
8	Questão 2 Os princípios o satisfazer. Um princípio de K deve depender:	de <i>Kerckhoff</i> são princ Kerckhoff fundamental	cípios que todos os sistemas cript diz que a segurança de um siste	ográficos devem
0.5/0.5	do segredo da chave e d só da chave, mas não d só da complexidade da só do segredo do algori  Questão 3 Qual destes p	lo segredo do algoritm encriptação.	redo da chave.	
-0.2/0.5	⊠ ElGamal □ Vigenère		☐ DES  ② AES	
	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 $g$ , Determine $g$ , dados $h$ ,		Determine $h$ , dados $g$ , $p$ e  Determine $p$ , dados $g$ , $h$ e	

	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	☐ $A$ é calculado por $g^a$ (mod $p$ ), $B$ por $g^b$ (mod $p$ ) e a chave comum secreta é $A \cdot B$ . ☐ $A$ é calculado por $a^g$ (mod $p$ ), $B$ por $b^g$ (mod $p$ ) e a chave comum secreta é $(ab)^g$ (mod $p$ ). ☐ $A$ é calculado por $a^g$ (mod $p$ ), $B$ por $b^g$ (mod $p$ ) e a chave comum secreta é $g^{ab}$ (mod $p$ ). ☐ $A$ é calculado por $g^a$ (mod $p$ ), $B$ por $g^b$ (mod $p$ ) e a chave comum secreta é $g^{ab}$ (mod $p$ ).
	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>☐ A quebra do protocolo é fácil.</li> <li>☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</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 <i>total secrecy</i> , se, e só se:  O protocolo pode ser quebrado em tempo polinomial.
-0.2/0.5	<ul> <li>O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.</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>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):
0/0.5	$\boxtimes$ 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 fácil 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 Alexandre Figueiredo - 48182 - MIEI Mark: 2.2/5 (total score: 2.2/5)

+84/1/14+

	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		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 3 3 4 4 4 4 4 5 5 5 5 5 5		Alexandra Eigenired
	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	por 10 questões de escolha múltipla. Nas questões ra preenchendo completamente o quadrado respecazul ou preta, cada resposta certa vale 0,5 valores, desconta 0,2 valores e marcações múltiplas anulam a
	Questão 1 Considere o g se, c só se:	um número negativo, s	s 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
-0.2/0.5	otin n é uma potência de un $ otin n$ é um número par.	n número primo.	n é um número primo ímpar. $n$ é um número primo.
			cípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
0.5/0.5	só da complexidade da só da chave, mas não de 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?
0.5/0.5	☐ DES ☐ ElGamal		☐ AES ☐ Vigenère
	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 $g$ , $h$ 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.
0.5/0.5	
	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:
0.2/0.5	
	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 quebra do protocolo é fácil.</li> <li>A encriptação torna-se lenta.</li> </ul>
	Duas mensagens podem ser codificadas pelo mesmo ciphertext.  Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
	<ul> <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:
0.2/0.5	<ul> <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> <li>Mulitplicação 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 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> <li>A operação de "adição" é mais complicada sobre curvas elípticas do que em F<sub>p</sub><sup>*</sup>.</li> <li>A operação de "adição" é mais fácil sobre curvas elípticas do que em F<sub>p</sub><sup>*</sup>.</li> </ul>

Miguel Balão Candeias - 50647 - MIEI Mark: 0/5 (total score: -1.3/5)

+87/1/8+

	Departamento de Matemá Criptografia		Faculdade de Ciências e Tecnologia — UNL '2018 Exame Final
	Número de aluno 0 0 0 0 1 1 1 1 1	← Marque o seu i drados respectivos d número e o curso ab	número de aluno preenchendo completamente os qua- la grelha ao lado ( <b>   </b> ) e escreva o nome completo, o aixo.
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 4 4	Nome: M.GU	VEL BALAO CANDEIAS
	5 5 5 5 6 6 6 7 7 7 7	Curso: M.EI	Número de aluno: 5064)  por 10 questões de escolha múltipla. Nas questões
	88888	marque a resposta con tivo ( ) com caneta cada resposta errada questão. Se a soma d	erta preenchendo completamente o quadrado respec- a azul ou preta, cada resposta certa vale 0,5 valores, desconta 0,2 valores e marcações múltiplas anulam a las classificações das questões de escolha múltipla der , será atribuído 0 valores como resultado final.
	Questão 1 Considere o g se, c só se:		definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5	igstyle n é uma potência de un $igstyle n$ é um número primo í		$n \in \text{um número primo.}$ $n \in \text{um número par.}$
	Questão 2 Os princípios d satisfazer. Um princípio de K deve depender:	de <i>Kerckhoff</i> são prin erckhoff fundamenta	cípios que todos os sistemas criptográficos devem l diz que <i>a segurança de um sistema criptográfico</i>
-0.2/0.5	só da chave, mas não do  do segredo da chave e d  só da complexidade da c  só do segredo do algorit	lo segredo do algorita encriptação.	mo.
	Questão 3 Qual destes pr	rotocolos criptográfic	cos é assimétrico?
-0.2/0.5	☐ Vigenère ☐ DES		ElGamal  AES
	Questão 4 O Discrete Logarithm Prod	blem (DLP) para a c	congruência $g^x \equiv h \pmod p$ é:
-0.2/0.5			Determine $h$ , dados $g$ , $p \in x$ .  Determine $g$ , dados $h$ , $p \in x$ .

	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:
-0.2/0.5	
	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>✓ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>✓ Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>✓ A quebra do protocolo é fácil.</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>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 exponencial.  Questão 9 — O funcionamento do RSA é baseado no seguinte:
-0.2/0.5	<ul> <li>Questão 9 O funcionamento do RSA é baseado no seguinte:</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>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):
-0.2/0.5	A solução do $DLP$ é mais complicada 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 $\mathbb{F}_p^*$ .
	A operação de "adição" é mais fácil sobre curvas elípticas do que em F*.