João Miguel Luís Santos - 42958 - MIEI Mark: 1.3/5 (total score: 1.3/5)

Questão 4

0.5/0.5

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

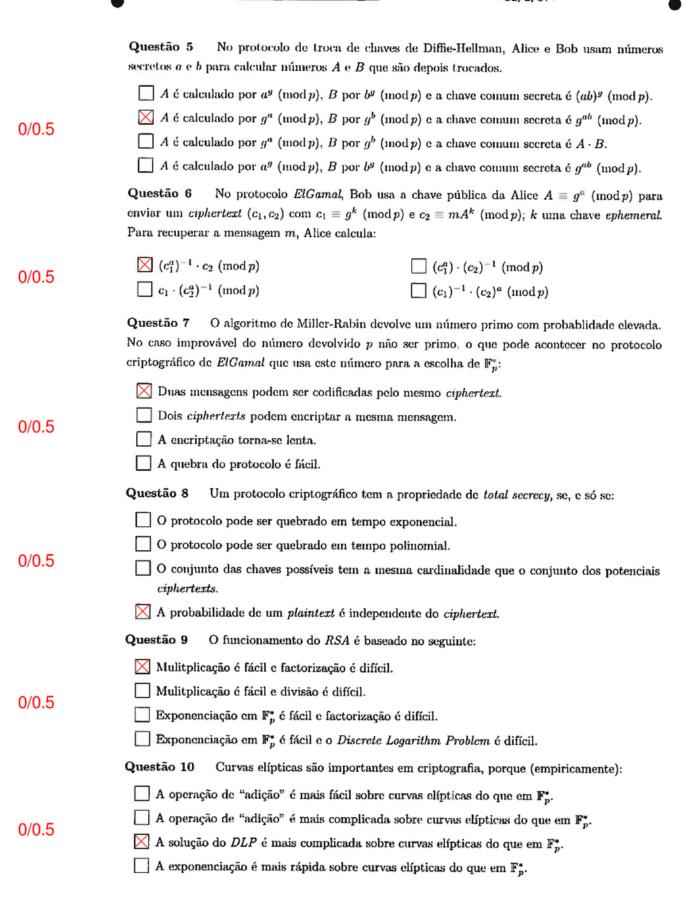
Determine p, dados g,  $h \in x$ .

•			+32/1/58+
	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		mero de aluno preenchendo completamente os qua- grelha ao lado (  ) e escreva o nome completo, o xo.
	2 2 2 2 3 3 3 3 3 4 4 4 4	Nome:	riquel Sonton
	5 5 5 5 5 6 6 6 7 7 7 7 7 7	O exame é composto	Número de aluno: 92958  por 10 questões de escolha múltipla. Nas questões
	9 9 6 9 9	tivo ( ) com caneta a 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, esconta 0,2 valores e marcações múltiplas anulam a s classificações das questões de escolha múltipla der erá atribuído 0 valores como resultado final.
	Questão 1 Considere o g se, e só se:	rupo Z/nZ. Pode-se o	lefinir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5	n é um número primo $n$ é uma potência de u		n é um número primo. $n$ é um número par.
			ípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
0.5/0.5	só do segredo do algori só da complexidade da do segredo da chave e d só da chave, mas não d	encriptação. lo segredo do algoritm	o.
	Questão 3 Qual destes p	rotocolos criptográfico	s é assimétrico?
0.5/0.5	ElGamal DES		☐ Vigenère ☐ AES

O Discrete Logarithm Problem (DLP) para a congruência  $g^x \equiv h \pmod{p}$  é:

Determine x, dados g, h e p.

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



João Miguel Peres Palma Neves - 45615 - MIEI Mark: 2.3/5 (total score: 2.3/5)

+33/1/56+

	Departamento de Matemá Criptografia	tica 8/7/2	Faculdade de Ciências e T 2018	ecnologia — UNL 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  7 7 7 7 7  8 8 8 8 8  9 9 9 9 9 9	Nome:	innero de aluno preenchendo con grelha ao lado ( ) e escreva ixo.  Muguel Teres Tala  Número de aluno: .  Por 10 questões de escolha múl rta preenchendo completamente azul ou preta, cada resposta ce lesconta 0,2 valores e marcações as classificações das questões de escrá atribuído 0 valores como re	na Weves  15615  Itipla. Nas questões o quadrado respectra vale 0,5 valores, múltiplas anulam a escolha múltipla der
-0.2/0.5	se, e só se:	rupo Z/nZ. Pode-se d de <i>Kercklwf</i> f são princ	definir uma multiplicação tal d  n é um número primo ís  n é uma potência de un  cípios que todos os sistemas cri	que $\mathbb{F}_n$ é um corpo impar. In número primo. Integráficos devem
0.5/0.5	só do segredo do algorit  do segredo da chave e d  só da chave, mas não do  só da complexidade da o	o segredo do algoritm	no.	
0.5/0.5	☐ Vigenère ☐ ElGamal (~  Questão 4	rotocolos criptográfico	☐ DES ☐ AES	
0.5/0.5	Determine $p$ , dados $q$ , $p$ Determine $p$ , dados $q$ , $p$	e x.	ongruência $g^x \equiv h \pmod{p}$ é:  Determine $x$ , dados $g$ , $h$ Determine $g$ , dados $h$ , $p$	-

	<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	$\square$ 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 $A \cdot B$ .
	$A$ é calculado por $g^a \pmod{p}$ , $B$ por $g^b \pmod{p}$ 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 =	
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 $\mathbb{F}_p^*$ :
	Dois <i>ciphertexts</i> podem encriptar a mesma mensagem.
0/0.5	A quebra do protocolo é fácil.
5/0.0	Duas mensagens podem ser codificadas pelo mesmo ciphertext. X
	A encriptação torna-se lenta. 🗴
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
	O protocolo pode ser quebrado em tempo exponencial.
0/0.5	O protocolo pode ser quebrado em tempo polinomial.
5/0.5	<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:
	$\square$ Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
0/0.5	Mulitplicação é fácil e factorização é difícil.
J/U.5	Exponenciação em $\mathbb{F}_p^*$ é fácil e o Discrete Logarithm Problem é difícil.
	Mulitplicação é fácil e divisão 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 $\mathbb{F}_p^*$ .
0/0.5	$\nearrow$ A solução do <i>DLP</i> é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\square$ A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\square$ A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

g ka | mg ke

João Pedro Monteiro Morgado Dias - 42205 - MIEI Mark: 3.8/5 (total score: 3.8/5)

		+45/1/32+
	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  2 2 2 2	← 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: Selvo Dias
	3 3 3 3 3 3 3 4 4 4 4 4 5 5 5 5 5 5 6 6 6 6 6 6 6 6 6	Curso: MIEI Número de aluno: 42205
	7 7 7 7 7 8 8 8 8 8 8 9 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
0.5/0.5	$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	n é uma potência de um número primo. $n$ é um número par.
		le Kerckhoff são princípios que todos os sistemas criptográficos devem erckhoff fundamental diz que a segurança de um sistema criptográfico
0.5/0.5		
	Questão 3 Qual destes pr	rotocolos criptográficos é assimétrico?
0.5/0.5	☐ AES ☐ DES	☐ Vigenère ☐ ElGamal
	Questão 4 O Discrete Logarithm Pro	$blem\;(DLP)$ para a congruência $g^x\equiv h\;(\operatorname{mod} p)$ é:
0.5/0.5		

	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.	os
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 $g^{ab} \pmod{p}$ .	
	$\square$ A é calculado por $a^g \pmod{p}$ , B por $b^g \pmod{p}$ e a chave comum secreta é $(ab)^g \pmod{p}$ .  A é calculado por $g^a \pmod{p}$ , B por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$ .	
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ par	ro
	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 ephemera	
	Para recuperar a mensagem $m$ , Alice calcula:	
0.5/0.5		
0.0, 0.0		
	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 protocol criptográfico de <i>ElGamal</i> que usa este número para a escolha de $\mathbb{F}_p^*$ :	
	Dois ciphertexts podem encriptar a mesma mensagem.	
0/0.5	A quebra do protocolo é fácil.	
0/0.5	A encriptação torna-se lenta.	
	Duas mensagens podem ser codificadas pelo mesmo ciphertext.	
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:	
	O protocolo pode ser quebrado em tempo exponencial.	
	O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais	S
0.5/0.5	ciphertexts.	
	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:	
	Exponenciação em $\mathbb{F}_p^*$ é fácil e o Discrete Logarithm Problem é difícil.	
0.5/0.5	Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.	
0.0/0.0	Mulitplicação é fácil e divisão é difícil.	
	Mulitplicação é fácil e factorização 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 $\mathbb{F}_p^*$ .	
-0.2/0.5	A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .	
	$\bigcirc$ A operação de "adição" é mais complicada 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 $\mathbb{F}_p^*$ .	

João Pedro Silva Borralho - 45456 - MIEI Mark: 2.1/5 (total score: 2.1/5)

+42/1/38+

	Departamento de Matemá Criptografia	itica 8/7/2	Faculdade de Ciências 018	e Tecnologia — UNL Exame Final
	Número de aluno  0 0 0 0 0  1 1 1 1 1 1		úmero de aluno preenchend grelha ao lado () e esc ixo.	
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 5 5 5 5 5 6 6 6 6 6	Nome: 5000 C		10: 45456
	7 7 7 7 7 8 8 8 8 8 8 9 9 9 9 9 9	marque a resposta cer tivo ( ) com caneta cada resposta errada e questão. Se a soma da	por 10 questões de escolha rta preenchendo completan azul ou preta, cada respos lesconta 0,2 valores e marca s classificações das questõe será atribuído 0 valores con	nente o quadrado respec- sta certa vale 0,5 valores, ações múltiplas anulam a s de escolha múltipla der
	Questão 1 Considere o g se, e só se:	grupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se	definir uma multiplicação	tal que $\mathbb{F}_n$ é um corpo
0/0.5	n é um número primo. n é uma potência de un		n é um número par	
,	Questão 2 Os princípios e satisfazer. Um princípio de k deve depender:		cípios que todos os sistema diz que <i>a segurança de u</i>	
0.5/0.5	só do segredo do algori só da chave, mas não d do segredo da chave e d só da complexidade da	lo segredo do algorita	no.	
	Questão 3 Qual destes p	rotocolos criptográfic	os é assimétrico?	
0.5/0.5	☐ AES ☐ DES		ElGamal Uigenère	
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	congruência $g^x \equiv h$ (mod	p) é:
0.5/0.5	Determine $h$ , dados $g$ , and Determine $x$ , dados $g$ , and $g$ , and $g$ , and $g$ , and $g$ , are determined as $g$ , and $g$ , are determined as $g$ , and $g$ , and $g$ , are determined as $g$ , a			-



	<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 $a^g \pmod{p}$ , $B$ 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 $A \cdot B$ .
	<b>Questão 6</b> 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 $\mathbb{F}_p^{\bullet}$ :
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:
	O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.
0/0.5	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:
	Exponenciação em $\mathbb{F}_p^*$ é fácil e o Discrete Logarithm Problem é difícil.
0.0/0.5	Mulitplicação é fácil e factorização é difícil.
0.2/0.5	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):
	$\triangle$ A solução do $DLP$ é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
0.2/0.5	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 $\mathbb{F}_p^*$ .  A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

João Ricardo Alpoim Gonçalves - 44929 - MIEI Mark: 2.2/5 (total score: 2.2/5)

-0.2/0.5

0.5/0.5

0.5/0.5

0.5/0.5

Departamento de Mat	emática Faculdade de Ci	iências e Tecnologia — UNI
Criptografia	8/7/2018	Exame Final
Número de aluno	- Marque o seu número de aluno pree	
00000	drados respectivos da grelha ao lado ( número e o curso abaixo.	) e escreva o nome completo, o
11111	Tamero e o cuiso abaixo.	
2 2 2 2 2	Nome: 1000 Ricardo Alpo	a françaline
3 3 3 3	Nome:	V
444		
5 5 5 5	Curso: MIEL Número	de aluno: 44929
6 6 6 6	Trumeto	de aluno.
77777	O exame é composto por 10 questões de	
8 8 8 8 8	marque a resposta certa preenchendo con tivo () com caneta azul ou preta, cada	
	orro ( ) com cariota anar ou preta; cada	resposta certa vale ti,o valores,
9 9 9 9	cada resposta errada desconta 0,2 valores	e marcações múltiplas anulam a
	cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das o um número negativo, será atribuído 0 valo	e marcações múltiplas anulam a questões de escolha múltipla der pres como resultado final.
uestão 1 Considere	cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das o um número negativo, será atribuído 0 valores o grupo Z/nZ. Pode-se definir uma multip	e marcações múltiplas anulam a questões de escolha múltipla der pres como resultado final.
Questão 1 Considere e, e só se: n é um número pri	cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das o um número negativo, será atribuído 0 valore o grupo Z/nZ. Pode-se definir uma multipumo.	e marcações múltiplas anulam a questões de escolha múltipla der pres como resultado final. licação tal que $\mathbb{F}_n$ é um corpo ero primo ímpar.
Questão 1 Considere e, e só se:  n é um número pri n é uma potência e Questão 2 Os princíp	cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das o um número negativo, será atribuído 0 valore o grupo Z/nZ. Pode-se definir uma multipumo.	e marcações múltiplas anulam a questões de escolha múltipla der pres como resultado final.  licação tal que $\mathbb{F}_n$ é um corpo ero primo ímpar.  ero par.  sistemas criptográficos devem
Questão 1 Considere c, c só se:  n é um número pri n é uma potência o questão 2 Os princípatisfazer. Um princípio e eve depender:	cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das o um número negativo, será atribuído 0 valores e o grupo Z/nZ. Pode-se definir uma multipumo.	e marcações múltiplas anulam a questões de escolha múltipla der pres como resultado final.  licação tal que $\mathbb{F}_n$ é um corpo ero primo ímpar.  ero par.  sistemas criptográficos devem
Questão 1 Considere  c, c só se:  n é um número pri  n é uma potência o  Questão 2 Os princíp  atisfazer. Um princípio e  eve depender:  do segredo da chav	cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das o um número negativo, será atribuído 0 valores e o grupo Z/nZ. Pode-se definir uma multipumo.	e marcações múltiplas anulam a questões de escolha múltipla der pres como resultado final.  licação tal que $\mathbb{F}_n$ é um corpo ero primo ímpar.  ero par.  sistemas criptográficos devem
Questão 1 Considere c, c só se:  n é um número pri n é uma potência o Questão 2 Os princíp atisfazer. Um princípio e eve depender:  do segredo da chav	cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das o um número negativo, será atribuído 0 valores e o grupo Z/nZ. Pode-se definir uma multipano.  In é um número primo.  In é um número de um número primo.  In é um número de um número que todos os de Kerckhoff são princípios que todos os de Kerckhoff fundamental diz que a segurançõe e e do segredo do algoritmo.	e marcações múltiplas anulam a questões de escolha múltipla der pres como resultado final.  licação tal que $\mathbb{F}_n$ é um corpo ero primo ímpar.  ero par.  sistemas criptográficos devem
euestão 1 Considere  c, c só se:  n é um número pri  n é uma potência o  uestão 2 Os princíp  utisfazer. Um princípio eve depender:  do segredo da chav  só da chave, mas m  só da complexidado	cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das o um número negativo, será atribuído 0 valores e o grupo Z/nZ. Pode-se definir uma multipano.  In é um número primo.  In é um número de um número primo.  In é um número de um número que todos os de Kerckhoff são princípios que todos os de Kerckhoff fundamental diz que a segurançõe e e do segredo do algoritmo.	e marcações múltiplas anulam a questões de escolha múltipla der pres como resultado final. licação tal que $\mathbb{F}_n$ é um corpo ero primo ímpar. ero par.
Questão 1 Considere c, e só se:  n é um número pri n é uma potência o questão 2 Os princíp atisfazer. Um princípio e eve depender: do segredo da chav só da chave, mas m só da complexidado só do segredo do al	cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das o um número negativo, será atribuído 0 valores e o grupo Z/nZ. Pode-se definir uma multiplication.  In é um número primo.  In é um número primo de um número que todos os de Kerckhoff são princípios que todos os de Kerckhoff fundamental diz que a segurançõe e e do segredo do algoritmo.  a da encriptação.	e marcações múltiplas anulam a questões de escolha múltipla der pres como resultado final.  licação tal que $\mathbb{F}_n$ é um corpo ero primo ímpar.  ero par.  sistemas criptográficos devem
n é um número pri n é um número pri n é uma potência o uestão 2 Os princíp tisfazer. Um princípio e ue depender: do segredo da chav só da chave, mas m só da complexidado só do segredo do al	cada resposta errada desconta 0,2 valores questão. Se a soma das classificações das o um número negativo, será atribuído 0 valores e o grupo Z/nZ. Pode-se definir uma multipara e o grupo Z/nZ. Pode-se definir uma multipara e um número primo.  In é um número de um número primo.  In é um número de um número que todos os de Kerckhoff são princípios que todos os de Kerckhoff fundamental diz que a segurançõe e e do segredo do algoritmo.  Todo de	e marcações múltiplas anulam a questões de escolha múltipla der pres como resultado final.  licação tal que $\mathbb{F}_n$ é um corpo ero primo ímpar.  ero par.  sistemas criptográficos devem

O Discrete Logarithm Problem (DLP) para a congruência  $g^x \equiv h \pmod{p}$  é:

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

Determine p, dados g,  $h \in x$ .

 $\mathbf{M}$  Determine x, dados g, h e 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.
0.5/0.5	$A$ 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 $(ab)^g \pmod{p}$ . $A$ 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	
	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>
	Duas mensagens podem ser codificadas pelo mesmo ciphertext.  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>□ O protocolo pode ser quebrado em tempo exponencial.</li> <li>☑ A probabilidade de um plaintext é independente do ciphertext.</li> </ul>
	Questão 9 O funcionamento do RSA é baseado no seguinte:
0.5/0.5	<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):
-0.2/0.5	<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>