Alexandre Miguel Lobo Ferreira - 47537 - MIEI Mark: 1.6/5 (total score: 1.6/5)

•			+6/1/50+
	Departamento de Matem Criptografia	ática - 8/7/3	Faculdade de Ciências e Tecnologia — UNI 2018 Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 1		número de aluno preenchendo completamente os qua a grelha ao lado () e escreva o nome completo, aixo.
	2 2 2 2 2 3 3 3 3 3		dre Mignel Lobo Forreira
	4 4 4 4 5 5 5 5 6 6 6 6 6	Curso: MIE]	Número de aluno: 47537
	7 7 7 8 8 8 8 8 9 9 9 9 9	marque a resposta ce tivo () com caneta cada resposta errada questão. Se a soma d	por 10 questões de escolha múltipla. Nas questões erta preenchendo completamente o quadrado respectazul ou preta, cada resposta certa vale 0,5 valores desconta 0,2 valores e marcações múltiplas anulam as classificações das questões de escolha múltipla des será atribuído 0 valores como resultado final.
	Questão 1 Considere o 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 uma potência de u		n é um número primo. n é um número par.
			cípios que todos os sistemas criptográficos devem l diz que a segurança de um sistema criptográfico
0.5/0.5	só da chave, mas não d só da complexidade da do segredo da chave e só do segredo do algor	encriptação. do segredo do algorita	mo.
	Questão 3 Qual destes p	protocolos criptográfic	cos é assimétrico?
0.5/0.5	☐ Vigenère ☐ DES		AES ElGamal
	Questão 4 O Discrete Logarithm Pr	oblem (DLP) para a o	congruência $g^x \equiv h \pmod{p}$ é:
-0.2/0.5	Determine g , dados h , Determine p , dados g ,		Determine h , dados g , $p \in x$. Determine x , dados g , $h \in p$.

	Questão 5 No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usam números secretos a e b para calcular números A e B que são depois trocados.			
0.5/0.5	\square $A \in \operatorname{calculado} \operatorname{por} a^g \pmod p$, $B \operatorname{por} b^g \pmod p$ e a chave comum secreta $e \pmod p$. \square $A \in \operatorname{calculado} \operatorname{por} g^a \pmod p$, $B \operatorname{por} g^b \pmod p$ e a chave comum secreta $e \pmod p$. \square $A \in \operatorname{calculado} \operatorname{por} g^a \pmod p$, $B \operatorname{por} g^b \pmod p$ e a chave comum secreta $e \pmod p$. \square $A \in \operatorname{calculado} \operatorname{por} a^g \pmod p$, $B \operatorname{por} b^g \pmod p$ e a chave comum secreta $e \pmod p$.			
	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 actor-				
	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 encriptação torna-se lenta. Dois ciphertexts podem encriptar a mesma mensagem. A quebra do protocolo é fácil.			
	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:			
0/0.5	A probabilidade de um plaintext é independente do ciphertext. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.			
	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 factorização é difícil.			
0/0.5	Mulitplicação é fácil e divisão 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):			
	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}^* .			
0/0.5	\boxtimes 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^* .			
	A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .			

Ana Gisela Lourenço Gomes - 41819 - MIEI Mark: 1.9/5 (total score: 1.9/5)

0.5/0.5

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

	•		+46/1/30+	
	Departamento de Mate Criptografia	emática 8/7/	Faculdade de Ciências e Tecnologia — UN 2018 Exame Fina	
	Número de aluno 0 0 0 0 0 1 1 1 1 2 2 2 2 2 2 3 3 3 3 3 3 4 4 4 4 4 5 5 5 5 5 6 6 6 6 6 7 7 7 7 7 7 8 8 8 8 8 9 9 9 9 9	O exame é composte marque a resposta e tivo () com caneta cada resposta errada questão. Se a soma o	Gisels Lourenço Gones	es es, a
	Questão 1 Considere sc, c só se:	o grupo Z/nZ. Pode-se	e definir uma multiplicação tal que \mathbb{F}_n é um corp	00
0/0.5	igwedge n é uma potência d $igwedge n$ é um número par	-	n é um número primo. n é um número primo ímpar.	
			ucípios que todos os sistemas criptográficos dever al diz que a segurança de um sistema criptográfic	
0.5/0.5	só da complexidade	e e do segredo do algorio e da encriptação. gorithmo, mas não do se ão do segredo do algorit	egredo da chave.	
	Questão 3 Qual dest	es protocolos criptográfi	icos é assimétrico?	
0.5/0.5	☐ AES ☐ Vigenère		ElGamal DES	
	Questão 4 O Discrete Logarithm	Problem (DLP) para a	congruência $g^x \equiv h \pmod{p}$ é:	
0.5/0.5	\square Determine x , dados			

 \square 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	
	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	 Duas mensagens podem ser codificadas pelo mesmo ciphertext. Dois ciphertexts podem encriptar a mesma mensagem. A quebra do protocolo é fácil. A encriptação torna-se lenta.
0.0/0.5	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, c só se: O protocolo pode ser quebrado em tempo exponencial. O protocolo pode ser quebrado em tempo polinomial.
-0.2/0.5	 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:
0/0.5	 ✓ Mulitplicação é fácil e factorização é difícil. ☐ Exponenciação em F_p[*] é fácil e factorização é difícil. ☐ Mulitplicação é fácil e livitação é 100 di
	☐ 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):
	\square 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^* .

André António Da Veiga - 41730 - MIEI Mark: 0.3/5 (total score: 0.3/5)

+53/1/16+

	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		úmero de aluno preenchendo completamente os qua- a grelha ao lado () e escreva o nome completo, o sixo.
	2 2 2 2 2 3 3 3 3 3 3 4 4 4 4		Antómio da Veiga
	5 5 5 5 5 6 6 6 6 6 7 7 7 7		Número de aluno: 41730 por 10 questões de escolha múltipla. Nas questões
	88888	marque a resposta ce tivo () com caneta cada resposta errada questão. Se a soma de	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 se, e só se:		definir uma multiplicação tal que F _n é um corpo
-0.2/0.5	n é um número par. n é um número primo.		n é um número primo ímpar. n é uma potência de um número primo.
Questão 2 Os princípios de Kerckhoff são princípios que todos os sistemas criptográficos de satisfazer. Um princípio de Kerckhoff fundamental diz que a segurança de um sistema criptográficos deve depender:			
0.5/0.5	só do segredo do algoridade da do segredo da chave e d só da chave, mas não de	encriptação. lo segredo do algorita	no.
	Questão 3 Qual destes pr	rotocolos criptográfic	os é assimétrico?
0.5/0.5	AES ElGamal		☐ Vigenère ☐ DES
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	congruência $g^x \equiv h \pmod{p}$ é:
-0.2/0.5	Determine g , dados h , p Determine p , dados g , h		Determine x , dados g , $h \in p$. 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.			
0.2/0.5	☐ 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 $g^{ab} \pmod{p}$. ☐ 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 $A \cdot B$.			
	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^* :			
0.5/0.5	 ☐ A quebra do protocolo é fácil. ☐ Dois ciphertexts podem encriptar a mesma mensagem. ☐ 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 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	Mulitplicação é fácil e divisão 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):			
	A solução do DLP é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .			
0.2/0.5	A operação de "adição" 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 operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .			

André Duarte Teixeira Trindade - 47258 - MIEI Mark: 2.2/5 (total score: 2.2/5)

1

+19/1/24+

	Departamento de Matemática Criptografia 8/7		Faculdade de Ciências e Tecnologia — 2018 Exame	
	Número de aluno 0 0 0 0 0 1 1 1 1 1 2 2 2 2 3 3 3 3 3 4 4 4 4 4 5 5 5 5 5 6 6 6 6 6 7 7 7 7 8 8 8 8 9 9 9 9 9	Nome:	número de aluno preenchendo completamente de a grelha ao lado () e escreva o nome complixo. Direcche de secreva o nome complixo. Número de aluno:	uestões respec- valores, ulam a
-0.2/0.5	se, e só se: n é um número primo n é um número primo e Questão 2 Os princípios o	rupo Z/nZ. Pode-se dímpar.	definir uma multiplicação tal que \mathbb{F}_n é um	imo. devem
0.5/0.5	só da complexidade da do segredo da chave e o só do segredo do algorid só da chave, mas não de	do segredo do algorita	gredo da chave.	
0.5/0.5	☐ AES ☐ ElGamal Questão 4	rotocolos criptográfic	☐ DES ☐ Vigenère	
0.5/0.5	Determine g , dados h , g Determine x , dados g , h	рех.	congruência $g^x \equiv h \pmod{p}$ é: Determine h , dados g , $p \in x$. 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.				
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	 Dois ciphertexts podem encriptar a mesma mensagem. ☐ A quebra do protocolo é fácil. ☐ Duas mensagens podem ser codificadas pelo mesmo ciphertext. ☐ A encriptação torna-se lenta. 				
	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 polinomial. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts. 				
	 ○ O protocolo pode ser quebrado em tempo exponencial. ○ 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	Exponenciação em \mathbb{F}_p^* é fácil e factorização é difícil. 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 exponenciação é mais rápida sobre curvas elípticas do que em \mathbb{F}_p^* .				
0.5/0.5	* \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^* .				
	☐ A operação de "adição" é mais fácil sobre curvas elípticas do que em F				

André Fialho Ferreira Rosa - 48043 - MIEI Mark: 3.6/5 (total score: 3.6/5)

+36/1/50+

	Departamento de Matemá Criptografia	tica 8/7/2	Faculdade de Ciências e Tecnologia — UNL 1018 Exame Final	
	Número de aluno 0 0 0 0 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 3 3 4 4 4 4 4 4 4 4 4	Curso: MIEI O exame é composto	Etallo Evera Rosa Número de aluno: 48043 por 10 questões de escolha múltipla. Nas questões rta preenchendo completamente o quadrado respec-	
	99999	tivo () com caneta cada resposta errada e questão. Se a soma da	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, 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	otin n é uma potência de un $ otin n$ é um número primo.	n número primo.	$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	
	Questão 2 Os princípios de Kerckhoff são princípios que todos os sistemas criptográficos devem satisfazer. Um princípio de Kerckhoff fundamental diz que a segurança de um sistema criptográfico deve depender:			
0.5/0.5	do segredo da chave e d só da complexidade da só do segredo do algorid só da chave, mas não de	encriptação. tluno, mas não do seg	redo da chave.	
	Questão 3 Qual destes pr	rotocolos criptográfic	os é assimétrico?	
0.5/0.5	ElGamal DES DES ■ DES		☐ Vigenère ☐ AES	
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	ongruência $g^x \equiv h \pmod p$ é:	
0.5/0.5			Determine x , dados g , $h \in p$. Determine p , dados g , $h \in x$.	

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 $g^{ab} \pmod p$. Questão 6 No protocolo $ElGamal$, Bob usa a chave pública da Alice $A \equiv g^a \pmod p$ enviar um $exphertext$ (c_1, c_2) com $c_1 \equiv g^k \pmod p$ e $c_2 \equiv mA^k \pmod p$; k uma chave $expherical points a mensagem m, Alice calcula: (c_1^a)^{-1} \cdot c_2 \pmod p (c_1^a)^{-1} \cdot (c_2)^a \pmod p (c_1^a)^{-1} \cdot (c_2)^a \pmod p Questão 7 O algoritmo de Miller-Rabin devolve um número primo com probablidade elev No caso improvável do número devolvido p não ser primo, o que pode acontecer no protocriptográfico de ElGamal que usa este número para a escolha de \mathbb{F}_p^*:$
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 ephemerar recuperar a mensagem m , Alice calcula:
0.5/0.5
No caso improvável do número devolvido p não ser primo, o que pode acontecer no prote criptográfico de <i>ElGamal</i> que usa este número para a escolha de \mathbb{F}_p^* :
 A quebra do protocolo é fácil. A encriptação torna-se lenta. 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:
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 potene ciphertexts.
A probabilidade de um plaintext é independente do ciphertext.
Questão 9 O funcionamento do RSA é baseado no seguinte:
 Mulitplicação é fácil e factorização é difícil. □ Exponenciação em F_p[*] é fácil e o Discrete Logarithm Problem é difícil. □ Mulitplicação é fácil e divisão é difícil. □ Exponenciação em 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^{\bullet} .
-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^* . A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .