André Marques de Carvalho Ferreira Victorino - 45067 - MIEI Mark: 3.1/5 (total score: 3.1/5)

	L-1L-		+52/1/18+
	Departamento de Matema Criptografia	ática 8/7/2	Faculdade de Ciências e Tecnologia — UNL 2018 Exame Final
V	Número de aluno 0 0 0 0 1 1 1 1 1	drados respectivos da número e o curso aba	
	2 2 2 2 2 3 3 3 3 3 4 4 4 4	Nome: Ash W.	é Victorino
	5 (5) 5 5 6 6 6 (6) 6 7 7 7 7 (7)	Curso: MTE J	Número de aluno: 145067
	88888	marque a resposta ce tivo () com caneta cada resposta errada e questão. Se a soma de	por 10 questões de escolha múltipla. Nas questões rta preenchendo completamente o quadrado respecazul 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:	grupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se	definir uma multiplicação tal que \mathbb{F}_n é um corpo
0.5/0.5	$ \prod n$ é um número primo. $ m$ $ n$ é uma potência de u		n é um número primo impar. n é um número par.
			cípios que todos os sistemas criptográficos devem 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 algori	encriptação. do segredo do algoritr	no.
	Questão 3 Qual destes p	orotocolos criptográfic	os é assimétrico?
0.5/0.5	☐ Vigenère ☑ ElGamal		☐ AES ☐ DES
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	congruência $g^{m{x}} \equiv h \pmod{p}$ é:
0.5/0.5	Determine x , dados g , Determine h , dados g ,		Determine g , dados h , $p \in x$. 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	\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 $g^{ab} \pmod{p}$. \square A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $A \cdot B$.
	\Box 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	
3.0/0.0	
	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 protocolo criptográfico de $ElGamal$ que usa este número para a escolha de \mathbb{F}_p^* :
	A quebra do protocolo é fácil.
0/0.5	Dois <i>ciphertexts</i> podem encriptar a mesma mensagem.
	 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:
	 O protocolo pode ser quebrado em tempo exponencial. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais
0.5/0.5	ciphertexts.
	A probabilidade de um plaintext é independente do ciphertext.
	O protocolo pode ser quebrado em tempo polinomial.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
	$igotimes_p$ Exponenciação em \mathbb{F}_p^* é fácil e factorização é difícil.
0.2/0.5	Mulitplicação é fácil e factorização é difícil.
	\square Exponenciação em \mathbb{F}_p^* é fácil e o <i>Discrete Logarithm Problem</i> é difícil.
	Mulitplicação é fácil e divisão é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
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 solução do <i>DLP</i> é mais complicada sobre curvas elípticas do que em F _p .
	\square A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .

André Revés Pereira - 45747 - MIEI Mark: 0.8/5 (total score: 0.8/5)

•		+17/1/28+
	Departamento de Matemá Criptografia	tica Faculdade de Ciências e Tecnologia — UNI 8/7/2018 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	Marque o seu número de aluno preenchendo completamente os qua drados respectivos da grelha ao lado () e escreva o nome completo, o número e o curso abaixo. Nome: André Revés Peneira
	6 6 6 6 6 7 7 7 7 7 8 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.
-0.2/0.5	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 n número primo. \square n é um número primo ímpar. \square 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
0.5/0.5	só do segredo do algorido de só da chave, mas não de do segredo da chave e do só da complexidade da	o segredo do algoritmo.
	Questão 3 Qual destes pa	rotocolos criptográficos é assimétrico?
0.5/0.5	_ AES _ DES	☐ Vigenère ElGamal
	Questão 4 O Discrete Logarithm Pro	$blem\;(DLP)$ para a congruência $g^{oldsymbol{x}}\equiv h\;(\operatorname{mod} p)\;$ é:

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

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

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

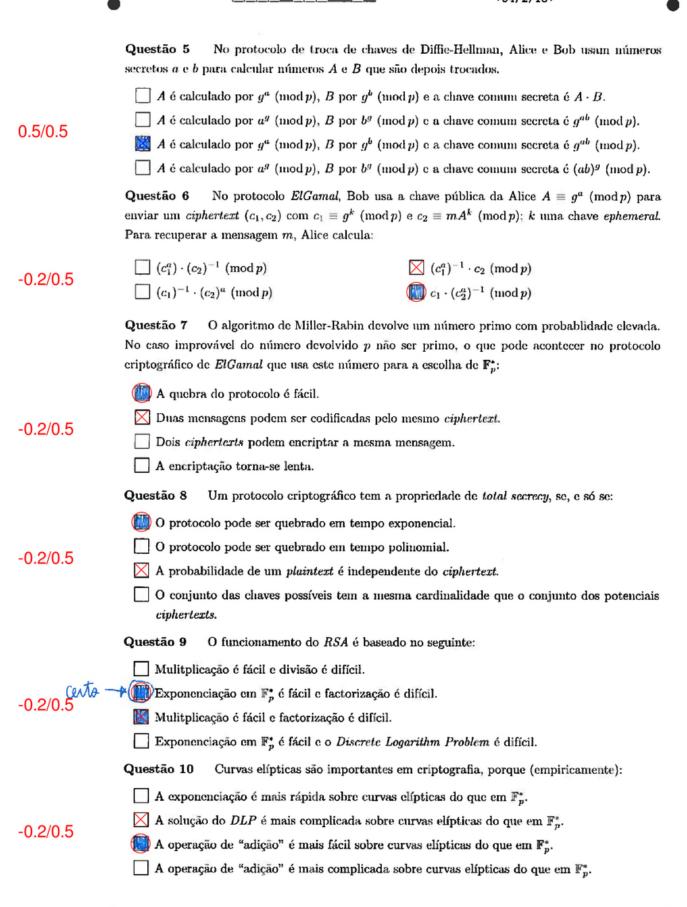
Determine g, dados h, $p \in x$.

-0.2/0.5

	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 (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 g^{ab} (mod p). ☐ 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 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 <i>ElGamal</i> que usa este número para a escolha de \mathbb{F}_p^* :
-0.2/0.5	 □ A encriptação torna-se lenta. ☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext. □ 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:
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 exponencial. O protocolo pode ser quebrado em tempo polinomial. A probabilidade de um plaintext é independente do ciphertext.
-0.2/0.5	 Questão 9 O funcionamento do RSA é baseado no seguinte: Mulitplicação é fácil e divisão é difícil. Exponenciação em F_p[*] é fácil e o Discrete Logarithm Problem é difícil. Exponenciação em F_p[*] é fácil e factorização é difícil. Mulitplicação é fácil e factorização é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
-0.2/0.5	 A exponenciação é mais rápida sobre curvas elípticas do que em F_p*. A operação de "adição" é mais fácil sobre curvas elípticas do que em F_p*. A operação de "adição" é mais complicada sobre curvas elípticas do que em F_p*.
	\triangle A solução do DLP é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .

André de Jesus Costa - 42023 - MIEI Mark: 0.1/5 (total score: 0.1/5)

			+54/1/14+
	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 1 1 1 2 2 2 2 2 3 3 3 3 3	drados respectivos da número e o curso abai	imero de aluno preenchendo completamente os qua- grelha ao lado () e escreva o nome completo, o ixo.
	4 4 4 4 5 5 5 5 5 6 6 6 6 6 7 7 7 7 7		Número de aluno:
	99999	tivo () com caneta cada resposta errada o questão. Se a soma da	azul ou preta, cada resposta certa vale 0,5 valores, lesconta 0,2 valores e marcações múltiplas anulam a la classificações das questões de escolha múltipla der será atribuído 0 valores como resultado final.
	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
-0.2/0.5	n é um número primo n é um número par.	ímpar.	\nearrow n é uma potência de um número primo. n é um número primo.
			cípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
-0.2/0.5	do segredo da chave e só da chave, mas não d só do segredo do algori só da complexidade da	do segredo do algoritm	no.
	Questão 3 Qual destes p	protocolos criptográfic	os é assimétrico?
0.5/0.5	☐ Vigenère ☐ DES		AES ElGamal
	Questão 4 O Discrete Logarithm Pr	oblem (DLP) para a c	congruência $g^x \equiv h \pmod p$ é:
0.5/0.5	Determine x , dados g , Determine h , dados g ,		Determine p , dados g , $h \in x$. Determine g , dados h , $p \in x$.



António José Sá Barreto - 45101 - MIEI Mark: 0.8/5 (total score: 0.8/5)

•		+40/1/42+
	Departamento de Matemá Criptografia	itica Faculdade de Ciências e Tecnologia — UNL 8/7/2018 Exame Final
	Número de aluno 0 0 0 0 0 0 1 1 0 1 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.
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 5 5 5 5	Nome: Antonio Jose Si Battido Curso: MIEI Número de aluno: 45101
	6 6 6 6 6 7 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 sc, e só se:	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 primo n é um número primo n	
		de Kerckhoff são princípios que todos os sistemas criptográficos devem Kerckhoff fundamental diz que a segurança de um sistema criptográfico
0.5/0.5	do segredo da chave e	do segredo do algoritmo. do segredo do algoritmo. ithmo, mas não do segredo da chave. encriptação.
	Questão 3 Qual destes p	protocolos criptográficos é assimétrico?
0.5/0.5	ElGamal	☐ Vigenère ☐ DES
	Questão 4 O Discrete Logarithm Pr	oblem (DLP) para a congruência $g^x \equiv h \pmod{p}$ é: 17.5.7 (mod 5)

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

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

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

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

-0.2/0.5

	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 $a^g \pmod{p}$, 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 $g^a \pmod{p}$, 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 $g^{ab} \pmod{p}$.
-0.2/0.5	Questão 6 No protocolo $ElGamal$, Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para enviar um $eiphertext \ (c_1, c_2) \pmod{c_1} \equiv g^k \pmod{p}$ e $c_2 \equiv mA^k \pmod{p}$; k uma chave $ephemeral$. Para recuperar a mensagem m , Alice calcula:
	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 encriptação torna-se lenta. ☐ Duas mensagens podem ser codificadas pelo mesmo ciphertext. ☐ A quebra do protocolo é fácil.
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
0.5/0.5	 □ O protocolo pode ser quebrado em tempo polinomial. □ O protocolo pode ser quebrado em tempo exponencial. □ A probabilidade de um plaintext é independente do ciphertext. □ 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:
-0.2/0.5	 Exponenciação em F_p[*] 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. Mulitplicação 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 F_p*. A operação de "adição" é mais complicada sobre curvas elípticas do que em F_p*. A solução do DLP é mais complicada sobre curvas elípticas do que em F_p*. A exponenciação é mais rápida sobre curvas elípticas do que em F_p*.

António Maria Lage de Sousa Leitão - 45316 - LM Mark: 3.6/5 (total score: 3.6/5)

•			+30/1/2+
	Departamento de Matemá Criptografia	tica Facu 8/7/2018	aldade de Ciências e Tecnologia — UNL Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 1 2 2 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 7 8 8 8 8 8 9 9 9 9 9 9	drados respectivos da grella número e o curso abaixo. Nome: Antana Maria Mari	de aluno preenchendo completamente os quada ao lado () e escreva o nome completo, o la ao lado () e escreva o nome completo, o la ao lado () e escreva o nome completo, o la ao lado () e escreva o nome completo, o la lado () e escreva o nome completo, o la lado () e escreva o nome completamente o la seconda múltipla. Nas questões de escolha múltipla de la lado () e escreva o nome completamente o quadrado respecta preta, cada resposta certa vale 0,5 valores, a 0,2 valores e marcações múltiplas anulam a ificações das questões de escolha múltipla der ribuído 0 valores como resultado final.
	Questão 1 Considere o gree, c só se: n é um número primo.	_	uma multiplicação tal que \mathbb{F}_n é um corpo \mathfrak{g} é um número par.
0.5/0.5	n é uma potência de un Questão 2 Os princípios d	n número primo.	n é um número primo ímpar. que todos os sistemas criptográficos devem ne a segurança de um sistema criptográfico
0.5/0.5	do segredo da chave e d só da chave, mas não do só da complexidade da d só do segredo do algorit	o segredo do algoritmo.	la chave.
	Questão 3 Qual destes pr	rotocolos criptográficos é as	simétrico?
0.5/0.5	☐ AES ☐ DES		/igenère ElGamal
	Questão 4 O Discrete Logarithm Pro-	blem (DLP) para a congrué	ència $g^x \equiv h \; (\operatorname{mod} p)$ é:
0.5/0.5		_	Determine x , dados g , h e p . Determine p , dados g , h e 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	 ☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext. ☑ Dois ciphertexts podem encriptar a mesma mensagem. ☑ A encriptação torna-se lenta. ☑ A quebra do protocolo é fácil.
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
0.5/0.5	 O protocolo pode ser quebrado em tempo exponencial. O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts. A probabilidade de um plaintext é independente do ciphertext.
	O protocolo pode ser quebrado em tempo polinomial.
0.5/0.5	 Questão 9 O funcionamento do RSA é baseado no seguinte: Exponenciação em 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. Exponenciação em F_p[*] é fácil e factorização é difícil.
	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 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^* .