			+51/1	/20+
	Departamento de Matemá Criptografia	ítica 8/7/20		s e Tecnologia — UNL Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 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	Nome:	fanso	na múltipla. Nas questões mente o quadrado respec- osta certa vale 0,5 valores, cações múltiplas anulam a cos de escolha múltipla der
	Questão 1 Considere o se, e só se:	grupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se d	lefinir uma multiplicaçã	io tal que \mathbb{F}_n é um corpo
-0.2/0.5	\bigcap n é um número primo \bigcap n é um número par.		n é um número por n é uma potência	rimo ímpar. de um número primo.
	Questão 2 Os princípios satisfazer. Um princípio de l deve depender:			nas criptográficos devem um sistema criptográfico
-0.2/0.5	do segredo da chave e	rithmo, mas não do seg do segredo do algoritm do segredo do algoritm a encriptação.	no.	
	Questão 3 Qual destes	protocolos criptográfico	os é assimétrico?	
0.5/0.5	ElGamal AES		□ DES□ Vigenère	
	Questão 4 O Discrete Logarithm Pr	$roblem~(DLP)~{ m para}~{ m a}~{ m c}$	ongruência $g^{m{r}} \equiv h$ (mo	d p) é:
0.5/0.5			Determine x , dade	

-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. 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 $A \cdot B$. 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 $g^{ab} \pmod{p}$.
	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	
	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 \mathbf{F}_p^{\bullet} :
0.5/0.5	 Duas mensagens podem ser codificadas pelo mesmo ciphertext. A encriptação torna-se lenta. A quebra do protocolo é fácil. Dois ciphertexts podem encriptar a mesma mensagem.
-0.2/0.5	 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 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	 Exponenciação em F_p[*] é fácil e o Discrete Logarithm Problem é difícil. Mulitplicação é fácil e factorização é difícil. Exponenciação em 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):
-0.2/0.5	 ✓ A solução do DLP é mais complicada 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*. ☐ A exponenciação é mais rápida sobre curvas elípticas do que em F_p*.
	•

Sofia Martinho de Almeida Costa - 53548 - EMF Mark: 3.6/5 (total score: 3.6/5)

+25/1/12+

	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 4 4 4 4 4 4 5 5 5 5 6 6 6 6 6 6 7 7 7 7 7 8 8 8 8 8 9 9 9 9 9	Nome: MMA Curso: MMA O exame é composto marque a resposta certivo () com caneta cada resposta errada d questão. Se a soma da	mero de aluno preenchendo completamente os quagrelha ao lado () e escreva o nome completo, o exo. Clinho de Almeida Gasta Número de aluno:
-0.2/0.5	se, e só se: n é um número primo. n é uma potência de un Questão 2 Os princípios o	rupo Z/nZ. Pode-se o m número primo. de <i>Kerckhof</i> f são princ	definir uma multiplicação tal que \mathbb{F}_n é um corpo $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$
0.5/0.5	satisfazer. Um principio de K deve depender: só da complexidade da só da chave, mas não d do segredo da chave e d só do segredo do algorit	encriptação. o segredo do algoritm lo segredo do algoritm	no.
0.5/0.5	☐ DES ☐ Vigenère Questão 4	rotocolos criptográfico	es é assimétrico? ElGamal \square AES n and n are a congruência $g^x \equiv h \pmod{p}$ é:
0.5/0.5	Determine g , dados h , p Determine x , dados g , h) e x.	Determine h , dados g , p e x . 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	☐ 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 g^a (mod p), B por g^b (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 a^g (mod p), B por b^g (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:
0.5/0.5	
	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^* :
0.5/0.5	 Duas mensagens podem ser codificadas pelo mesmo ciphertext. A encriptação torna-se lenta. Dois ciphertexts podem encriptar a mesma mensagem. 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. 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:
0.5/0.5	 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 operação de "adição" é mais fácil sobre curvas elípticas do que em F_p*. A exponenciação é mais rápida 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*.
	,

Stylianos Neocleous - 41694 - MIEI Mark: 3.1/5 (total score: 3.1/5)

_					
		 _			

+88/1/6+

	Departamento de Matemá Criptografia	tica 8/7/20	Faculdade de Ciências e Tecn 018	nologia — UNL Exame Final
	Número de aluno 0 0 0 0 0 1 3 1 1 1		mero de aluno preenchendo compl grelha ao lado (■) e escreva o n xo.	•
	2 2 2 2 2 3 3 3 3 3 4 4 4 4		o, Mac Oran	
	5 5 5 5 6 6 6 7 7 7 7 7	Curso: M.E.1.	Número de aluno:	1694
	88888	marque a resposta cer tivo () com caneta a cada resposta errada d questão. Se a soma da	ta preenchendo completamente o c azul ou preta, cada resposta certa lesconta 0,2 valores e marcações ma s classificações das questões de esco será atribuído 0 valores como resul-	quadrado respec- vale 0,5 valores, últiplas anulam a olha múltipla der
	Questão 1 Considere o g se, e só se:		definir uma multiplicação tal que	
-0.2/0.5	n é um número par. n é um número primo.		n é um número primo ímp n ó uma potência de um n	
		-	cípios que todos os sistemas cript diz que a segurança de um sistem	**
0.5/0.5	só da complexidade da do segredo da chave e d só do segredo do algori só da chave, mas não d	do segredo do algoritn	redo da chave.	
	Questão 3 Qual destes p	rotocolos criptográfico	os é assimétrico?	
0.5/0.5	☐ Vigenère☐ DES		ElGamal 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 h , dados g , g Determine x , dados g , g		Determine g , dados h , p e dados g , h e dados g .	

	Questão 5 No protocolo de troca de chaves de l secretos a e b para calcular números A e B que são de	Diffie-Hellman, Alice e Bob usam números epois trocados.
0.5/0.5	A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$	e a chave comum secreta é $g^{ab} \pmod{p}$. e a chave comum secreta é $A \cdot B$.
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chaenviar um <i>ciphertext</i> (c_1, c_2) com $c_1 \equiv g^k \pmod{p}$ e corresponding a mensagem m , Alice calcula:	have pública da Alice $A \equiv g^a \pmod p$ para $e_2 \equiv mA^k \pmod p$; k uma chave $ephemeral$.
0/0.5		$(c_1^a)^{-1} \cdot c_2 \pmod{p}$ $c_1 \cdot (c_2^a)^{-1} \pmod{p}$
	Questão 7 — O algoritmo de Miller-Rabin devolve un No caso improvável do número devolvido p não ser criptográfico de ElGamal que usa este número para a	
0.5/0.5	 ☐ A encriptação torna-se lenta. ☑ Duas mensagens podem ser codificadas pelo mest ☐ A quebra do protocolo é fácil. ☐ Dois ciphertexts podem encriptar a mesma mensa 	
	Questão 8 Um protocolo criptográfico tem a propr	riedade de total secrecy, se, e só se:
0.5/0.5	 A probabilidade de um plaintext é independente O protocolo pode ser quebrado em tempo expone O conjunto das chaves possíveis tem a mesma ca ciphertexts. O protocolo pode ser quebrado em tempo polimo 	encial. ardinalidade que o conjunto dos potenciais
	Questão 9 O funcionamento do RSA é baseado no	
0.5/0.5	 Mulitplicação é fácil e divisão é difícil. Mulitplicação é fácil e factorização é difícil. Exponenciação em F_p é fácil e o Discrete Logariti Exponenciação em F_p é fácil e factorização é difícil 	hm Problem é difícil.
	Questão 10 Curvas elípticas são importantes em cr	riptografia, porque (empiricamente):
-0.2/0.5	 A operação de "adição" é mais complicada sobre A operação de "adição" é mais fácil sobre curvas X A solução do DLP é mais complicada sobre curva A exponenciação é mais rápida sobre curvas elípt 	elípticas do que em \mathbb{F}_p^* . as elípticas do que em \mathbb{F}_p^* .

Tiago Granadeiro Pires Madeira - 45112 - MIEI Mark: 1.4/5 (total score: 1.4/5)

+39/1/44+

	Departamento de Matemá Criptografia	tica 8/7/20	Faculdade de Ciências e Tecnologia — UNL 018 Exame Final
[4	Número de aluno 0 0 0 0 0 1 1 1 2 2 1		mero de aluno preenchendo completamente os qua- grelha ao lado () c escreva o nome completo, o xo.
	2 2 2 2 X 3 3 3 3 3 X 4 4 4 4	•	Hadrion.
	5 X 5 5 5 6 6 6 6 6 7 7 7 7 7 7	Curso: M. IEI	por 10 questões de escolha múltipla. Nas questões
	88888	tivo () com caneta 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, lesconta 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 g se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se o	lefinir uma multiplicação tal que \mathbb{F}_n é um corpo
0/0.5	\nearrow n é uma potência de un n é um número primo.	n número primo.	$n \in \text{um número primo ímpar.}$ $n \in \text{um número par.}$
			rípios 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 chave, mas não d só da complexidade da do segredo da chave e o	o segredo do algoritm encriptação.	0.
	Questão 3 Qual destes p	rotocolos criptográfico	os é assimétrico?
0.5/0.5	☐ DES ☐ AES		✓ Vigenère✓ ElGamal
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	ongruência $g^{m{x}} \equiv h \pmod{p}$ é:
0.5/0.5	Determine h , dados g , g Determine x , dados g , h		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.
-0.2/0.5	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 $A \cdot B$. 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	
	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^* :
	Duas mensagens podem ser codificadas pelo mesmo ciphertext.
0.0/0.5	A encriptação torna-se lenta.
0.2/0.5	A quebra do protocolo é fácil.
0-0	Dois ciphertexts podem encriptar a mesma mensagem.
orta	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
	O protocolo pode ser quebrado em tempo exponencial.
-0.2/0.5	O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.
	O protocolo pode ser quebrado em tempo polinomial.
	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.
0.5/0.5	Mulitplicação é fácil e factorização é difícil.
0.0, 0.0	Exponenciação em \mathbb{F}_p^* é fácil e o Discrete Logarithm Problem é difícil.
	\sqsubseteq Exponenciação em \mathbb{F}_p^* é fácil e factorização 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^* .
0/0.5	$igstyle A$ 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^* .

Tiago José Batista da Conceição - 46265 - MIEI Mark: 2.1/5 (total score: 2.1/5)

+43/1/36+

	Departamento de Matemá Criptografia	tica 8/7/20	Faculdade de Ciências e Tecnologia — UNL 018 Exame Final	
	Número de aluno 0 0 0 0 0 1 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: Tago	you Batista da Conceição	
	5 5 5 5 5 6 6 7 7 7 7	Curso: MIEI O exame é composto	Número de aluno: 46265 por 10 questões de escolha múltipla. Nas questões	
	8 8 8 8 8 9 9 9 9	marque a resposta cer 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 será atribuído 0 valores como resultado final.	
Questão 1 Considere o grupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se definir uma multiplicação tal que \mathbb{F}_n é um corpo se, e só se:				
0/0.5	n é um número primo n é um número primo n	ímpar.	$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	
	Questão 2 Os princípios de Kerckhoff são princípios que todos os sistemas criptográficos deven 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 do segredo do algoritmo. i só da chave, mas não do segredo do algoritmo. □ só da complexidade da encriptação. □ só do segredo do algorithmo, mas não do segredo da chave. 			
	Questão 3 Qual destes p	rotocolos criptográfico	os é assimétrico?	
0.5/0.5	☐ AES ☐ DES		☐ Vigenère ElGamal	
	Questão 4 O Discrete Logarithm Problem (DLP) para a congruência $g^x \equiv h \pmod{p}$ é:			
0.5/0.5			Determine h , dados g , p e x . Determine x , dados g , h e 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	☐ 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 $(ab)^g \pmod{p}$. 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:			
0/0.5				
	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	 Dois ciphertexts podem encriptar a mesma mensagem. Duas mensagens podem ser codificadas pelo mesmo ciphertext. A encriptação torna-se lenta. A quebra do protocolo é fácil. 			
-0.2/0.5	Questão 8 Um protocolo criptográfico tem a propriedade de <i>total secrecy</i> , 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 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:			
0/0.5	 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	\square A operação de "adição" é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .			
	\boxtimes 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^* .			
	\bigcirc A exponenciação é mais rápida sobre curvas elípticas do que em \mathbb{F}_p^* .			