	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.
	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.
-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:
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 exponenciação 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^* .

Tiago Miguel Dias Santos Bica - 47207 - MIEI Mark: 3.8/5 (total score: 3.8/5)

			+5/1/52	2+
	Departamento de Matemá Criptografia	ítica 8/7/2	Faculdade de Ciências e 018	Tecnologia — UNL Exame Final
	Número de aluno 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		unero de aluno preenchendo e grelha ao lado () e escret xo.	
	2 2 2 2 3 3 3 3 3 4 4 4 4 5 5 5 5 5 5	Bica	Juguel Dias	
	6 6 6 6 6 7 7 7 8 8 8 8 8 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 ra preenchendo completamenta azul ou preta, cada resposta desconta 0,2 valores e marcaças classificações das questões escrá atribuído 0 valores como	múltipla. Nas questões nte o quadrado respec- certa vale 0,5 valores, ões múltiplas anulam a de escolha múltipla der
	Questão 1 Considere o g se, e só se:		definir uma multiplicação t	
-0.2/0.5		un número primo.	n é um número prime n é um número prime	
	Questão 2 Os princípios satisfazer. Um princípio de I deve depender:	***	cípios que todos os sistemas diz que <i>a segurança de um</i>	
0.5/0.5	só da chave, mas não d só da complexidade da só do segredo do algor do segredo da chave e	encriptação. ithmo, mas não do seg	redo da chave.	
	Questão 3 Qual destes p	protocolos criptográfic	os é assimétrico?	
0.5/0.5	DES ElGamal		☐ Vigenère ☐ AES	
	Questão 4 O Discrete Logarithm Pr	oblem (DLP) para a c	eongruência $g^x \equiv h \; (\operatorname{mod} p)$) é:
0.5/0.5			Determine h, dados g	

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 $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $A \cdot B$. 0.5/0.5erto - (mod p), B por g^b (mod p) e a chave comum secreta é g^{ab} (mod p). \square A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ c 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 $g^{ab} \pmod{p}$. No protocolo ElGamal, Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para 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 ephemeral. Para recuperar a mensagem m, Alice calcula: $(c_1^a)^{-1} \cdot c_2 \pmod{p}$ 0.5/0.5Questão 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}_{v}^{*} : A quebra do protocolo é fácil. 🖦 Dois ciphertexts podem encriptar a mesma mensagem. 0.5/0.5🔝 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 conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts. A probabilidade de um plaintext é independente do ciphertext. -0.5/0.5O protocolo pode ser quebrado em tempo polinomial. O protocolo pode ser quebrado em tempo exponencial. Questão 9 O funcionamento do RSA é baseado no seguinte: Mulitplicação é fácil e divisão é difícil. Exponenciação em F, é fácil e o Discrete Logarithm Problem é difícil. 0/0.5Mulitplicação é fácil e factorização é difícil. Exponenciação em F_p é fácil e factorização é difícil. Curvas elípticas são importantes em criptografia, porque (empiricamente): 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 \mathbb{F}_p^* . 0.5/0.5A operação de "adição" é mais fácil sobre curvas elípticas do que em F_n. igsqcup A solução do DLP é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* . $^\circ$

Tito Miguel de Sousa Ribeiro Martins Ferreira - 45743 - MIEI Mark: 2.2/5 (total score: 2.2/5)

•			+55/1/12+
	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 2 3 3 3 3 3 4 4 4 4 4 5 5 5 5 6 6 6 6 6 7 7 7 7 7 8 8 8 8 8 9 9 9 9 9	Nome:	ninero de aluno preenchendo completamente os quagrelha ao lado () e escreva o nome completo, o ixo. Liguel de Souse Ribeiro Número de aluno:
,	Questão 1 Considere o g se, e só se:		definir uma multiplicação tal que \mathbb{F}_n é um corpo n é um número primo.
-0.2/0.5		de <i>Kerckhoff</i> são princ	n é um número primo ímpar. 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 do segredo da chave e d só da complexidade da só do segredo do algori	do segredo do algorita encriptação.	no.
	Questão 3 Qual destes p	rotocolos criptográfico	os é assimétrico?
0.5/0.5	☐ Vigenère		☐ AES
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	congruência $g^x \equiv h \; (\operatorname{mod} p) \; \acute{\mathrm{e}}$:
0.5/0.5	Determine x , dados g ,		
	Determine h , dados g ,	pex.	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	☐ $A \notin \text{calculado por } a^g \pmod{p}, B \text{ por } b^g \pmod{p} \text{ e a chave comum secreta } \notin g^{ab} \pmod{p}.$ ☐ $A \notin \text{calculado por } a^g \pmod{p}, B \text{ por } b^g \pmod{p} \text{ e a chave comum secreta } \notin (ab)^g \pmod{p}.$ ☐ $A \notin \text{calculado por } g^a \pmod{p}, B \text{ por } g^b \pmod{p} \text{ e a chave comum secreta } \notin g^{ab} \pmod{p}.$ ☐ $A \notin \text{calculado por } g^a \pmod{p}, B \text{ por } g^b \pmod{p} \text{ e a chave comum secreta } \notin A \cdot B.$
	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:
-0.2/0.5	
	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	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 <i>ciphertext</i> .
	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
0.5/0.5	ciphertexts. 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.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
-0.2/0.5	 Mulitplicação é fácil e factorização é difícil. □ Exponenciação em F_p[*] é fácil e factorização é difícil. □ Mulitplicação é fácil e divisão é difícil. □ Exponenciação em F_p[*] é fácil e o Discrete Logarithm Problem é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0.5/0.5	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^* .
	\square A operação de "adição" é mais complicada 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^* .

Tomás Emanuel Taborda Mendes da Silva - 47339 - MIEI Mark: 0.1/5 (total score: 0.1/5)

	•		+18/1/26+
	Departamento de Matema Criptografia		Faculdade de Ciências e Tecnologia — UNL 7/2018 Exame Final
	Número de almo 0 0 0 0 0 1 1 1 1 1 2 2 2 2 2	número e o curso al	número de aluno preenchendo completamente os quada grelha ao lado () e escreva o nome completo, o abaixo.
	3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Curso:M.I.E.	Número de aluno: 4 7339
	8888	marque a resposta c tivo () com caneta cada resposta errada questão. Se a soma d	to por 10 questões de escolha múltipla. Nas questões certa preenchendo completamente o quadrado respecta azul ou preta, cada resposta certa vale 0,5 valores, a desconta 0,2 valores e marcações múltiplas anulam a das classificações das questões de escolha múltipla der o, será atribuído 0 valores como resultado final.
	Questão 1 Considere o g se, c só se:	rupo Z/nZ. Pode-se	se definir uma multiplicação tal que \mathbb{F}_n é um corpo
-0.2/0.5	n é um número primo n n é um número primo.	і́шраг.	otin n é uma potência de um número primo. $ otin n$ é um número par.
	Questão 2 Os princípios de satisfazer. Um princípio de K deve depender:	le <i>Kerckhoff</i> são prin erckhoff fundamenta	incípios que todos os sistemas criptográficos devem al diz que a segurança de um sistema criptográfico
0.5/0.5	só da complexidade da le só da chave, mas não do do segredo da chave e de só do segredo do algorit	o segredo do algorita o segredo do algorita	tino.
	Questão 3 Qual destes pr	otocolos criptográfic	icos é assimétrico?
0.5/0.5	☐ Vigenère ☐ DES		ElGamal AES
	Questão 4 O Discrete Logarithm Prob	blem (DLP) para a c	congruência $g^x \equiv h \pmod{p}$ é:
-0.2/0.5	\boxtimes Determine x , dados g , h Determine g , dados h , p		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 númer secretos a e b para calcular números A e B que são depois trocados.
0.2/0.5	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 $a^g \pmod{p}$, 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 $g^{ab} \pmod{p}$.
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ par 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>ephemere</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 protocol criptográfico de <i>ElGamal</i> que usa este número para a escolha de \mathbb{F}_p^* :
0.5/0.5	 □ A quebra do protocolo é fácil. □ A encriptação torna-se lenta. ☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.
	Dois <i>ciphertexts</i> 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.
0.2/0.5	O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciai 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:
0.2/0.5	 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. 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 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^* . A solução do DLP é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .

Tomás Manuel Cambiaes Teles - 45344 - MIEI Mark: 0.5/5 (total score: 0.5/5)

			+/2/1/38+
	Departamento de Matemá Criptografia	tica 8/7/20	Faculdade de Ciências e Tecnologia — UNL 118 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 co.
	2 2 2 2 2 3 3 3 3 3 4 4 4 3 3	Noine: Tormas	Teles
	5 5 5 5 6 6 6 6 6 7 7 7 7 7		Número de aluno: .45.3.44
	88888	marque a resposta certivo () com caneta a cada resposta errada de questão. Se a soma das	ca preenchendo completamente o quadrado respec- nzul 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, c só se:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se d	efinir uma multiplicação tal que \mathbb{F}_n é um corpo
-0.2/0.5		de <i>Kerckhoff</i> são princ	n é um número primo ímpar. n é um número primo. n é um número primo. n é um número primo.
0.5/0.5	deve depender: do segredo da chave e o só da complexidade da só da chave, mas não d só do segredo do algori	do segredo do algoritm encriptação. o segredo do algoritme	о.
-0.2/0.5	Questão 3 Qual destes p	rotocolos criptográfico	s é assimétrico?
-0.2/0.0	Vigenère Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a co	$igorimsize igorimsize \operatorname{ElGamal}$ ongruência $g^{f r} \equiv h \pmod p$ é:
-0.2/0.5		p e x.	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	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 $A \cdot B$. 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>eiphertext</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^* :
0/0.5	 A quebra do protocolo é fácil. ∑ Duas mensagens podem ser codificadas pelo mesmo ciphertext. Dois ciphertexts podem encriptar a mesma mensagem. A encriptação torna-se lenta.
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
0/0.5	 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	 Exponenciação em F_p[*] é fácil e factorização é difícil. Mulitplicação é fácil e factorização é difícil. Mulitplicação é fácil e divisão é difícil. Exponenciação em F_p[*] é fácil e o Discrete Logarithm Problem 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 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[*].
	\square A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* .