Ricardo Nazir - 48057 - MIEI Mark: 0.2/5 (total score: 0.2/5)



+62/1/58+

	Departamento de Matemát Criptografia	tica 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 ( <b>()</b> ) e escreva o nome completo, o xo.
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 5 5 5 6 5 5		North
	6 6 6 6 6 7 7 7 7 M 8 8 8 8 9 9 9 9 9	O exame é composto marque a resposta certivo ( ) com caneta cada resposta errada d	Número de aluno: 48.057.  Número de aluno: 48.057.  por 10 questões de escolha múltipla. Nas questões ta preenchendo completamente o quadrado respecazul 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
	Questão 1 Considere o g se, e só se:		será atribuído $0$ valores como resultado final.  lefinir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
0/0.5	n é um número primo í $n$ é um número par.	ímpar.	
			ípios que todos os sistemas criptográficos devem diz que a segurança de um sistema criptográfico
0/0.5	só da chave, mas não d  do segredo da chave e d  só do segredo do algorid  só da complexidade da	do segredo do algoritn	no.
	Questão 3 Qual destes p	rotocolos criptográfico	os é assimétrico?
0.5/0.5	ElGamal  AES		☐ Vigenère ☐ DES
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	ongruência $g^x \equiv h \pmod p$ é:
-0.2/0.5	Determine $x$ , dados $g$ , $h$ Determine $p$ , dados $g$ , $h$		Determine $g$ , dados $h$ , $p \in x$ .  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 $g^a$ (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 $p$ ).
	<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:
0.2/0.5	
	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 $\mathbb{F}_p^*$ :
)/0.5	<ul> <li>A quebra do protocolo é fácil.</li> <li>         ∑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.     </li> <li>         ☐ Dois ciphertexts podem encriptar a mesma mensagem.     </li> <li>         ☐ A encriptação torna-se lenta.     </li> </ul>
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
)/0.5	<ul> <li>O protocolo pode ser quebrado em tempo exponencial.</li> <li>O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.</li> </ul>
	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	<ul> <li>Exponenciação em F<sub>p</sub><sup>*</sup> 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 factorização é difícil.</li> <li>Mulitplicação é fácil e divisão é difícil.</li> </ul>
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0.2/0.5	<ul> <li>A operação de "adição" é mais complicada sobre curvas elípticas do que em \( \mathbb{F}_p^* \).</li> <li>A exponenciação é mais rápida sobre curvas elípticas do que em \( \mathbb{F}_p^* \).</li> <li>A solução do \( DLP \) é mais complicada sobre curvas elípticas do que em \( \mathbb{F}_p^* \).</li> </ul>
	A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

Rodrigo Miquelino Bernardo - 48534 - MIEI Mark: 1/5 (total score: 1/5)

•			+63/1/56+
	Departamento de Matemá Criptografia	itica Faculdad 8/7/2018	de de Ciências e Tecnologia — UNL Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1		uno preenchendo completamente os qua- lado ( ) e escreva o nome completo, o
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 5 5 5 5 5		obrado.
	6 6 6 6 6 7 7 7 7 7 8 8 8 8 8 8 9 9 9 9 9 9	O exame é composto por 10 que marque a resposta certa preenche tivo ( ) com caneta azul ou pre cada resposta errada desconta 0,2 questão. Se a soma das classificaç	Número de aluno:4.8534
	Questão 1 Considere o g se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma	a multiplicação tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5	otin n é uma potência de u $ otin n$ é um número primo.	_	un número primo ímpar. un número par.
			odos os sistemas criptográficos devem segurança de um sistema criptográfico
-0.2/0.5		thmo, mas não do segredo da ch lo segredo do algoritmo.	ave.
	Questão 3 Qual destes p	rotocolos criptográficos é assime	étrico?
-0.2/0.5	DES AES	⊠ ElGa □ Viger	
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a congruência	$g^x \equiv h \pmod{p}$ é:
0.5/0.5	Determine $g$ , dados $h$ , $p$ Determine $p$ , dados $g$ , $h$		emine $x$ , dados $g$ , $h \in p$ .  emine $h$ , 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 $a^g \pmod{p}$ , $B$ 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 $g^{ab} \pmod{p}$ . ∴ $A$ 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 $g^{ab} \pmod{p}$ .
	<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:
0/0.5	
	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	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.
-0.2/0.5	Questão 9 — O funcionamento do RSA é baseado no seguinte:
	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):
0.5/0.5	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 $\mathbb{F}_p^*$ .  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 $\mathbb{F}_p^*$ .

Rúben Martins Dantas da Cunha - 46317 - MIEI Mark: 1.5/5 (total score: 1.5/5)

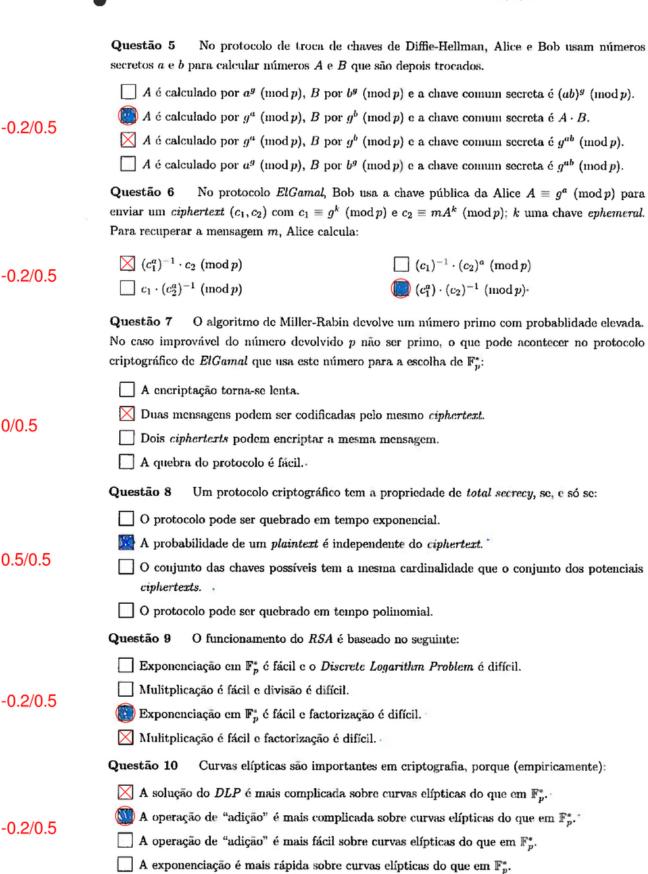
•			+77/1/28+	
	Departamento de Matemá Criptografia	tica E 8/7/201	Faculdade de Ciências e Tecnologia — UN 8 Exame Fina	
	Número de aluno  0 0 0 0 0  1 1 1 1 1  2 2 2 2 2  3 3 3 3 3 3  4 4 4 4 4  5 5 5 5 5  6 6 6 6 6  7 7 7 7 7  8 8 8 8 8  9 9 9 9 9	Nome:	Número de aluno:	es e
-0.2/0.5	se, e só se:  n é um número par.  n é um número primo í	rupo Z/nZ. Pode-se del	rá atribuído $0$ valores como resultado final.  finir uma multiplicação tal que $\mathbb{F}_n$ é um corp $n$ é uma potência de um número primo. $n$ é um número primo.	
		erckhoff fundamental di	oios que todos os sistemas criptográficos deven iz que <i>a segurança de um sistema criptográfic</i>	
-0.2/0.5	só da chave, mas não do do segredo da chave e d só do segredo do algorit	o segredo do algoritmo. lo segredo do algoritmo.		
	Questão 3 Qual destes pr	rotocolos criptográficos	é assimétrico?	
0.5/0.5	ElGamal  Vigenère	<u> </u>	AES DES	
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a con	gruência $g^x \equiv h \pmod p$ é:	
0.5/0.5	Determine $h$ , dados $g$ , $p$ Determine $x$ , dados $g$ , $h$	_	Determine $p$ , dados $g$ , $h \in x$ .  Determine $g$ , dados $h$ , $p \in x$ .	

	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 $\mathbb{F}_p^*$ :
0.5/0.5	<ul> <li>☐ A quebra do protocolo é fácil.</li> <li>☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>☐ A encriptação torna-se lenta.</li> <li>☐ Dois ciphertexts podem encriptar a mesma mensagem.</li> </ul>
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
	O protocolo pode ser quebrado em tempo polinomial.  O protocolo pode ser quebrado em tempo exponencial.
0.5/0.5	A probabilidade de um plaintext é independente do ciphertext.  O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexts.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
0.2/0.5	<ul> <li>Exponenciação em F<sub>p</sub><sup>*</sup> é fácil e o Discrete Logarithm Problem é difícil.</li> <li>Exponenciação em F<sub>p</sub><sup>*</sup> é fácil e factorização é difícil.</li> <li>Mulitplicação é fácil e factorização é difícil.</li> <li>Mulitplicação é fácil e divisão é difícil.</li> </ul>
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0.2/0.5	<ul> <li>A operação de "adição" é mais fácil sobre curvas elípticas do que em F<sub>p</sub>*.</li> <li>A exponenciação é mais rápida sobre curvas elípticas do que em F<sub>p</sub>*.</li> <li>A solução do DLP é mais complicada sobre curvas elípticas do que em F<sub>p</sub>*.</li> </ul>
	$\square$ A operação de "adição" é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

Salvador Rosa Mendes - 50503 - MIEI Mark: 0.5/5 (total score: 0.5/5)

+26/1/10+

	Departamento de Matemá Criptografia		Faculdade de Ciências e Tecnologia — UNL /2018 Exame Final
	Número de aluno  0		número de aluno preenchendo completamente os quada grelha ao lado ( ) e escreva o nome completo, o paixo.
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 4 5 6 5 5	Nome: Salvac	doc Hendes  Número de aluno: 50503
	6 6 6 6 6 7 7 7 7 7 8 8 8 8 8 9 9 9 9 9	O exame é composto marque a resposta ce tivo () com caneta cada resposta errada questão. Se a soma d	o por 10 questões de escolha múltipla. Nas questões erta preenchendo completamente o quadrado respec- a azul ou preta, cada resposta certa vale 0,5 valores, desconta 0,2 valores e marcações múltiplas anulam a las classificações das questões de escolha múltipla der , será atribuído 0 valores como resultado final.
	Questão 1 Considere o gr se, e só se:		e definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
0/0.5	igwedge n é uma potência de un $igwedge n$ é um número primo.	número primo.	$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $
	Questão 2 Os princípios d satisfazer. Um princípio de Ko deve depender:	e <i>Kerckhoff</i> são prin erckhoff fundamenta	ncípios que todos os sistemas criptográficos devem al diz que a segurança de um sistema criptográfico
0.5/0.5	só do segredo do algorit do segredo da chave e de só da complexidade da c	o segredo do algorita encriptação.	imo.
	Questão 3 Qual destes pr	otocolos criptográfic	cos é assimétrico?
-0.2/0.5	<ul><li>─ Vigenère</li><li>✓ ElGamal</li></ul>	Certo -	DES'
	Questão 4 O Discrete Logarithm Prob	olem (DLP) para a o	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 $g$ , $p \in x$ .  Determine $p$ , dados $g$ , $h \in x$ .



Salúquia Cristina Dias Norte Marreiros - 47775 - MIEI Mark: 2.2/5 (total score: 2.2/5)

			+1/1/60+	
	Departamento de Matemá Criptografia	itica 8/7/2	Faculdade de Ciências e Tecnologia — 2018 Exame F	
	Número de aluno 0 0 0 0 0 1 1 1 1 1		número de aluno preenchendo completamente os la grelha ao lado (  ) e escreva o nome comple aixo.	-
	2 2 2 2 2 2 3 3 3 3 3 3 3 3 4 4 4 4 4 5 5 5 5 5 6 6 6 6 6		Número de aluno: 47775	
	6 6 6 6 6 7 7 7 7 8 8 8 8 8 9 9 9 9 9	O exame é composto marque a resposta certivo ( ) com caneta cada resposta errada e questão. Se a soma de	o por 10 questões de escolha múltipla. Nas que erta preenchendo completamente o quadrado re a azul ou preta, cada resposta certa vale 0,5 va desconta 0,2 valores e marcações múltiplas anul las classificações das questões de escolha múltipl , será atribuído 0 valores como resultado final.	estões espec- dores,
	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 c	corpo
-0.2/0.5	n é um número par. $n$ é um número primo.		$\nearrow$ $n$ é uma potência de um número prin $\bigcirc$ $n$ é um número primo ímpar.	no.
			ncípios que todos os sistemas criptográficos de al diz que <i>a segurança de um sistema criptogr</i>	
0.5/0.5	só da complexidade da só da chave, mas não d do segredo da chave e d só do segredo do algorit	o segredo do algorita	mo.	
	Questão 3 Qual destes p	rotocolos criptográfic	cos é assimétrico?	
0.5/0.5	☐ AES ☐ DES			
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	congruência $g^x \equiv h \pmod{p}$ é:	
0.5/0.5	Determine $g$ , dados $h$ , $p$ Determine $h$ , dados $g$ , $p$		Determine $p$ , dados $g$ , $h \in x$ .  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	☐ $A$ 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 $g^a \pmod{p}$ , $B$ 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 $g^{ab} \pmod{p}$ .
	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>☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>☑ A quebra do protocolo é fácil.</li> <li>☑ Dois ciphertexts podem encriptar a mesma mensagem.</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.
0.5/0.5	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:
	$\square$ Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
-0.2/0.5	Exponenciação em $\mathbb{F}_p^*$ é fácil e o Discrete Logarithm Problem é difícil.
	Mulitplicação é fácil e divisão é difícil.
	<ul> <li>Mulitplicação é fácil e factorização é difícil.</li> <li>Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):</li> </ul>
	A operação de "adição" é mais complicada sobre curvas clípticas do que em $\mathbb{F}_p^*$ .
-0.2/0.5	A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\boxtimes$ A solução do $DLP$ é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\square$ A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .