David Canilhas Romão - 49309 - MIEI Mark: 3.1/5 (total score: 3.1/5)

•			+2/1/58+
	Departamento de Matemá Criptografia	tica 8/7/2	Faculdade de Ciências e Tecnologia — UNL 018 Exame Final
0,3	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	Nome: David Nome: David Curso: MIEI O exame é composto marque a resposta certivo () com caneta cada resposta errada d questão. Se a soma da	ninero de aluno preenchendo completamente os quagrelha ao lado () e escreva o nome completo, o ixo. Número de aluno: 49309 por 10 questões de escolha múltipla. Nas questões ta preenchendo completamente o quadrado respectazul ou preta, cada resposta certa vale 0,5 valores, lesconta 0,2 valores e marcações múltiplas anulam a se classificações das questões de escolha múltipla der será atribuído 0 valores como resultado final.
0/0.5	Questão 1 Considere o g se, c só se: ightharpoonup n é uma potência de un ightharpoonup n é um número primo.		definir uma multiplicação tal que \mathbb{F}_n é um corpo $\hfill n$ é um número par. $\hfill n$ 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 complexidade da só da chave, mas não d do segredo da chave e d só do segredo do algoria	o segredo do algoritm lo segredo do algoritn	no. ×
0.5/0.5	DES Vigenère	rotocolos criptográfico	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 , $p \in x$. Determine x , dados g , $h \in p$.

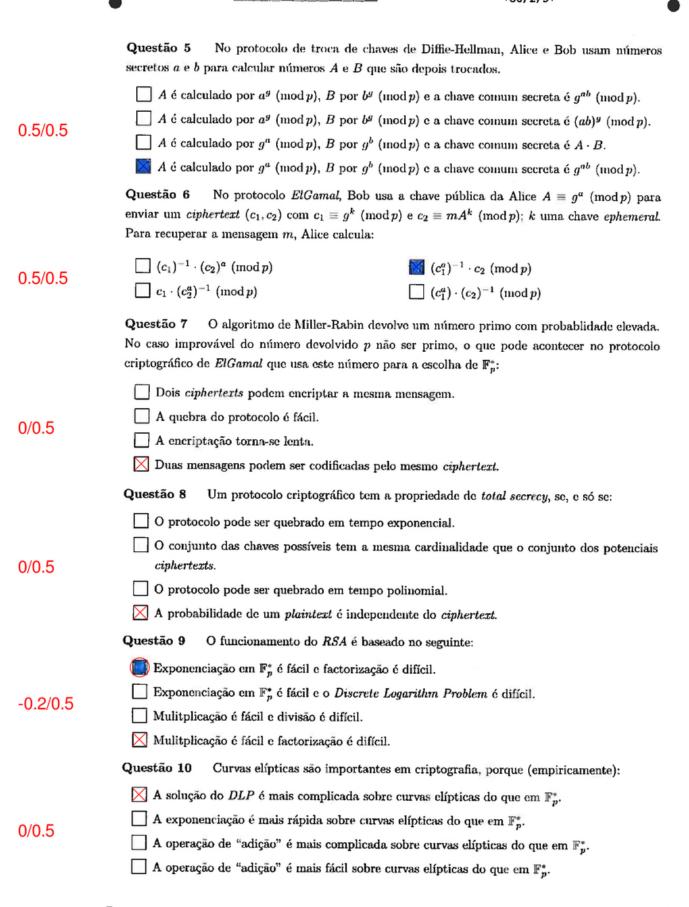
	Questão 5 No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usam núme	ro:
	secretos \underline{a} e \underline{b} para calcular números A e B que são depois trocados.	
	\square A é calculado por $a^g \pmod{p}$, B por $b^g \pmod{p}$ e a chave comum secreta é $(ab)^g \pmod{p}$).
0.5/0.5	$A \in \text{calculado por } a^g \pmod{p}$, $B \text{ por } b^g \pmod{p}$ e a chave comum secreta $ext{c} g^{ab} \pmod{p}$.	
	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 $g^{ab} \pmod{p}$.	
	Questão 6 No protocolo ElGamal, Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ pa	
	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 ephemer Para recuperar a mensagem m , Alice calcula:	ral
0.5/0.5		
	Questão 7 O algoritmo de Miller-Rabin devolve um número primo com probablidade elevad	la.
	No caso improvável do número devolvido p não ser primo, o que pode acontecer no protoco	olo
	criptográfico de <i>ElGamal</i> que usa este número para a escolha de \mathbb{F}_p^* :	
	Dois ciphertexts podem encriptar a mesma mensagem.	
0.2/0.5	□ 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 total secrecy, se, e só se:	
	O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potencia ciphertexts.	is
0.5/0.5	O protocolo pode ser quebrado em tempo exponencial.	
	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:	
	Mulitplicação é fácil e factorização é difícil.	
0.5/0.5	\square Exponenciação em \mathbb{F}_p^* é fácil e o Discrete Logarithm Problem é difícil.	
0.5/0.5	Mulitplicação é fácil e divisão é difícil.	
	Exponenciação em \mathbb{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^* . \rightthreetimes	
	\square A operação de "adição" é mais fácil 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^* .	
	\bigcirc A operação de "adição" é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .	

David Rito Vaz - 41821 - MIEI Mark: 2.8/5 (total score: 2.8/5)

Criptografia

+86/1/10+ Departamento de Matemática Faculdade de Ciências e Tecnologia — UNL 8/7/2018 Exame Final Número de aluno Marque o seu número de aluno preenchendo completamente os quadrados respectivos da grelha ao lado () e escreva o nome completo, o 0 0 0 0 0 número e o curso abaixo. 1 1 1 2 2 2 2 2 2 Nome: David Rito Vot 3 3 3 3 4 4 4 4 5 5 5 5 5 Curso: MIEI Número de aluno: 41871 6 6 6 6 7 7 7 7 7 O exame é composto por 10 questões de escolha múltipla. Nas questões 8 8 📓 8 8 marque a resposta certa preenchendo completamente o quadrado respectivo (com caneta azul ou preta, cada resposta certa vale 0,5 valores, 9 9 9 9 9 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. Considere o grupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se definir uma multiplicação tal que \mathbb{F}_n é um corpo n é um número primo impar. n é um número primo.

Questão 1 se, e só se: n é uma potência de um número primo. 0.5/0.5n é um número par. 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: só da complexidade da encriptação. 🔣 só da chave, mas não do segredo do algoritmo. 0.5/0.5só do segredo do algorithmo, mas não do segredo da chave. do segredo da chave e do segredo do algoritmo. Questão 3 Qual destes protocolos criptográficos é assimétrico? ☐ AES DES 0.5/0.5ElGamal Vigenère Questão 4 O Discrete Logarithm Problem (DLP) para a congruência $g^r \equiv h \pmod{p}$ é: Determine g, dados h, $p \in x$. Determine p, dados q, $h \in x$. 0.5/0.5Determine x, dados g, $h \in p$. Determine h, dados g, $p \in x$.



Dinis Costa Cabanas - 43111 - MIEI Mark: 4.3/5 (total score: 4.3/5)



+94/1/54+

	Departamento de Matemá	ática Faculdade de Ciências e Tecnologia — UN		
	Criptografia	8/7/2		Exame Final
	Número de aluno 0 0 0 0 0 1 1		úmero de aluno preenchendo a grelha ao lado (■) e escre ixo.	
	2 2 2 2 2 3 3 3 3 3 4 4 4 4 4		Costa Cabanas	
	5 5 5 5 6 6 6 6 7 7 7 7 7		Número de aluno	
	88888	marque a resposta cel tivo () com caneta cada resposta errada e questão. Se a soma de	por 10 questões de escolha rta preenchendo completame azul ou preta, cada resposta desconta 0,2 valores e marcaç as classificações das questões será atribuído 0 valores com-	ente o quadrado respec- a certa vale 0,5 valores, ções múltiplas anulam a de escolha múltipla der
	Questão 1 Considere o g se, c só se:	rupo Z/nZ. Pode-se	definir uma multiplicação (tal que \mathbb{F}_n é um corpo
0 E/0 E	\square n é um número par.		n é um número prim	o ímpar.
0.5/0.5	$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $		🌉 n é uma potência de	um número primo.
	Questão 2 Os princípios o satisfazer. Um princípio de K deve depender:		cípios que todos os sistemas diz que a segurança de um	
0.5/0.5	só da chave, mas não de do segredo da chave e d só da complexidade da só do segredo do algorit	lo segredo do algorita encriptação.	no.	
	Questão 3 Qual destes pr	rotocolos criptográfic	os é assimétrico?	
0.5/0.5	☐ DES ☐ Vigenère		ElGamal AES	
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	ongruência $g^x\equiv h\ (\mathrm{mod} p)$	é:
0.5/0.5	Determine p , dados g , h Determine x , dados g , h			

	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 $g^{ab} \pmod{p}$. ☐ A é calculado por $g^a \pmod{p}$, B por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$. ☐ 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>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^* :
	Dois ciphertexts podem encriptar a mesma mensagem.
0.5/0.5	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:
	O protocolo pode ser quebrado em tempo polinomial.
0.5/0.5	O protocolo pode ser quebrado em tempo exponencial.
0.0/0.0	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:
	Mulitplicação é fácil e factorização é difícil.
0.5/0.5	Exponenciação em \mathbb{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 divisão é difícil. Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
	e in the state of
	A operação de "adição" é mais fácil sobre curvas elípticas do que em \mathbb{F}_p^* . A exponenciação é mais rápida 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^* .
	\boxtimes A solução do DLP é mais complicada sobre curvas elípticas do que em \mathbb{F}_p^* .

Diogo Almeida Pereira - 44640 - MIEI Mark: 1.5/5 (total score: 1.5/5)

+58/1/6+

	Departamento de Matemá Criptografia	tica 8/7/2	Faculdade de Ciências e Tecnologia — UNL 2018 — Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		úmero de aluno preenchendo completamente os qua- a grelha ao lado (■) e escreva o nome completo, o iixo.
	2 2 2 2 2 3 3 3 3 3	Nome: Those	Almida Perin
	5 5 5 5 6 6	Curso: MIE 1	Número de aluno: 44640
	7 7 7 7 7 8 8 8 8 8 8 9 9 9 9 9 9	marque a resposta ce tivo (■) com caneta cada resposta errada e questão. Se a soma da	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 sc, 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	$\ \ \ \ \ \ \ \ \ \ \ \ \ $	-	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 complexidade da só da chave, mas não de do segredo da chave e d só do segredo do algorit	o segredo do algorita lo segredo do algorita	no.
	Questão 3 Qual destes pr	rotocolos criptográfic	os é assimétrico?
0.5/0.5	ElGamal DES		☐ AES ☐ Vigenère
	Questão 4 O Discrete Logarithm Pro	blem (DLP) para a c	congruência $g^x \equiv h \pmod{p}$ é:
0.5/0.5			Determine g , dados h , $p \in x$. Determine x , dados g , $h \in p$.

0.5/0.5	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. $A \in \text{calculado por } g^a \pmod{p}, B \text{ por } g^b \pmod{p} \text{ e a chave comum secreta } e A \cdot B.$ $A \in \text{calculado por } a^g \pmod{p}, B \text{ por } b^g \pmod{p} \text{ e a chave comum secreta } e g^{ab} \pmod{p}.$ $A \in \text{calculado por } g^a \pmod{p}, B \text{ por } g^b \pmod{p} \text{ e a chave comum secreta } e g^{ab} \pmod{p}.$ $A \in \text{calculado por } a^g \pmod{p}, B \text{ por } b^g \pmod{p} \text{ e a chave comum secreta } e (ab)^g \pmod{p}.$ $A \in \text{calculado por } a^g \pmod{p}, B \text{ por } b^g \pmod{p} \text{ e a chave comum secreta } e (ab)^g \pmod{p}.$ $A \in \text{calculado por } a^g \pmod{p}, B \text{ por } b^g \pmod{p} \text{ e a chave comum secreta } e (ab)^g \pmod{p}.$ $A \in \text{calculado por } a^g \pmod{p}, B \text{ por } b^g \pmod{p} \text{ e a chave comum secreta } e (ab)^g \pmod{p}.$ $A \in \text{calculado por } a^g \pmod{p}, B \text{ por } b^g \pmod{p} \text{ e a chave comum secreta } e (ab)^g \pmod{p}.$ $A \in \text{calculado por } a^g \pmod{p}, B \text{ por } b^g \pmod{p} \text{ e a chave comum secreta } e (ab)^g \pmod{p}.$
-0.2/0.5 _{erto}	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:
	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.
-0.2/0.5	 Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se: O protocolo pode ser quebrado em tempo 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:
0.5/0.5	 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. Exponenciação em F_p[*] é fácil e factorização é difícil.
-0.2/0.5	 Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente): 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 solução do DLP é mais complicada sobre curvas elípticas do que em F_p*. A operação de "adição" é mais complicada sobre curvas elípticas do que em F_p*.

Diogo Filipe Carlos Duarte - 41817 - MIEI Mark: 0/5 (total score: -0.6/5)

			+16/1/30+	
	Departamento de Matemá Criptografia	tica 8/7/2	Faculdade de Ciências e Tec 018	nologia — UNL Exame Final
	Número de aluno 0 0 0 0 0 1 2 1 1 1 1		imero de aluno preenchendo comp a grelha ao lado () e escreva o s ixo.	
	2 2 2 2 2 3 3 3 3 3 4 4 4 4	Nome:	Filipe Carlos Dua	1
	5 5 5 5 6 6 6	Curso:	MIFI Número de aluno:	1.18.12
	7 7 7 7 8 8 8 8 8 9 9 9 9	marque a resposta cel tivo () com caneta cada resposta errada e questão. Se a soma da	por 10 questões de escolha múltip rta preenchendo completamente o azul ou preta, cada resposta certa desconta 0,2 valores e marcações m as classificações das questões de esc será atribuído 0 valores como resu	quadrado respec- a vale 0,5 valores, últiplas anulam a colha múltipla der
	Questão 1 Considere o g se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$. Pode-se	definir uma multiplicação tal qu	e \mathbb{F}_n é um corpo
-0.2/0.5	\nearrow n é uma potência de un n é um número primo.	-	$\ \ \ \ \ \ \ \ \ \ \ \ \ $	oar.
			cípios que todos os sistemas cript diz que <i>a segurança de um siste</i>	
-0.2/0.5	 ☐ do segredo da chave e o ☑ só da chave, mas não d ⑥ só da complexidade da ☐ só do segredo do algoridade 	o segredo do algoritm encriptação.	10.	
	Questão 3 Qual destes p	rotocolos criptográfic	os é assimétrico?	
-0.2/0.5	☐ Vigenère ☐ DES		ElGamal AES	
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	congruência $g^x\equiv h\ (\mathrm{mod} p)$ é:	
0.5/0.5	Determine x , dados g , h Determine g , dados h , g		Determine h , dados g , p e Determine p , dados g , h e	

	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	
	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. □ Dois ciphertexts podem encriptar a mesma mensagem. □ Duas mensagens podem ser codificadas pelo mesmo ciphertext. □ A quebra do protocolo é fácil.
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 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.
0.2/0.5	 Questão 9 O funcionamento do RSA é baseado no seguinte: Mulitplicação é fácil e divisão é difícil. Mulitplicação é fácil e factorização é difícil. Exponenciação em F_p[*] é fácil e factorização 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	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^* . 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^* .