



Departamento de Matemática  
Criptografia

Faculdade de Ciências e Tecnologia — UNL  
8/7/2018 Exame Final

Número de aluno

0	0	0	0	
1	1	1	1	1
2	2		2	2
3	3	3	3	3
	4	4	4	4
	5	5	5	5
6	6	6		6
7		7	7	7
8	8	8	8	8
9	9	9	9	9

← 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.

Nome: Guilherme Faria

Curso: MIEI Número de aluno: 47260

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 grupo  $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multiplicação tal que  $\mathbb{F}_n$  é um corpo se, e só se:

- ☐  $n$  é um número primo ímpar.
- ☒  $n$  é uma potência de um número primo.
- ☐  $n$  é um número par.
- ☐  $n$  é um número primo.

Questão 2 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 do segredo do algoritmo, mas não do segredo da chave.
- ☒ só da chave, mas não do segredo do algoritmo.
- ☐ só da complexidade da encriptação.
- ☒ do segredo da chave e do segredo do algoritmo.

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

- ☒ ElGamal
- ☐ Vigenère
- ☐ AES
- ☒ DES

Questão 4

O *Discrete Logarithm Problem (DLP)* para a congruência  $g^x \equiv h \pmod{p}$  é:

- ☐ Determine  $p$ , dados  $g$ ,  $h$  e  $x$ .
- ☒ Determine  $x$ , dados  $g$ ,  $h$  e  $p$ .
- ☐ Determine  $h$ , dados  $g$ ,  $p$  e  $x$ .
- ☒ Determine  $g$ , dados  $h$ ,  $p$  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.

- ☐  $A$  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  $y^a \pmod{p}$ ,  $B$  por  $y^b \pmod{p}$  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 *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:

- ☒  $(c_1^a)^{-1} \cdot c_2 \pmod{p}$  ☐  $(c_1^a) \cdot (c_2)^{-1} \pmod{p}$
- ☐  $c_1 \cdot (c_2^a)^{-1} \pmod{p}$  ☐  $(c_1)^{-1} \cdot (c_2)^a \pmod{p}$

**Questão 7** O algoritmo de Miller-Rabin devolve um número primo com probabilidade 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.
- ☐ Dois *ciphertexts* 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 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*.

**Questão 9** O funcionamento do *RSA* é baseado no seguinte:

- ☐ Multiplicação é fácil e divisão é difícil.
- ☐ Exponenciação em  $\mathbb{F}_p^*$  é fácil e factorização é difícil.
- ☒ Multiplicação é fácil e factorização 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):

- ☒ A operação de "adição" é mais fácil 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 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  $\mathbb{F}_p^*$ .



+80/1/22+

Departamento de Matemática  
Criptografia

Faculdade de Ciências e Tecnologia — UNL  
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	5
6	6	6	6	6
7	7	7	7	7
8	8	8	8	8
9	9	9	9	9

← 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.

Nome:	Heitor da Silva Cordeiro			
	Moniz			
Curso:	MIEI		Número de aluno:	45809

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 grupo  $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multiplicação tal que  $\mathbb{F}_n$  é um corpo se, e só se:

- 0.5/0.5
- |  |  |
|--|--|
| <input checked="" type="checkbox"/> $n$ é um número par.                   | <input type="checkbox"/> $n$ é um número primo.                  |
| <input checked="" type="checkbox"/> $n$ é uma potência de um número primo. | <input checked="" type="checkbox"/> $n$ é um número primo ímpar. |

**Questão 2** 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*:

- 0.5/0.5
- |   |
|---|
| <input type="checkbox"/> só da complexidade da encriptação.                       |
| <input type="checkbox"/> só do segredo do algoritmo, mas não do segredo da chave. |
| <input checked="" type="checkbox"/> só da chave, mas não do segredo do algoritmo. |
| <input type="checkbox"/> do segredo da chave e do segredo do algoritmo.           |

**Questão 3** Qual destes protocolos criptográficos é *assimétrico*?

- 0.5/0.5
- |   |                                   |
|---|-----------------------------------|
| <input type="checkbox"/> DES                | <input type="checkbox"/> Vigenère |
| <input checked="" type="checkbox"/> ElGamal | <input type="checkbox"/> AES      |

**Questão 4**

O *Discrete Logarithm Problem (DLP)* para a congruência  $g^x \equiv h \pmod{p}$  é:

- 0/0.5
- |  |   |
|--|---|
| <input type="checkbox"/> Determine $g$ , dados $h$ , $p$ e $x$ . | <input checked="" type="checkbox"/> Determine $x$ , dados $g$ , $h$ e $p$ . |
| <input type="checkbox"/> Determine $p$ , dados $g$ , $h$ e $x$ . | <input checked="" type="checkbox"/> Determine $h$ , dados $g$ , $p$ 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.

- ☒  $A$  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  $g^{ab} \pmod{p}$ .  
☐  $A$  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 *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:

- ☒  $(c_1^a)^{-1} \cdot c_2 \pmod{p}$  ☐  $(c_1)^{-1} \cdot (c_2)^a \pmod{p}$   
☐  $(c_1^a) \cdot (c_2)^{-1} \pmod{p}$  ☐  $c_1 \cdot (c_2^a)^{-1} \pmod{p}$

**Questão 7** O algoritmo de Miller-Rabin devolve um número primo com probabilidade 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.  
☒ A encriptação torna-se lenta.  
☐ A quebra do protocolo é fácil.  
☒ Duas mensagens podem ser codificadas pelo mesmo *ciphertext*.

**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*.  
☐ O protocolo pode ser quebrado em tempo exponencial.  
☐ O protocolo pode ser quebrado em tempo polinomial.

**Questão 9** O funcionamento do *RSA* é baseado no seguinte:

- ☐ Multiplicação é fácil e divisão é difícil.  
☒ Multiplicação é fácil e factorização é difícil.  
☐ Exponenciação em  $\mathbb{F}_p^*$  é fácil e factorização 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):

- ☐ 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  $\mathbb{F}_p^*$ .  
☐ A operação de "adição" é mais complicada sobre curvas elípticas do que em  $\mathbb{F}_p^*$ .  
☒ A solução do *DLP* é mais complicada sobre curvas elípticas do que em  $\mathbb{F}_p^*$ .





Departamento de Matemática  
Criptografia

Faculdade de Ciências e Tecnologia — UNL  
8/7/2018 Exame Final

Número de aluno

0	0	0	0	0
1	1	1	1	1
2	<input checked="" type="checkbox"/>	2	<input checked="" type="checkbox"/>	2
3	3	3	3	3
<input checked="" type="checkbox"/>	4	1	4	4
5	5	<input checked="" type="checkbox"/>	5	5
6	6	6	6	<input checked="" type="checkbox"/>
7	7	7	7	7
8	8	8	8	8
9	9	9	9	9

← 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.

Nome: Henrique José Tavares do Vale

Curso: MIEI Número de aluno: 42526

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 grupo  $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multiplicação tal que  $\mathbb{F}_n$  é um corpo se, e só se:

-0.2/0.5

- ☒  $n$  é um número primo.
- ☐  $n$  é um número primo ímpar.
- ☒  $n$  é uma potência de um número primo.
- ☐  $n$  é um número par.

Questão 2 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:

0/0.5

- ☐ do segredo da chave e do segredo do algoritmo.
- ☐ só da complexidade da encriptação.
- ☐ só do segredo do algoritmo, mas não do segredo da chave.
- ☒ só da chave, mas não do segredo do algoritmo.

Questão 3 Qual destes protocolos criptográficos é assimétrico?

0.5/0.5

- ☐ AES
- ☐ Vigenère
- ☒ ElGamal
- ☐ DES

Questão 4

O Discrete Logarithm Problem (DLP) para a congruência  $g^x \equiv h \pmod{p}$  é:

-0.2/0.5

- ☒ Determine  $x$ , dados  $g$ ,  $h$  e  $p$ .
- ☒ Determine  $g$ , dados  $h$ ,  $p$  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.

- ☐  $A$  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 *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:

- ☐  $(c_1)^{-1} \cdot (c_2)^a \pmod{p}$  ☐  $(c_1^a) \cdot (c_2)^{-1} \pmod{p}$
- ☒  $(c_1^a)^{-1} \cdot c_2 \pmod{p}$  ☒  $c_1 \cdot (c_2^a)^{-1} \pmod{p}$

**Questão 7** O algoritmo de Miller-Rabin devolve um número primo com probabilidade 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*.
- ☐ A quebra do protocolo é fácil.
- ☐ 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:

- ☒ 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:

- ☒ Multiplicação é fácil e factorização é difícil.
- ☐ Exponenciação em  $\mathbb{F}_p^*$  é fácil e factorização é difícil.
- ☐ Exponenciação em  $\mathbb{F}_p^*$  é fácil e o *Discrete Logarithm Problem* é difícil.
- ☒ Multiplicação é fácil e divisão é difícil.

**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 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 operação de "adição" é mais fácil sobre curvas elípticas do que em  $\mathbb{F}_p^*$ .



Departamento de Matemática  
Criptografia

Faculdade de Ciências e Tecnologia — UNL  
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	5
6	6	6	6	6
7	7	7	7	7
8	8	8	8	8
9	9	9	9	9

← 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.

Nome: Hugo Mochão

Curso: MIEI Número de aluno: 47231

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 grupo  $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multiplicação tal que  $\mathbb{F}_n$  é um corpo se, e só se:

- ☐  $n$  é um número primo ímpar. ☒  $n$  é uma potência de um número primo.
- ☐  $n$  é um número primo. ☐  $n$  é um número par.

**Questão 2** 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.
- ☐ só do segredo do algoritmo, mas não do segredo da chave.
- ☒ do segredo da chave e do segredo do algoritmo.

**Questão 3** Qual destes protocolos criptográficos é *assimétrico*?

- ☒ ElGamal ☐ Vigenère
- ☒ AES ☐ DES

**Questão 4**

O *Discrete Logarithm Problem (DLP)* para a congruência  $g^x \equiv h \pmod{p}$  é:

- ☐ Determine  $h$ , dados  $g$ ,  $p$  e  $x$ . ☐ Determine  $p$ , dados  $g$ ,  $h$  e  $x$ .
- ☒ Determine  $x$ , dados  $g$ ,  $h$  e  $p$ . ☐ Determine  $g$ , dados  $h$ ,  $p$  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.

- ☐  $A$  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  $g^a \pmod{p}$ ,  $B$  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  $(ab)^g \pmod{p}$ .

**Questão 6** 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:

- ☒  $(c_1^a) \cdot (c_2)^{-1} \pmod{p}$  ☐  $c_1 \cdot (c_2^a)^{-1} \pmod{p}$
- ☐  $(c_1)^{-1} \cdot (c_2)^a \pmod{p}$  ☒  $(c_1^a)^{-1} \cdot c_2 \pmod{p}$

**Questão 7** O algoritmo de Miller-Rabin devolve um número primo com probabilidade 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.
- ☐ Dois *ciphertexts* 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 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:

- ☐ Multiplicação é fácil e divisão é difícil.
- ☒ Multiplicação é fácil e factorização é difícil.
- ☐ Exponenciação em  $\mathbb{F}_p^*$  é fácil e o *Discrete Logarithm Problem* é difícil.
- ☒ Exponenciação em  $\mathbb{F}_p^*$  é fácil e factorização é difícil.

**Questão 10** Curvas elípticas são importantes em criptografia, porque (empiricamente):

- ☒ 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  $\mathbb{F}_p^*$ .
- ☐ A operação de "adição" é mais complicada sobre curvas elípticas do que em  $\mathbb{F}_p^*$ .
- ☒ A solução do *DLP* é mais complicada sobre curvas elípticas do que em  $\mathbb{F}_p^*$ .





Departamento de Matemática  
Criptografia

Faculdade de Ciências e Tecnologia — UNL  
8/7/2018 Exame Final

Número de aluno

0	0	0	0	0
1	<input checked="" type="checkbox"/>	1	1	1
2	2	2	2	2
3	3	3	3	3
<input checked="" type="checkbox"/>	4	4	<input checked="" type="checkbox"/>	4
5	5	5	5	<input checked="" type="checkbox"/>
6	6	6	6	6
7	7	<input checked="" type="checkbox"/>	7	7
8	8	8	8	8
9	9	9	9	9

← 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.

Nome: Hélio Torres Aguiar
Curso: MIEI
Número de aluno: 41745

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 grupo  $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multiplicação tal que  $\mathbb{F}_n$  é um corpo se, e só se:

- ☒  $n$  é uma potência de um número primo. ☒  $n$  é um número primo.  
☐  $n$  é um número par. ☐  $n$  é um número primo ímpar.

**Questão 2** 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.  
☐ do segredo da chave e do segredo do algoritmo.  
☐ só do segredo do algoritmo, mas não do segredo da chave.

**Questão 3** Qual destes protocolos criptográficos é *assimétrico*?

- ☐ DES ☐ AES  
☐ Vigenère ☒ ElGamal

**Questão 4**

O *Discrete Logarithm Problem (DLP)* para a congruência  $g^x \equiv h \pmod{p}$  é:

- ☐ Determine  $p$ , dados  $g$ ,  $h$  e  $x$ . ☒ Determine  $g$ , dados  $h$ ,  $p$  e  $x$ .  
☐ 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.

- ☐  $A$  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  $g^{ab} \pmod{p}$ .
- ☐  $A$  é calculado por  $a^g \pmod{p}$ ,  $B$  por  $b^g \pmod{p}$  e a chave comum secreta é  $(ab)^g \pmod{p}$ .

**Questão 6** 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:

- ☒  $(c_1^a)^{-1} \cdot c_2 \pmod{p}$  ☐  $c_1 \cdot (c_2^a)^{-1} \pmod{p}$
- ☒  $(c_1)^{-1} \cdot (c_2)^a \pmod{p}$  ☐  $(c_1^a) \cdot (c_2)^{-1} \pmod{p}$

**Questão 7** O algoritmo de Miller-Rabin devolve um número primo com probabilidade 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.
- ☐ 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:

- ☐ 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:

- ☒ Exponenciação em  $\mathbb{F}_p^*$  é fácil e factorização é difícil.
- ☐ Multiplicação é fácil e divisão é difícil.
- ☒ Multiplicação é fácil e factorização 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):

- ☐ 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 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  $\mathbb{F}_p^*$ .