



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: João de Sousa Falcão Henriques
Curso: MIEI
Número de aluno: 42650

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 primo ímpar. ☐ 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 chave, mas não do segredo do algoritmo.
☐ só da complexidade da encriptação.
☐ 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*?

- ☐ AES ☐ DES
☒ ElGamal ☐ Vigenère

Questão 4

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

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

Certa



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 $a^g \pmod{p}$, 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 *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:

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

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^* :

- ☒ 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.

Questão 8 Um protocolo criptográfico tem a propriedade de *total secrecy*, se, e só se:

- ☐ 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.
- ☐ 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:

- ☒ Exponenciação em \mathbb{F}_p^* é fácil e o *Discrete Logarithm Problem* é difícil.
- ☒ Multiplicação é fácil e factorização é difícil.
- ☐ Exponenciação em \mathbb{F}_p^* é fácil e factorização é difícil.
- ☐ Multiplicação é fácil e divisão 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 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 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: Luis Duarte Martins Bastos de Oliveira

Curso: MIEI Número de aluno: 41894

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 primo ímpar. ☐ 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*:

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

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

- ☒ ElGamal ☐ AES
☐ DES ☐ Vigenère

Questão 4

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

- ☒ Determine x , dados g , h e p . ☐ Determine p , dados g , h e x .
☒ Determine g , dados h , p e x . ☐ 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 $A \cdot B$.
- ☐ 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:

- | | |
|--|---|
| <input type="checkbox"/> $c_1 \cdot (c_2^a)^{-1} \pmod{p}$ | <input type="checkbox"/> $(c_1^a) \cdot (c_2)^{-1} \pmod{p}$ |
| <input type="checkbox"/> $(c_1)^{-1} \cdot (c_2)^a \pmod{p}$ | <input checked="" type="checkbox"/> $(c_1^a)^{-1} \cdot c_2 \pmod{p}$ |

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.
- ☐ A encriptação torna-se lenta.
- ☒ Duas mensagens podem ser codificadas pelo mesmo *ciphertext*.

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*.
- ☒ 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:

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

- ☒ 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^* .
- ☐ 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: Manuel António de Melo
Chinopa de Sousa Ribeiro
Curso: M.I.E.I. Número de aluno: 47257

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 do segredo do algorithmo, mas não do segredo da chave. ☒ só da chave, mas não do segredo do algoritmo. ☐ do segredo da chave e do segredo do algoritmo.

Questão 3 Qual destes protocolos criptográficos é assimétrico?

- ☐ Vigenère ☐ AES ☒ ElGamal ☐ 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 g , dados h , p e x . ☐ Determine p , dados g , h 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 $a^g \pmod{p}$, 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 $g^{ab} \pmod{p}$.

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:

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

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 encriptação torna-se lenta.
- ☒ A quebra do protocolo é fácil.
- ☐ Dois *ciphertexts* podem encriptar a mesma mensagem.
- ☒ Duas mensagens podem ser codificadas pelo mesmo *ciphertext*.

Questão 8 Um protocolo criptográfico tem a propriedade de *total secrecy*, se, e só se:

- ☐ 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. ✓
- ☐ 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:

- ☒ 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 factorização é difícil. ✓
- ☐ Multiplicação é fácil e divisão 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^* . ✓
- ☒ 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^* . ✓



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	<input checked="" type="checkbox"/>	3	3
<input checked="" type="checkbox"/>	4	4	4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>	5	5	5
6	6	6	6	6
7	7	7	7	7
8	8	8	<input checked="" type="checkbox"/>	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:	Manuel Maria Silva Barbas			
Curso:	MIEI	Número de aluno:	45384	

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 ímpar.
☐ 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*:

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

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

- ☐ Vigenère ☐ AES
☐ DES ☒ ElGamal

Questão 4

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

- ☒ 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 $a^g \pmod{p}$, 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 *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^* :

- ☒ 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:

- ☐ O protocolo pode ser quebrado em tempo polinomial.
☐ O protocolo pode ser quebrado em tempo exponencial.
☒ 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:

- ☐ 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.
☒ Multiplicação é fácil e factorização 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^* .



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: ... Marcelo Filipe Cantinho ...
... Ramos ...
Curso: ... MIEI ... Número de aluno: ... 43099 ...

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 sc, e só se:

- ☐ n é um número primo. ☐ n é um número par.
☐ n é um número primo ímpar. ☒ n é uma potência de 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 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.
☐ só da complexidade da encriptação.

Questão 3 Qual destes protocolos criptográficos é assimétrico?

- ☒ ElGamal ☒ AES
☐ DES ☐ Vigenère

Questão 4

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

- ☐ Determine g , dados h , p e x . ☐ Determine p , dados g , h 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:

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

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^* :

- ☐ A encriptação torna-se lenta.
- ☐ A quebra do protocolo é fácil.
- ☐ Dois *ciphertexts* podem encriptar a mesma mensagem.
- ☒ 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*.
- ☐ O protocolo pode ser quebrado em tempo polinomial.
- ☐ 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:

- ☒ 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 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^* .
- ☐ 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^* .