José Francisco Ribeiro - 49546 - MIEI
Mark: 1.2/5 (total score: 1.2/5)

+20/1/22+

Departamento de Matemática **Faculdade de Ciências e Tecnologia — UNL**
Criptografia **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
5	5	■	5	5
6	6	6	6	■
7	7	7	7	7
8	8	8	8	8
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: José Francisco Ribeiro

Curso: MIEI Número de aluno: 49546

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:

0/0.5

- ☐ n é um número primo.
- ☐ n é um número primo ímpar.
- ☐ n é um número par.
- ☒ 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*:

0.5/0.5

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

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

0.5/0.5

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

Questão 4

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

0.5/0.5

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

-0.2/0.5

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 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 $g^{ab} \pmod p$.
- [x] A é calculado por $g^a \pmod p$, B por $g^b \pmod p$ e a chave comum secreta é $A \cdot B$.
- [x] A é calculado por $g^a \pmod p$, B por $g^b \pmod p$ e a chave comum secreta é $g^{ab} \pmod p$.

0/0.5

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:

- [x] $(c_1^a)^{-1} \cdot c_2 \pmod p$
- [ ] $(c_1)^{-1} \cdot (c_2)^a \pmod p$
- [ ] $c_1 \cdot (c_2^a)^{-1} \pmod p$
- [ ] $(c_1^a) \cdot (c_2)^{-1} \pmod p$

-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 $\mathbb{F}_p^*$:

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

-0.2/0.5

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

- [x] O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais *ciphertexts*.
- [ ] O protocolo pode ser quebrado em tempo polinomial.
- [x] A probabilidade de um *plaintext* é independente do *ciphertext*.
- [ ] O protocolo pode ser quebrado em tempo exponencial.

0.5/0.5

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

- [ ] Exponenciação em $\mathbb{F}_p^*$ é fácil e o *Discrete Logarithm Problem* é difícil.
- [ ] Mulitplicação é fácil e divisão é difícil.
- [x] Mulitplicação é fácil e factorização é difícil.
- [ ] Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.

-0.2/0.5

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

- [x] 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 $\mathbb{F}_p^*$.
- [x] A solução do *DLP* é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$.

João André Furtado Teixeira - 48047 - MIEI
Mark: 0/5 (total score: -0.2/5)

Departamento de Matemática **Faculdade de Ciências e Tecnologia — UNL**
Criptografia **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 André Furtado Teixeira

Curso: MIEI Número de aluno: 48047

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 uma potência de um número primo.
- [x] 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*:

-0.2/0.5

- [ ] só do segredo do algorithmo, mas não do segredo da chave.
- [ ] só da complexidade da encriptação.
- [x] do segredo da chave e do segredo do algoritmo.
- [ ] só da chave, mas não do segredo do algoritmo.

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

-0.2/~~0.5~~
certo

- [ ] Vigenère
- [ ] ElGamal
- [x] DES
- [x] AES

Questão 4

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

0.5/0.5

- [ ] Determine g, dados h, p e x.
- [ ] Determine h, dados g, p e x.
- [ ] Determine p, dados g, h e x.
- [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.

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 $g^{ab} \pmod p$.
- [x] 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:

-0.2/0.5

- [x] $(c_1^a) \cdot (c_2)^{-1} \pmod p$
- [ ] $(c_1^a)^{-1} \cdot c_2 \pmod p$
- [ ] $(c_1)^{-1} \cdot (c_2)^a \pmod p$
- [ ] $c_1 \cdot (c_2^a)^{-1} \pmod p$

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*.
- [x] 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:

0/0.5

- [ ] 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.
- [ ] 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:

0/0.5

- [ ] Exponenciação em $\mathbb{F}_p^*$ é fácil e o *Discrete Logarithm Problem* é difícil.
- [ ] Mulitplicação é fácil e divisão é difícil.
- [ ] Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
- [ ] Mulitplicação é fácil e factorização 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 $\mathbb{F}_p^*$.
- [ ] 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 $\mathbb{F}_p^*$.
- [x] A operação de "adição" é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$.

João Carlos Cristo Reis - 43914 - MIEI
Mark: 1.7/5 (total score: 1.7/5)

+22/1/18+

Departamento de Matemática — Faculdade de Ciências e Tecnologia — UNL
Criptografia — 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 Carlos Cristo Reis

Curso: MIEI Número de aluno: 43914

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 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*:

0.5/0.5

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

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

0.5/0.5

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

Questão 4

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

0.5/0.5

- ☐ 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.

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 $g^{ab} \pmod p$.
- [x] 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:

-0.2/0.5

- [x] $(c_1^a)^{-1} \cdot c_2 \pmod p$
- [ ] $c_1 \cdot (c_2^a)^{-1} \pmod p$
- [x] $(c_1)^{-1} \cdot (c_2)^a \pmod p$
- [ ] $(c_1^a) \cdot (c_2)^{-1} \pmod p$

Questão 7 O algoritmo de Miller-Rabin devolve um número primo com 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 encriptação torna-se lenta.
- [x] Duas mensagens podem ser codificadas pelo mesmo *ciphertext*.
- [ ] A quebra do protocolo é fácil.
- [x] Dois *ciphertexts* podem encriptar a mesma mensagem.

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

0.5/0.5

- [ ] O protocolo pode ser quebrado em tempo exponencial.
- [x] 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 polinomial.

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

-0.2/0.5

- [ ] Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
- [x] Mulitplicação é fácil e factorização é difícil.
- [ ] Mulitplicação é fácil e divisão é difícil.
- [x] Exponenciação em $\mathbb{F}_p^*$ é fácil e o *Discrete Logarithm Problem* é difícil.

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

0/0.5

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

João Daniel da Luz Mota - 47598 - MIEI
Mark: 2.4/5 (total score: 2.4/5)

+35/1/52+

Departamento de Matemática **Faculdade de Ciências e Tecnologia — UNL**
Criptografia **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 número e o curso abaixo.

Nome: João Daniel Mota

Curso: MIEI Número de aluno: 47598

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 uma potência de um número primo.
- ☐ n é um número par.
- ☐ n é um número primo ímpar.
- ■ 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*:

0.5/0.5

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

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

0/0.5

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

Questão 4

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

0.5/0.5

- ☐ 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.

0.5/0.5

- [x] 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:

0.5/0.5

- [ ] $(c_1^a) \cdot (c_2)^{-1} \pmod p$
- [ ] $c_1 \cdot (c_2^a)^{-1} \pmod p$
- [ ] $(c_1)^{-1} \cdot (c_2)^a \pmod p$
- [x] $(c_1^a)^{-1} \cdot c_2 \pmod p$

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.
- [x] 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:

0.5/0.5

- [ ] O protocolo pode ser quebrado em tempo polinomial.
- [x] 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:

-0.2/0.5

- [ ] Exponenciação em $\mathbb{F}_p^*$ é fácil e o *Discrete Logarithm Problem* é difícil.
- [x] Mulitplicação é fácil e factorização é difícil.
- [ ] Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
- [ ] Mulitplicação é fácil e divisão é difícil.

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

0.5/0.5

- [ ] 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 $\mathbb{F}_p^*$.
- [x] 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 $\mathbb{F}_p^*$.

João Manuel Calixto Figueira - 41734 - MIEI
Mark: 2.2/5 (total score: 2.2/5)

+85/1/12+

Departamento de Matemática **Faculdade de Ciências e Tecnologia — UNL**
Criptografia **8/7/2018** **Exame Final**

Número de aluno

0	0	0	0	0
1	■	1	1	1
2	2	2	2	2
3	3	3	■	3
■	4	4	4	■
5	5	5	5	5
6	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: João Manuel Calixto Figueira

Curso: MIEI Número de aluno: 41734

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 uma potência de um número primo.
- [x] 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*:

0.5/0.5

- [ ] só da complexidade da encriptação.
- [ ] só do segredo do algorithmo, mas não do segredo da chave.
- [x] 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*?

0.5/0.5

- [ ] AES
- [x] ElGamal
- [ ] Vigenère
- [ ] DES

Questão 4

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

0.5/0.5

- [ ] Determine p, dados g, h e x.
- [ ] Determine g, dados h, p e x.
- [x] Determine x, dados g, h e p.
- [ ] Determine h, dados g, p e x.

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.

- [x] 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 $g^{ab} \pmod p$.
- [ ] A é calculado por $g^a \pmod p$, B por $g^b \pmod p$ e a chave comum secreta é $A \cdot B$.

-0.2/0.5

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:

- [x] $(c_1^a)^{-1} \cdot c_2 \pmod p$
- [ ] $c_1 \cdot (c_2^a)^{-1} \pmod p$
- [ ] $(c_1)^{-1} \cdot (c_2)^a \pmod p$
- [ ] $(c_1^a) \cdot (c_2)^{-1} \pmod p$

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 $\mathbb{F}_p^*$:

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

-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 exponencial.
- [ ] O protocolo pode ser quebrado em tempo polinomial.
- [ ] O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais *ciphertexts*.
- [x] A probabilidade de um *plaintext* é independente do *ciphertext*.

-0.2/0.5

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

- [ ] Exponenciação em $\mathbb{F}_p^*$ é fácil e o *Discrete Logarithm Problem* é difícil.
- [x] Mulitplicação é fácil e factorização é difícil.
- [ ] Mulitplicação é fácil e divisão é difícil.
- [ ] Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.

0.5/0.5

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 $\mathbb{F}_p^*$.
- [x] A solução do *DLP* é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$.