João Miguel Luís Santos - 42958 - MIEI
Mark: 1.3/5 (total score: 1.3/5)

+32/1/58+

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
3	3	3	3	3
■	4	4	4	4
5	5	5	■	5
6	6	6	6	6
7	7	7	7	7
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: João Miguel Santos

Curso: MIEI — Número de aluno: 42958

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

0.5/0.5

- ☐ só do segredo do algorithmo, mas não do segredo da chave.
- ☐ só da complexidade da encriptação.
- ☐ 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*?

0.5/0.5

- ■ ElGamal
- ☐ Vigenère
- ☐ DES
- ☐ 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 x, dados g, h e p.
- ☐ Determine p, dados g, h 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.

0/0.5

- ☐ 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 $g^a \pmod p$, 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 $g^{ab} \pmod p$.

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:

0/0.5

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

Questão 7 O algoritmo de Miller-Rabin devolve um número primo com 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 $\mathbb{F}_p^*$:

0/0.5

- ☒ 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:

0/0.5

- ☐ 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:

0/0.5

- ☒ 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.
- ☐ 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 $\mathbb{F}_p^*$.
- ☐ 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 $\mathbb{F}_p^*$.

João Miguel Peres Palma Neves - 45615 - MIEI
Mark: 2.3/5 (total score: 2.3/5)

+33/1/56+

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 Miguel Peres Palma Neves

Curso: MIEI Número de aluno: 45615

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 par.
- ☐ n é um número primo ímpar.
- ■ n é um número primo.
- ☒ 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

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

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

0.5/0.5

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

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

g^k mA^k
$m g^{ak}$
$(g^{ka})^{-1}$ $m g^{ka}$
$(g^k)^{-1} \cdot (mA^k$
g^{a^2}

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

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

Questão 7 O algoritmo de Miller-Rabin devolve um número primo com 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 $\mathbb{F}_p^*$:

0/0.5

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

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

0/0.5

- [ ] 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*.

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

0/0.5

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

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

0/0.5

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

João Pedro Monteiro Morgado Dias - 42205 - MIEI
Mark: 3.8/5 (total score: 3.8/5)

+45/1/32+

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 Pedro Dias

Curso: MIEI Número de aluno: 42205

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

- ☐ 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*:

0.5/0.5

- ☐ 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 algorithmo, mas não do segredo da chave.

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

0.5/0.5

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

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

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

0.5/0.5

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:

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

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 $\mathbb{F}_p^*$:

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

0.5/0.5

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

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

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

-0.2/0.5

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

João Pedro Silva Borralho - 45456 - MIEI
Mark: 2.1/5 (total score: 2.1/5)

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
5	■	5	■	5
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 Borralho

Curso: MIEI Número de aluno: 45456

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 par.
- [x] n é uma potência de um número primo.
- [ ] 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

- [ ] 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.
- [ ] só da complexidade da encriptação.

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

0.5/0.5

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

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

- [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 $g^{ab} \pmod p$.
- [ ] 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 $A \cdot B$.

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

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

Questão 7 O algoritmo de Miller-Rabin devolve um número primo com 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 $\mathbb{F}_p^*$:

0/0.5

- [ ] A encriptação torna-se lenta.
- [ ] Dois *ciphertexts* podem encriptar a mesma mensagem.
- [x] 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:

0/0.5

- [ ] 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.
- [x] A probabilidade de um *plaintext* é independente do *ciphertext*.

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.
- [ ] 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

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

João Ricardo Alpoim Gonçalves - 44929 - MIEI
Mark: 2.2/5 (total score: 2.2/5)

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 Ricardo Alpoim Gonçalves

Curso: MIEI Número de aluno: 44929

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

- [x] 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*:

0.5/0.5

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

Questão 3 Qual destes protocolos criptográficos é *assimétrico*?

0.5/0.5

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

Questão 4

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

0.5/0.5

- [x] 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.

0.5/0.5

- ☒ 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 $(ab)^g \pmod p$.
- ☐ 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 *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

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

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

- ☐ A encriptação torna-se lenta.
- ☐ Dois *ciphertexts* podem encriptar a mesma mensagem.
- ■ 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:

-0.2/0.5

- ■ 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:

0.5/0.5

- ☒ Mulitplicação é fácil e factorização é difícil.
- ☐ 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.

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

-0.2/0.5

- ■ 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 $\mathbb{F}_p^*$.