Pedro Gonçalves Cabaço - 45409 - MIEI Mark: 2.1/5 (total score: 2.1/5)

		+31/1/60+
	Departamento de Matemát Criptografia	cica Faculdade de Ciências e Tecnologia — UNI 8/7/2018 Exame Final
	Número de aluno  0 0 0 0 0  1 1 1 1 1  2 2 2 2 2 2	← 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.
	3 3 3 3 3 3 3 4 4 4 5 5 5 5 5 5 6 6 6 6 6 6	Nome: Radra Caba & 0  Curso: MIEI Número de aluno: 55509
	77777	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 gr se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
0.5/0.5	n é um número primo. $n$ é um número primo í	mpar. $n$ é um número par. $n$ é uma potência de um número primo.
		le Kerekhoff são princípios que todos os sistemas criptográficos devem erckhoff fundamental diz que a segurança de um sistema criptográfico
0.5/0.5	só da chave, mas não do só do segredo do algorit do segredo da chave e d só da complexidade da	chmo, mas não do segredo da chave. o segredo do algoritmo.
	Questão 3 Qual destes pr	rotocolos criptográficos é assimétrico?
0.5/0.5	☐ AES  ElGamal	☐ DES ☐ Vigenère
	Questão 4 O Discrete Logarithm Pro	$blem\;(DLP)$ para a congruência $g^x\equiv h\;(\mathrm{mod}p)\;$ é:
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.
0/0.5	
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para enviar um <i>ciphertext</i> $(c_1, c_2)$ com $c_1 \equiv g^k \pmod{p}$ e $c_2 \equiv mA^k \pmod{p}$ ; $k$ uma chave <i>ephemeral</i> . Para recuperar a mensagem $m$ , Alice calcula:
0/0.5	
	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 $\mathbb{F}_p^*$ :
0.5/0.5	<ul> <li>Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>A encriptação torna-se lenta.</li> <li>Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>A quebra do protocolo é fácil.</li> </ul>
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, e só se:
-0.2/0.5	<ul> <li>✓ A probabilidade de um plaintext é independente do ciphertext.</li> <li>☐ O protocolo pode ser quebrado em tempo polinomial.</li> <li>☐ O conjunto das chaves possíveis tem a mesma cardinalidade que o conjunto dos potenciais ciphertexte.</li> </ul>
	ciphertexts.  © O protocolo pode ser quebrado em tempo exponencial.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
-0.2/0.5	$oldsymbol{\cdot}$ Exponenciação em $\mathbb{F}_p^{\bullet}$ é fácil e factorização é difícil.
	Exponenciação em $\mathbb{F}_p^*$ é fácil e o Discrete Logarithm Problem é difícil.
	<ul> <li>✓ Mulitplicação é fácil e divisão é difícil.</li> <li>✓ Mulitplicação é fácil e factorização é difícil.</li> </ul>
	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 exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\boxtimes$ A solução do $DLP$ é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	A operação de "adição" é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

Pedro Miguel Estrela de Moura - 47435 - MIEI Mark: 2.4/5 (total score: 2.4/5)

+71/1/4	10+
Departamento de Matemática Faculdade de Ciências e S/7/2018	e Tecnologia — UNL Exame Final
Número de aluno   Marque o seu número de aluno preenchendo drados respectivos da grelha ao lado ( ) e escrenúmero e o curso abaixo.	
2 2 2 2 2 Nome: Pade Myul Est.	
4 4 4 4 5 5 5 5 6 Curso:	
O exame é composto por 10 questões de escolha marque a resposta certa preenchendo completame tivo ( ) com caneta azul ou preta, cada respost cada resposta errada desconta 0,2 valores e marca questão. Se a soma das classificações das questões um número negativo, será atribuído 0 valores com	ente o quadrado respec- a certa vale 0,5 valores, ções múltiplas anulam a de escolha múltipla der
Questão 1 Considere o grupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multiplicação se, e só se:	tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5 $n$ é um número primo. $n$ é um número primo $n$ é um número primo $n$ é um número par. $n$ é um potência do	
Questão 2 Os princípios de Kerckhoff são princípios que todos os sistema satisfazer. Um princípio de Kerckhoff fundamental diz que a segurança de un deve depender:	
só da complexidade da encriptação.  do segredo da chave e do segredo do algoritmo.  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	
$egin{aligned} \mathbf{Quest\~ao} & 4 \ & \mathbf{O} & Discrete & Logarithm & Problem & (DLP) \  ext{para a congru\'encia} & g^x \equiv h \  ext{(mod } p) \end{aligned}$	o) é:
-0.2/0.5 Determine $h$ , dados $g$ , $p \in x$ . Determine $x$ , dados $p$ . Determine $p$ , dados $p$ . Determine $p$ , dados $p$ .	-

	<b>Questão 5</b> 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	
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para enviar um <i>ciphertext</i> $(c_1, c_2)$ com $c_1 \equiv g^k \pmod{p}$ e $c_2 \equiv mA^k \pmod{p}$ ; $k$ uma chave <i>ephemeral</i> . Para recuperar a mensagem $m$ , Alice calcula:
0.5/0.5	
	Questão 7 — O algoritmo de Miller-Rabin devolve um número primo com probablidade elevada. No caso improvável do número devolvido $p$ não ser primo, o que pode acontecer no protocolo criptográfico de $ElGamal$ que usa este número para a escolha de $\mathbb{F}_p^{\bullet}$ :
0.5/0.5	<ul> <li>☐ A quebra do protocolo é fácil.</li> <li>☐ Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>☐ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>☐ A encriptação torna-se lenta.</li> </ul>
	Questão 8 Um protocolo criptográfico tem a propriedade de total secrecy, se, c só se:
0.5/0.5	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	<ul> <li>Exponenciação em F<sub>p</sub><sup>*</sup> é fácil e o Discrete Logarithm Problem é difícil.</li> <li>Exponenciação em F<sub>p</sub><sup>*</sup> é fácil e factorização é difícil.</li> <li>Mulitplicação é fácil e factorização é difícil.</li> <li>Mulitplicação é fácil e divisão é difícil.</li> </ul>
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
	$\boxtimes$ A solução do $DLP$ é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
-0.2/0.5	$\blacksquare$ 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 $\mathbb{F}_p^*$ .

Pedro Miguel Gonçalves Rocha - 45323 - MIEI Mark: 0.7/5 (total score: 0.7/5)

		+93/1/56+
	Departamento de Matemás Criptografia	tica Faculdade de Ciências e Tecnologia — UNI 8/7/2018 Exame Final
	Número de aluno  0 0 0 0 0  1 1 1 1 1 1	← 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.
	2 2 2 2 2 3 3 3 3 3	Nome: Redro. Higual Gongolius Rocho
	5 5 5 5 6 6 6 6 6 7 7 7 7 7	Curso: . MIEI Número de aluno: . 45.3ム.ネ
	8 8 8 8 8 9 9 9 9	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 g se, e só se:	rupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se definir uma multiplicação tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5	otin n é uma potência de un $ otin n$ é um número primo s	
		de Kerckhoff são princípios que todos os sistemas criptográficos devem erckhoff fundamental diz que a segurança de um sistema criptográfico
0.5/0.5	só da chave, mas não d	lo segredo do algoritmo.
	Questão 3 Qual destes p	rotocolos criptográficos é assimétrico?
-0.2/0.5	☐ Vigenère  AES	DES ElGamal
	Questão 4 O Discrete Logarithm Pro	$ablem\;(DLP)\;{ m para\;a\;congru\hat{e}ncia\;}g^{f r}\equiv h\;({ m mod}p)\;{ m \acute{e}};$
-0.2/0.5	Determine $x$ , dados $g$ , $h$ Determine $p$ , dados $g$ , $h$	V V

	<b>Questão 5</b> 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	
	Questão 6 No protocolo <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para enviar um <i>ciphertext</i> $(c_1, c_2)$ com $c_1 \equiv g^k \pmod{p}$ e $c_2 \equiv mA^k \pmod{p}$ ; $k$ uma chave <i>ephemeral</i> . Para recuperar a mensagem $m$ , Alice calcula:
0/0.5	
	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 $\mathbb{F}_p^*$ :
0.5/0.5	<ul> <li>A encriptação torna-se lenta.</li> <li>□ A quebra do protocolo é fácil.</li> <li>☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> </ul>
	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.  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:
0/0.5	<ul> <li>Exponenciação em F<sub>p</sub><sup>*</sup> é fácil e o Discrete Logarithm Problem é difícil.</li> <li>Exponenciação em F<sub>p</sub><sup>*</sup> é fácil e factorização é difícil.</li> <li>Mulitplicação é fácil e factorização é difícil.</li> <li>Mulitplicação é fácil e divisão é difícil.</li> </ul>
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0.2/0.5	<ul> <li>A exponenciação é mais rápida sobre curvas elípticas do que em F<sub>p</sub>*.</li> <li>A operação de "adição" é mais complicada sobre curvas elípticas do que em F<sub>p</sub>*.</li> <li>A operação de "adição" é mais fácil sobre curvas elípticas do que em F<sub>p</sub>*.</li> </ul>
	$\boxtimes$ A solução do $DLP$ é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

Pedro Miguel Laforêt Barroso - 45578 - MIEI Mark: 2.2/5 (total score: 2.2/5)

			+34/1/54+
	Departamento de Matema Criptografia	ática 8/7/20	Faculdade de Ciências e Tecnologia — UNI 018 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  5 5 5 5  6 6 6 6 6  7 7 7 7 7 7  8 8 8 8 8  9 9 9 9 9	Nome: Padvo 3  Curso: H151  O exame é composto p marque a resposta cert tivo () com caneta a cada resposta errada de questão. Se a soma das	
-0.2/0.5	Questão 1 Considere o $n$ se, e só se: $n$ é um número primo $n$ é um número	grupo $\mathbb{Z}/n\mathbb{Z}$ . Pode-se de	lefinir uma multiplicação tal que $\mathbb{F}_n$ é um corpo $\boxtimes n$ é uma potência de um número primo.
(orto 0.5/0.5	satisfazer. Um princípio de la deve depender:  Só da chave, mas não de do segredo da chave e só da complexidade da	Kerckhoff fundamental o do segredo do algoritmo do segredo do algoritmo	no.
0.5/0.5		orotocolos criptográficos	
0.5/0.5	•	<i>p</i> e <i>x</i> .	ongruência $g^x \equiv h \pmod{p}$ é:  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.
	$\bigcap$ A é calculado por $a^g \pmod{p}$ , B por $b^g \pmod{p}$ e a chave comum secreta é $(ab)^g \pmod{p}$ .
0.5/0.5	$A$ é calculado por $g^a \pmod{p}$ , $B$ por $g^b \pmod{p}$ e a chave comum secreta é $A \cdot B$ .
0.0/0.0	$A$ é calculado por $g^a \pmod{p}$ , $B$ por $g^b \pmod{p}$ e a chave comum secreta é $g^{ab} \pmod{p}$ . $\vee$
	$\square$ 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 <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para enviar um <i>ciphertext</i> $(c_1, c_2)$ com $c_1 \equiv g^k \pmod{p}$ e $c_2 \equiv mA^k \pmod{p}$ ; $k$ uma chave <i>ephemeral</i> . Para recuperar a mensagem $m$ , Alice calcula:
	92=
-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 $\mathbb{F}_p^{\bullet}$ :
	A quebra do protocolo é fácil.
	A encriptação torna-se lenta.
-0.2/0.5	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.
0.5/0.5	ciphertexts.  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.
0.5/0.5	A probabilidade de um plaintext é independente do ciphertext.
	O protocolo pode ser quebrado em tempo exponencial.
	Questão 9 O funcionamento do RSA é baseado no seguinte:
	Mulitplicação é fácil e factorização é difícil. ×
0.0/0.5	Exponenciação em $\mathbb{F}_p^*$ é fácil e o Discrete Logarithm Problem é difícil.
-0.2/0.5	■ Mulitplicação é fácil e divisão é difícil.×
	$\square$ Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0.5/0.5	$\blacksquare$ A solução do $DLP$ é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ . $\checkmark$
	A exponenciação é mais rápida sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\square$ A operação de "adição" é mais fácil sobre curvas elípticas do que em $\mathbb{F}_p^*$ .
	$\square$ A operação de "adição" é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .

Rafael Santos Cruz - 48257 - MIEI Mark: 0.8/5 (total score: 0.8/5)

			+64	s/1/54+
	Departamento de Matemá Criptografia	tica 8/7/2		cias e Tecnologia — UNL Exame Final
	Número de aluno 0 0 0 0 0 1 1 1 1 1		grelha ao lado (🔳) e	endo completamente os qua- escreva o nome completo, o
	2 2 2 2 2 3 3 3 3 3 3 4 4 4 4 4 5 5 5 5 5 5 5 5 5		Santos Cru	
	6 6 6 6 6 7 7 7 7 7 8 8 8 8 8 9 9 9 9 9	O exame é composto marque a resposta certivo ( ) com caneta cada resposta errada o questão. Se a soma de	por 10 questões de esc rta preenchendo comple azul ou preta, cada re lesconta 0,2 valores e m	aluno: 4825 †  colha múltipla. Nas questões etamente o quadrado respecsposta certa vale 0,5 valores, narcações múltiplas anulam a stões de escolha múltipla der como resultado final.
	Questão 1 Considere o g se, e só se:			ıção tal que $\mathbb{F}_n$ é um corpo
-0.2/0.5	$ \bigcirc $ $n$ é um número par. $ \bigcirc $ $n$ é uma potência de un	m número primo.	n é um número $n$ é um número	-
	Questão 2 Os princípios o satisfazer. Um princípio de K deve depender:			temas criptográficos devem de um sistema criptográfico
0.5/0.5	só da complexidade da só da chave, mas não d do segredo da chave e d só do segredo do algoria	o segredo do algoritn lo segredo do algorita	no.	
	Questão 3 Qual destes p	rotocolos criptográfic	os é assimétrico?	
0.5/0.5	<ul><li>AES</li><li>Vigenère</li></ul>	(210)	ElGamal  DES	
	Questão 4 O Discrete Logarithm Pro	oblem (DLP) para a c	congruência $g^x \equiv h$ (n	nod <i>p</i> ) é:
-0.2/0.5			Determine $h$ , da	

	<b>Questão 5</b> 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 $A \cdot B$ . ☐ $A$ 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 <i>ElGamal</i> , Bob usa a chave pública da Alice $A \equiv g^a \pmod{p}$ para enviar um <i>ciphertext</i> $(c_1, c_2)$ com $c_1 \equiv g^k \pmod{p}$ e $c_2 \equiv mA^k \pmod{p}$ ; $k$ uma chave <i>ephemeral</i> . Para recuperar a mensagem $m$ , Alice calcula:
0.2/0.5	
	Questão 7 — O algoritmo de Miller-Rabin devolve um número primo com probablidade elevada. No caso improvável do número devolvido $p$ não ser primo, o que pode acontecer no protocolo criptográfico de $ElGamal$ que usa este número para a escolha de $\mathbb{F}_p^*$ :
0.2/0.5	<ul> <li>☐ A encriptação torna-se lenta.</li> <li>☑ Duas mensagens podem ser codificadas pelo mesmo ciphertext.</li> <li>☐ Dois ciphertexts podem encriptar a mesma mensagem.</li> <li>☐ A quebra do protocolo é fácil.</li> </ul>
	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.
0.2/0.5	<ul> <li>□ O protocolo pode ser quebrado em tempo polinomial.</li> <li>□ O protocolo pode ser quebrado em tempo exponencial.</li> <li>□ A probabilidade de um plaintext é independente do ciphertext.</li> </ul>
	Questão 9 O funcionamento do RSA é baseado no seguinte:
	Mulitplicação é fácil e factorização é difícil.
0.2/0.5	<ul> <li>Exponenciação em F<sub>p</sub> é fácil e o Discrete Logarithm Problem é difícil.</li> <li>Mulitplicação é fácil e divisão é difícil.</li> </ul>
	Exponenciação em $\mathbb{F}_p^*$ é fácil e factorização é difícil.
	Questão 10 Curvas elípticas são importantes em criptografia, porque (empiricamente):
0.5/0.5	$\square$ 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 $\mathbb{F}_p^*$ .
	$\square$ A operação de "adição" é mais complicada sobre curvas elípticas do que em $\mathbb{F}_p^*$ .