EPITA
ÉCOLE D'INGENIEURS EN INFORMATIQUE

Chiffrement et Codes Correcteurs

Nasko Karamanov

1 Cryptography and elliptic curves

Learning Outcomes
— Use the algorithms of a given cryptosystem scheme
— Use an attack algorithm to decrypt cipher message.
— Identify algorithms that are susceptible to be not quantum resistant
— Explain some standard techniques of perturbation/secure of standard cryptosystems.

Question 1-1 Let $E : y^2 = x^3 + 2x + 3$ over $\mathbb{F}_7$ and $P = (2,1)$.

a) Is the point $(3,4)$ on the curve ?

b) Check that P is on the curve.

c) What are the coordinates of $-P$?

d) Give a formula for the inverse of $Q(x_Q, y_Q)$ as an element of $E(\mathbb{F}_7)$.

e) Calculate $2P$.

f) List all the points on the curve.

g) Check that the number of points is in the interval given by Hasse's theorem.

h) Give the table for the addition.

i) Show that P is a generator of $E(\mathbb{F}_7)$.

j) If $Q = (3,1)$ what is $\log_P(Q)$?

Training session

k) Same questions for $E : y^2 = x^3 + x + 2$ over $\mathbb{F}_5$ and $P = (1,2)$

l) Same questions for $E : y^2 = x^3 + 2x + 5$ over $\mathbb{F}_{11}$ and $P = (0,4)$

Question 1-2

a) Explain how one can adapt the square and multiply algorithm for fast calculation of nP.

b) Let $E : y^2 = x^3 + 3x + 2$ over $E(\mathbb{F}_{23})$ and $P = (0, 5)$. Calculate $13P$.

Question 1-3 The Menezes-Vanstone cryptosystem is a variant of ElGamal for elliptic curves. The schema is given in the following table.

Alice	Bob
KeyGen	
Choose p prime, E elliptic curve and a generator $G \in E(\mathbb{F}_p)$	
	Choose $b < \mathrm{Card}E(\mathbb{F}_p)$, $K_b = bG$ Bob's private key : $\mathrm{sk} = b$
Public key : $\mathrm{pk} = (p, g, K_b)$	
Encryption	
Choose $a < p$ Choose a pair of messages $\boldsymbol{m} = (\boldsymbol{m}_1, \boldsymbol{m}_2) \in (\mathbb{Z}/p\mathbb{Z})^2$ $K_a = aG$, $K_1 = a(K_b) = (x_1, y_1)$ $\boldsymbol{c}_1 \equiv x_1 \boldsymbol{m}_1 \mod p$ $\boldsymbol{c}_2 \equiv y_1 \boldsymbol{m}_2 \mod p$ $\boldsymbol{c} = \mathrm{Enc}(\boldsymbol{m}, \mathrm{pk}) = (K_a, \boldsymbol{c}_1, \boldsymbol{c}_2)$	
Decryption	
	$K_2 = bK_a = (x_2, y_2)$ $\boldsymbol{m}'_1 \equiv x_2^{-1} \boldsymbol{c}_1 \mod p$ $\boldsymbol{m}'_2 \equiv y_2^{-1} \boldsymbol{c}_2 \mod p$ $\mathrm{Dec}(\boldsymbol{c}, \mathrm{sk}) = (\boldsymbol{m}'_1, \boldsymbol{m}'_2)$

a) Discribe the space of messages $\mathscr{M}$ and ciphers $\mathscr{C}$.

b) Check that $K_1 = K_2$

c) Check the validity of this cryptosystem.

d) Alice and Bob use this cryptosystem with $E : y^2 = x^3 + 2x + 1$ over $\mathbb{F}_{23}$ and $G = (2, 6)$ of order 30. Bob's private key is $\mathrm{sk} = 4$. Bob received the message : $\boldsymbol{c} = ((18, 21), 16, 6)$. What is the message Alice sent ?

e) Is this cryptosystem quantum resistant ?

Question 1-4 The Digital Signature ECDSA (Elliptic curve digital signature algorithm) has the following scheme (in general it is applied to $h(\boldsymbol{m})$ where h is an hashing function).

Alice	Bob
KeyGen	
Choose p prime, E elliptic curve and a generator $G \in E(\mathbb{F}_p)$ of order n	
Choose $a < n$, $K_a = aG$ Alice's private key : sk $= a$	
Public key : pk $= (p, n, G, E, K_a)$	
Sign	
Choose $k < n$ Choose a message $\boldsymbol{m} = \in (\mathbb{Z}/n\mathbb{Z})$ $M = kG = (x_M, y_M)$ and $r = x_M \mod n$ $\boldsymbol{c} = (\boldsymbol{m} + ar)k^{-1} \mod n$ If $r = 0$ or $\boldsymbol{c} = 0$ start again $\sigma = (r, \boldsymbol{c})$	
Verify	
	$B = \boldsymbol{c}^{-1}(\boldsymbol{m}G + rK_a) = (x_B, y_B)$ If $r \equiv x_B \mod n$ retourne 1

Validity : $\boldsymbol{c}^{-1}(\boldsymbol{m}G + rK_a) = k(\boldsymbol{m} + ar)^{-1}(\boldsymbol{m}G + raG) = k(\boldsymbol{m} + ar)^{-1}(\boldsymbol{m} + ar)G = kG$
and we are checking the equality of the first coordinate.

a) Alice uses this signature with $E : y^2 = x^3 + 2x + 2$, $G = (5,1)$ and $n = 19$. She chooses $a = 7$, calculates $K_a = aG = (0,6)$ and publishes her public key. Bob received the message 26 signed with $\sigma = (7,17)$. Was the message sent by Alice ?

b) Is this signature scheme quantum resistant ?

Question 1-5 Let $E : y^2 = x^3 + 2x + 6$ over $\mathbb{F}_7$, $P = (1,3)$ a generator of $E(\mathbb{F}_7)$ and $Q = (4,6)$.

a) Give a lower and upper bound for $\log_P Q$.

b) Calculate $\log_P Q$

Training session

c) Same questions with $E : y^2 = x^3 + 2x + 2$ over F_{13}, $P = (3,3)$ and $Q = (6,3)$.