Cryptography and Network Security (CS60065)

AUTUMN, 2021-2022

TA: Tapadyoti Banerjee and Rijoy Mukherjee

Course Instructor: Prof. Dipanwita Roy Chowdhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur
West Bengal 721302, India

TUTORIAL: 6
DATE: 10th November 2022

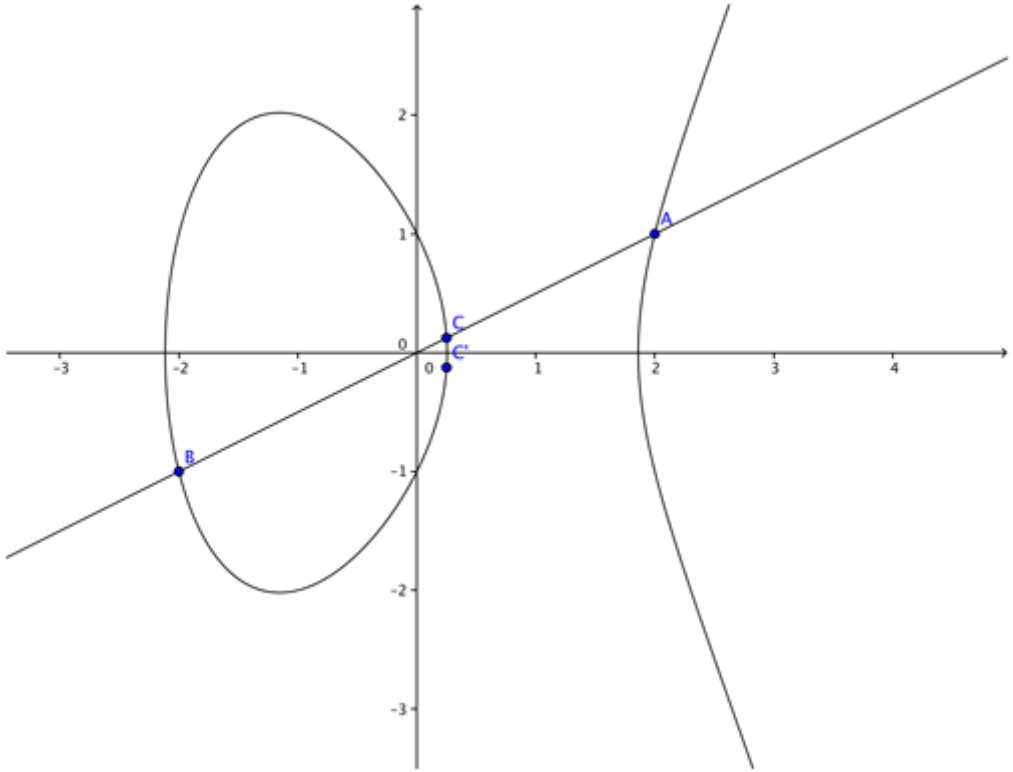
QUESTION : 1 (Elliptic curve cryptography)

Let's consider the elliptic curve: $y^2 = x^3 - 4x + 1$
And the two points A (2, 1) and B (-2, -1), which both lie on the curve. We now want to find an answer for A + B which we would also like to lie on the elliptic curve.

QUESTION : 1 (Elliptic curve cryptography)

Let's consider the elliptic curve: $y^2 = x^3 - 4x + 1$
And the two points A (2, 1) and B (-2, -1), which both lie on the curve. We now want to find an answer for A + B which we would also like to lie on the elliptic curve.

Graph:



QUESTION : 2 (Elliptic curve cryptography)

Let's consider the elliptic curve: $y^2 = x^3 - 5x + 4$
And the two points A (1, 0) and B (0, 2), which both lie on the curve. We now want to find an answer for A + B which we would also like to lie on the elliptic curve.

QUESTION : 3 (Elliptic curve cryptography)

Calculate whether a certain point belongs to a certain elliptic curve over a finite field.
Let's consider the elliptic curve: $y^2 = x^3 + 7 \pmod{17}$

(a) Calculate it for the point The point P1 {5, 8}
(b) Calculate it for the point The point P2 {9, 15}

QUESTION : 4 (Hash Concept)

Suppose H(m) is a collision resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages x, x' with $x \neq x'$, we have $H(x) \neq H(x')$? Explain your answer.

QUESTION : 5 (Hash Concept)

Find and explain the concept (or, an application) of the hash function in the DES algorithm.

QUESTION : 6 (MAC Concept)

Suppose that Bob sends an authenticated message to Alice. Now consider the following scenario:
1. Alice may forge a different message and claim that it came from John.
2. John can deny sending the message. Because it is possible for Mary to forge a message.

Determine the following which is true?
(A) Both A and B are false
(B) A is false
(C) B is false
(D) Both are true.

State the reason behind your answer.

(Not applicable, if not in your syllabus)

QUESTION : 7 (The ElGamal public key cryptosystem)

Alice and Bob agree to use the prime p = 1373 and the base g = 2 for communications using the ElGamal public key cryptosystem.

(i) Alice chooses a = 947 as her private key. What is the value of her public key A?

(b)Bob chooses b = 716 as his private key, so his public key is $B \equiv 2^{716} \equiv 469 \pmod{1373}$. Alice encrypts the message m = 583 using the ephemeral key k = 877. What is the cipher text (c1, c2) that Alice sends to Bob?

(Not applicable, if not in your syllabus)

QUESTION : 8 (Rabin Cryptosystem)

Suppose we want to decrypt the cipher text y = 23 by using the Rabin Cryptosystem. Illustrate the procedure with this toy example by considering by considering the public key, n = 77.