

LTCC basic course – Exam 2026

Cryptography – Mathematical Ciphers

All three questions carry equal marks. Answer all questions.

1. In Python (or similar), write some code to perform the addition and scalar multiplication of points on an elliptic curve modulo N . Implement Lenstra's elliptic curve factoring algorithm to find a non-trivial factor of

$$N = 2275060742667628746889724923.$$

You need to build in some checks in your code that tell you where in the process an integer occurred that cannot be inverted modulo N , running the Euclidean algorithm on that number and N . You possibly need to repeat the process many times with different randomly generated elliptic curves and base points, until a factor of N can be found. Present your code and produce a sample output for the factorisation of N . Feel free to use LLMs to assist with the code, the main criterion is that the code is working and can factor the integer using elliptic curves.

2. A message was encrypted using an RSA cipher with public key

$$(N, e) = (2275060742667628746889724923, 65537)$$

An intercepted message was found to be the integer

$$C = 1930151148580674728679137382.$$

Use the factorisation of $N = pq$ found in question 1 and perform all steps necessary to decrypt the message, resulting in an integer $M < N$. (If you didn't complete question 1, the integer can also be factorised using Mathematica or similar.) The integer M represents a plaintext message that was encoded by concatenating two digits per character, according to the alphabet

$$\{\text{SPACE} = 00, \text{A} = 01, \text{B} = 02, \dots, \text{Z} = 26, ? = 27, ! = 28\},$$

The message should come out as plain English words.

3. Let $P = (X_P, Y_P)$, $Q = (X_Q, Y_Q)$ be two distinct points on a Montgomery curve,

$$BY^2 = X^3 + AX^2 + X, \quad B(A^2 - 4) \neq 0.$$

Show that the X coordinates of the points P , Q , $P + Q = (X_+, Y_+)$ and $P - Q = (X_-, Y_-)$ satisfy the relationship

$$X_+ X_- (X_P - X_Q)^2 = (X_P X_Q - 1)^2.$$