

LTCC basic course

Cryptography – Mathematical Ciphers

Mock exam

2026

1. Write Python code (or similar) to solve the discrete logarithm problem

$$23^x = c = 499382170599 \pmod{p = 567248431103}, \quad (1)$$

using the index calculus, involving the set of 6 prime factors

$$\Pi = \{2, 3, 5, 7, 11, 13\}. \quad (2)$$

That is, generate numbers j so that $23^j \pmod{p}$ can be written as a product of only powers $l \in \Pi$ and solve a linear system

$$\sum_{l \in \Pi} e_{j_k}(l) \cdot x_l = j_k \pmod{p-1}, \quad k = 1, \dots, 6. \quad (3)$$

Then find an integer m such that $h \cdot g^{-m} \pmod{p}$ has the same property and thus obtain $x \pmod{p-1}$.

2. A message was encrypted and sent to Alice using an ElGamal cipher with prime $p = 567248431103$ and base $g = 23$. Alice's public key is the number $A = g^a \pmod{p} = 518346147095$. An intercepted message consists of the pair of integers

$$c_1 = 499382170599, \quad c_2 = 364671335738. \quad (4)$$

Use your result from question 1 (or otherwise) and go through all necessary steps to obtain the plaintext message M – this is an integer less than p . 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 $P = (X_P, Y_P)$ be a point on a Montgomery curve,

$$BY^2 = X^3 + AX^2 + X, \quad B(A^2 - 4) \neq 0. \quad (5)$$

Show that the X coordinates of the points $P = (X_P, Y_P)$ and $2P = (X_{2P}, Y_{2P})$ satisfy the relationship

$$4X_{2P}X_P(X_P^2 + AX_P + 1) = (X_P^2 - 1)^2. \quad (6)$$