

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

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

Solutions

1

To find linear congruence relations between the indices

$$x_2 = \log_{23}(2), \quad x_3 = \log_{23}(3), \quad \dots, \quad x_{13} = \log_{23}(17), \quad (7)$$

we use the following Python code:

```
import random
p = 567248431103
g = 23
primes = [2,3,5,7,11,13]
num_eqns = 0
while num_eqns < len(primes):
    j = random.randrange(2,p-1)
    gj = modpower(g,j,p)
    indices = [0 for prime in primes]
    for prime in primes:
        while gj%prime==0:
            indices[primes.index(prime)] += 1
            gj //= prime
    if gj == 1:
        num_eqns += 1
        print(j, indices)
```

The sample output below is a list of numbers j_k , $k = 1, \dots, 6$ and corresponding coefficient vectors $e_{j_k}(l)$, $l \in \Pi$,

```
77443154712 [8, 4, 0, 2, 1, 3]
321470441838 [6, 5, 2, 0, 5, 0]
391915443387 [21, 3, 1, 2, 0, 1]
295909791210 [4, 6, 6, 0, 2, 0]
158931552592 [0, 1, 0, 0, 1, 2]
406042733204 [1, 9, 2, 0, 1, 3]
```

We use a linear solver to solve the system of congruences

$$\sum_{l \in \Pi} e_{j_k}(l) \cdot x_l = j_k \pmod{p-1}, \quad k = 1, \dots, 6, \quad (8)$$

obtaining

$$\begin{aligned} x_2 &= 495967876646, & x_3 &= 632719672076, & x_5 &= 832802618093, \\ x_7 &= 230790225225, & x_{11} &= 431936582826, & x_{13} &= 398010295498. \end{aligned} \quad (9)$$

In the last step we randomly generate an integer m such that $c \cdot 23^{-m} \pmod{p}$ is a product only of prime divisors in Π . Adapting the code above slightly, we

find e.g.

$$m = 489487805312 \implies c \cdot 23^{-m} = 2 \cdot 3 \cdot 5^5 \cdot 13^4 \pmod{p}. \quad (10)$$

This means the solution to the discrete logarithm problem is given by

$$x = m + x_2 + x_3 + 5x_5 + 4x_{13} = 22165 \pmod{p-1} \quad (11)$$

2

From question 1, the solution of the discrete logarithm problem $g^x = c_1 \pmod{p}$ is $x = 22165$. The interceptor can use this to find the message M via the relation

$$c_2 = M \cdot A^k \pmod{p}. \quad (12)$$

So they first compute A^k (using e.g. the method of repeated squaring) and the inverse of A^k (using the extended Euclidean algorithm),

$$A^k = 458255280933 \pmod{p}, \quad (A^k)^{-1} = A^{-k} = 201803488200 \pmod{p}, \quad (13)$$

then multiplying the result by c_2 to obtain M :

$$M = c_2 \cdot A^{-k} = 151400230125 \pmod{p}. \quad (14)$$

Using the given encoding scheme, the message reads ON WAY.

3

We need to describe the doubling of a point $P = (X_P, Y_P)$ on the Montgomery curve. The line connecting the point P and $2P = (X_{2P}, Y_{2P})$ is tangent to the curve at P . To compute the slope m , we formally differentiate the equation of the curve,

$$2Bydy = (3x^2 + 2Ax + 1)dx \implies m = \frac{dy}{dx}\bigg|_P = \frac{3X_P^2 + 2AX_P + 1}{2BY_P}. \quad (15)$$

We also find (but not use)

$$c = Y_P - mX_P = \frac{X_P - X_P^3}{2BY_P}. \quad (16)$$

Inserting $y = mx + c$ into the equation of the curve, we find a cubic in x ,

$$B(mx + c)^2 = x^3 + Ax^2 + x \implies x^3 + (A - Bm^2)x^2 + (1 - 2Bcm)x - Bc^2 = 0. \quad (17)$$

The sum of the x coordinates of the points P and $2P$ (counting X_P twice) is the negative of the coefficient of the quadratic term,

$$\begin{aligned} 2X_P + X_{2P} &= Bm^2 - A = \frac{(3X_P^2 + 2AX_P + 1)^2}{4(X_P^3 + AX_P^2 + X_P)} - A \\ \implies 4X_{2P}X_P(X_P^2 + AX_P + 1) &= X_P^4 - 2X_P^2 + 1 = (X_P^2 - 1)^2. \end{aligned} \quad (18)$$