Cryptanalysis (COMPGA18/COMPM068)
Public Key Answers

Mary Maller & Nicolas T. Courtois

1 Index Calculus

Working in the group $\mathbb{Z}^*_{2099}$, this question uses index calculus to solve an instance of the discrete log problem. We shall show a method to find $\log_{11} 793 \mod 2099$. It may help to note that because 11 generates $\mathbb{Z}^*_{2099}$, we have that the function $\log_{11} : \mathbb{Z}^*_{2099} \mapsto \mathbb{Z}^+_{2098}$ is an isomorphism. This means that it is invertible and that for all $x, y \in \mathbb{Z}^*_{2099}$, $\log_{11}(x \cdot y) = \log_{11}(x) + \log_{11}(y)$.

(i) (a) Using the $factor()$ command in Sage, check whether 2099 is prime.

(b) Working modulo 2099, use Sage to find which of the following is false:

i. $11^9 = 2^5 3^3 5^7$
ii. $11^{44} = 2^4 3^3 5^4$
iii. $11^{49} = 2^5 3^6 5^5$
iv. $11^{52} = 2^8 3^6 5^2$
v. $11^{73} = 2^3 3^3 5^0$

To calculate $11^4 4$ in Sage do the following:

$$\begin{aligned} sage: &\quad K = IntegerModRing(2099) \\ sage: &\quad K(11)\hat{}(44). \end{aligned}$$

(c) Using 3 of the above equations, find a system of linear equations over $\mathbb{Z}_{2098}$ which involve $L_2 = \log_{11}(2)$, $L_3 = \log_{11}(3)$, $L_5 = \log_{11}(5)$ and are linearly independent modulo 2.

(ii) We now wish put this into matrix form and then invert the matrix. An issue here is that Z_{2098} is not a field i.e its non-zero elements do not form a group under multiplication. Gaussian elimination can be difficult over fields as if there is a non-invertible coefficient, you would have to find a new system of linear equations. To deal with this issue, we shall solve the system of equations modulo 1049 and modulo 2, and then apply the Chinese Remainder Theorem to get the solution modulo 2098.

(a) Is 1049 prime?

(b) Write the system of equations from part i) in matrix form (i.e. $M\mathbf{L} = \mathbf{v}$ for M a matrix and $\mathbf{L}$, $\mathbf{v}$ vectors).

(c) Calculate $M^{-1} \mod 2$. Verify your answer in Sage using the following commands.

$$\begin{aligned} sage: &\quad M = matrix([[1,1,1],[0,1,0],[1,1,0]]); \\ sage: &\quad M\hat{\ }(-1) \end{aligned}$$

(d) $M^{-1} \mod 1049$ can be calculated in Sage as follows.

$$\begin{aligned} sage: &\quad R = IntegerModRing(1049) \\ sage: &\quad R33 = MatrixSpace(R,3,3) \\ sage: &\quad N = R33([[\cdot,\cdot,\cdot],[\cdot,\cdot,\cdot],[\cdot,\cdot,\cdot]]); \\ sage: &\quad NI = N\hat{\ }(-1) \\ sage: &\quad NI \end{aligned}$$

Verify that

$$M^{-1} \mod 1049 = \begin{pmatrix} 4 & -7 & 3 \\ -4 & 7 & 347 \\ -1 & 2 & -1 \end{pmatrix}.$$

(e) Find L_2, L_3, L_5 modulo 1049 and modulo 2 respectively either either by hand or using Sage. Multiplying a vector $\mathbf{v}$ by a matrix NI in Sage can be done in the following manner:

$$\begin{aligned} sage: &\quad R31 = MatrixSpace(R,3,1) \\ sage: &\quad v = R31([\cdot,\cdot,\cdot]); \\ sage: &\quad NI * v \end{aligned}$$

(iii) Given that $1 * 1049 - 524 * 2 = 1$, use the Chinese Remainder Theorem to find L_2, L_3, L_5 modulo 2098. We thus have that $11^{L_i} = i \mod 2099$. Check your answers in Sage.

(iv) Given that $793 \cdot 11^{32} \mod 2099 = 480$, find the prime factorisation of $793 \cdot 11^{32} \mod 2099$.

(v) Use your answers from parts iii) and iv) to find $\log_{11}(793 \mod 2099)$. We have thus found ans such that $11^{ans} = 793$.
Hint: $\log_{11}(793 \mod 2099) \in \mathbb{Z}^+_{2098}$.

Answer:

(i) (a) 2099 is prime.

(b) (iii) is false.

(c) • $9 = 5L_2 + 3L_3 + 7L_5$.

- $44 = 2L_2 + 3L_3 + 5L_5$.
- $73 = 3L_2 + 3L_3 + 0L_5$.

(ii) (a) Yes.

(b)

$$\begin{pmatrix} 5 & 3 & 7 \\ 4 & 3 & 4 \\ 3 & 3 & 0 \end{pmatrix} \begin{pmatrix} L_2 \\ L_3 \\ L_5 \end{pmatrix} = \begin{pmatrix} 9 \\ 44 \\ 73 \end{pmatrix}.$$

(c)

$$M^{-1} \mod 2 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

(d) N/A

(e)

$$\begin{pmatrix} L_2 \\ L_3 \\ L_5 \end{pmatrix} = \begin{pmatrix} 996 \\ 427 \\ 6 \end{pmatrix} \mod 1049 \text{ and } \begin{pmatrix} L_2 \\ L_3 \\ L_5 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \mod 2$$

(iii) To find x such that $x = a \mod 1049$ and $x = b \mod 2$ we first find $1_{1049} = (-524) * 2 \mod 2098 = 1050$ and $1_2 = 1 * 1049 \mod 2098 = 1049$. Then $x = a * 1_{1049} + b * 1_2 \mod 2098$. Hence

$$L_2 = 996 * 1050 + 1 * 1049 \mod 2098 = 2045.$$

Using the same method we get that

$$\begin{pmatrix} L_2 \\ L_3 \\ L_5 \end{pmatrix} = \begin{pmatrix} 2045 \\ 1476 \\ 6 \end{pmatrix}.$$

(iv)

$$480 = 2^5 \times 3 \times 5.$$

(v)

$$\begin{aligned} 793 \times 11^{32} &= 2^5 \times 3 \times 5 \mod 2099 \\ \implies \log_{11}(793) + 32 &= 5L_2 + L_3 + L_5 \mod 2098 \\ \implies \log_{11}(793) &= 5 \times 2045 + 1476 + 6 - 32 \mod 2098 \\ \implies \log_{11}(793) &= 1185 \end{aligned}$$