187 - Day 05

Wednesday, April 11, 2018 9:06 AM

12 choices for a

a must be coprime to 26

Day 05 – Ciphers Using Modular Arithmetic (cont.)

Affine cipher

$|K| = 12 \times 26 \rightarrow$ 26 choices for b $0 \le b \le 25$

A key is given by a pair of integers (a, b) where a **relatively prime** to 26 and $0 \le b \le 25$.

For each plaintext number x and ciphertext number y,

- Encryption function $y = E(x) = ax + b \mod p$
- Decryption function $x = D(y) = a^{-1}(y - b) \mod 26$

Example. Decrypt the ciphertext **E K T W Q M R V R V W Q M T F**, knowing that the plaintext starts with **GO** and it was encrypted with an affine cipher modulo 26.

we know: G → E, O → K

we find (a, b) that were used to encrypt this plaintext

$G = 6$, $O = 14$

$\boxed{ax + b = y \mod 26}$

$4 = E$, $10 = K$

we solve the system $\begin{cases} 6a + b = 4 \ (1) \\ 14a + b = 10 \ (2) \end{cases}$ in mod 26

$(2) - (1)$: $8a = 6 \mod 26$

So either $a = 4$ or $a = 17$ (soln is no longer unique)

If $a = 4 \Rightarrow 6 \cdot 4 + b = 4.$

$b = 4 - 24 = -20 = 6 \mod 26$

If $a = 17 \Rightarrow 6 \cdot 17 + b = 4$

$b = \dots\ 6$

$(a, b) = \cancel{(4, 6)}$ or $(17, 6)$ a must be coprime to 26

1

plaintext ↕ plaintext number

A → 0, B → 1, ⋮, Z → 25

$y = ax + b \mod 26$

$x = a^{-1}(y - b) \mod 26$

ciphertext numbers ↕ ciphertext

In mod 26, use the multiplication table to find a^{-1}

Ans: Gone with the wind.

Modulo arithmetic on matrices

Definition 1. *Let A, B be $m \times n$ matrices with integer entries. We say that A and B are* ***congruent modulo*** *m if*

$$a_{i,j} \equiv b_{i,j} \mod m$$

for all entries $a_{i,j}, b_{i,j}$. We write $A \equiv B \mod m$.

Definition 2. *Let m be a given modulus and let A be an $n \times n$ matrix with integer entries. A is said to be* ***invertible modulo*** *m if there exists an $n \times n$ matrix B such that*

$$AB = I \mod m \quad \text{and} \quad BA = I \mod m.$$

We write "$A^{-1} = B \mod m$" to denote B is the inverse of A modulo m.

Definition 3. *The* ***determinant*** *of A modulo m is $\det(A)$ reduced mod m.*

Theorem 1. *If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an integer entries then the determinant of A under modulo m is given by*

$$\det(A) = ad - bc \mod m.$$

A is invertible modulo m if and only if $\det(A)$ is relatively prime to m. In this case, the inverse is given by

$$A^{-1} = \det(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \mod m$$

Hill cipher

Definition 4. *Hill cipher is a* ***block cipher*** *where* ***pairs of plaintext letters*** *are encrypted by the transformation*

$$Y = AX \mod 26$$

where A is a 2×2 invertible matrix modulo 26.

Example. Use the Hill cipher with key matrix $A = \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix}$ to encrypt the message "MISSING"

$\begin{bmatrix} M \\ I \end{bmatrix} \to \begin{bmatrix} 12 \\ 8 \end{bmatrix} \to \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix} \begin{bmatrix} 12 \\ 8 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 22 \times 12 + 13 \times 8 \\ 11 \times 12 + 5 \times 8 \end{bmatrix}$

$= \begin{bmatrix} 4 + 0 \\ 2 + 14 \end{bmatrix} \text{ mod } 26$

$= \begin{bmatrix} 4 \\ 16 \end{bmatrix} \to \begin{bmatrix} E \\ Q \end{bmatrix}$

$\begin{bmatrix} S \\ S \end{bmatrix} \to \begin{bmatrix} 18 \\ 18 \end{bmatrix} \to \begin{bmatrix} 6 \\ 2 \end{bmatrix} \to \begin{bmatrix} G \\ C \end{bmatrix}$

$\begin{bmatrix} I \\ N \end{bmatrix} \to \begin{bmatrix} 8 \\ 13 \end{bmatrix} \to \begin{bmatrix} 7 \\ 23 \end{bmatrix} \to \begin{bmatrix} H \\ X \end{bmatrix}$

$\begin{bmatrix} G \\ K \end{bmatrix} \to \begin{bmatrix} 6 \\ 10 \end{bmatrix} \to \begin{bmatrix} 2 \\ 12 \end{bmatrix} \to \begin{bmatrix} C \\ M \end{bmatrix}$

use "K" to pad at the end

cipher text: EQGC HXCM

Decryption is given by $X = A^{-1}Y \mod 26.$

Example. Decrypt the message **Z G W Q**, knowing it was encrypted using Hill cipher modulo 26 with the key $A = \begin{bmatrix} 3 & 7 \\ 9 & 10 \end{bmatrix}$

$$\begin{bmatrix} Z \\ G \end{bmatrix} \to \begin{bmatrix} 25 \\ 6 \end{bmatrix} \to \begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 25 \\ 6 \end{bmatrix} = \dots = \begin{bmatrix} 0 \\ 11 \end{bmatrix} \to \begin{bmatrix} A \\ L \end{bmatrix}$$

$$\begin{bmatrix} W \\ Q \end{bmatrix} \to \begin{bmatrix} 22 \\ 16 \end{bmatrix} \to \begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 22 \\ 16 \end{bmatrix} = \dots = \begin{bmatrix} 18 \\ 14 \end{bmatrix} \to \begin{bmatrix} S \\ O \end{bmatrix}$$

plaintext "ALSO"

$$A^{-1} = \det(A)^{-1} \cdot \begin{bmatrix} 10 & -7 \\ -9 & 3 \end{bmatrix} = \det(A)^{-1} \begin{bmatrix} 10 & 19 \\ 17 & 3 \end{bmatrix}$$

+26

+26

$$\det(A) = 3 \times 10 - 9 \times 7 = -33 = 19 \mod 26$$

$$A^{-1} = 19^{-1} \begin{bmatrix} 10 & 19 \\ 17 & 3 \end{bmatrix} = 11 \cdot \begin{bmatrix} 10 & 19 \\ 17 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 11 \times 10 & 11 \times 19 \\ 11 \times 17 & 11 \times 3 \end{bmatrix} = \begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \mod 26$$

Example. You have intercepted the ciphertext

D L H I V D L Z H I P N E U

which you know to be produced by a Hill cipher modulo 26 using a 2×2 matrix. Moreover, you strongly suspect that the first four letters of the message is the word **DEAR**. Decrypt the message.

$$\begin{array}{cc|cc|cc|c} D & L & H & I & V & D & \cdots \\ 3 & 11 & 7 & 8 & 21 & 3 & \end{array}$$

$$\begin{bmatrix} D \\ L \end{bmatrix} \leftrightarrow \begin{bmatrix} D \\ E \end{bmatrix} \qquad \begin{bmatrix} H \\ I \end{bmatrix} \to \begin{bmatrix} A \\ R \end{bmatrix}$$

$$\begin{array}{cc|cc|} 3 & 4 & 0 & 17 \\ D & E & A & R \end{array}$$

We want to find A^{-1} s.t. $A^{-1}\begin{bmatrix} 3 \\ 11 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \end{bmatrix} \bmod 26$

$$A^{-1}\begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 0 \\ 17 \end{bmatrix} \bmod 26$$

So we solve: $A^{-1}\begin{bmatrix} 3 & 7 \\ 11 & 8 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 4 & 17 \end{bmatrix}$

$$A^{-1} = \begin{bmatrix} 3 & 0 \\ 4 & 17 \end{bmatrix} \cdot \underbrace{\begin{bmatrix} 3 & 7 \\ 11 & 8 \end{bmatrix}^{-1}}$$

$$= \begin{bmatrix} 3 & 0 \\ 4 & 17 \end{bmatrix} \cdot \begin{bmatrix} 18 & 7 \\ 11 & 23 \end{bmatrix} = \begin{bmatrix} 2 & 21 \\ 25 & 3 \end{bmatrix} \bmod 26$$

Now use $X = A^{-1} \cdot Y$ to decrypt.

Euclidean algorithm - Berlekamp version

The Euclidean algorithm is the process which yields the greatest common divisor d of two given integers A and B where $A > B$. The Berlekamp's algorithm is a slight modification of the Euclidean algorithm that can also give us the inverse of B mod A.

Algorithm:

1. Set $r_{-2} = A, r_{-1} = B, p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$
2. For each $k = 0, 1, 2, \ldots$ compute the following

$$r_{k-2} = a_k r_{k-1} + r_k$$
$$p_k = a_k p_{k-1} + p_{k-2}$$
$$q_k = a_k q_{k-1} + q_{k-2}$$

3. Stop at step n where $r_n = 0$

Then $r_{n-1} = \gcd(A, B)$. Furthermore, in the case $\gcd(A, B) = 1$ then

$$B \cdot (-1)^n p_{n-1} = 1 + A \cdot (-1)^n q_{n-1}$$

Example. find the inverse of 115 in modulo 12659,

k	r	a	p	q
-2	12659		0	1
-1	115		1	0
0				
1				
2				