Affine Cipher

If key $= (\alpha, \beta)$, encrypt each character by

$$p \longmapsto \alpha p + \beta \pmod{26}$$

Ex. key $= (5, 3)$

plaintext = R
17

$$17 \longmapsto 5 \cdot 17 + 3$$
$$\equiv 7 + 3$$
$$\equiv 10$$

ciphertext = K

Decrypt this example:

ciphertext = 10

$$10 \equiv 5 \cdot p + 3 \pmod{26}$$

What is p?

$$10 - 3 \equiv 5 \cdot p \pmod{26}$$
$$7 \equiv 5 \cdot p$$

by table, $p \equiv 17 \pmod{26}$

Solving $C \equiv \alpha \cdot p + \beta \pmod{26}$ decrypts.

However, sometimes this equation has

no solutions.

The essential problem is

$$x \longmapsto \alpha x \pmod{26}$$

may fail to be a surjective.

It may also have multiple solutions.

i.e. $x \longmapsto \alpha x \pmod{26}$

may fail to be injective.

We need α chosen from

$\{1, 3, 5, \ldots, \cancel{13}, \ldots, 25\}$

(odds except 13)

i.e.

α which are coprime to 26

$$\gcd(\alpha, 26) = 1$$

(this is only an observation right now)

Inverses in Modular Arithmetic

Defⁿ. If y satisfies $xy \equiv 1 \pmod{n}$ then y is the multiplicative inverse of $x \bmod n$.

We write x^{-1} or $\frac{1}{x}$ for this.

Example. $3^{-1} \equiv 2 \pmod 5$

$\frac{1}{3} \equiv 2 \pmod 5$

Warning! Not everything has a multiplicative inverse.

Eg. 2 has no mult. inverse mod 4

because
$0 \cdot 2 \equiv 0$
$1 \cdot 2 \equiv 2$ ← never get 1
$2 \cdot 2 \equiv 0$
$3 \cdot 2 \equiv 2$

Defⁿ. An element of $\mathbb{Z}/n\mathbb{Z}$ is called invertible if it has an inverse.

We call the set of invertible elements mod n the unit group, denote $(\mathbb{Z}/n\mathbb{Z})^*$.

Eg. $(\mathbb{Z}/26\mathbb{Z})^* = \{1,3,5,7,9,11,15,17,19,21,23,25\}$

Note (Exercise).

$\alpha \in \mathbb{Z}/n\mathbb{Z}$ is invertible if and only if $x \longmapsto \alpha x \pmod{n}$ is bijective.

Hill Cipher (1929)

key = { n = dimension; E = encryption matrix $n \times n$; D = decryption matrix $n \times n$ } entries mod 26

$DE = I$

Encryption: block-by-block

a block is a sequence of n letters, viewed as a vector $\vec{p}$ mod 26.

$$\vec{p} \longmapsto E\vec{p}$$

Decryption:

$$\vec{c} \longmapsto D\vec{c}$$

Correctness:

$$\vec{p} \xmapsto{\text{enc}} E\vec{p} \xmapsto{\text{dec}} DE\vec{p} = I\vec{p} = \vec{p}$$

$=$

Ex. plaintext (MAT)(HEM)(ATI)(CSX)

$\vec{v}_1 = \begin{pmatrix} 12 \\ 0 \\ 19 \end{pmatrix}$ $\vec{v}_2$ $\vec{v}_3$ $\vec{v}_4$

key

$n = 3$

$$E = \begin{pmatrix} 23 & 5 & 18 \\ 19 & 20 & 10 \\ 13 & 8 & 19 \end{pmatrix}$$

$$D = \begin{pmatrix} 8 & 15 & 16 \\ 11 & 25 & 12 \\ 20 & 23 & 21 \end{pmatrix}$$

encryption of 1st block:

$$E\vec{v}_1 = \begin{pmatrix} 23 & 5 & 18 \\ 19 & 20 & 10 \\ 13 & 8 & 19 \end{pmatrix} \begin{pmatrix} 12 \\ 0 \\ 19 \end{pmatrix}$$

$$= \begin{pmatrix} 20 \\ 2 \\ 23 \end{pmatrix} \pmod{26}$$

So MAT $\mapsto$ UCX

Decrypt.

$$\begin{pmatrix} 8 & 15 & 16 \\ 11 & 25 & 12 \\ 20 & 23 & 21 \end{pmatrix} \begin{pmatrix} 20 \\ 2 \\ 23 \end{pmatrix} = \begin{pmatrix} 12 \\ 0 \\ 19 \end{pmatrix}$$