Kai Soon 869815

COMP90043 CRYPTOGRAPHY & SECURITY

CRACKING THE HILL CIPHER

Key Space

Intuitively, one would think that the total number of possible keys is 31^{m^2} (31 permutations of m^2), but the decryption algorithm requires a key matrix to be inverted. Therefore, the number of possible keys that cannot be inverted must be taken into account.

The following is the generalised formula for the total number of possible keys of a Hill Cipher with a key square matrix of size m and modulo of 31,

$$
\begin{aligned}
&31^{m^2}(1-31^{-1})(1-31^{-2})(1-31^{-3})\dots(1-31^{-m})\\
&=31^{m^2}\cdot\prod_{i=1}^{m}(1-31^{-i})\\
&=\prod_{i=1}^{m}31^{m^2}(1-31^{-i})\\
&=\prod_{i=1}^{m}(31^{m}-31^{m-i})
\end{aligned}
$$

Chosen Plain-text Attack

The following converts all four blocks of plaintext and cipher-text into its integer representation,

$$
\begin{bmatrix}C\\T\\R\\L\end{bmatrix}=\begin{bmatrix}2\\19\\17\\11\end{bmatrix}=\begin{bmatrix}p_{1,1}\\p_{2,1}\\p_{3,1}\\p_{4,1}\end{bmatrix}
\qquad
\begin{bmatrix}H\\G\\P\\P\end{bmatrix}=\begin{bmatrix}7\\6\\15\\15\end{bmatrix}=\begin{bmatrix}c_{1,1}\\c_{2,1}\\c_{3,1}\\c_{4,1}\end{bmatrix}
$$

$$
\begin{bmatrix}C\\A\\P\\S\end{bmatrix}=\begin{bmatrix}2\\0\\15\\18\end{bmatrix}=\begin{bmatrix}p_{1,2}\\p_{2,2}\\p_{3,2}\\p_{4,2}\end{bmatrix}
\qquad
\begin{bmatrix}H\\O\\F\\L\end{bmatrix}=\begin{bmatrix}7\\14\\5\\11\end{bmatrix}=\begin{bmatrix}c_{1,2}\\c_{2,2}\\c_{3,2}\\c_{4,2}\end{bmatrix}
$$

$$
\begin{bmatrix}H\\O\\M\\E\end{bmatrix}=\begin{bmatrix}7\\14\\12\\4\end{bmatrix}=\begin{bmatrix}p_{1,3}\\p_{2,3}\\p_{3,3}\\p_{4,3}\end{bmatrix}
\qquad
\begin{bmatrix}T\\T\\S\\I\end{bmatrix}=\begin{bmatrix}19\\19\\18\\8\end{bmatrix}=\begin{bmatrix}c_{1,3}\\c_{2,3}\\c_{3,3}\\c_{4,3}\end{bmatrix}
$$

$$
\begin{bmatrix}P\\G\\U\\P\end{bmatrix}=\begin{bmatrix}15\\6\\20\\15\end{bmatrix}=\begin{bmatrix}p_{1,4}\\p_{2,4}\\p_{3,4}\\p_{4,4}\end{bmatrix}
\qquad
\begin{bmatrix}D\\A\\C\\R\end{bmatrix}=\begin{bmatrix}3\\0\\2\\17\end{bmatrix}=\begin{bmatrix}c_{1,4}\\c_{2,4}\\c_{3,4}\\c_{4,4}\end{bmatrix}
$$

The encryption of the four blocks of plaintext can be expressed as the following matrix equation,

$$\begin{bmatrix} k_{1,1} & k_{1,2} & k_{1,3} & k_{1,4} \\ k_{2,1} & k_{2,2} & k_{2,3} & k_{2,4} \\ k_{3,1} & k_{2,2} & k_{3,3} & k_{3,4} \\ k_{4,1} & k_{2,2} & k_{4,3} & k_{4,4} \end{bmatrix} \begin{bmatrix} p_{1,1} & p_{1,2} & p_{1,3} & p_{1,4} \\ p_{2,1} & p_{2,2} & p_{2,3} & p_{2,4} \\ p_{3,1} & p_{2,2} & p_{3,3} & p_{3,4} \\ p_{4,1} & p_{2,2} & p_{4,3} & p_{4,4} \end{bmatrix} \text{mod} 31 = \begin{bmatrix} c_{1,1} & c_{1,2} & c_{1,3} & c_{1,4} \\ c_{2,1} & c_{2,2} & c_{2,3} & c_{2,4} \\ c_{3,1} & c_{2,2} & c_{3,3} & c_{3,4} \\ c_{4,1} & c_{2,2} & c_{4,3} & c_{4,4} \end{bmatrix}$$

$$\therefore KP \,\text{mod} 31 = C$$
$$K = CP^{-1}\text{mod} 31$$

Rearranging the matrix equation enables us to solve for the key matrix K. Solving for K requires us to evaluate $P^{-1}\text{mod}31$, and note that P is a matrix, not an integer, therefore the way the inverse modulo of a matrix is computed differed to that of the inverse modulo of an integer.

$$\begin{aligned} P^{-1}\text{mod}31 &= \det(P)^{-1} \cdot \text{adj}(P)\text{mod}31 \\ &= \det(P)^{-1}\text{mod}31 \cdot \text{adj}(P)\text{mod}31 \end{aligned}$$

where $\det(P)$ is the determinant of P

$\text{adj}(P)$ is the adjunct matrix of P

The following function written in Python is used to compute the inverse modulo of the determinant of P,

```
def modInv(a, m):
    for i in range(1, m):
        if (i*a) % m == 1:
            return i
    raise ValueError(str(a) +" has no inverse mod " + str(m))
```

$$\therefore \det(P)^{-1}\text{mod}31 = 9$$

The following function written in Python is used to compute the adjunct matrix of P,

```
import numpy as np
def adj(A, m):
    n = len(A)
    A_adj = np.zeros([n, n])
    for i in range(n):
        for j in range(n):
            minor_mat = get_minor(A, j, i)
            minor_det = int(round(np.linalg.det(minor_mat)))
            A_adj[i][j] = ((-1) ** (i + j) * minor_det) % m
    return A_adj
```

$$\therefore \text{adj}(P)\text{mod}31 = \begin{bmatrix} 24 & 17 & 14 & 27 \\ 28 & 18 & 6 & 25 \\ 17 & 23 & 12 & 26 \\ 29 & 28 & 0 & 14 \end{bmatrix}$$

$$\therefore P^{-1}\text{mod}31 = \begin{bmatrix} 30 & 29 & 2 & 26 \\ 4 & 7 & 23 & 8 \\ 29 & 21 & 15 & 17 \\ 13 & 4 & 0 & 2 \end{bmatrix}$$

$K = CP^{-1}\text{mod}31$

$$\therefore K = \begin{bmatrix} 22 & 12 & 26 & 9 \\ 12 & 20 & 30 & 2 \\ 26 & 19 & 12 & 27 \\ 17 & 4 & 0 & 28 \end{bmatrix}$$

To decrypt a cipher-text encrypted by the key K, the inverse of K must be evaluated,

$$\begin{aligned} KP\,\text{mod}31 &= C \\ P &= K^{-1}C\,\text{mod}31 \\ &= K^{-1}\text{mod}31 \cdot C\,\text{mod}31 \end{aligned}$$

The process of evaluating the inverse of K is identical to that of evaluating the inverse of P,

$$\begin{aligned} K^{-1}\text{mod}31 &= \det(K)^{-1} \cdot \text{adj}(K)\text{mod}31 \\ &= \det(K)^{-1}\text{mod}31 \cdot \text{adj}(K)\text{mod}31 \end{aligned}$$

For $K^{-1}\text{mod}31$ to exist, $\det(K)^{-1}\text{mod}31$ must exist. As such, $\det(K)$ and 31 must be co-primes, therefore not all permutations of the matrix K can be a possible key to this system.

$$\therefore K^{-1}\text{mod}31 = \begin{bmatrix} 16 & 19 & 16 & 29 \\ 2 & 22 & 13 & 24 \\ 26 & 11 & 17 & 11 \\ 21 & 13 & 15 & 10 \end{bmatrix}$$

To decrypt the cipher-text, the cipher-text must be divided into blocks of four and arranged as the following cipher-text matrix,

Cipher-text Matrix

!	m	j	p	v	t	z	m	k	b	i	?	b	z	r	y	v	l	w	.	o	n	f	g	?	u	o
l	y	?	a	r	n	y	?	j	t	a	s	k	o	a	p	b	m	e	j	i	j	y	i	r	n	r
p	a	.	.	f	r	e	q	t	d	n	l	e	s	a	i	o	w	m	y	t	r	g	b	b	?	i
u	i	m	d	u	u	f	v	o	r	!	q	s	f	w	.	l	a	q	b	g	i	e	c	?	m	,

Every group of four characters in the cipher-text are placed as columns of the cipher-text matrix. All characters in this matrix are translated to its corresponding integer representation.

Cipher-text Matrix - Integers

29	12	9	15	21	19	25	12	10	1	8	28	1	25	17	24	21	11	22	27	14	13	5	6	28	20	14
11	24	28	0	17	13	24	28	9	19	0	18	10	14	0	15	1	12	4	9	8	9	24	8	17	13	17
15	0	27	27	5	17	4	16	19	3	13	11	4	18	0	8	14	22	12	24	19	17	6	1	1	28	8
20	8	12	3	20	20	5	21	14	17	29	16	18	5	22	27	11	0	16	1	6	8	4	2	28	12	26

Rearranging the system of equation enables the cipher-text matrix to be decrypted to the plaintext matrix,

$$KP \bmod 31 = C$$

$$P = K^{-1}C \bmod 31$$

The decrypted cipher-text integers are,

Decrypted Plaintext Matrix - Integers

5	12	30	15	17	8	11	8	18	19	30	4	17	14	11	30	30	12	30	24	17	15	4	12	18	30	3
14	0	2	19	0	2	6	19	26	30	13	18	24	30	4	14	14	14	21	30	6	17	30	1	30	17	14
17	13	17	14	15	30	14	7	30	8	4	18	30	18	2	13	17	17	4	11	4	8	13	4	0	0	12
30	24	24	6	7	0	17	12	8	18	2	0	19	4	19	4	30	4	17	0	30	12	20	17	19	13	27

Translating the integers into characters produces,

Decrypted Plaintext Matrix

f	m		p	r	i	l	i	s	t		e	r	o	l			m		y	r	p	e	m	s		d
o	a	c	t	a	c	g	t	,		n	s	y		e	o	o	o	v		g	r		b		r	o
r	n	r	o	p		o	h		i	e	s		s	c	n	r	r	e	l	e	i	n	e	a	a	m
	y	y	g	h	a	r	m	i	s	c	a	t	e	t	e		e	r	a		m	u	r	t	n	.

The decrypted text is therefore:

“for many cryptographic algorithms, it is necessary to select one or more very large prime numbers at random.”