Lecture 9.5

It is important to Note that, despite its good diffusion properties, the Hill cipher is NOT secure. The cipher has many weakness. For one, because $A0=0$, a block of spaces in the plaintext will always be encrypted as a block of spaces in the ciphertext, regardless of the encryption matrix A. More importantly, the cipher is subject to a so-called known plaintext attack. If an eavesdropper intercepts some ciphertext for which a small amount of the corresponding plaintext happens to be known, it is immediately possible to recover the key and therefore decrypt the rest of the Cipertext.

Example

Example Eve intercepts the following encrypted message sent by Alice

"EFNOR. AHIFNEPL.TSZS, RSKT. ZBBRFVUPF VZLFHNTV"

Eve knows that Alice uses a Hill cipher with block length 3, but she does not know the secret encryption matrix. Eve also knows that Alice begins all of her correspondence with "My dear love". Decrypt the message.

Solution (1) EFN, OR., AHI

$\updownarrow$

(5, 6, 14), (15, 18, 28), (1, 8, 9) ciphertext block.

(2) The first three blocks of the plaintext:

MY␣ DEAR␣ L

$\updownarrow$

(13, 25, 0), (4, 5, 1), (18, 0, 2) plaintext block

$\Rightarrow$

$$A^{-1}\begin{bmatrix}5\\6\\14\end{bmatrix}=\begin{bmatrix}13\\25\\0\end{bmatrix}, \quad A^{-1}\begin{bmatrix}15\\18\\28\end{bmatrix}=\begin{bmatrix}4\\5\\1\end{bmatrix}, \quad A^{-1}\begin{bmatrix}1\\8\\9\end{bmatrix}=\begin{bmatrix}18\\0\\12\end{bmatrix}$$

Since ~~Alice~~ Eve remembers the column method of matrix multiplication, she knows that these three equations can be written as a single equation in a matrix form:

$$A^{-1}\underbrace{\begin{bmatrix}5 & 15 & 1\\6 & 18 & 8\\14 & 28 & 9\end{bmatrix}}_{C} = \underbrace{\begin{bmatrix}13 & 4 & 18\\25 & 5 & 0\\0 & 1 & 12\end{bmatrix}}_{P}$$

C: cipher text

P: plain text

$$\therefore \quad A^{-1} = P \cdot C^{-1}, \quad \text{if } C \text{ is invertible}$$

~~Eve~~ Compute $C^{-1} = \begin{bmatrix}5 & 15 & 1\\6 & 18 & 8\\14 & 28 & 9\end{bmatrix}^{-1} = \begin{bmatrix}19 & 8 & 23\\0 & 5 & 2\\22 & 1 & 0\end{bmatrix}$

This allows Eve to compute the decryption matrix:

$$A^{-1} = PC^{-1} = \begin{bmatrix}13 & 4 & 18\\25 & 5 & 0\\0 & 1 & 12\end{bmatrix} \cdot \begin{bmatrix}19 & 8 & 23\\0 & 5 & 2\\22 & 1 & 0\end{bmatrix} = \begin{bmatrix}5 & 26 & 17\\11 & 22 & 5\\3 & 17 & 2\end{bmatrix}$$

Using A^{-1}, Eve can now decrypt Alice's entire message:

"My dear love, run away with me at midnight."

As indicated in the example, the Hill cipher is NOT secure at all. The main problem is that the cipher is linear: each component of ~~the~~ a ciphertext block is a simple linear combination of the components of the plaintext block. This linearity property allows Eve to break the cipher by solving a system of linear equations.

For this reason, all modern block ciphers have a non-linear component. Often this takes the form of so-called S-boxes. An S-box is an operation that scrambles the symbols of the alphabet in a non-linear way. For example, consider the following S-box: an operation from $\mathbb{Z}_{29}$ to $\mathbb{Z}_{29}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
S(x)	17	9	27	2	20	12	21	26	16	18	4	24	23	7	19	14	28	29	1	15	10	22	6	5	25	11	13	3	8

- A ... diffusion matrix.
- ~~The~~ Carrying out the three basic steps: Key mixing, diffusion, S-box is called a round.
- The more round a block cipher has, the better its diffusion and non-linearity properties.

Example Encrypt the message "I like math" using the above block cipher, and the key

1, 1, 3, 3, 5, 5, 7, 7, 9, 9, 11, 11

Solution

I like Math

↓

(9, 0, 12), (9, 11, 5), (0, 13, 1), (20, 8, 0)

↓ Key missing + $\begin{bmatrix} 1 \\ 1 \\ 3 \end{bmatrix}$

(10, 1, 15), (10, 12, 8), (1, 14, 4), (21, 9, 3)

↓ Diffion: multiply by A

(28, 3, 9), ...

Def. A toy block cipher : on alphabet $\mathbb{Z}_{29}$ with block size 3.

The key : 12 elements $k_1, k_2, \cdots, k_{12}$ in $\mathbb{Z}_{29}$.

To encrypt a ~~ptext~~ plaintext block, regard the block as a 3-dim. column vector.

Then repeat the following steps 3 times. All operations are carried out modulo 29.

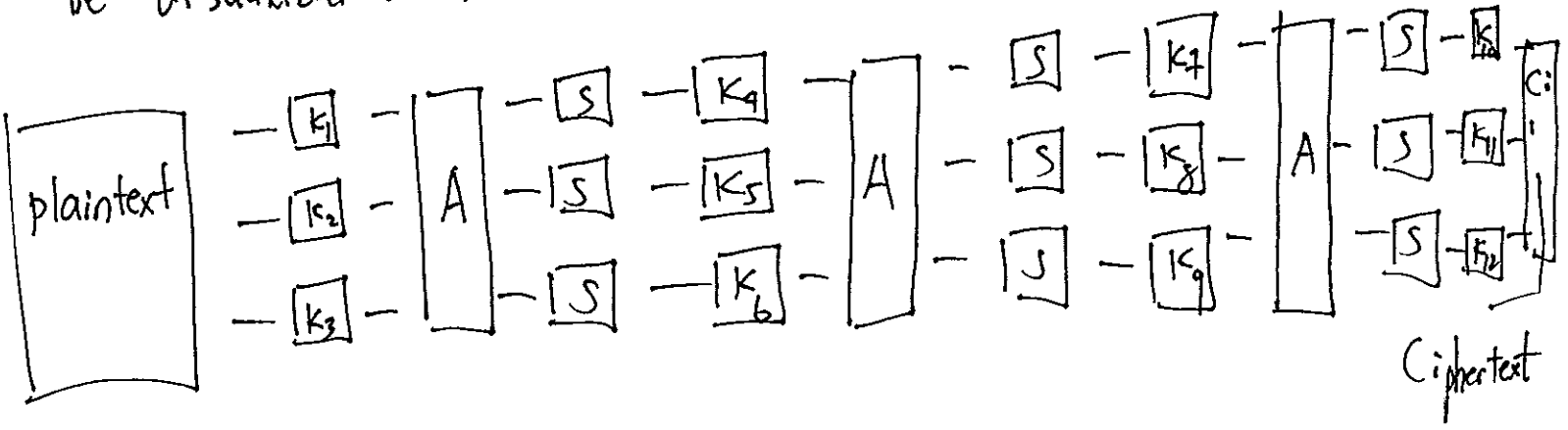
1. Key mixing : add the next three components of the key to the component of the vector.
2. diffusion : multiply the vector by the fixed 3×3 matrix A

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

3. S-box application : Apply S-box to each component of the vector.

Finally apply one ~~one~~ more key mixing at the end.

The resulting vector is the cipher text block. The cipher can be visualized as follows:



↓ S-box

Round 1 ~~[8 6 2]~~ (8, 2, 18), ...

↓ key mixing $\begin{bmatrix} 3 \\ 5 \\ 5 \end{bmatrix}$

(11, 7, 23)

↓ Diffusion

(7, 28, 8)

↓ S-box

Round 2 (26, 8, 16)

↓ key mixing $\begin{bmatrix} 7 \\ 7 \\ 9 \end{bmatrix}$

(4, 15, 25)

↓ Diffusion

(22, 19, 20)

↓ S-box

Round 3 (6, 15, 10)

↓ key mixing $\begin{bmatrix} 9 \\ 11 \\ 11 \end{bmatrix}$

(15, 26, 21)

Repeat the same procedure with the remaing blocks:

Cipher ~~text~~ block: (15, 26, 21), (7, 24, 1), (2, 16, 23), (7, 20, 22)

Ciphertex: "OZUGXABPWGTV"

The cipher actually uses in the real world:

AES, the advanced encryption standard.

- alphabet size, block size, number of rounds, design of s-boxes, ... differ.
- However the basic structure is the same/similar.
- AES use: alphabet size: 256
  block size: between 16 and 32 bytes.
  S-box: complicated.

Extra-credit: Exercise 4.9.4, 4.9.5