暨南大學
JINAN UNIVERSITY

Lecture 2 – Supplement

-Cryptographic Algorithms and Protocols

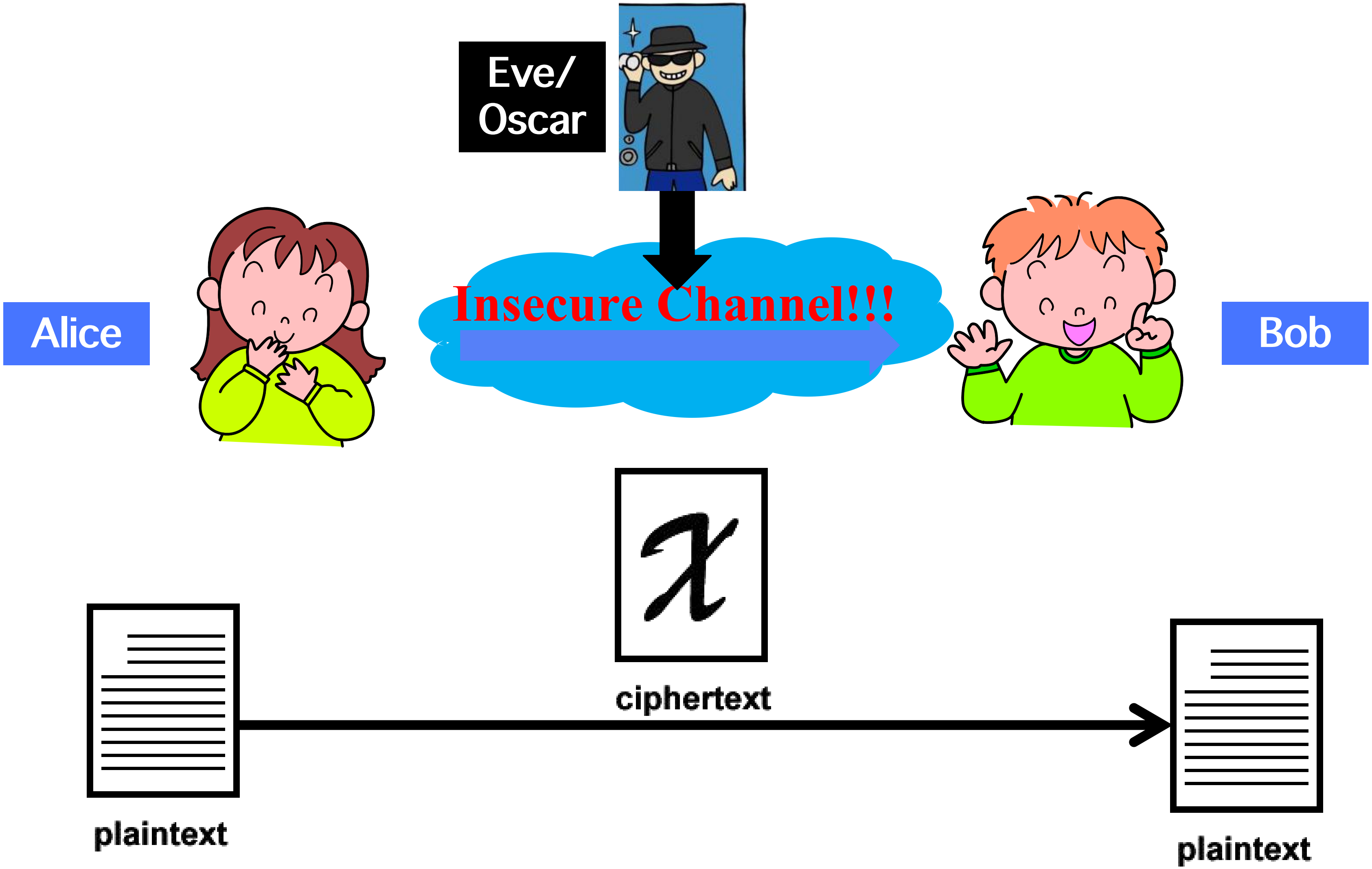
Huang, Xiujie (黄秀姐)

Office: Nanhai Building, #411

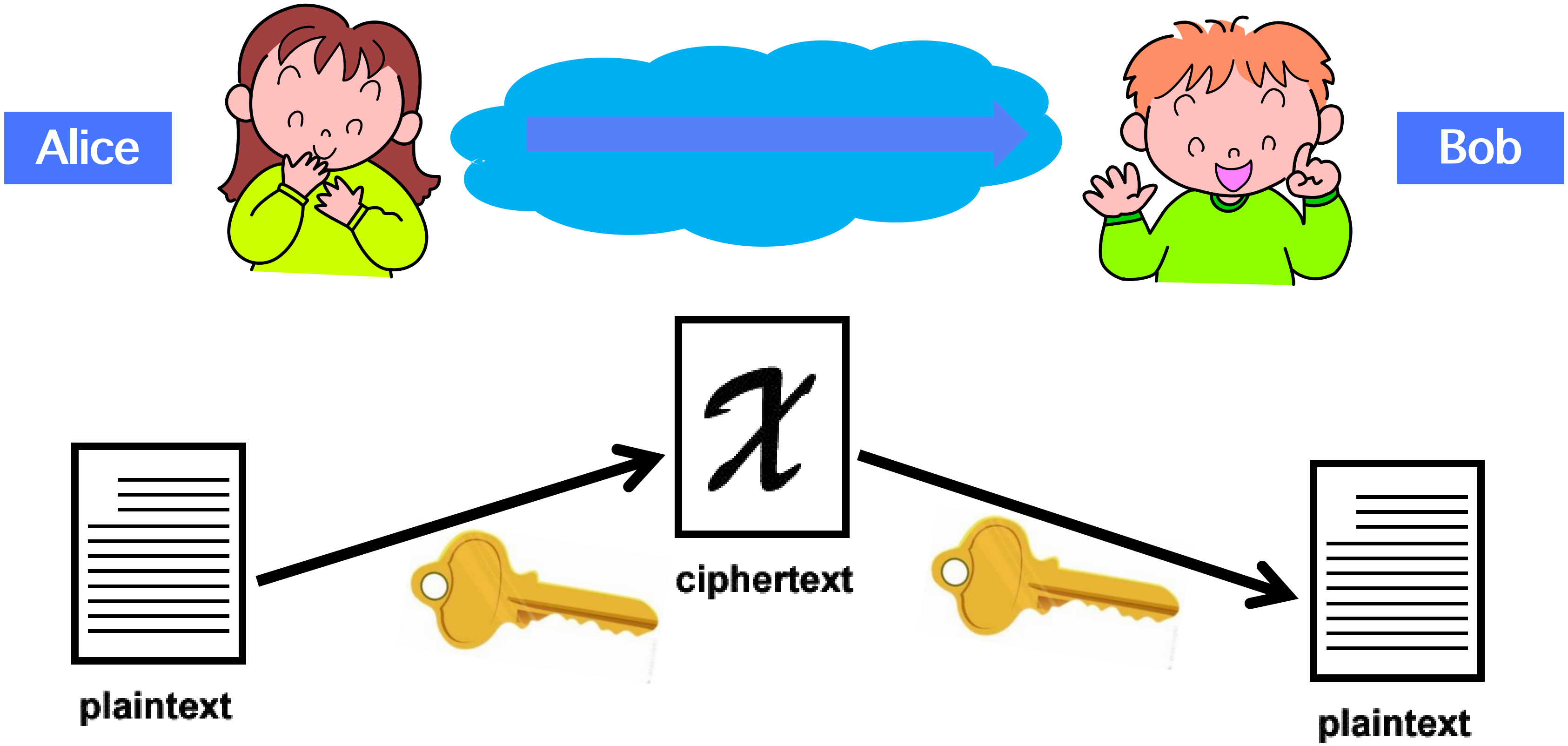
E-mail: t_xiujie@jnu.edu.cn

Dept. Computer Science

Intuition on Cryptography



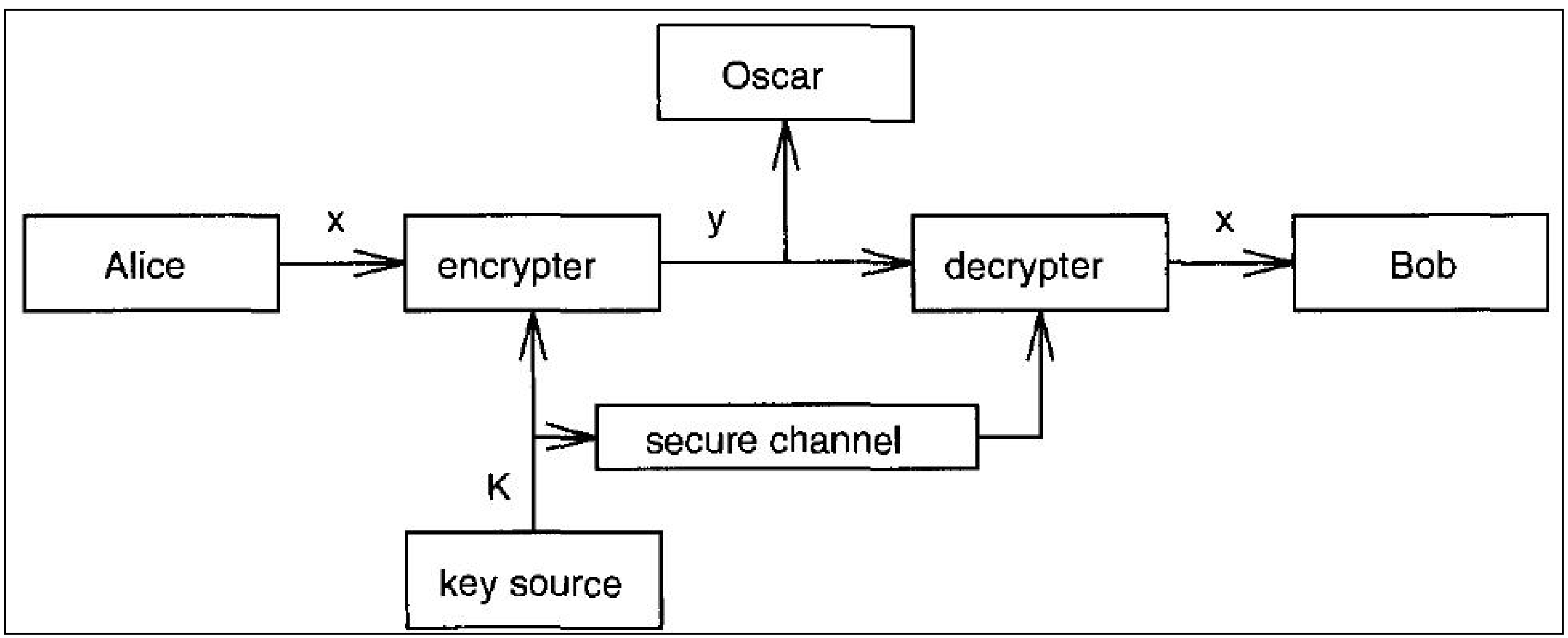
Symmetric-Key Cryptosystem (SKC)



Cryptographic Communication System

Protocol:

- A and B choose a random key K by a secure channel
- A wants to sent a string message $\mathbf{x}=x_1x_2\ldots x_n$
- A computes $y_i=e_K(x_i)$ and the resulting string $\mathbf{y}=y_1y_2\ldots y_n$ is sent over the insecure channel
- B receives $\mathbf{y}=y_1y_2\ldots y_n$ and decrypts $x_i=d_K(y_i)$ to obtain $\mathbf{x}=x_1x_2\ldots x_n$



Statistical Properties of the English Language

Beker and Piper's Table for
Probabilities of occurrence of the 26 letters

letter	probability	letter	probability
A	.082	N	.067
B	.015	O	.075
C	.028	P	.019
D	.043	Q	.001
E	.127	R	.060
F	.022	S	.063
G	.020	T	.091
H	.061	U	.028
I	.070	V	.010
J	.002	W	.023
K	.008	X	.001
L	.040	Y	.020
M	.024	Z	.001

The thirty most common digrams:

$TH, HE, IN, ER, AN, RE, ED, ON, ES, ST,$
$EN, AT, TO, NT, HA, ND, OU, EA, NG, AS,$
$OR, TI, IS, ET, IT, AR, TE, SE, HI, OF.$

The twelve most common trigrams:

$THE, ING, AND, HER, ERE, ENT,$
$THA, NTH, WAS, ETH, FOR, DTH.$

Ciphertext-only attack on the Substitution Cipher

- **See Example 2.11 on Pages 42-44.**
  Ciphertext from a substitution cipher:

```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

letter	frequency	letter	frequency
A	0	N	9
B	1	O	0
C	15	P	1
D	13	Q	4
E	7	R	10
F	11	S	3
G	1	T	2
H	4	U	5
I	5	V	5
J	11	W	8
K	1	X	6
L	0	Y	10
M	16	Z	20

Stage 2: Look at digrams, especially those of the form –Z or Z-.

$$d_K(W) = d.$$

Stage 1

$$d_K(Z) = e$$

C, D, F, J, M, R, Y

t, a, o, i, n, s, h, r

Ciphertext-only attack on the Substitution Cipher

- **See Example 2.11 on Pages 42-44.**
  Ciphertext from a substitution cipher:

```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Our friend from Paris examined his empty glass with surprise, as if evaporation had taken place while he wasn't looking. I poured some more wine and he settled back in his chair, face tilted up towards the sun.[1]

Attack on Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Jack

Key K =1

MFUVTNFFUBUFJHIU

MEETING

letusmeetateight

Lucy

Ciphertext-only attack on the Affine cipher

- See Example 2.10 on Pages 41-42.

Ciphertext from an Affine cipher:

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH $e_K(x) = ax + b$

letter	frequency	letter	frequency
A	2	N	1
B	1	O	1
C	0	P	2
D	7	Q	0
E	5	R	8
F	4	S	3
G	0	T	0
H	5	U	2
I	0	V	4
J	0	W	0
K	5	X	2
L	2	Y	1
M	2	Z	0

Beker and Piper's statistical table

letter	probability	letter	probability
A	.082	N	.067
B	.015	O	.075
C	.028	P	.019
D	.043	Q	.001
E	.127	R	.060
F	.022	S	.063
G	.020	T	.091
H	.061	U	.028
I	.070	V	.010
J	.002	W	.023
K	.008	X	.001
L	.040	Y	.020
M	.024	Z	.001

Ciphertext-only attack on the Affine cipher

- **See Example 2.10 on Pages 41-42.**
  Ciphertext from an Affine cipher:

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH

$$e_K(x) = ax + b$$

~~Try~~ 1: R is the encryp- tion of e and D is the encryption of t

$$\begin{cases} e_K(4) = 17 \\ e_K(19) = 3 \end{cases} \qquad \begin{cases} 4a + b = 17 \\ 19a + b = 3. \end{cases} \Rightarrow a = 6, b = 19 \text{ (in } \mathbb{Z}_{26})$$

$$\gcd(a, 26) = 2 > 1$$

~~Try~~ 2: R is the encryption of e and E is the encryption of t $\Rightarrow$ $a = 13$

~~Try~~ 3: R is the encryption of e and H is the encryption of t $\Rightarrow$ $a = 8$

Try 4: R is the encryption of e and K is the encryption of t

$\Rightarrow$ $a = 3, b = 5$ $\Rightarrow$ $d_K(y) = 9y - 19$

$\Rightarrow$ algorithmsarequitegeneraldefinitionsofarit
hmeticprocesses

Permutation Cipher - Example 2.7

Suppose $m = 6$ and the key is the following permutation π:

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

$$K_\pi = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

we see that the permutation π^{-1} is the following:

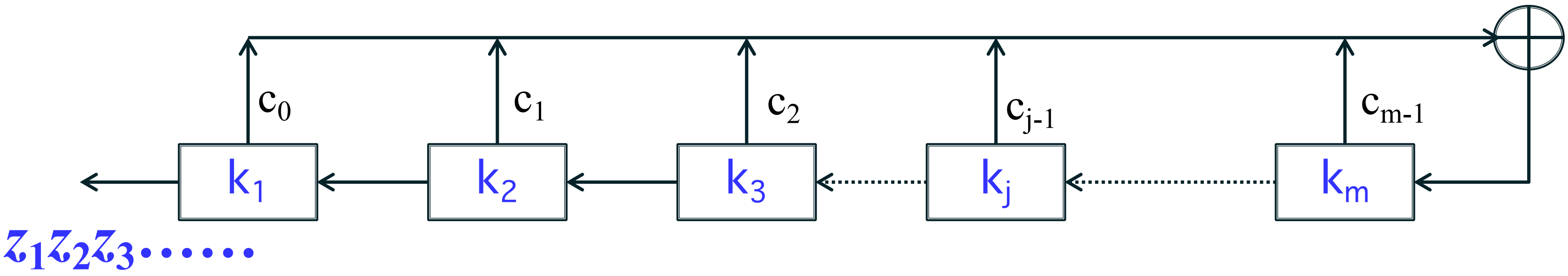
x	1	2	3	4	5	6
$\pi^{-1}(x)$	3	6	1	5	2	4

Plaintext: sheseIlsseashellsbytheseashore.

Partition: shesel | lsseas | hellsb | ythese | ashore

Encryption: EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS

General LFSR of Binary Steam Ciphers



$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \mod 2$$

Stream Ciphers - Example 2.8

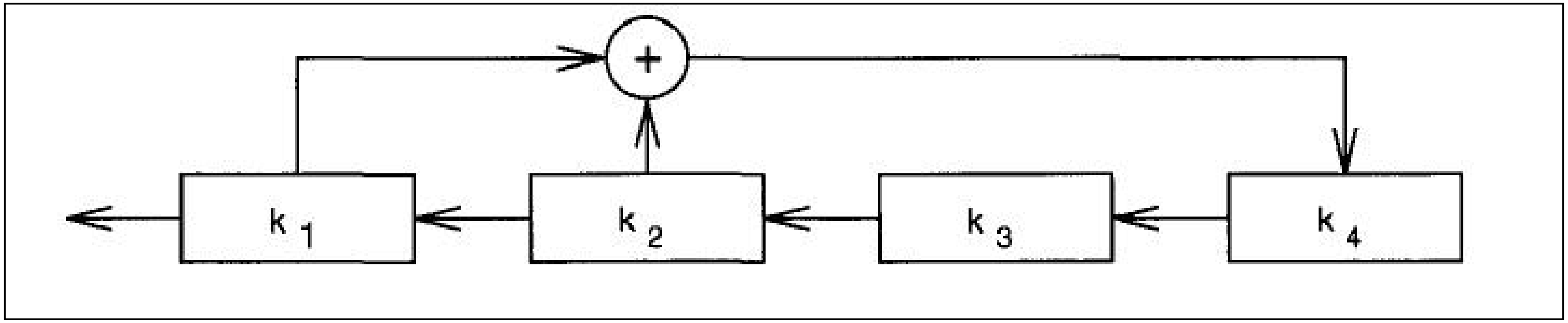
Suppose $m = 4$ and the keystream is generated using the linear recurrence

$$\boxed{z_{i+4} = (z_i + z_{i+1}) \bmod 2,}$$

$i \geq 1$. If the keystream is initialized with any vector other than $(0, 0, 0, 0)$, then we obtain a keystream of period 15. For example, starting with $(1, 0, 0, 0)$, the keystream is

$$\boxed{1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1 \cdots .}$$

Any other non-zero initialization vector will give rise to a cyclic permutation of the same keystream. □



Known-plaintext attack on the LFSR Stream cipher

Oscar has a plaintext string $x_1 x_2 \cdots x_n$

and the corresponding ciphertext string $y_1 y_2 \cdots y_n$

Encryption rule: $y_i = (x_i + z_i) \bmod 2.$

Keystream generator: $z_{m+i} = \sum_{j=0}^{m-1} c_j z_{i+j} \bmod 2$

$(z_1, \ldots, z_m) = (k_1, \ldots, k_m)$

KEY? $\boxed{k_1, k_2, \cdots, k_m; c_0, c_1 \cdots, c_{m-1}}$

Then he can compute the keystream bits $z_i = (x_i + y_i) \bmod 2$

$\longrightarrow (k_1, k_2, \ldots, k_m) = (z_1, z_2, \ldots, z_m)$

Known-plaintext attack on the LFSR Stream cipher

$\boxed{c_0, c_1 \cdots, c_{m-1}}$ **?**

$$z_{m+i} = \sum_{j=0}^{m-1} c_j z_{i+j} \bmod 2$$

$$(z_{m+1}, z_{m+2}, \ldots, z_{2m}) = (c_0, c_1, \ldots, c_{m-1}) \begin{pmatrix} z_1 & z_2 & \cdots & z_m \\ z_2 & z_3 & \cdots & z_{m+1} \\ \vdots & \vdots & & \vdots \\ z_m & z_{m+1} & \cdots & z_{2m-1} \end{pmatrix}$$

$\Downarrow$

$$(c_0, c_1, \ldots, c_{m-1}) = (z_{m+1}, z_{m+2}, \ldots, z_{2m}) \begin{pmatrix} z_1 & z_2 & \cdots & z_m \\ z_2 & z_3 & \cdots & z_{m+1} \\ \vdots & \vdots & & \vdots \\ z_m & z_{m+1} & \cdots & z_{2m-1} \end{pmatrix}^{-1}$$

Autokey Cipher - Example 2.9

Suppose the key is $K = 8$, and the plaintext is

Plaintext:	rendezvous.
Integers of Plaintext:	17 4 13 3 4 25 21 14 20 18
Keystream:	8 17 4 13 3 4 25 21 14 20
Encryption:	25 21 17 16 7 3 20 9 8 12
Ciphertext:	ZVRQHDUJIM.