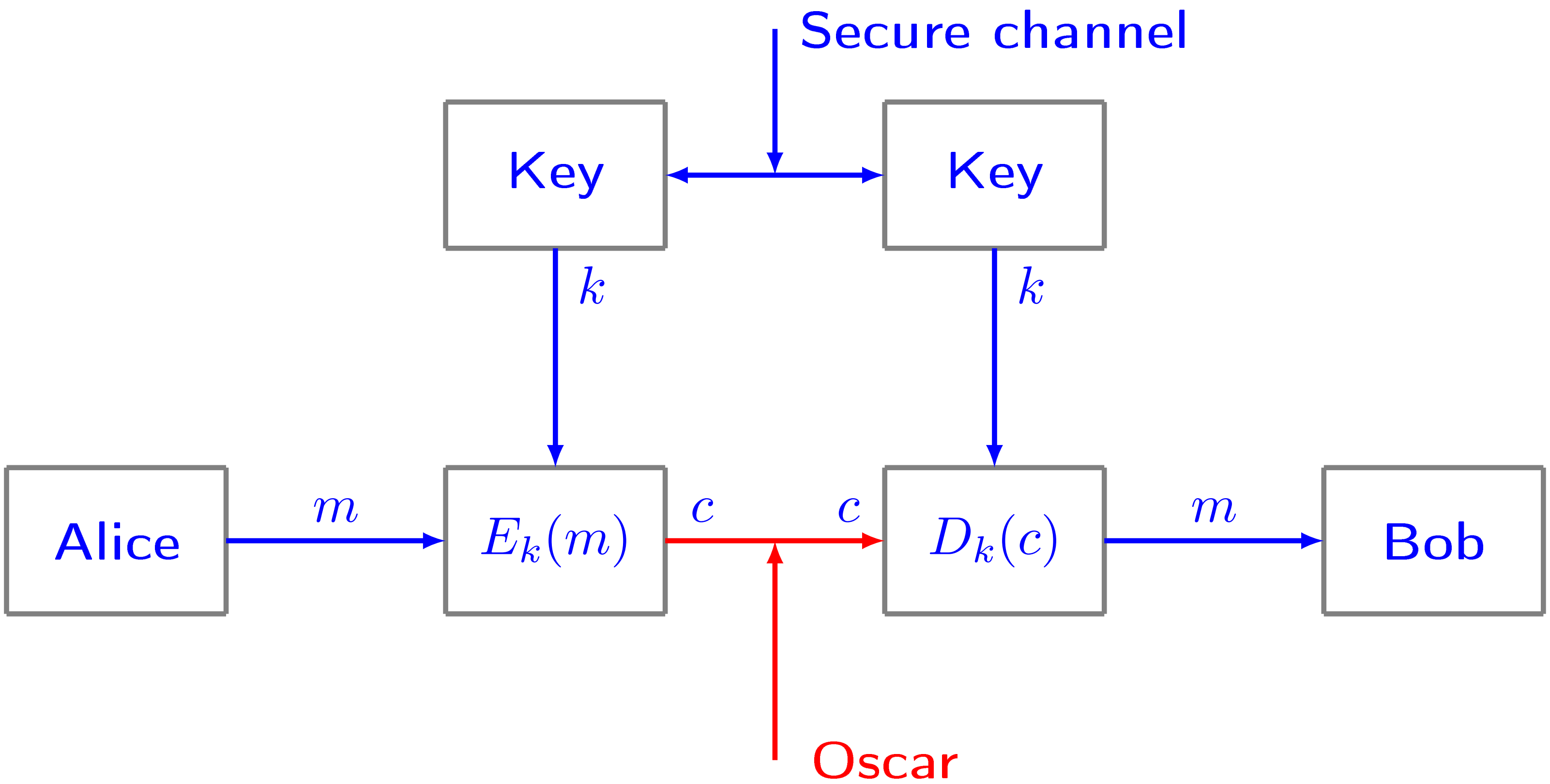
Elementary Cryptosystems

1. The General Cryptographic Model



Definition. A cryptosystem is an ordered five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ where

- $\mathcal{P}$ is a finite set of plaintexts;
- $\mathcal{C}$ is a finite set of cryptotexts;
- $\mathcal{K}$ is a finite set of keys;
- $\mathcal{E} = \{E_k : \mathcal{P} \to \mathcal{C}\}$ and $\mathcal{D} = \{D_k : \mathcal{C} \to \mathcal{P}\}$ are sets of enciphering transformations and deciphering transformations indexed by the elements of $\mathcal{K}$ with the property $D_k(E_k(x)) = x$ for every $x \in \mathcal{P}$ and every $k \in \mathcal{K}$.

Sometimes we require also the property $E_k(D_k(x)) = x$ for every $x \in \mathcal{P}$ and every $k \in \mathcal{K}$.

2. Some Symmetric Cryptosystems

2.1. Simple substitution

Caesar's cipher

I	C	A	M	E	I	S	A	W	I	C	O	N	Q	U	E	R	E	D
L	F	D	P	H	L	V	D	Z	L	F	R	Q	T	X	H	U	H	G

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$$

$$\begin{aligned} E_k(x) &= x + k \pmod{26}, \\ D_k(y) &= y - k \pmod{26}. \end{aligned}$$

For Caesar we have $k = 3$

Encoding: $\mathrm{A} \to 0, \mathrm{B} \to 1, \mathrm{C} \to 2, \ldots, \mathrm{Z} \to 25$.

affine cipher

$$
\begin{aligned}
\mathcal{P} &= \mathcal{C} = \mathbb{Z}_{26}, \\
\mathcal{K} &= \{k = (a, b) \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}\}, \\
|\mathcal{K}| &= \varphi(26) \cdot 26 = 12 \cdot 26 = 312, \\
E_k(x) &= ax + b \pmod{26}, \\
D_k(y) &= a^{-1}(y - b) \pmod{26}.
\end{aligned}
$$

Example: For $k = (7, 3)$ we have

$E_k(x) = 7x+3$, and $D_k(y) = 7^{-1}(y-3) = 15(y-3) = 15y-19 = 15y+7$.

Thm 1. Let $a \neq 0$, b and $m \neq 0$ be integers and consider the congruence (*) $ax \equiv b \pmod{m}$. Then

(i) (*) has a solution iff $\gcd(a, m)$ divides b;

(ii) if (*) has a solution it has exactly $d = \gcd(a, m)$ different solutions;

(iii) if x_0 is a solution to (*) and $m = m'd$ then all solutions are given by $x = x_0 + km'$, where $k = 0, 1, \ldots, d - 1$.

general simple substitution

$\mathcal{P} = \mathcal{C} = \mathcal{X} = \{A, \ldots, Z\}$,

$\mathcal{K} = S_{\mathcal{X}}$

$E_\pi(x) = \pi(x)$;

$D_\pi(y) = \pi^{-1}(y)$.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
T U R I N G M A C H E B D F J K L O P Q S V W X Y Z
```

```
P E A R L H A R B O U R
K N T O B A T O U J S O
```

2.2. Playfair

C	R	Y	P	T
O	E	N	I	G
M	A	B	D	F
H	K	L	Q	S
U	V	W	X	Z

Plaintext:	CR	YP	TO	GR	AP	HY
Cryptotext:	RY	PT	CG	ET	DR	LC

2.3. Vigenére

- $m \in \mathbb{Z}^+$
- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$, $\mathcal{K} = \mathbb{Z}_{26}^m$,
- Let $(x_1, \ldots, x_m)$ be a message and let $k = (k_1, \ldots, k_m)$ be a key.
- Enciphering:

$$E_k(x_1, \ldots, x_m) = (x_1 + k_1 \pmod{26}, \ldots, x_m + k_m \pmod{26}).$$

- Deciphering:

$$D_k(y_1, \ldots, y_m) = (y_1 - k_1 \pmod{26}, \ldots, y_m - k_m \pmod{26}).$$

Example.

Plaintext: THIS CRYPTOSYSTEM IS NOT SECURE

Key: CIPHER

T	H	I	S	C	R	Y	P	T	O	S	Y	S	T	E	M
19	7	8	18	2	17	24	15	19	14	18	24	18	19	4	12
C	I	P	H	E	R	C	I	P	H	E	R	C	I	P	H
2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7
21	15	23	25	6	8	0	23	8	21	22	15	20	1	19	19
V	P	X	Z	G	I	A	X	I	V	W	P	U	B	T	T

Cryptotext: VPXZGIAXIVWPUBTT...

2.4. Hill's cipher

$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$, $m \in \mathbb{N}$ -fixed.

$\mathcal{K} =$ the invertible $m \times m$ matrices over $\mathbb{Z}_{26}$

$$
\begin{aligned}
E_k(x) &= xK \pmod{26}, \\
D_k(y) &= yK^{-1} \pmod{26}.
\end{aligned}
$$

Example.

$$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}, \; K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

JULY $\longrightarrow (9, 20, 11, 24)$

$$
\begin{aligned}
(9,20)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} &= (3,4) \rightarrow \mathrm{DE} \\
(11,24)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} &= (11,22) \rightarrow \mathrm{LW} \\
(3,4)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} &= (9,20) \rightarrow \mathrm{JU} \\
(11,22)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} &= (11,24) \rightarrow \mathrm{LY}
\end{aligned}
$$

Example.

$$K = \begin{pmatrix} 9 & 5 & 0 \\ 0 & 1 & 3 \\ 5 & 18 & 2 \end{pmatrix}, \; K^{-1} = \begin{pmatrix} 0 & 12 & -5 \\ -5 & -6 & 9 \\ -7 & 11 & -3 \end{pmatrix}$$

LONDON $\longrightarrow (11, 14, 13, 3, 14, 13)$

$$(11,14,13)\begin{pmatrix} 9 & 5 & 0 \\ 0 & 1 & 3 \\ 5 & 18 & 2 \end{pmatrix} = (8,17,16) \to \text{ISQ}$$

$$(3,14,13)\begin{pmatrix} 9 & 5 & 0 \\ 0 & 1 & 3 \\ 5 & 18 & 2 \end{pmatrix} = (14,13,16) \to \text{ODQ}$$

$$(8,17,16)\begin{pmatrix} 0 & 12 & -5 \\ -5 & -6 & 9 \\ -7 & 11 & -3 \end{pmatrix} = (11,14,13) \to \text{LON}$$

$$(14,3,16)\begin{pmatrix} 0 & 12 & -5 \\ -5 & -6 & 9 \\ -7 & 11 & -3 \end{pmatrix} = (3,14,13) \to \text{DON}$$

2.5. One time pad

- Alice wishes to send Bob n messages which are zero or one.
- Sometime earlier Alice and Bob met and flipped an unbiased coin n times.
- They both recorded the sequence of random tosses as a string $k \in \{H, T\}^n$.
- Alice encrypts her messages $m_1, \ldots, m_n$ as follows:

$$c_i = E(m_i) = \begin{cases} m_i, & \text{if } k_i = H, \\ m_i \oplus 1, & \text{if } k_i = T. \end{cases}$$

- Alice then sends the cryptograms $c_1, \ldots, c_n$ to Bob.

- Bob can decrypt easily by

$$m_i = D(c_i) = \begin{cases} c_i, & \text{if } k_i = H, \\ c_i \oplus 1, & \text{if } k_i = T. \end{cases}$$

- The cryptogram reveals no new information about the message.

- The key should be at least as long as the plaintext.

- This holds even if the opponent has **unlimited** computing power.

2.6. Permutation ciphers

Let $\mathcal{X} = \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$ and let $m \geq 2$ be a fixed integer.

Let $\mathcal{P} = \mathcal{C} = \mathcal{X}^m$.

Let $\mathcal{K} = S_m$ (here S_m is the symmetric group acting on $\{1, \ldots, m\}$).

Given a key $\pi \in \mathcal{K}$, the enciphering and deciphering transformations are given by

$$E_\pi(x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(m)})$$

$$D_\pi(y_1, y_2, \ldots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \ldots, y_{\pi^{-1}(m)}),$$

where π^{-1} is the inverse to π.

Example 1. Let $m = 10$ and let the key be

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 9 & 2 & 5 & 8 & 1 & 4 & 10 & 7 \end{pmatrix} = (1\ 3\ 9\ 10\ 7)(2\ 6\ 8\ 4\ )(5).$$

Clearly, $\pi^{-1} = (1\ 7\ 10\ 9\ 3)(2\ 4\ 8\ 6)(5)$

and the plaintext

`T H I S I S T H E W   I N T E R O F O U R   D I S C O N T E N T`

is enciphered to

`I S E H I H T S W T   T O U N R O I E R F   S N N I O E D C T T`

The parameter m is kept secret and can be considered as a part of the key

The general permutation cipher can be considered as a specil case of the Hill cipher.

Set $\mathcal{X} = \mathbb{Z}_{26}$. With every permutation we associate a permutation matrix $K = (k_{ij})_{m \times m}$

$$k_{i,j} = \begin{cases} 1 & \text{if } i = \pi(j), \\ 0 & \text{otherwise.} \end{cases}$$

Clearly,

$$K_\pi^{-1} = K_{\pi^{-1}} = K_\pi^T.$$

so in the example above

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

We have

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10})K = (x_3, x_6, x_9, x_2, x_5, x_8, x_1, x_4, x_{10}, x_7),$$

the permutation of the symbols in any block can be obtained by multiplication by a suitable permutation matrix.

We ca use different euristics:

1) Use a $n \times m$ table:

T	H	I	S	I	S
T	H	E	W	I	N
T	E	R	O	F	O
U	R	D	I	S	C
O	N	T	E	N	T

So the cryptotext is `TTTUO HHERN IERDT SWOIE IIFSN SNOCT`.

The key is the pair (n, m). In this case $k = (5, 6)$.

This is ageneral permutation with key

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & 29 & 30 \\ 1 & 7 & 13 & 19 & \ldots & 24 & 30 \end{pmatrix}.$$

2) Use forbidden fields in the table.

T		H	I	S	I
S	T	H		E	W
I	N	T	E	R	
O	F		O	U	R
D	I	S	C		O
	N	T	E	N	T

The cryptotext is `TSIOD TNFIN HHTST IEOCE SERUN IWROT`.

3) Another possibility: columnar transposition using a codeword.

Take e.g. `TABLE`.

T	A	B	L	E
5	1	2	4	3
T	H	I	S	I
S	T	H	E	W
I	N	T	E	R
O	F	O	U	R
D	I	S	C	O
N	T	E	N	T

The cryptotext is `HTNFI TIHTO SEIWR ROTSE EUCNT SIODN`.

2.7. Stream Ciphers

Idea: Use the key k to generate a sequence $z_1, z_2, z_3, \ldots$ called a called a key sequence that is used further to encipher the plaintext:

$$y = y_1 y_2 y_3 \ldots = E_{z_1}(x_1) E_{z_2}(x_2) E_{z_3}(x_3) \ldots.$$

The element z_i is obtained as the value of some function that depends on the key k and the first $i-1$ plaintexts

$$z_i = f_i(k, x_1, \ldots, x_{i-1}).$$

The enciphering transformations are indexed not by the elements of $\mathcal{K}$, but by the elements of the key sequence z_i.

Def. A stream cipher is an ordered 7-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{F}, \mathcal{E}, \mathcal{D})$, where $\mathcal{P}$ and $\mathcal{C}$ are the sets of plaintexts and ciphertexts, respecitively, $\mathcal{K}$ is the keyset, $\mathcal{L}$ is the alphabet of the key stream, and $\mathcal{F}$ is a sequence of functions $f_1, f_2, f_3, \ldots$, where

$$f_i : \mathcal{K} \times \mathcal{P}^{i-1} \to \mathcal{L}.$$

For every $z \in \mathcal{L}$ there exist an enciphering rule $E_z \in \mathcal{E}$ and a deciphering rule $D_z \in \mathcal{D}$:

$$E_z : \mathcal{P} \to \mathcal{C}, \quad D_z : \mathcal{C} \to \mathcal{P},$$

which satisfy $D_z(E_z(x)) = x$ for every $x \in \mathcal{P}$.

The diffrence from the general definition of a cryptosystem is that the enciphering and deciphering transformations depend on the key sequence and not directly on the key k.

Block ciphers can be considered as a special case of stream ciphers with $z_i = k$ for all $i \geq 1$.

A stream cipher is said to be sinchronous if the key sequence $z_1, z_2, z_3, \dots$ does not depend on the plaintext,i.e. $f_i : \mathcal{K} \to \mathcal{L}$.

A stream cipher for which the key sequence depends on the plaintext is called asynchronous.

A stream cipher is called periodic with period d if $z_{i+d} = z_i$ for all $i \geq 1$.

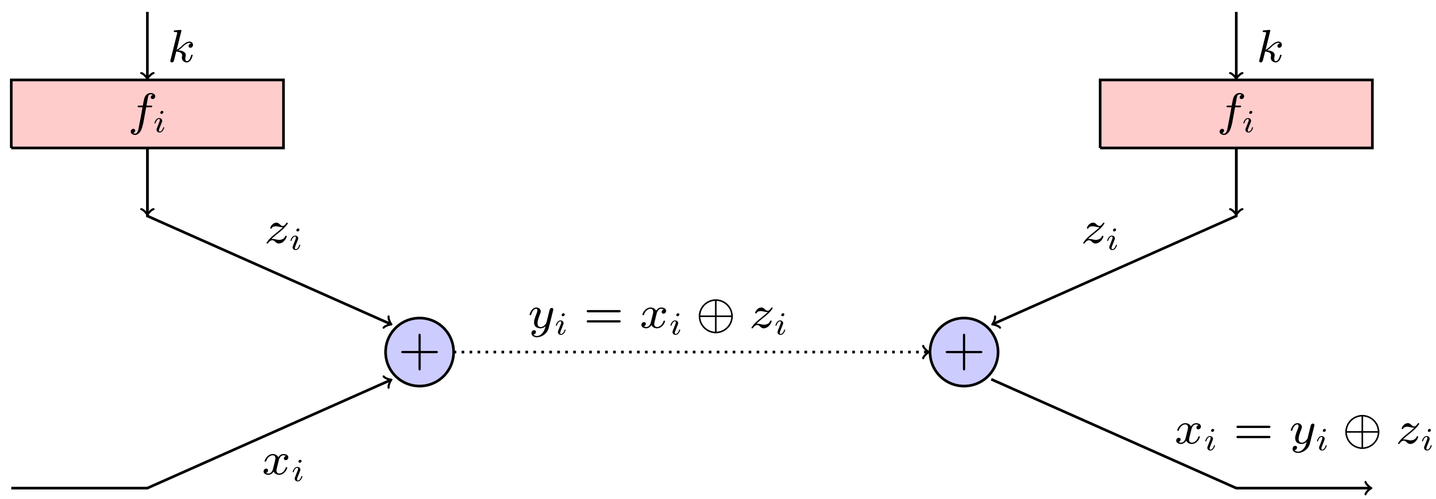
Some times we may the existence of a preperiod, i.e. $z_{i+d} = z_i$ for all $i \geq n_0$.

In the case of Vigenère's cipher with key $k = (k_1, \dots, k_m)$ we have a sinchronous cipher with $z_{jm+i} = k_i, i = 1, \dots, m$, for $j = 1, 2, \dots$. Here, the enciphering and the deciphering transformations indexed with z are $E_z(x) = x + z$ and $D_z(y) = y - z$, addition and multipliction are performed in $\mathbb{Z}_{26}$.

Very often stream ciphers are used with binary alphabets, i.e. $\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathbb{Z}_2$. In this case enciphering and deciphering are identical and consist in addition modulo 2:

$$E_z(x) = x \oplus z, \;\; D_z(y) = y \oplus z.$$

The picture below represents such a cipher.


k
f_i
z_i
x_i
$y_i = x_i \oplus z_i$
k
f_i
z_i
$x_i = y_i \oplus z_i$

A possible option to create a (sinchronous) key stream is to use a linear recurrence sequence over $\mathbb{Z}_2$ Let the first m terms of the sequence be fixed:

$$z_0 = b_0, z_1 = b_1, \ldots, z_{m-1} = b_{m-1}$$

and let it satisfy the following recurrence equation:

$$z_{i+m} = c_0 z_i \oplus c_1 z_{i+1} \oplus \ldots \oplus c_{m-i} z_{i+m-1},$$

where $c_, c_1, \ldots, c_{m-1}$ be some suitably chosen constants from $\mathbb{Z}_2$.

W.l.o.g. we assume that $c_0 = 1$; otherwise the recurrence equation is of smaller order than m.

The key is of length $2m$ and consists of the bits $b_0, b_1, \ldots, b_{m-1}$ and $c_0, c_1, \ldots, c_{m-1}$, where $(b_0, \ldots, b_{m-1}) \neq (0, \ldots, 0)$.

For a suitable choice of $c_0, \ldots, c_{m-1}$, the sequence (z_i) has period $2^m - 1$, which is the maximal period that can be achieved.

Linear feedback shift register (LFSR)

A linear feedback shift register consists of m cells $S_0, S_1, \ldots, S_{m-1}$

Each cell contains a binary symbol $\{0, 1\}$.

A LFSR works in discrete moments of time: $t, t+1, t+2, \ldots$.

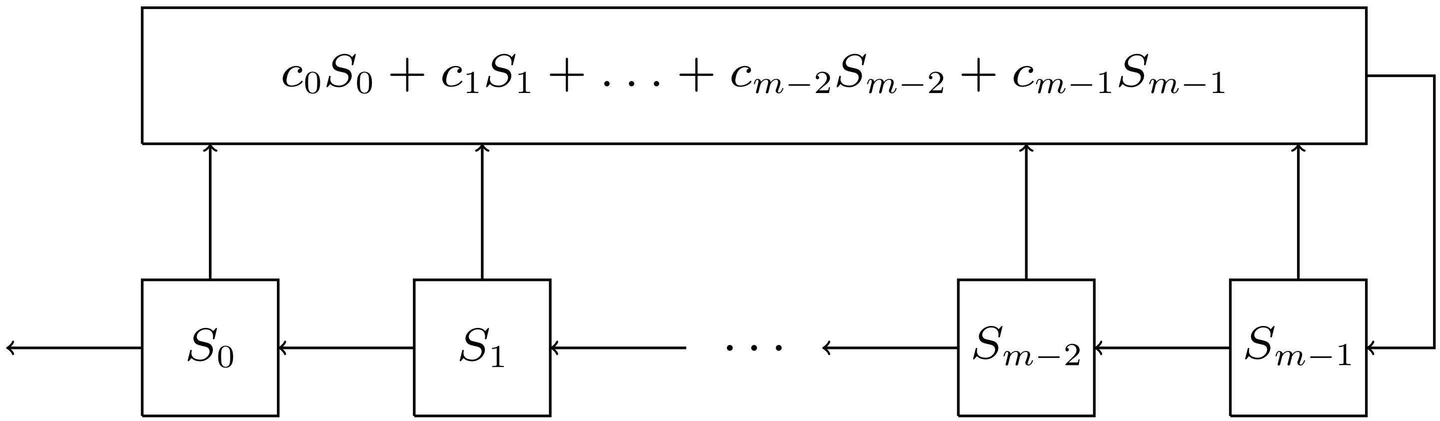
Initially the cells $S_0, \ldots, S_{m-1}$ contain the m-tuple $(b_0, \ldots, b_{m-1})$.

At each step (moment of time) the register performs the following operations:

1) outputs the content of the cell S_0;

2) the content of each of the cells $S_1, \ldots, S_{m-1}$ is moved to the cell to the right, i.e. $S_{i-1} \leftarrow S_i$, $i = 1, \ldots, m-1$;

3) the new value of S_{m-1} is given by $S_{m-1} \leftarrow \sum_{j=0}^{m-1} c_j S_j$.

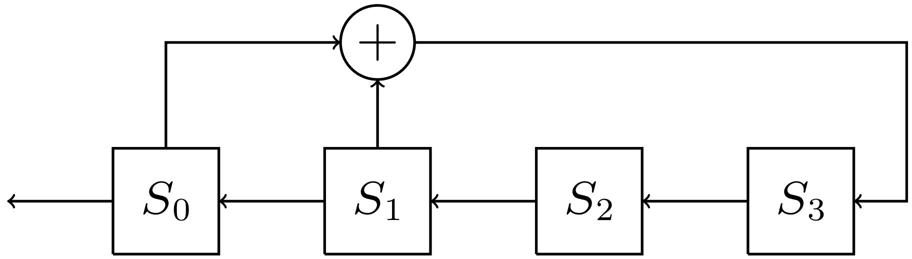


Denote by $S_i(t)$ the content of S_i in moment t.

The work of the shift register can be described by

$$\left| \begin{array}{lcl} S_i(t+1) & = & S_{i+1}(t), \;\; i = 0, \ldots, m-2, \\ S_{m-1}(t+1) & = & c_0 S_0(t) + c_1 S_1(t) + \ldots + c_{m-1} S_{m-1}(t). \end{array} \right.$$

Example 2. Consider a LFSR with$m = 4$ that generates a sequence satisfying the recurrence equation $z_{i+4} = z_i \oplus z_{i+1}$.



If the LFSR contains initially $(b_0, b_1, b_2, b_3) = (1, 0, 0, 0)$, then its work is described by the table below.

t	S_0	S_1	S_2	S_3
0	1	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	1	0	0
4	1	0	0	1
5	0	0	1	1
6	0	1	1	0
7	1	1	0	1
8	1	0	1	0
9	0	1	0	1
10	1	0	1	1
11	0	1	1	1
12	1	1	1	1
13	1	1	1	0
14	1	1	0	0
15	1	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

The first column contains the sequence generated by the register. It has period 15 which is the largest possible period for a register of this size.

$$(1,0,0,0,1,0,0,1,1,0,1,0,1,1,1),1,0,0,0,1,0,0,\ldots.$$

The LFSR that uses the equation

$$z_{i+4} = z_{i+3} + z_{i+2} + z_{i+1} + z_i,$$

generates only a sequence of period 5 for every initial vector.

t	S_0	S_1	S_2	S_3
0	1	0	0	0
1	0	0	0	1
2	0	0	1	1
3	0	1	1	0
4	1	1	0	0
5	1	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

2.8. Autokey

The next cipher is an example for an asynchronous stream cipher The alleged author is Vigenère.

The idea is to use the plaintext as a stream cipher.

Let $m \geq 1$ be a positive integer. Take

$\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathbb{Z}_{26}$, $\mathcal{K} = \mathbb{Z}_{26}^m$.

If the plaintext is $x_0 x_1 x_2 \ldots$, and $K = k_0 k_1 \ldots k_{m-1}$, then we set $z_i = k_i$ for $i = 0, 1, \ldots, m-1$ and $z_i = x_{i-m}$ for $i \geq m$.

The enciphering and deciphering transformations are given by $E_z(x) = x + z \pmod{26}$ and $D_z(y) = y - z \pmod{26}$.

Example 3. Consider an Autokey-cipher with $m = 3$, and key-word MAY$=$ $(14, 0, 24)$.

Plaintext: `thepathoftherighteous`.

Ciphertext: `FHCIHXWOYAVJKPKYBKVNW`:

t	h	e	p	a	t	h	o	f	t	h	e	r	i	g	h	t	e
m	a	y	t	h	e	p	a	t	h	o	f	t	h	e	r	i	g
19	7	4	15	0	19	7	14	5	19	7	4	17	8	6	7	19	4
12	0	24	19	7	4	15	0	19	7	14	5	19	7	4	17	8	6
5	7	2	18	7	23	22	14	24	0	21	9	10	15	10	24	1	10
F	H	C	I	H	X	W	O	Y	A	V	J	K	P	K	Y	B	K

The deciphering is obvious.

We recover the first three letters using the key.

For the remaining letters we use the plaintext already recovered.

ciphertext	key sequence sequence	deciphering	plaintext
F	M	$5 - 12 = 19$	t
H	A	$7 - 0 = 7$	h
C	Y	$2 - 24 = 4$	e
I	T	$8 - 19 = 15$	p
H	H	$7 - 7 = 0$	a
X	E	$23 - 4 = 19$	t
W	P	$22 - 15 = 7$	h
$\vdots$	$\vdots$	$\vdots$	$\vdots$