Transposition cipher

A Latin alphabet

$t > 1$ block size

1) key space all permutations on $1, 2, \dots, t$ (transpositions)

2) encryption

pl.-text

$$m = \underbrace{m_1 m_2 \dots m_t}_{t} \mid \underbrace{m_{t+1} m_{t+2} \dots m_{2t}}_{t} \mid \dots \underbrace{\quad}_{t}$$

$$c = c_1 c_2 \dots c_t \mid c_{t+1} c_{t+2} \dots c_{2t} \mid \dots$$

$$= m_{e(1)} m_{e(2)} \dots m_{e(t)} \mid m_{t+e(1)} m_{t+e(2)} \dots m_{t+e(t)} \mid \dots$$

e encryption key

3) decryption with inversion $d = e^{-1}$

$$m = c_{d(1)} c_{d(2)} \dots c_{d(t)} \mid c_{t+d(1)} \dots c_{t+d(t)} \mid \dots$$

$$c_{d(i)} = m_{e(d(i))} = m_i$$

$$c_{t+d(i)} = m_{t+e(d(i))} = m_{t+i}$$

...

Cryptanalysis.

observation: represent pl.-text as an array with t columns:

$$\begin{vmatrix} m_1 & m_2 & \dots & m_t \\ m_{t+1} & m_{t+2} & \dots & m_{2t} \\ \dots & & & \end{vmatrix} \xrightarrow{\text{perm. of columns acc. to } e} (*) \begin{vmatrix} m_{e(1)} & m_{e(2)} & \dots & m_{e(t)} \\ m_{t+e(1)} & \dots & & m_{t+e(t)} \\ \dots & & & \end{vmatrix}$$

...		
$m_{(s-1)t+1}\ m_{(s-1)t+2} \ldots m_{s\cdot t}$	<---- cryptanalysis	$m_{(s-1)t+c(1)} \ldots m_{(s-1)t+c(t)}$

for pl.-text of size $s \cdot t$ characters

problem: given cipher-text recover pl.-text

---

t may be secret.

belongs to a reasonable range as $20 \le t \le 50$

$\Rightarrow$ assume t is known

Algorithm

1. cipher-text into an array with t columns, like (*).

2. try to find in a row a permuted word or a common syllabus like
   - tRat
   - tRe
   - tRere is
   - tRere are
   - tion
   - ...

   permute back relevant columns to get this word (guess)

3. check the guess with other rows

   e.g.

t	R	a	t	
t	i	o	n	

part of a word $\Rightarrow$ guess was probably correct

4. extend the guesses to finally decrypt the cipher-text.

Example. cipher-text of 30 characters and $t = 10$

1	2	3	4	5	6	7	8	9	10
R	a	t	e	n	c	a	e	t	d
y	n	o	s	t	a	i	p	z	t
d	s	k	o	n	x	d	a	n	z

tRe in the first row

t	3,9
R	1
e	4,8

overall 4 possibilities for the

3	1	4
t	R	e
o	y	s
k	d	o

3	1	8
t	R	e
o	y	p
k	d	a

9	1	4
t	R	e
z	y	s
n	d	o

9	1	6
t	R	e
z	y	p
n	d	a

tion in the second row

t	5, 10
i	7
o	3
n	2

2 possibilities

5	7	3	2
n	a	t	a
t	i	o	n
n	d	k	s

or

10	7	3	2
d	a	t	a
t	i	o	n
z	d	k	s

← English word.

⇒

9	1	4	10	7	3	2
t	R	e	d	a	t	a
z	y	s	t	i	o	n
n	d	o	z	d	k	s

5	6	8
n	c	e
t	a	p
n	x	a

not sensible.

⇒

9	1	8	10	7	3	2
t	R	e	d	a	t	a
z	y	p	t	i	o	n

4	5	6
e	n	c
s	t	a

⇒ plain-text

padding.

Cryptanalysis is effective if
N c-text length $\geq 3 \cdot t$ (2t still may work)

---

double transposition
by Norwegian Resistance during WW1.

apply two transpositions with
block size t_1, t_2

$\equiv$ single transposition with block
size $lcm(t_1, t_2)$
least common multiple.

if $gcd(t_1, t_2) = 1$

$\Rightarrow lcm(t_1, t_2) = t_1 \cdot t_2$

e.g. $t_1 = 23$, $t_2 = 29$ $\Rightarrow$ block size of
a double trans. is 667.

---

modern block ciphers as AES

many rounds,
one round is a combination of substitutions
and transpositions.

AES is a SPN
instead of trans. (perm.) linear
transforms are used.

G-Schreiber

German cipher machine used

during WW2 in Navy.

message → encoded by 5-bit groups by public teleprinter code → encryption cipher-text is a seq. of 5-bit groups too

CCITT2 was used

letter shift symbols, LS	5-bit groups	figure shift symbols, FS
A	11000	–
B	10011	?
		0
...	...	1 ...
Z	10001	+
LS	11111	LS
FS	11011	FS
		...
SP	00100	SP space

encoding HELLO 12 AND ...

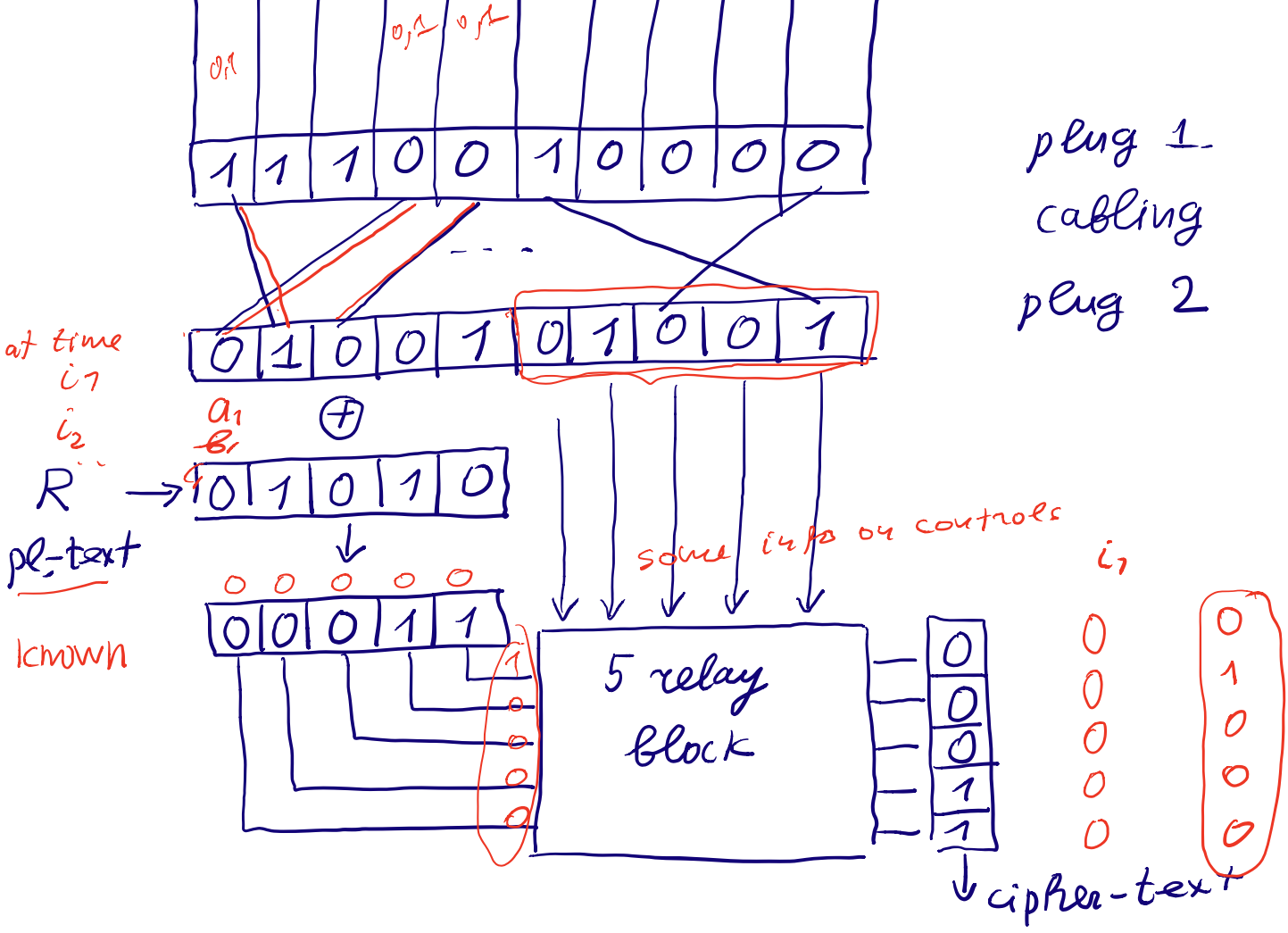
H	E	L	L	O
00101	10000	01001	01001	00011
1	2	LS	A	...
11101	11001	11111	11000	

Machine

47 53 59 61 64 65 67 69 71 73

positions on wheels each position may have 2 values 0, 1.

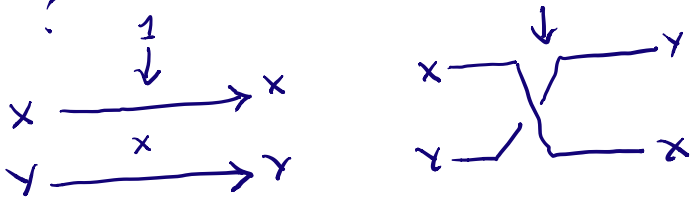
wheels



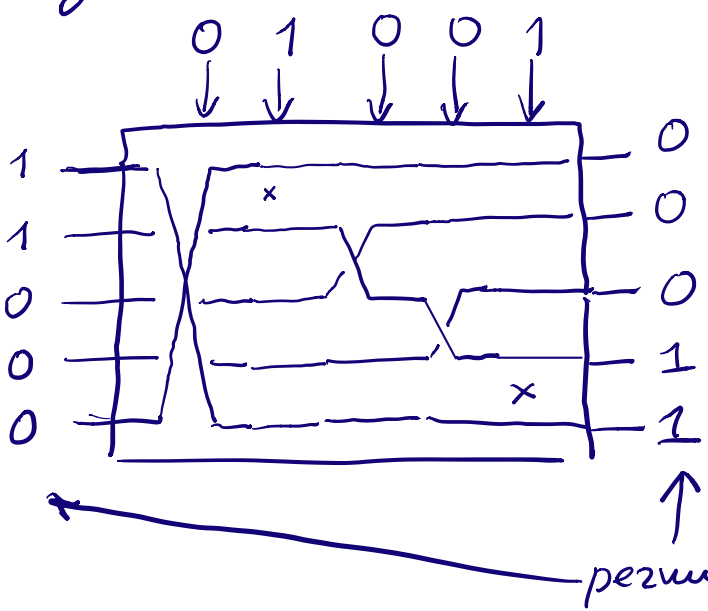
R ⟶ 11000

How relays work ?

one relay



5-relay block



Key system

distributed centrally.

- long-term key : 0,1 distribution on wheels, cabling
- daily key : initial position on some 5 wheels
- message key (IV) : initial position of the rest 5 wheels.

↑ chosen by an operator and sent in clear before cipher-text or encrypted somehow.

---

broken during WW2

1) German encrypted non-classified information along with classified
   ⇒ known pl-text attack.
2) German operators tended not to change message key.

First Assignment.

implement known pl-text attack:

given pl-text and relevant cipher-text

recover internal settings (long term key) of the machine. 0,1 dist. on wheels + cabling.

Algorithm

1. in the cipher-text find positions
$i_1, i_2, \ldots, i_n$
of 5-bit groups 00000, 11111
recover first 5 positions on plug 2
for those moments.

2. reconstruct cabling to the
first 5 positions on plug 2.
By testing periodicity.

i_1 $a_1\ a_2\ a_3\ a_4\ a_5$
i_2 $b_1\ b_2\ b_3\ b_4\ b_5$
...
i_n $c_1\ c_2\ c_3\ c_4\ c_5$

$\Rightarrow$ sequence of values in the 1st position
i_1 i_2 i_n
$a_1 \ldots b_1 \ldots c_1$
Has period $\in 47, 53, 59, \ldots, 73$
assume 47 if $i_2 \equiv i_1 \bmod 47$
$\Rightarrow a_1 = b_1$
if not reject 47

3. recover 0,1 distribution on
5 relevant wheels
connected to the first 5 positions
on plug 2.
$j_1\ j_2 \ldots j_n$

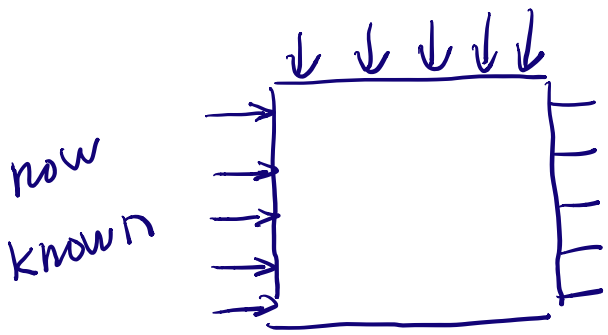
4. find positions in the cipher-text
of 5-bit groups of weight 1 and 4.
01111

01060 10111

00001 11110

10 5-bit groups

5-relay block.



study how the relay block works
get some information about control
bits at times $j_1 j_2 \ldots j_n$

5. use periodicity to recover cabling to the rest of positions on plug 2.

6. reconstruct 0,1-distribution on the rest of the wheels.

that is all!