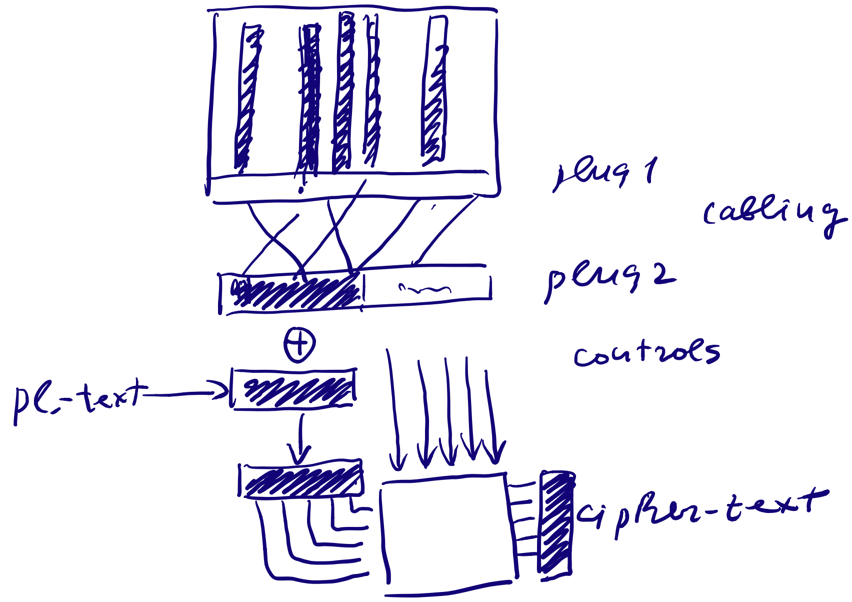
G-Schreiber

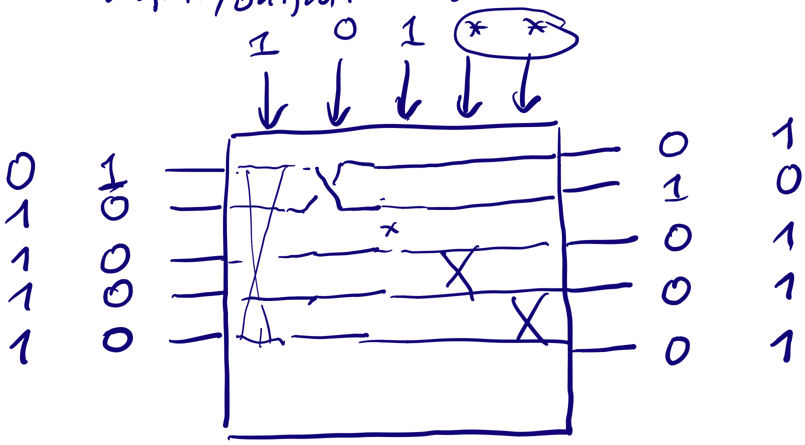
stage 4 Cryptanalysis

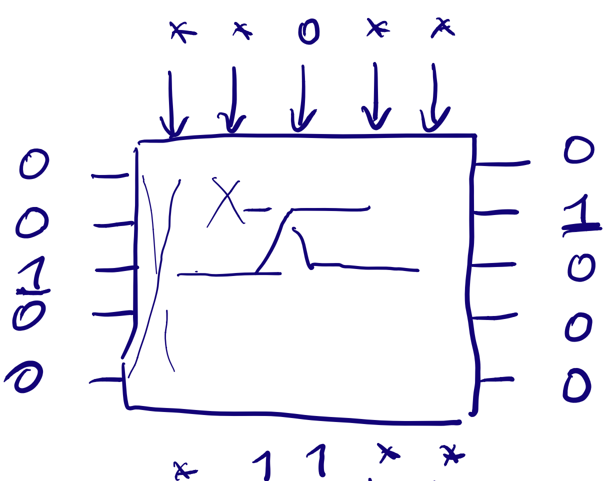


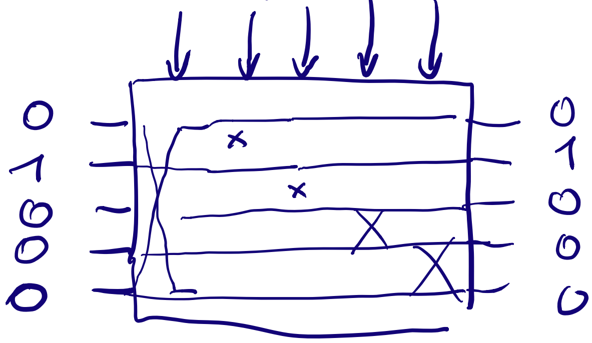
result of stages 1, 2, 3

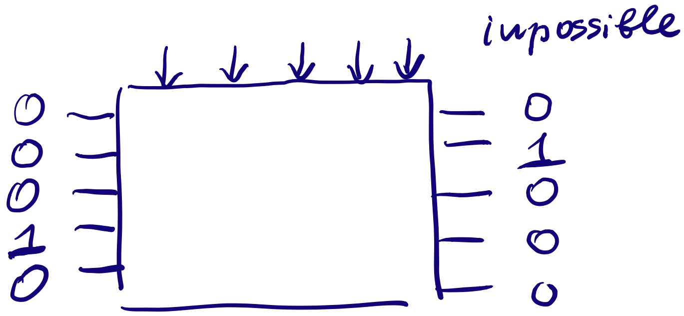
given input/output to 5-relay block
recover some info on control bits.

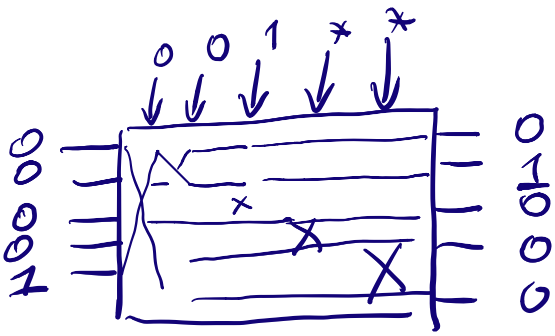
input/output 5-bit groups of weight 1, 4.











collect all such inform. for poss. input/output of weight 1 and 4.

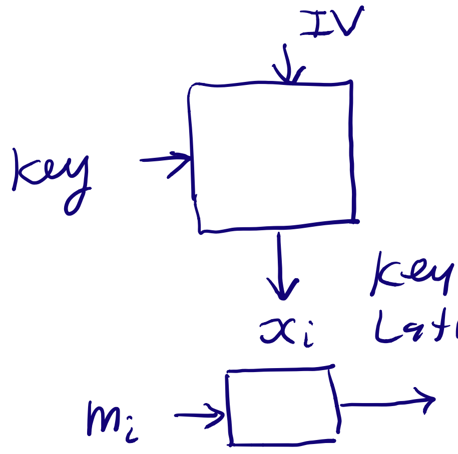
inputs		01000	
10000		101**	
01000		*11**	
00100		**0**	

...

Hagelin

M-209

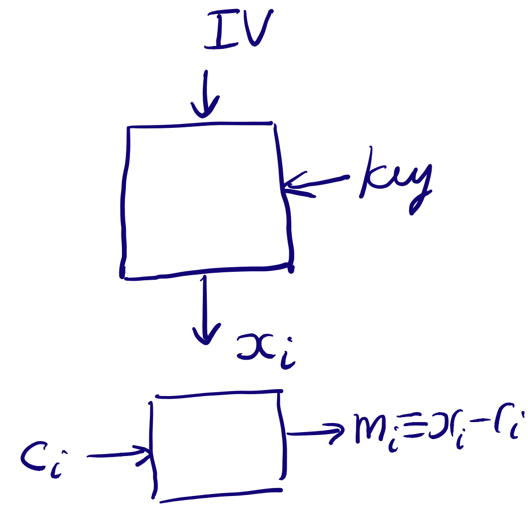
at a glance



key-stream $\in$ Latin alphabet

$c_i \equiv x_i - m_i \mod 26$

char. by $0, 1, \ldots, 25$

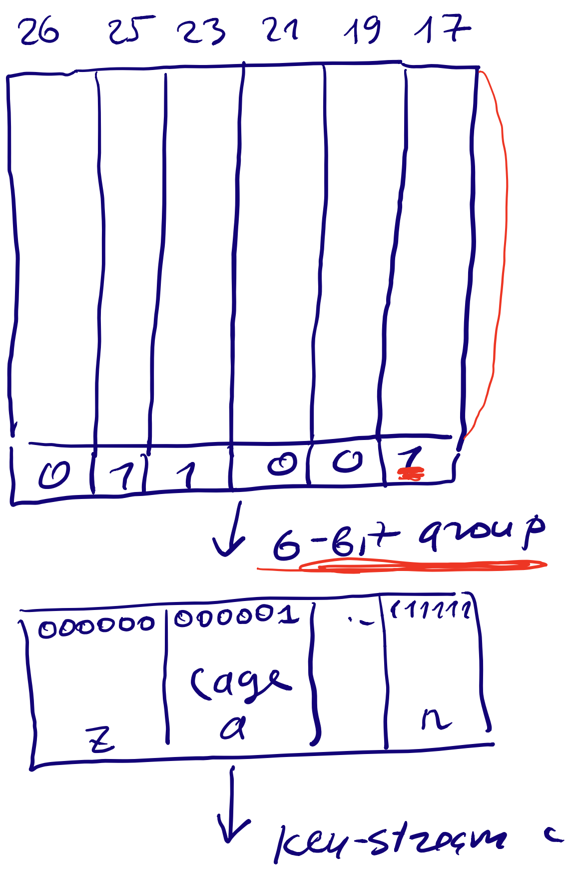


Mathematical model of M-209

positions on wheels

the wheels can rotate simultaneously.

each position may have two values 0, 1.



cage : 6-bit groups $\rightarrow$ Latin alphabet

$m \rightarrow \boxed{} \rightarrow c \equiv x - m \mod 26$.

key : 0, 1 - distribution on wheels

$26 + 25 + \ldots + 17 = 131$

2^{131}

$\Rightarrow$ # 0,1-dist. is 2

cage

message key (IV) initial positions of the wheels.

Cryptanalysis.

cipher-text only attack
given c-text recover pl.-text

Known plain-text attack
given some pl.-text and relevant c-text
find the cipher key.

1. brute force, complexity = | key-space | > 2^{131}

2. period of the cipher.

$$t = 26 \cdot 25 \cdot 23 \cdot 21 \cdot 19 \cdot 17 \approx 10^8$$

Hagelin (M-209) is a Vigenère cipher with block size t.

if cipher-text length > $\underline{100 \cdot t \approx 10^{10}}$ to recover apply frequency analysis pl.-text.

3. more efficient approach.

observations

1) 6-bit groups are correlated.

2) key-stream is not uniform

cage : 6-bit groups $\rightarrow$ Latin
$2^6 = 64$ $|\,..\,| = 26$

26 / 64
best possibility for cage

12 cha. appear 3 times
14 cha. 2 time

$12\cdot 3+14\cdot 2=64$

$\overset{3}{AAA} \quad \ldots \quad \overset{2}{ZZ} \quad \ldots$

3) cipher-text is not uniform

$$m \longrightarrow \boxed{} \xleftarrow{} x \quad \longrightarrow c \equiv x - m \mod 26$$

not uniform

$\Leftarrow$

c not uniform.

4) when one bit of the 6-bit group is fixed $\Rightarrow$ non uniformity increases.

cage : $(* * * * * *) \longrightarrow$ alphabet A

cage : $(* * * * * 0) \longrightarrow A$

cage $(* * * * * 1) \longrightarrow A$

two different distributions on A.

different distributions of the cipher-text

cage is not correlation immune function of order 1.

Efficient Cryptanalysis.

Start with analysing right most wheel (17 positions)

$c_1\ c_2 \ldots c_n$ cipher-text

cipher-text as an array with 17 rows

$C(1) = c_1\ c_{1+17}\ c_{1+2\cdot 17} \ldots \leftarrow M(1) = m_1\ m_{1+17}\ m_{1+2\cdot 17}$

$C(2) = c_2\ c_{2+17}\ c_{2+2\cdot 17} \ldots \leftarrow M(2) = m_2\ m_{2+17} \ldots$

$\ldots$

$C(17) = c_{17}\ c_{2\cdot 17}\ c_{3\cdot 17} \ldots \leftarrow M(17) = m_{17}\ m_{2\cdot 17} \ldots$

positions on wheel-17	0-1 dist. on wheel-17	
1	A_0: 0 … 0	A_1: 1 … 1
2		
17	A_1: 1 … 1	A_0: 0 … 0

find distribution

events A_0 position on wheel-17 is 0
A_1 1

2 possibilities for 0,1-dist. on wheel-17 instead of 2^{17}

distribution of char. in $C(i)$ is defined by A_0
(frequency) or A_1.

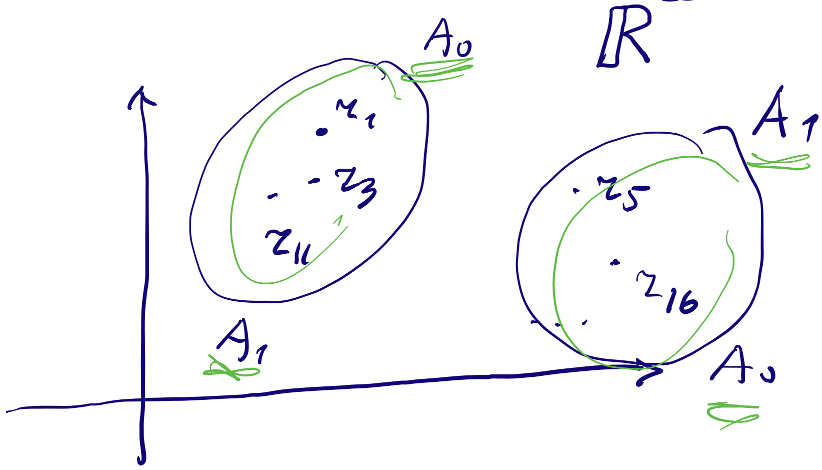
---

compute frequencies of characters in $C(i)$

$r_i = (r_{i0}\ r_{i1} \dots r_{i25})$
$\qquad\quad a \quad b \ \dots \ z$

have 17 distributions $r_1\ r_2 \dots r_{17}$

$\mathbb{R}^{26}$



Do that for all other wheels

overall $2^6 = 64$ possibilities for 0,1-dist. on all 6 wheels.

$64 < 2^{131}$

II. check which distribution out of 64 is correct.

for each distribution generate 6-bit group

fix a 6-bit group

$\boxed{a_1\, a_2\, a_3\, a_4\, a_5\, a_6 \text{ input to the cage at times } i_1 \dots i_T}$

$\downarrow$

$\boxed{\text{key stream } x_{i_1} = \dots = x_{i_T} = x}$

$\Leftarrow$

system equations

$c_{i_1} \equiv x - m_{i_1}, \quad c_{i_2} \equiv x - m_{i_2}, \ldots, c_{i_T} \equiv x - m_{i_T}$

known

unknown with known distribution.

x unknown.

frequencies of char. in $\boxed{c_{i_1} \, c_{i_2} \ldots c_{i_T}}$

test it is a shift of frequencies

of $\boxed{-m_{i_1}, -m_{i_2}, \ldots, -m_{i_T}}$

done with the same trick as in

cryptanalysis of Vigenère cipher.

$\Rightarrow$ finding a single 0,1-dist. on all wheels.

III find cage

fix one 6-bit group $\boxed{a_1 a_2 \ldots a_6}$

appears as input to the cage at

times $i_1 \, i_2 \ldots i_T$

then $\boxed{c_{i_j} \equiv x - m_{i_j}}$ frequencies are known

freq. $\quad$ cage$(a_1 a_2 \ldots a_6)$ $\quad ''$

find a shift x

$\Rightarrow$ recover pl.-text

2000 characters are enough to recover pl.-text.

of cipher-text

100 ch. for known pl.-text attack.