Kapitola 2

Výpočet rotorů v Enigmě 1

Konstrukce přístroje Enigma - obsah

Polsko 1926

Odposlechnuté zprávy Wehrmachtu

```
MFNOJ WYFHJ EXZZD BJNDS BECFE NGQOU CFWZE RBSFQ WCUCQ
XCKTT RDOAC VDYPM XYOFF HMSOZ THOSD HFPDI UKWRD MNDZX
BYMIA FXXTA WWFYS

NEVGW YCJUM IYFCW JXMDR TBIFU PQDMH RPCOX WYXTJ YQXZG
CQMSP CJHGA OMHEV QFCGX SXATA HXFHV HZBED VALPY ZPMPW
JNPDY RZXKJ DDQZO

NEVGW YIPUC AVKHH FTAPT ZVYXV KRJIG APWAT LWBQH UJASR
JMBSF KDVRN IUOXV FKLQG MPSWY EDYHP LSICW ALFPZ XOOFZ
BNZUX DCEKG PXJON
```


Index koincidence

```
MFNOJ WYFHJ EXZZD BJNDS BECFE NGQOU CFWZE RBSFQ WCUCQ
NEVGW YCJUM IYFCW JXMDR TBIFU PQDMH RPCOX WYXTJ YQXZG

XCKTT RDOAC VDYPM XYOFF HMSOZ THOSD HFPDI UKWRD MNDZX
CQMSP CJHGA OMHEV QFCGX SXATA HXFHV HZBED VALPY ZPMPW

BYMIA FXXTA WWFYS
JNPDY RZXKJ DDQZO


NEVGW YCJUM IYFCW JXMDR TBIFU PQDMH RPCOX WYXTJ YQXZG
NEVGW YIPUC AVKHH FTAPT ZVYXV KRJIG APWAT LWBQH UJASR

CQMSP CJHGA OMHEV QFCGX SXATA HXFHV HZBED VALPY ZPMPW
JMBSF KDVRN IUOXV FKLQG MPSWY EDYHP LSICW ALFPZ XOOFZ

JNPDY RZXKJ DDQZO
BNZUX DCEKG PXJON
```

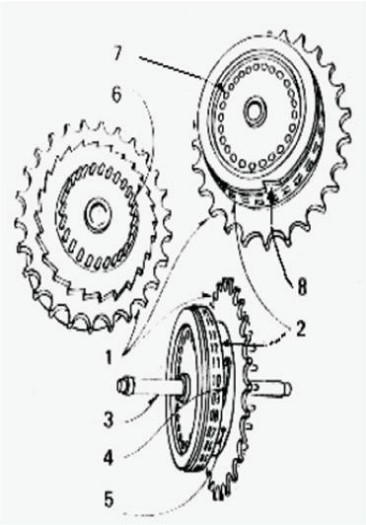
závěry:

Špionáž

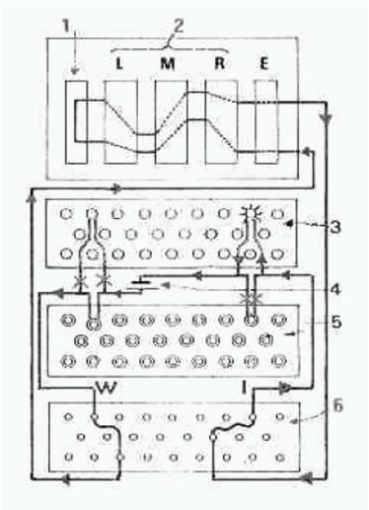
- francouzská špionáž získala manuál pro operátory vojenského přístroje Enigma komcem roku 1931 (generál Gustave Bertrand)
- německým agentem byl Hans-Thilo Schmidt (1888-1944)
- později předal francouzské špionáži také denní klíče pro měsíce září a říjen 1932
- počátkem prosince 1932 dostalo polské Biuro Szyfrów kopie těchto dokumentů na základě dohody o vojenské spolupráci mezi Polskem, Francií a Velkou Británií
- v Německu si zakoupili volně prodejnou komerční variantu přístroje Enigma

Enigma

Schéma rotoru



Elektrické schéma přístroje



Nastavování přístroje - obsah

Denní klíče

denní klíč říkal, jak má být nastavený přístroj Enigma v daném dni na začátku šifrování libovolné zprávy

denní klíč sestával z

- pořadí rotorů, např. `II, III, I`, bylo v té době stejné po celý čtvrt roku,
- polohy abecedních kroužků na rotorech, např. `KUB`
- propojení v propojovací desce, např. `AU, CR, DK, JZ, LN, PS`
- základní nastavení, tj. jaká písmena jsou vidět v malých okénkách, např. `UFW`

Klíč zprávy

- po nastavení přístroje podle denního klíče měla obsluha zvolit náhodnou trojici písmen, kupříkladu `HTS`
- to je klíč zprávy
- poté ji napsat dvakrát za sebou, tj. `HTS HTS`
- pak tuto šestici zašifrovat pomocí přístroje nastaveného podle denního klíče, výsledkem bylo `NEV GWY`
- poté ručně přenastavit rotory tak, aby v okénkách byl vidět klíč zprávy
- a začít šifrovat samotnou zprávu
- tak například zpráva `AHOJ` byla zašifrována jako `JCRI`

Porušení pravidel bezpečnosti

- všechny klíče zpráv byly ve stejném dni šifrovány pomocí stejného klíče (stejného nastavení přístroje)
- každý konkrétní klíč zprávy byl šifrován dvakrát pomocí dvou různých klíčů (tj. různých nastavení přístroje)
- porušení pravidel bezpečnosti bylo počátkem matematické analýzy šifry

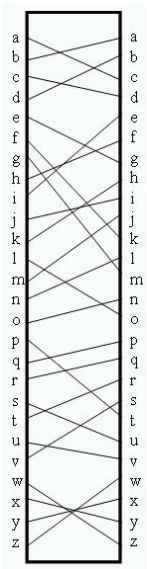
Konec roku 1932

tři nejlepší absolventi kurzu kryptoanalýzy, který uspořádalo Biuro Szyfrów v roce 1928 pro posluchače matematiky na univerzitě v Poznani

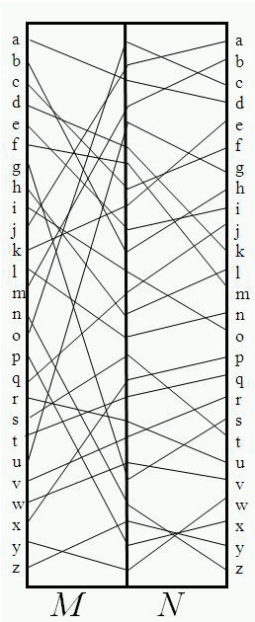
Matematický model Enigmy - obsah

- *Matematický model Enigmy*
  Model rotoru
  Opakování permutací
  Statický model

Matematický model rotoru



Násobení rotorů



Grafické znázornění permutace

```
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
b d a c i h e k j m f n g o l q r t v p s u z y x w
```


Graf složené permutace

```
a b c d e f g
b c a e f g d

b c a e f g d
e f g a d c b


a b c d e f g
e f g a d c b
```


Změna jmen prvků permutované množiny

```
a b c d e f g
b c a e f g d
```


Řešitelnost rovnice $U = X^{-1}VX$, nutná podmínka

Pokud mají U, V stejný typ

Kdy jsou dvě permutace konjugované

věta: jsou-li U,V dvě permutace na konečné množině Ω, pak existuje permutace X na množině Ω, pro kterou platí, že U=X-1VX právě když permutace U,V mají stejný cyklický typ

kolik takových permutací X existuje ?