Application Problems

Cryptography

Ahto Buldas ahto.buldas@ttu.ee
Aleksandr Lenin aleksandr.lenin@ttu.ee
Jaan Priisalu jaan.priisalu@ttu.ee

September 18, 2018

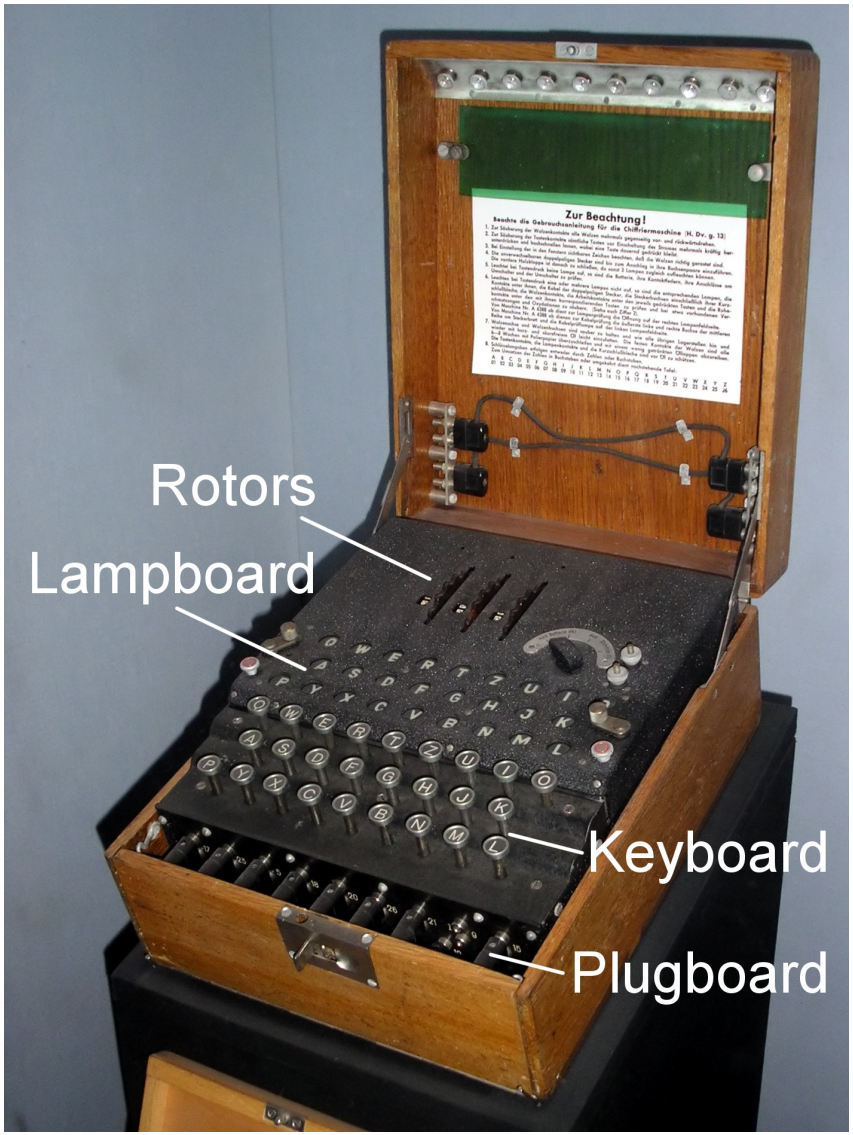
Topics

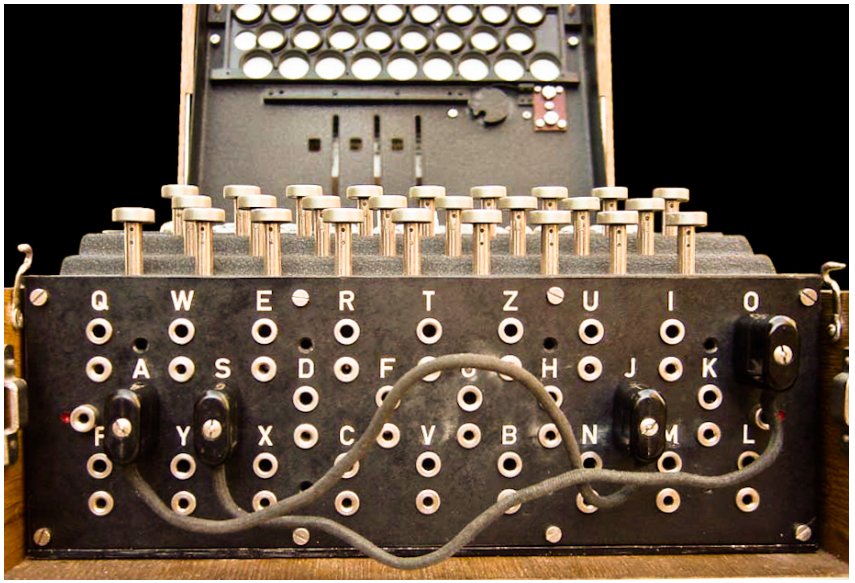
1. History
   - Signal Intelligence Cooperation
   - Enigma
   - Venona
   - Russian Diplomatic Communication
2. Implementation details
   - Block chipher modes
3. Tools for study

Cryptanalysis known pairing

- France
- Poland
- United Kingdom

- Japan
- Finland
- Estonia


Zur Beachtung!
Rotors
Lampboard
Keyboard
Plugboard


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

Breaking Enigma

Breaking basis method is Friedman's Index of Coincidence - statistics of letter pairwise sequencies.

Reasons of breaking Enigma:

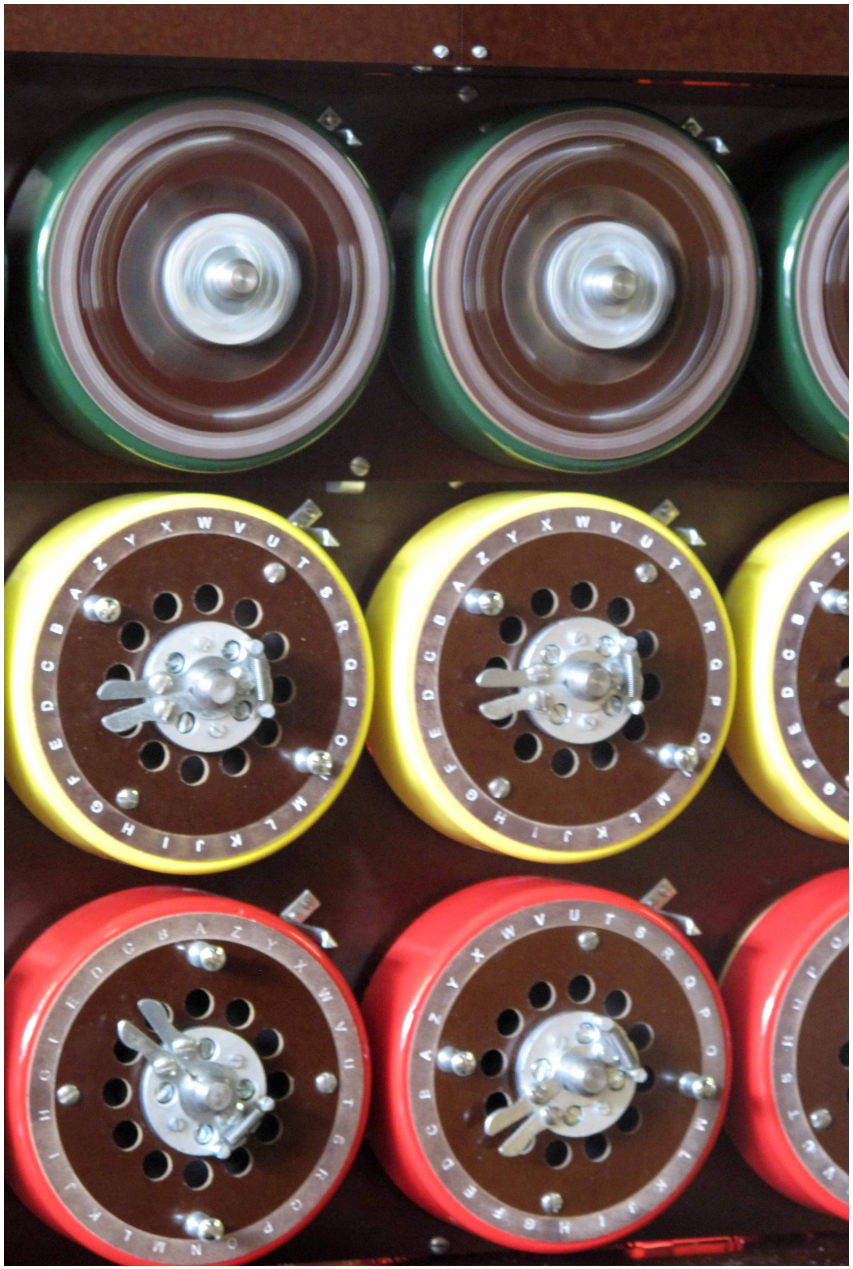
- Open commercial design
- Avoiding one substitution
- Plaintext partial predictability
- Operating discipline
- International cooperation

Roles:

FR Obtaining machines

PL Method development

UK Consolidation and industrialisation



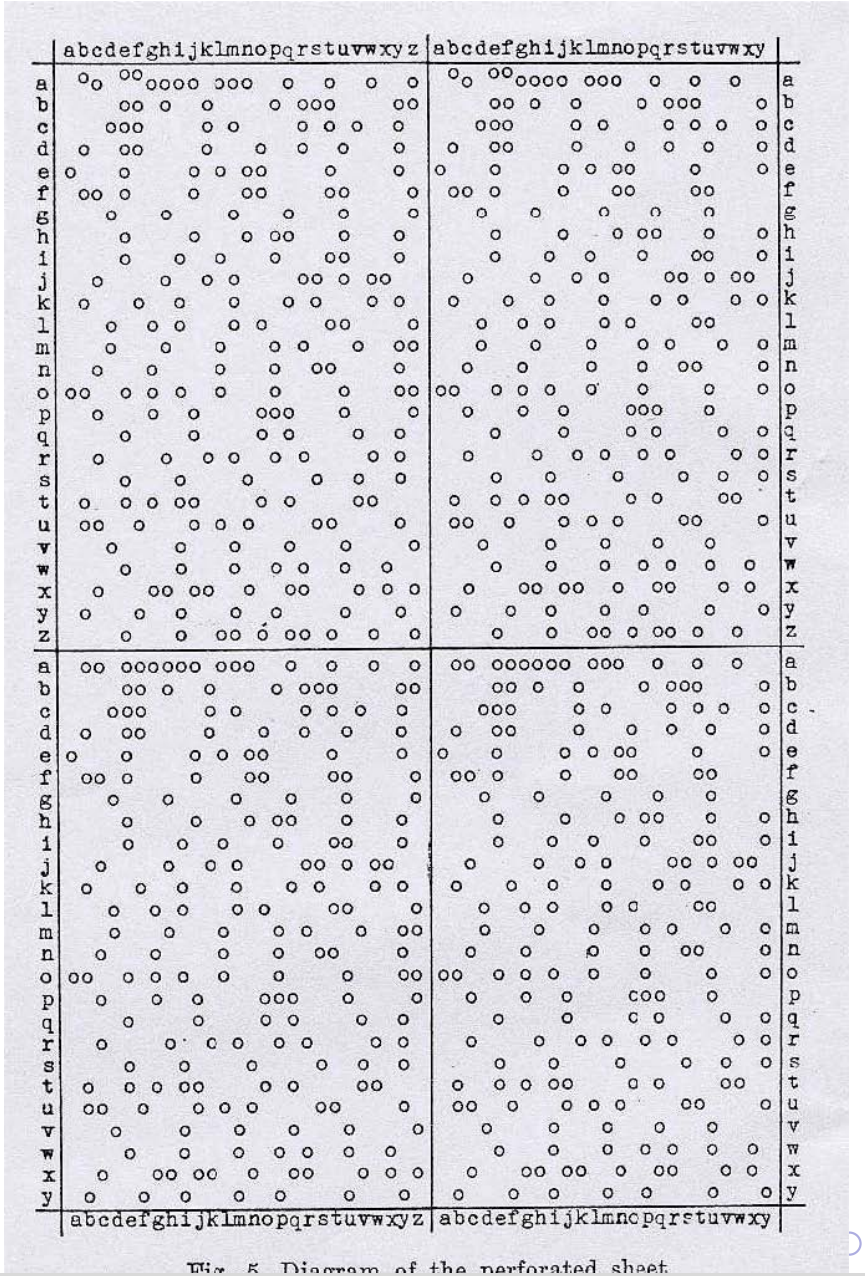


Fig. 5. Diagram of the perforated sheet

Venona

Russians reused keys.

Project 1946-1980

Decryption rate

1942	1.8%
1943	15.0%
1944	49.0%
1945	1.5%

One-time Pad

Plaintext x is divided into blocks $x = x_1 x_2 \dots x_m$.
Ciphertext is y also divided into blocks $y = y_1 y_2 \dots y_m$, where every ciphertext block y_i is computed by

$$y_i = x_i \oplus z_i \quad ,$$

where z_i is the key intended for the encryption of x_i.
The keys z_i are mutually independent and uniformly random.

Key reuse

If all keys are the same $z_i = k \; \forall i$ and we know one plaintext-ciphertext pair (x_j, y_j) then we can decrypt all pairs as $k = x_j \oplus y_j$.

If we know that key is re-used one time $z_m = z_n = k$, then

$$\begin{aligned} y_m \oplus y_n &= x_m \oplus k \oplus x_n \oplus k \\ &= x_m \oplus x_n \quad . \end{aligned}$$

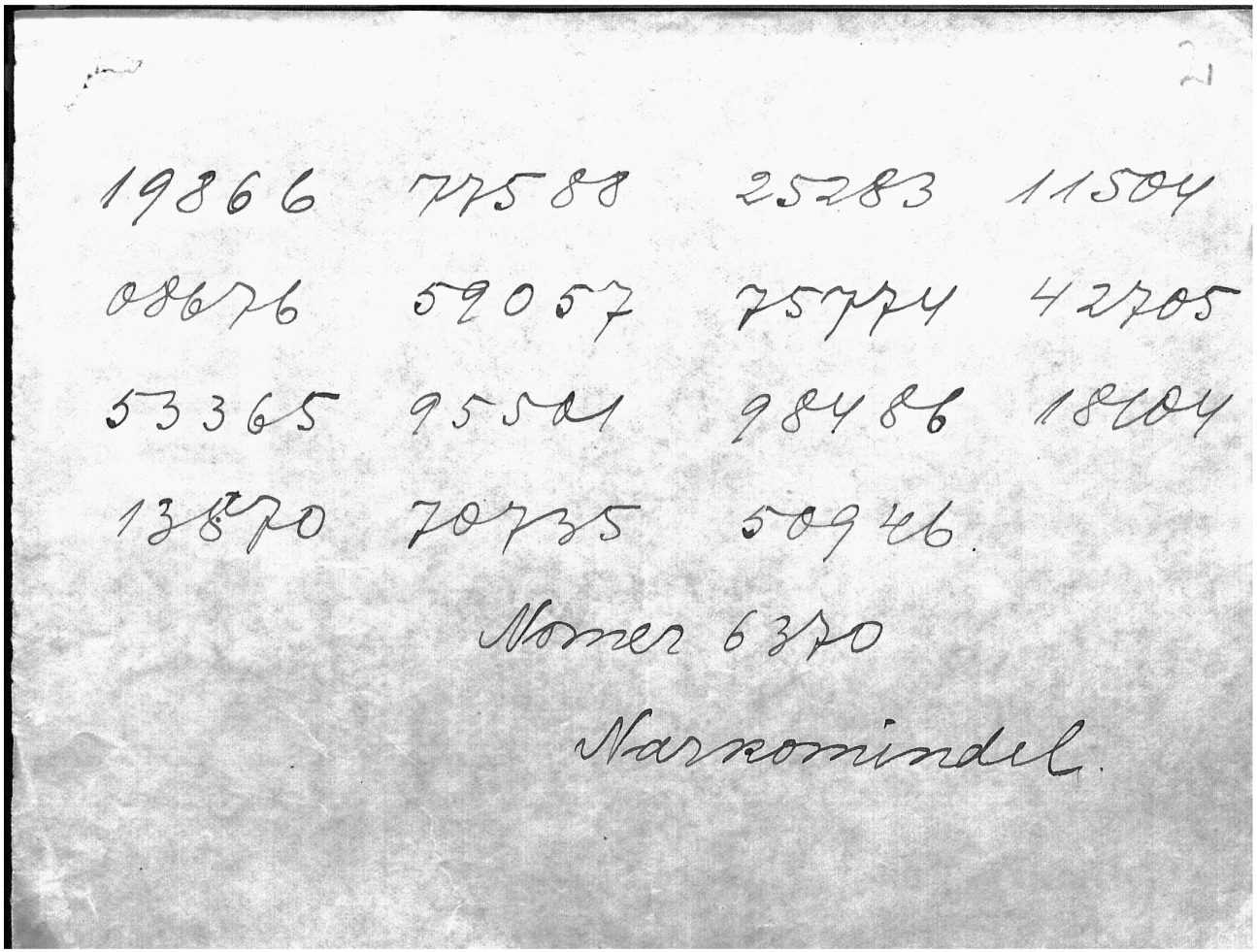
XOR-ed texts can be attacked by pair frequency matrix.

Tallinn Telegrams

Some intercepted telegrams of Russian Tallinn Embassy with Moscow are preserved.

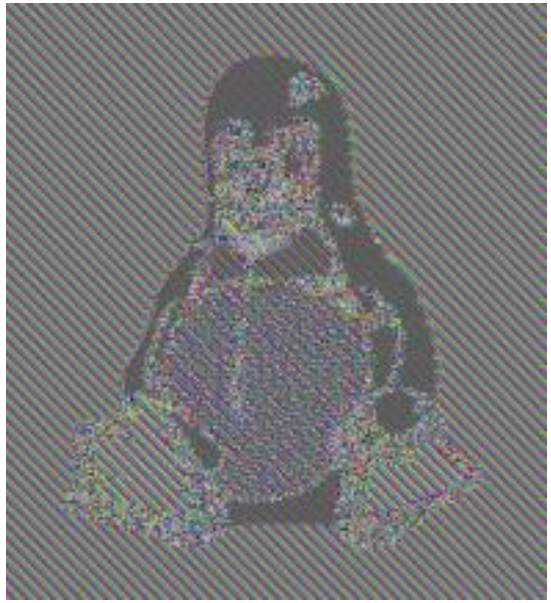
They were misclassified in Estonian State Archive.

Content is not random, autocorrelation does exist.

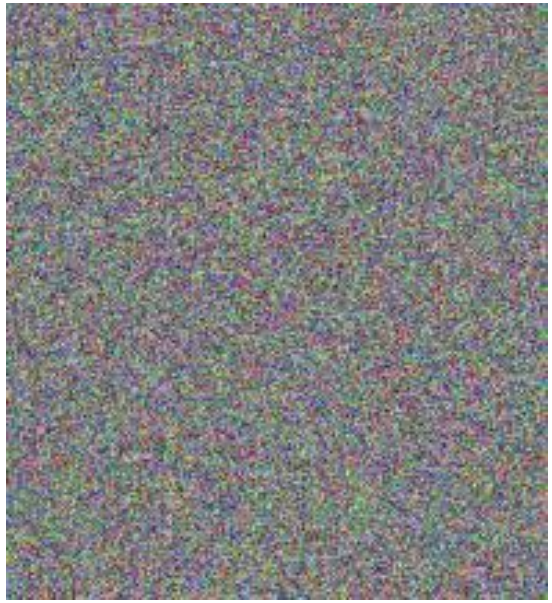

2
19866 77588 25283 11504
08676 59057 75774 42705
53365 95541 98486 18404
13870 70735 50946
Nomer 6370
Narkomindel.

Block cipher modes

Original file



ECB encrypted



CBC encrypted

Mode properties

Mode	Encrypt	Decypt	Random read
ECP	Parallel	Parallel	Yes
CBC	No	Parallel	Yes
CFB	No	Parallel	Yes
OFB	No	No	No

PKI practical problems

- Dutch DigiNotar
- Swedish BankId
- Estonian ID card negative moduli
- Taiwan ID card weak random
- Infineon weak key generation

Keypair roles

SEIS original keypair roles

signature	No recovery allowed
authentication	Arbitrary challange
encryption	Key recovery desired

FinID optimised authetication and encryption keypairs together.

Tools to consider

- cryptool.org
- openssl
- Cryptographers Workbench