Application Problems
Introduction to Combinatorics and Cryptography

Ahto Buldas ahto.buldas@ttu.ee
Jaan Priisalu jaan.priisalu@ttu.ee

November 24, 2016
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
History
Implementation details
Tools for study

Signal Intelligence Cooperation
Enigma
Venona
Russian Diplomatic Communication

Ahto Buldas ahto.buldas@ttu.ee, Jaan Priisalu jaan.priisalu
Application Problems
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
Ahto Buldas ahto.buldas@ttu.ee, Jaan Priisalu jaan.priisalu
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 $x = x_1 x_2 \ldots x_m$. Ciphertext is $y$ also divided into blocks $y = y_1 y_2 \ldots y_m$, where every ciphertext block $y_i$ is computed by

$$y_i = x_i \oplus z_i,$$

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

$$y_m \oplus y_n = x_m \oplus k \oplus x_n \oplus k$$
$$= x_m \oplus x_n .$$

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.
History
Implementation details
Tools for study

Signal Intelligence Cooperation
Enigma
Venona
Russian Diplomatic Communication

Ahto Buldas ahto.buldas@ttu.ee, Jaan Priisalu jaan.priisalu

Application Problems
Block cipher modes

Original file

ECB encrypted

CBC encrypted
## Mode properties

<table>
<thead>
<tr>
<th>Mode</th>
<th>Encrypt</th>
<th>Decrypt</th>
<th>Random read</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECP</td>
<td>Parallel</td>
<td>Parallel</td>
<td>Yes</td>
</tr>
<tr>
<td>CBC</td>
<td>No</td>
<td>Parallel</td>
<td>Yes</td>
</tr>
<tr>
<td>CFB</td>
<td>No</td>
<td>Parallel</td>
<td>Yes</td>
</tr>
<tr>
<td>OFB</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
PKI practical problems

- Dutch DigiNotar
- Swedish BankId
- Estonian ID card negative moduli
- Taiwan ID card weak random
Keypair roles

SEIS original keypair roles

- **signature**: No recovery allowed
- **authentication**: Arbitrary challenge
- **encryption**: Key recovery desired

FinID optimised authentication and encryption keypairs together.
Tools to consider

- cryptool.org
- openssl
- Cryptographers Workbench