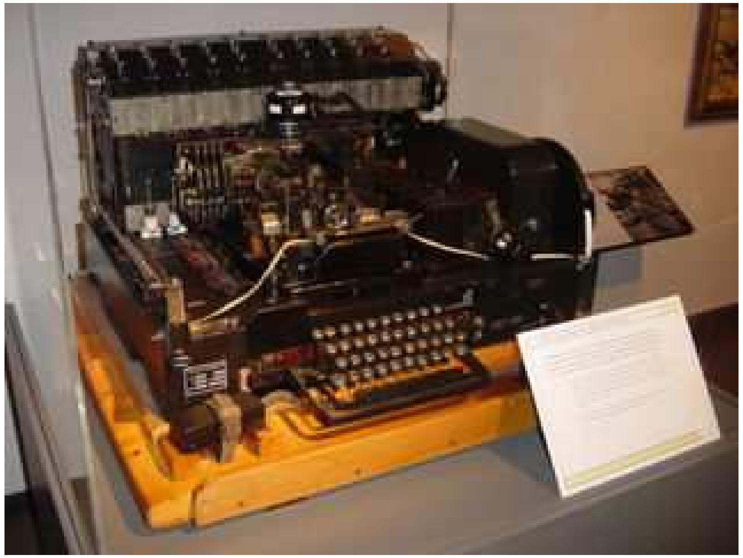
Swedish Analysis of Nazi Crypto TTYs

How Beurling et al. broke the Siemens & Halske T52 crypto teleprinter

Sven M. Hallberg

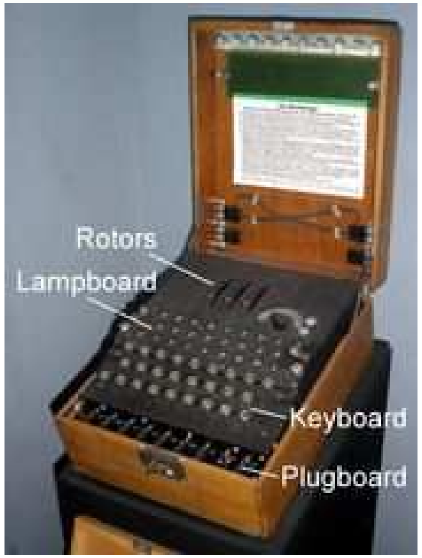
`pesco@khjk.org`

Siemens & Halske T52



- electromechanical teleprinter
- automatic en-/decryption
- *heavy!* (>100kg)

Compare: Enigma



- only switches, plugs, lamps, and wheels
- lightweight field device
- rel. simple substitution cipher

Overview

- Setting
  - political
  - technological
- Cryptanalysis
  - deciphering
  - algorithmic analysis
  - machine reverse engineering
- Conclusion

Setting

1940

- Germany still neutral with Russia
- Russia had just invaded Finland
- Germany fights allies in Norway
- Sweden neutral
  ⇒ eager to know what's going on around it

Swedish cryptanalysis division

- founded early on by good foresight
- routinely intercepting radio traffic
- already good at breaking codebooks
- head of Russion section: Arne Beurling

Russian codebook crypto

- per-word substitution codebooks
- superenciphered with one-time pads
- BAD: pads often reused

  $\Rightarrow$ “repeats”

“Severely unreadable”

- tons of unusual intercepts come in
- symbols not grouped for human handling
- 26 letters + 6 digits = 32 characters

⇒ machine crypto!?

Teleprinter alphabet

- “Baudot code” alias ITA 2.
- only five bits per character
  ⇒ two modes: *letter/figure shift*

Teleprinter alphabet

Letter shift	*Code Pulses*	*Figure shift*	*Intercept*
A	11000	–	
B	10011	?	
	...		
Y	10101	6	
Z	10001	+	
Carriage return	00010	Carriage return	1
New line	01000	New line	2
Letter shift	11111	Letter shift	3
Figure shift	11011	Figure shift	4
Space	00100	Space	5
Empty character	00000	Empty character	6

Teleprinter cryptography

- bit-wise XOR stream ciphers already known
- pseudorandom key streams also a known idea
- usually generated using random-pattern pin wheels

Pin wheels

- conceptually: a wheel circumscribed with a number of random bits
- bits represented by presence/absence of pins
  - “read” mechanically
- turn one (or more) positions to “generate” next bit

Pin wheels (cont.)

- bank of wheels for multiple bits
- each wheel has different period (number of bits)
- coprime wheel periods maximizes whole stream's period

Cryptanalysis

Disclaimer

- Beurling broke the original T52 in just two weeks.
- He refused to talk about exactly *how* he did it.
- This talk presents only a plausible reconstruction.

An example intercept

```
hier35mbz35qrv54b35kk35qep45qw55wt55qi55ru55tw
3355553535umum35veve35zrddlh5fny13qukd4gehnswo
```

Remember:

3 – letter shift   4 – figure shift   5 – space

So read:

```
HIER MBZ QRV? KK QEP 12 25 18 47 52 UMUM VEVE
```

...garbled...

An example intercept

```
hier35mbz35qrv54b35kk35qep45qw55wt55qi55ru55tw
3355553535umum35veve35zrddlh5fny13qukd4gehnswo
```

Remember:

3 – letter shift   4 – figure shift   5 – space

Attack vectors:

- reused IVs
- frequent use of typical sequences
  - `35`
  - `QRV` also maybe?

Let's have some depth

Supposed that a set of messages has been received, all encrypted with the same key (i.e. QEP vector).

```
1.  alzgj1guh4hjplhn6n5bve3cquhgfbjn...
2.  np3umwfz31nmykmjhb625fmquhfdfz45...
3.  grqumaa4jtqflqmhjiegtvfwpoi32slk...
4.  lyzgj1oryydrqknhjn51akfd5vcerwrv...
    .
    .
    .
```

Looking for repeats

Assume that bigraph repeats represent 35:

A	L	**Z**	**G**	**J**	**1**	G	U	H	4	H	J	P	L	. . .
		3	5	3	5									
N	P	3	**U**	**M**	**W**	**F**	Z	3	1	N	M	Y	K	. . .
			3	5	3	5								
G	R	Q	**U**	**M**	A	A	4	J	T	Q	F	L	Q	. . .
			3	5										
L	Y	**Z**	**G**	**J**	**1**	O	R	Y	Y	D	R	Q	K	. . .
		3	5	3	5									
	⋮													

A first guess

Assume an additive superposition (XOR) cipher was used. That would imply the characteristic weakness

$$m + m' = (a + k) + (b + k) = a + b$$

for messages in depth, where

$$\begin{aligned} a, b &= \text{plaintexts} \\ m, m' &= \text{ciphertexts} \end{aligned}$$

A first guess

Assume an additive superposition (XOR) cipher was used. That would imply the characteristic weakness

$$m + m' = (a + k) + (b + k) = a + b$$

for messages in depth, where

$$\begin{array}{rcl} a, b & = & \text{plaintexts} \\ m, m' & = & \text{ciphertexts} \end{array}$$

Unfortunately, the above does not hold in our case. *But...*

...it almost does!

In the fourth column of the example:

- several 3’s encrypt to U
- several 5’s encrypt to G

$$\begin{array}{cc@{\qquad}cc} \mathrm{U} & 1\mathbf{1}100 & 3 & 11\mathbf{1}11 \\ \mathrm{G} & 0\mathbf{1}011 & 5 & 00\mathbf{1}00 \\ \hline & 1\mathbf{0}111 & & 11\mathbf{0}11 \end{array}$$

- They match *up to a permutation*!
- Other columns show exactly the same effect.

Second guess

Hypothesis. *The cipher is an additive superposition followed by a random permutation* σ.

$$m = \sigma(a + k)$$

Second guess

Hypothesis. *The cipher is an additive superposition followed by a random permutation* σ*.*

$$m = \sigma(a + k)$$

NB: $m = \sigma a + k$ would also appear possible *a priori*, but can be ruled out later.

How to uncover the permutation

- look for pairings like 3-5 with a single 1 or 0 in their difference
- see where it moves in the ciphertext

  ⇒ one element of the permutation discovered
- need at least four distinct such pairings
- lucky us: 35 + QRV do the trick!

3	11**1**11	3	111**1**1	Q	1**1**101	3	**1**1111
5	00**1**00	Q	111**0**1	R	0**1**010	V	**0**1111
	11**0**11		000**1**0		1**0**111		**1**0000

Reverse engineering

- How are the 5 keystream bits generated?
  - safe to assume pin wheels
- How is the permutation generated?

How is the permutation generated

- Beurling knew about *relay switches* from telephone exchanges
- depending on the input, current goes down one wire or another
- with these, “cross switches” can be built
  - depending on input, two wires are either crossed or passed through

How is the permutation generated (cont.)

- Permutations can be decomposed into a series of transpositions.

⇒ A sequence of several cross switches can implement any permutation.

- Pin wheels could provide the inputs.
- How many switches in what arrangement?

Determining permutation switch wirings

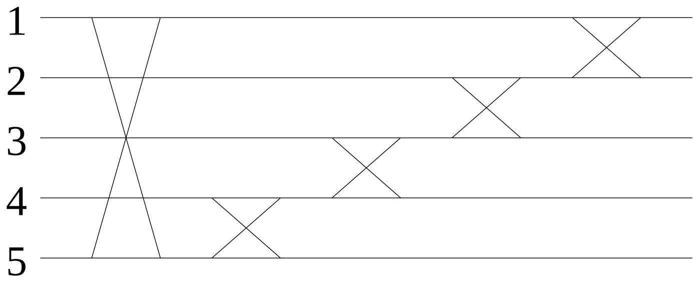
- have five wires to permute
- decomposing discovered permutations gives clues:

$$[53421] = (51) \circ (234) = (51) \circ (23) \circ (34)$$

⇒ need at least switches to cross wires

- 5 and 1
- 2 and 3
- 3 and 4

A typical permutation wiring



- Turns out there are never more than 5 transpositions involved.

⇒ There are five cross switches.

The machine

- note: safe to assume the machine processes one character per step
- need 5 keystream bits for each character
- need 5 random bits for the permutation

⇒ the T52 has a drum of 10 pin wheels

Pin wheel patterns

- still need to find periods and actual pin patterns of the 10 wheels
- easy by manually deciphering a long sequence of text

→ reveals stream of 10-bit words

Pin wheel patterns (cont.)

- lucky us: original T52 moves all wheels by one position per step
- just record the bit patterns until it starts repeating

⇒ Complete machine state known now!

NB. Indeed: The derived wheel patterns turn out coprime, supporting our assumptions.

The mystery is solved.

We have derived the entire build-up and encryption state of the machine!

- 5-bit Baudot code teleprinter
- additive superposition (XOR) cipher
- followed by random permutation
- random bits provided by 10 pin wheels
  - QEP numbers initialize 5 of 10 wheels

Automating decryption

- Swedes promptly built automatic decryption machines
- find secret states once by manual deciphering
- enter QEP numbers into decryptor
- type ciphertext
- decryptor prints cleartext :)

Conclusion

Cryptanalysis is black magic. . .

. . . plus:

- experience
- intuition
- reasoning
- perseverence

Thanks for listening.

- Bengt Beckman: *Codebreakers — Arne Beurling and the Swedish Crypto Program during World War II*, Oxford University Press 2003
- Lars Ulfving, Frode Weierud: *The Geheimschreiber Secret — Arne Beurling and the success of Swedish signals intelligence*, appeared in “Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory”, Springer Verlag 2000
- T52d simulator (Windows)

  `http://frode.web.cern.ch/frode/crypto/simula/t52/`