About the Swedish analysis of Nazi Germany's crypto teleprinters

Sven Moritz Hallberg
sm@khjk.org

May 2006

The machine called Enigma, widely famous for being used by German armies during World War II to secretly (or so they hoped) communicate among troops, was a field device. It was portable, simple to operate, as well as relatively cheap to produce, containing neither electrical motors nor any coding/decoding assembly. It was, however, not the only crypto device employed by the Germans.

The Siemens & Halske T52 (in its several variants), commonly referred to as the *Geheim-* or *G-Schreiber* (German for "secretly-writer"), was a teleprinter[1] with integrated encryption/decryption facility. It was cryptographically superior to the Enigma and, by its nature, much more sophisticated in terms of its electro-mechanical engineering. Due to the latter, it was also *much* bulkier, weighing no less than 100kg, excluding the transport case. Therefore it was used as a stationary unit, primarily by the German air force, navy, and for diplomatic purposes. In total, about 600 units were in operation. It must be noted that this text only covers the first two models, T52a and T52b. The later variants featured improved designs, eliminating some of the earlier flaws.

From April 1940, Swedish authorities gained access to large quantities of T52-encrypted telegraph traffic. With Norway just invaded and significant parts of Finland already surrendered to Russia, the Swedes were obviously interested in the plaintexts and, having been quite successful at breaking Russian and French crypto already, promptly tried their luck in deciphering the German messages.

Swedish cryptanalysis operations

Sweden had established a cryptanalysis group as part of its signal intelligence service well before the war. The swedish crypto guru of the time, Yves Gyldén, had remarked as early as 1931 that a useful crypto section should be formed with several years of foresight, so as to be trained and well-established as soon as its services became critical:

> "When forced by circumstances, it is possible to build up an effective cryptology and cryptanalysis operation in the course of a few years. However, during this time, mistakes are inevitable, time is

[1] i.e. an electrial printer connected to an identical machine through a telegraph line, printing out characters sent from the other side, and vice-versa

> lost, and exploitable errors on the part of the enemy are not utilized. It is therefore necessary that such an organization be ready to go into action on the first day of mobilization — even better, a few days earlier — carefully trained, equipped, organized, and staffed to immediately take advantage of, and exploit, enemy mistakes and errors."

In fact, Swedish troops had already intercepted and broken several encrypted telegrams from Russia during the First World War. The plaintexts were then given to Germany, in exchange for access to results and methods of the German cryptanalysis agency. This ironically laid the foundations for Sweden's later efforts.

Regular radio signal interception began around 1930 on several coastal defense ships, targeted at the Russian navy. While no dedicated cryptanalysis department existed at the time, several courses on cryptology were already being held for selected staff members.

1937 saw a reorganization of the Swedish defense staff and it included the formation of a signal collection department and a crypto department. The latter commenced work with several courses and lectures held in particular by Yves Gyldén and the compilation of language statistics, essential for the cryptanalytic work. New talents were continuously sought and discovered from conscripts working for the department, course participants, as well as through published test exercises.

Immediately after the outbreak of war, full-scale cryptanalysis of foreign radio traffic began. The department was organized into four sections, responsible for French, English, Russian, and German traffic, respectively. Efforts were quite successful. The French section, headed by Gyldén, for instance had to deal with a so-called code book, a fixed mapping of entire words to corresponding secret numbers. This kind of cipher was Gyldén's speciality and the section could celebrate continued successes until France fell to Germany.

The Russian section was considered most important by Sweden but it, along with Germany, was also expected to present the most complications. The section was headed by Arne Beurling, a professor of mathematics from the university of Uppsala who had proven his cryptological talent earlier by single-handedly breaking an encryption device that had then just been bought for use by the Swedish forces. The Russians were, like the French, using code books, but additionally *super-enciphered* the thus coded messages. As Beurling had to discover, the super-encipherment was performed with one-time pads, theoretically unbreakable. However, since the continuous distribution of fresh one-time pads is a logistical challenge, the Russians partly resorted to using (parts of) the same pad for several messages. This gave Beurling an entry and the cipher was soon broken.

While with time the Russians grew more and more wary and eventually significantly strengthened their system, Arne Beurling was soon to be occupied with a new task.

German machine crypto

Sometime in 1940, while Beurling was working on the Russian codes, he received a number of intercepts of unknown origin which looked rather unusual.

Conventionally, the letters of encrypted messages were grouped into blocks of five, for easier handling by human operators. These telegrams, however, appeared as an uninterrupted sequence of characters, without any spaces. Also, telegrams (often transmitted in Morse code) commonly used just the 26 letters of the roman alphabet. These messages also used them, but with the addition of the digits 1–6. It appears peculiar that only the first six are used, not all ten. This might hint that the total number of characters in the alphabet is somehow more significant than the actual digits. Noting that the total number of characters, 32, incidentally equals 2^5, Beurling (correctly) suspected that a binary representation was somehow involved.

Beuerling next inspected the messages in a familiar way. He looked for repeating character sequences, a characteristic effect of encrypting two messages with the same key: two equal characters at the same place in the two messages would due to the identical encryption state also result in the same output. Indeed the messages showed such repeats, but not in the same positions as it would normally have to be the case. Beurling thought the cause to be some error in recording the telegrams and inquired about how they had been collected. Only then was he told the fact that Germany had leased a number of Swedish telegraph lines to communicate with its troops in Norway. The lines had promptly been tapped and Beurling was looking at what a Swedish Telecom operator had described as having become "severely unreadable".

It was now apparent that the Germans were using automatic machine crypto and, even though Beurling knew nothing about teleprinters at the time, it explained the absence of letter grouping and the 32-character alphabet. The randomly distributed repeats, however, still remained a mystery to him and he demanded access to all the collected material. The complete set of intercepts filled a whole closet in a Stockholm listening station. Looking through it, Beurling discovered that material collected in particular on May 25 and 27 did not show the "flaw" in repeat distribution and consequently decided to take these messages with him.

Arne Beurling goes to work

Beurling did not like to talk about how exactly he broke the G-Schreiber cipher, but it is probably safe to assume that with his new knowledge about the intercepts, he familiarized himself somewhat with teleprinter technology and whatever was known about teleprinter cryptography. Nevertheless, it is important to note that this section represents merely a likely *reconstruction* of his work.

Teleprinters

The principle of a teleprinter is simply that two machines are connected by some sort of telecommunications line, like the Swedish telegraph cables, and transmit coded characters over the line which are automatically output (printed or punched) by the receiver. For the character representation on the line, the German machines used the common standard, a 5-bit binary encoding called International Telegraph Alphabet No 2, or Baudot code. Because 5 bits gave not much room over the standard 26 letters, the machines actually operated in

Letter shift	*Code Pulses*	*Figure shift*	*Intercept notation*
A	11000	−	
B	10011	?	
C	01110	:	
D	10010	“Who’s there?”	
E	10000	3	
F	10110	Country-specific	
G	01011	Country-specific	
H	00101	Country-specific	
I	01100	8	
J	11010	Bell	
K	11110	(	
L	01001	)	
M	00111	.	
N	00110	,	
O	00011	9	
P	01101	0	
Q	11101	1	
R	01010	4	
S	10100	’	
T	00001	5	
U	11100	7	
V	01111	=	
W	11001	2	
X	10111	/	
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

Table 1: Baudot code

one of two modes, called letter and figure shift. These were activated by sending a certain control code that then determined the interpretation of the following code points, until the next shift.

Table 1 summarizes the ITA 2 code.[2] Notice the fourth column, *Intercept notation*. In the encrypted stream, all control codes like shifts, new line, etc. lost their meaning. The Swedish wire-tappers had therefore adjusted their equipment to always print in letter mode and show the control codes as the digits 1–6, to more directly represent the transmitted code stream.

[2]The code bits (also called *pulses*, wrt. their electrical representation) are here shown, from left to right, in the order of transmission by the German equipment.

Teleprinter cryptography

Soon after the advent of teleprinters, it was noticed that it was quite easy to encipher the transmitted text, by using what was referred to as *additive superposition*, or just super-position for short. The idea is to produce, in parallel to the plain text bit-stream, a random *key stream* and bit-wise add them, modulo 2. This operation is relatively easy to realize electro-mechanically and if the key stream is truly random the technique is equivalent to a one-time pad system.

To avoid the logistics of true one-time pads, the idea of machine-generating a pseudo-random stream was born. This was usually accomplished by wheels with equidistant positions around their circumference that could indicate either 0 or 1, usually represented by some sort of pin being either present or absent. Then, for each bit, a certain pin position would be read to yield the corresponding key bit. Of course a single wheel would soon have cycled through all its pins and start repeating the same sequence, diminishing cryptographic security. To counter this, multiple wheels would be used.

Beurling's analysis

The German intercepts were not completely enciphered, only certain sections, so Beurling could read lots of operator chat. A typical intercept could look like this:

```
hier35mbz35qrv54b35kk35qep45qw55wt55qi55ru55tw
3355553535umum35veve35zrddlh5fny13qukd4gehnswo
```

Remember that the digits represent control characters.

`3` – letter shift `4` – figure shift `5` – space

So, taking figure shift into account, the above would actually represent:

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

The meanings of the many abbreviations were of course known to the Swedish tappers/cryptanalysts. First, the sending station reports with its identifier MBZ and asks for confirmation; QRV is standard code for "do you understand". The next abbreviation, KK, is for German "klar" ("clear"). At the end, UMUM and VEVE stand for "umschalten" ("switch") and the confirmation "verstanden" ("understood"). These two trigger words presumably automatically switched the machines into crypto mode. They were always preceded by QEP and a set of numbers, appearently that part of the crypto variable which (is supposed to) change for each new message, to avoid the transmission of different plaintexts with the same key. That effect was termed *depth* and the German operators did in fact produce great numbers of it, as evidenced by the repeats Beurling had found.

These repeats were indeed the entry into breaking the code. Recall that for a repeat to occur among two messages using the same key, plaintext characters at equal positions within the messages had to be identical. While this might happen relatively often for single characters, it is already much more unusual for digraphs, consecutive pairs of characters. So it appears likely that a digraph repeat should represent a very frequent digraph. Observe in the example above, the operators' habit of typing "35" (letter shift, space) between words. That

was done because it somewhat suppressed the annoying but frequent effect of text becoming unreadable when line noise caused the receiver to erroneously shift into figure mode.

Now suppose that Beurling was faced with the following set of messages, all encrypted with the same key:

```
 1.  alzgj1guh4hjplhn6n5bve3cquhgfbjn...
 2.  np3umwfz31nmykmjhb625fmquhfdfz45...
 3.  grqumaa4jtqflqmhjiegtvfwpoi32slk...
 4.  lyzgj1oryydrqknhjn51akfd5vcerwrv...
 5.  lezgkvrvanbwe6mjutgbtrv36h4h1cs1...
 6.  bota3wfusgoda2jiunykriyytsfscogb...
 7.  yeyzl42dyd5lmhloimuqtge5shbzsheb...
 8.  rkzgbwflix6azemkey4dwombocxq6lbl...
 9.  ccnrwwgkotv5llumcd3e4r3iyhjasla6...
10.  1txumsmu4vvntzjnfiw35sdedotpmand...
```

Upon close inspection, several repeats can be spotted and Beurling would assume them to correspond to the digraph 35:

A	L	**Z** 3	**G** 5	**J** 3	**1** 5	G	U	H	4	H	J	P	L	...
N	P	3	**U** 3	**M** 5	**W** 3	**F** 5	Z	3	1	N	M	Y	K	...
G	R	Q	**U** 3	**M** 5	A	A	4	J	T	Q	F	L	Q	...
L	Y	**Z** 3	**G** 5	**J** 3	**1** 5	O	R	Y	Y	D	R	Q	K	...
L	E	**Z** 3	**G** 5	K	V	R	V	A	N	B	W	E	6	...
B	O	T	A	3	**W** 3	**F** 5	U	S	G	O	D	A	2	...
Y	E	Y	Z	L	4	2	D	Y	D	5	L	M	H	...
R	K	**Z** 3	**G** 5	B	**W** 3	**F** 5	L	I	X	6	A	Z	E	...
C	C	N	R	W	W	G	K	O	T	V	5	L	L	...
1	T	X	**U** 3	**M** 5	S	M	U	4	V	V	N	T	Z	...

A first guess that the cipher at hand might actually be of the additive superposition type quickly leads to the realization that this is not the case. At the same time, however, and through a bit of coincidence, it does provide a valuable hint as to what *is* being used.

For the following discussion, let $+$ denote bit-wise addition modulo 2 and remember that in that setting $x - y = x + y$.

The central weakness of additive-superposition ciphers is that when depth occurs, i.e. two messages a and b are enciphered with the same key stream k,

$$m = a + k, \quad m' = b + k$$

the difference of the ciphertexts equals the difference of the plaintexts.

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

Then, whereever a or b can be guessed, everything else is also revealed. In our G-Schreiber example, however, we find that the above equality does not hold. Take for example the fourth column, where several 3's are assumed to encrypt to U and several 5's to G. Observe the differences:

U	1**1**100	3	11**1**11
G	0**1**011	5	00**1**00
	1**0**111		11**0**11

They are *almost* the same, except for the single 0 appearing in the wrong place. Checking against the other columns containing both 3 and 5, we find the same effect:

J	110**1**0	W	11**0**01
M	001**1**1	1	00**0**10
	111**0**1		11**0**11

Always just a single 0, but in differing places. To recapitulate, we have assumed a certain plaintext (with fairly good confidence) and are inspecting the ciphertext under the additional hypothesis that additive superposition was used. We have found that the ciphertext *almost* meets our expectations $(3 + 5)$, *except* that a certain bit seems to move around — or maybe, all of them?

Beurling now poses just this

Hypothesis. *The Nazi cipher is in fact an additive superposition, but followed by a random permutation σ.*

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

Looking at the differences above, we can assume that, in the fourth column for instance, one part of the permutation would be the mapping $3 \mapsto 2$. If we can find more pairs of characters whose difference has one distinctive bit like $3 + 5$, we should be able to reconstruct the entire permutation for any column in which enough of these characters appear.

Note that at this point we cannot be sure whether the permutation actually occurs before or after the superposition. Both $m = \sigma(a + k)$ and $m = \sigma a + k$ would explain our observations. To see how, first note that the permutation distributes over addition:

$$\sigma(x + y) = \sigma x + \sigma y$$

Then:

$$\begin{aligned} & \sigma(a + k) + \sigma(b + k) &=& \sigma(a + b) \\ \wedge\quad & (\sigma a + k) + (\sigma b + k) &=& \sigma(a + b) \end{aligned}$$

Luckily, we can discover that a wrong guess here would not hurt our efforts for the moment. Suppose the Geheimschreiber performs $m = \sigma a + k$ but we work in accordance with our assumption above, $m = \sigma(a + k)$. If we have managed

to find the permutation we could reconstruct the key and then decrypt any remaining ciphertext. Let σ' be the inverse of σ. We would *want* to calculate

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

but would *actually* get

$$\sigma'(\sigma a + k) + a = \sigma'\sigma a + \sigma' k + a = \sigma' k \quad .$$

However, when we use this false key for decryption, our mistakes cancel out:

$$\sigma'(\sigma b + k) + \sigma' k = \sigma'\sigma b + \sigma' k + \sigma' k = b$$

We cannot tell just now whether our permuted view of the keystream would have an adverse effect on further analysis, because we do not have any clues, yet, about how the key bits are generated. We can confirm our hypothesis, though, by trying the other alternative. If that one is wrong, our mistake will *not* cancel out. Analogous to before, what we would try to calculate is

$$k = \sigma a + k + \sigma a$$

but we would actually get

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

and, trying decryption,

$$\sigma(a + k) + \sigma k = \sigma a + \sigma k + \sigma k = \sigma a \quad ,$$

an easily detected mismatch. So, for the purpose of presentation, let it be betrayed that Beurling has taken the right guess above, whether it was *really* his first choice or not.

As hinted above, we can find some more character pairs with distinctive differences like 3 and 5, to help us discover the permutations. Remember the abbreviation QRV — "do you understand". It was very commonly sent in the beginning of messages and Beurling thought that quite possibly, the German operators would also follow this habit after switching to crypto mode, to see whether everything was set up alright. After all, line noise was a common problem and could have garbled the transmission of one of the QEP numbers, or something similar. Coincidentally, the letters Q, R, and V, together with 3 and 5, provide us with just the kind of pairings we need!

3	111**1**1	Q	1**1**101	3	**1**1111
Q	111**0**1	R	0**1**010	V	**0**1111
	0001**0**		1**0**111		**1**0000

Looking for a likely place for QRV to appear, compare what we know about the second and third messages:

2)	N	P	3	**U**	**M**	**W**	**F**	Z	3	1	N	M	Y	K
				3	5	3	5							
3)	G	R	Q	**U**	**M**	A	A	4	J	T	Q	F	L	Q
				3	5	*?*	*?*							

In message 2, 3535 occurs where message 3 only shows a single 35. In fact the following plaintext of message 3 must be different from 35 because otherwise the ciphertext would need to equal WF, the same as in message 2. So maybe, the 35 of message 3 is followed by QRV? In that case, each column should agree with

our hypothesis, i.e. the difference between the plaintext characters should be a permutation of the difference between the ciphertext characters. And indeed, the invariant holds for both columns:

W	11001	3	11111	F	10110	5	00100
A	11000	Q	11101	A	11000	R	01010
	00001		00010		01110		01110

The same situation also occurs between messages 4 and 5 and with some tenacy, one can discover several more probable QRV's and 35's:

A	L	**Z**	**G**	**J**	**1**	G	U	H	4	H	J	P	L	...
		3	5	3	5	3	5	3	5					
N	P	3	**U**	**M**	**W**	**F**	Z	3	1	N	M	Y	K	...
			3	5	3	5	Q	R	V					
G	R	Q	**U**	**M**	A	A	4	J	T	Q	F	L	Q	...
			3	5	Q	R	V							
L	Y	**Z**	**G**	**J**	**1**	O	R	Y	Y	D	R	Q	K	...
		3	5	3	5	Q	R	V						
L	E	**Z**	**G**	K	V	R	V	A	N	B	W	E	6	...
		3	5	Q	R	V	3	5						
B	O	T	A	3	**W**	**F**	U	S	G	O	D	A	2	...
					3	5								
Y	E	Y	Z	L	4	2	D	Y	D	5	L	M	H	...
R	K	**Z**	**G**	B	**W**	**F**	L	I	X	6	A	Z	E	...
		3	5		3	5								
C	C	N	R	W	W	G	K	O	T	V	5	L	L	...
1	T	X	**U**	**M**	S	M	U	4	V	V	N	T	Z	...
			3	5										

To find the permutations, recall the four special pairs of characters at our disposal: 3-5, 3-Q, Q-R, and 3-V. If one of these pairs appears in some column, we can, just as in the 3-5 example earlier, compare the plaintext and ciphertext differences to detect the movement of the distinctive bit, revealing one element of the permutation. Since our four special differences all have the distinctive bit in a different place, if we can find all four pairs in one column, the entire permutation is revealed. Take for example, the seventh column:

3	**1**1111	Q	1**1**101	3	11**1**11	3	111**1**1
V	**0**1111	R	0**1**010	5	00**1**00	Q	111**0**1
	10000		1**0**111		11**0**11		0001**0**
G	0101**1**	O	00**0**11	G	0101**1**	G	0**1**011
R	0101**0**	A	11**0**00	F	1011**0**	O	0**0**011
	0000**1**		11**0**11		1110**1**		0**1**000
$\Rightarrow$	$1 \mapsto 5$		$2 \mapsto 3$		$3 \mapsto 4$		$4 \mapsto 2$

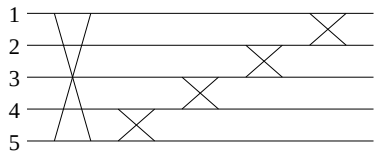
The only remaining possibility is $5 \mapsto 1$ and we have discovered the permutation for column seven: [53421]. The key for this column is now given by $k = \sigma' c + a$

where $c = \sigma(a + k)$, i.e. c is any ciphertext character (from this column) with known corresponding plaintext a.

Deciphering the thus broken columns, we might be able to guess some more plaintext words which in turn might enable us to break yet more columns, and so on. We can discover quite a bit of plaintext by this method, but it is not completely satisfactory. It is slow and tedious and depends on our ability to correctly and continuously guess new plaintext words, all in all requiring a rather large number of messages in depth. To be able to reliably decrypt all traffic, we should find out how the German machines generated the stream of key characters and permutations in the first place! If we knew that, we could hope to discover their internal state once and then routinely decrypt everything just by emulating the receiver.

As for the key bits for the superposition, it seems very probable that Beurling assumed the G-Schreiber to use pin-wheels. As he put it himself, "all engineers used wheels at the time". But how were the permutations generated? Here, Beurling remembered hearing about the use of *relay switches* telephone exchanges. Depending on the position of the switch, current would be directed to one output wire or another. He noticed that a transposition could be readily realized by such a switch: the two input wires would be cross-connected to the output wires if the switch was closed or connected straight through when it was open. A random setting of these switches could then be produced in the same way as the rest of the key bits, presumably by rotating pin-wheels.

We know there are five output signals to be permuted. Under the above assumption, the only question that remains is how many transposition switches there are and how they are connected to the output wires. Luckily, the discovered actual permutations provide some hints as to how the switches might be arranged. For instance, in column seven, as we discovered above, the permutation is [53421], which is uniquely decomposed into the transposition (51) and the cyclic permutation (234). The latter is readily realized as $(23) \circ (34)$, although other combinations are possible. While the wiring of the switches to the output lines could well be variable, it *most* probably would not change within the same message (probably not even within the same day), so inspecting further permutations should sooner or later provide enough information to determine the switch arrangement. Indeed, in our example, only a few more uncovered columns suffice to arrive with fairly good confidence at the following likely arrangement:



Now each of the discovered permutations corresponds to a five-bit pattern, presumably generated by pin-wheels, just like the five-bit key characters. They are not the same, so for every character there are ten random bits and we want to know how they are generated. If there are wheels involved, we might hope for repetition to occur somewhere, and indeed, after Beurling had deciphered about 100 consecutive positions manually, it became noticable that the individual bits of the ten-bit wide stream had started to repeat at varying positions. For instance, the sequence of bits in the first place might have repated after 47

characters, while the second-place bit would start repeating after 61, and so on. Unsurprisingly, these numbers turn out to be pair-wise coprime, maximizing the period of the 10-bit stream as a whole. Now this definately looks like each bit is generated by a single wheel, circumscribed with a random bit pattern. Further, the wheels most likely step by exactly one position for each character because otherwise the repeat positions would, in all probability, not appear so fittingly coprime.

So the mystery is solved. Unless we have made a mistake with one of our assumptions, we now know the construction of the Geheimschreiber, including, for as long as they are valid, the bit patterns on the pin-wheels, their initial positions, and the arrangement of the transposition switches.

Swedish apparatus

With Beurling's solution in hand, the Swedish cryptanalysts could now proceed to "industrialize" the processing of incoming intercepts.

Some final loose ends were quick to tie up, given a few messages in sufficient depth. First, it's easy to discover what exactly the QEP numbers at the beginning of messages mean: To little surprise, they provide the initial settings for five of the ten pin-wheels, to be set by the operators before switching to crypto with the UMUM/VEVE exchange. Exactly which wheels those were, as well as the initial settings for the other five wheels was fixed for each day and changed at midnight. The wheels' pin patterns, as it turns out, were never changed. Modifications to the transposition switch arrangement were infrequent and stopped completely after April 1 1942.

So, every day, some messages in depth were required from which a section of 20 to 50 positions had to be deciphered by hand. The appearing keystream could be fitted to the known wheel patterns in order to determine the fixed settings for the day. From there on, messages could be decrypted "mechanically". In fact, soon after establishing this routine, the Swedish built their own machines, termed "apps" from *apparat*. They exactly emulated the decryption behaviour of the G-Schreiber and were connected to an ordinary teleprinter: After initializing the app, cyphertext could be typed and the app decrypted it, sending the plaintext back to be printed.

References

[1] Bengt Beckman: *Codebreakers — Arne Beurling and the Swedish Crypto Program during World War II*, Oxford University Press 2003

[2] 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