Willard's System

Niels O. Faurholt
MJ, DAA, retired
DDIS Technical-Historical Collection
faurholt@fasttvnet.dk

Abstract

Willard's cryptosystem is an unusual system, designed by an otherwise unknown American around 1870. It was used for a short period of time by the Danish Ministry of Foreign Affairs. The article describes the system. Furthermore the article mentions an interesting and lively period of Danish crypto activities 1873 - 1918.

1 Background

For a few years before 1873 the Danish Ministry of Foreign Affairs (MFA) used for its enciphered communication a crypto system invented by a person named Willard, presumably an American. It has not been possible to find more information about Willard. According to papers in the MFA he was an acquaintance of the Danish diplomatic representative in Washington D.C., and the MFA must have bought the system around 1870. In 1873 a Danish school teacher, Gravers Pedersen, who later took the name Orloff, showed to the MFA that messages enciphered in Willard's system could fairly easily be broken by simple cryptanalysis. The result was that the MFA stopped using Willard's system, and on 18th October 1873 introduced a new system, invented by Mr. Orloff, for its enciphered communication. However, Willard's system is a curious invention, even if it had a short life in the Danish MFA.

2 Danish Crypto Activities 1873 - 1918

Before going into the details of Willard's system I would like to mention the remarkable crypto activity in Denmark from 1873 to about 1918. The inspirator was professor Julius Petersen (1839-1910). He was teaching mathematics at the Polytechnical University and later became professor of mathematics at Copenhagen University. He was for a few years from 1875 very active in cryptography, before he went on to other fields of mathematics and geometry. He is mostly known for his contribution to graph theory. In 1875 he, anonymously[1], wrote a remarkable series of articles in the Danish weekly journal ”Nær og Fjern” (Near and Far) about seven international and Danish cryptographic systems, describing the systems and showing how they could be broken. At least three of the systems had been in use in the Danish MFA. Each article ended with some ciphertexts in that system, and amateur cryptanalysts had two weeks to solve them and report them to the journal, before the solutions were given in the next issue. The systems described were:

Carré Indéchiffrable (Vigenère type)
Willard's System
Léopold Auvray's System
Wheatstone's Cryptograph
Clausen's Apparatus (Danish Military)
Orloff's System
Orloff's Modified System.

Julius Petersen followed up with a paper&pencil system of his own later in 1875. It is assumed that it originally should have been included in the series in the journal. It was a rather complicated system, and Julius Petersen consid-

[1] The articles were written under a pseudonym: 46,9,4 – 57,3,5. The meaning of this is not known, but might indicate page, line and place in a book, as seen in book ciphers. However, the authorship of Julius Petersen is strongly indicated by three facts:

a. Immediately after the articles in ”Nær og Fjern”, where he demonstrated the lack of secure cryptosystems, Julius Petersen published his own (unbreakable) Système Cryptographique.

b. Alexis Køhl in an unpublished article in 1916 refers to the articles in ”Nær og Fjern”, that ”long ago were written by the late Julius Petersen”, as his inspiration for going into cryptography. Køhl publishes his first system in 1876.

c. The plaintext used in one of the examples in the Willard article in ”Nær og Fjern” is a quote from one of Julius Petersen's own mathematical textbooks (observation by Knud Nissen, Aarhus Academy).

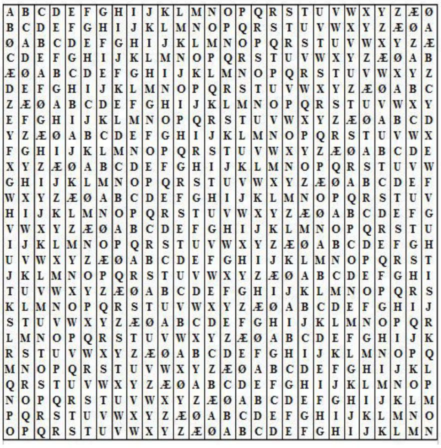
Proceedings of the 1st Conference on Historical Cryptology, pages 129– 132,
Uppsala, Sweden, 18-20 June, 2018

ered it unbreakable which in principle probably was correct at the time. It seems likely that Julius Petersen's intention with the series in "Nær og Fjern" was the creation of a Danish "Black Chamber". The successful problem solvers might be recruited for such an organisation. However, there was no political will to support such a project, and nothing came out of it. In his footsteps followed the Danish engineer, Alexis Køhl (1846-1920) who openly admitted that Julius Petersen was his inspirator. Køhl started with two paper&pencil systems in 1876, not unlike Petersen's from 1875, and in 1883 Køhl presented his Automatic Cryptograph, based om Rasmus Malling-Hansen's Writing Ball (now in Musée des Arts et Métiers in Paris). Køhl continued constructing crypto systems, a paper&pencil system in 1888, a cryptograph in the late 1880es (now in Deutsches Museum im München), other cryptographs around 1890 and around 1913 (both now in the Danish Technical Museum). His last devices are from 1917-18. Army captain (later colonel) E.J.Sommerfeldt was another inventor of cryptosystems, and his cryptograph was adopted by the Danish army in 1883 and used for a number of years.

3 Willard's System

The description of the system is mainly based on professor Julius Petersen's article from 13th June 1875. The heart of the system is a table consisting of 28 columns with a Danish alphabet that in addition to the standard 26 characters has the letters Æ and Ø. (Figure 1)

The table is constructed as follows: In the top **row** are the letters **A** to **Ø**. In the second **row** is the alphabet starting with **B**. The **A-column** is filled in alphabetic order, but every second place is left open. When the bottom of the A-column is reached, the alphabet is continued upwards in the empty spaces. The rows are then filled alphabetically, starting with the letters in the A-column. When **Ø** is reached the row continues with **A**. The system "hardware" is simply 28 cardboard sticks, each corresponding to one of the columns in the table. The top letter on each stick is called the key letter. The set is enclosed in a red cardboard box (Figure 3).

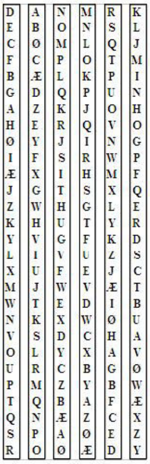


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	A
Ø	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	A	B
Æ	Ø	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N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

Figure 1: Willard's Table

4 Encipherment/Decipherment

A keyword must be ordered, here e.g. DANMARK. From the keyword we choose the columns (sticks) to be used for the encipherment, here the columns with the key letters D,A,N,M,R,K (repeated letters are skipped). The sticks are laid up, so that they form a rectangle. (Figure 2 and 3)



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

Figure 2: Sticks, selected according to ordered keyword

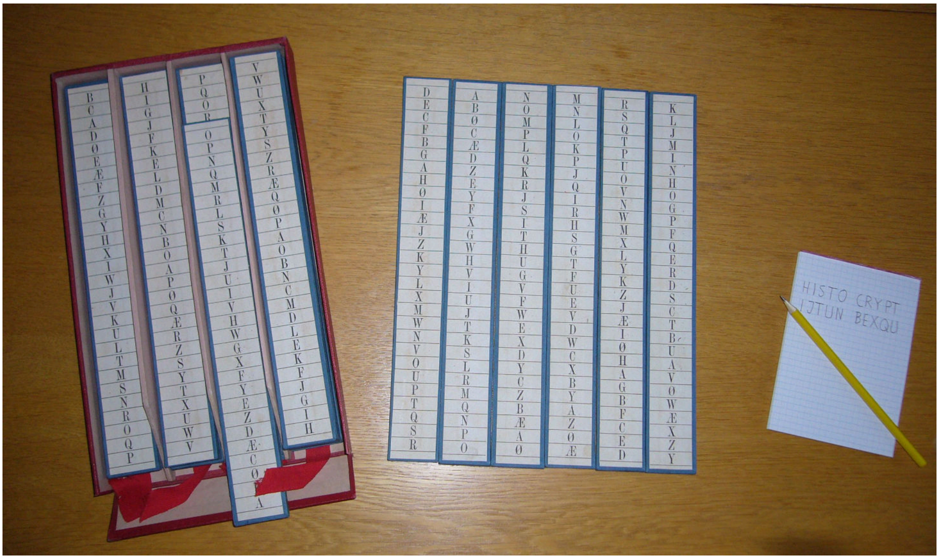


Figure 3: Willard "hardware" and the encipherment process

You want to encipher the word "HISTOCRYPT". You find the first plaintext letter "H" in the first column. The corresponding cipher letter stands x places above or below "H". This must be agreed beforehand. If the agreed rule is "x=go down 2", you go two places down from "H" in the first column and find the cipher letter *"I"*. The second plaintext letter "I" is found in the second column. Down 2 gives cipher letter *"J"*. The third plaintext letter "S" is found in the third column. Down 2 gives cipher letter *"T"*. And so on. If a plaintext letter is at the bottom of a column, you go to the top of that column to find the cipher letter.

Plaintext HISTOCRYPT thus becomes ciphertext

IJTUN BEXQU

Decipherment is performed in exactly the same manner, except that you go "up 2" from the cipher letter.

5 Security

How secure is this system? As the Danish school teacher showed in 1873, it is not particularly secure.If you have a cipher message long enough (15 - 20 times the length of the keyword) it can be broken. The periodicity is the weak point. Another weak point is that if you have to count many places up or down in the columns, it will be difficult and give frequent errors. So normally you could assume that 5 places up or down will be the maximum. The length of the keyword will also for practical reasons seldom exceed 6 -10 letters. In theory all the sticks could be used, 28 in all, but that would give a very cumbersome operation.

6 Cryptanalysis

Due to the construction of the Willard table, breaking the cipher depends largely upon the number of steps you go up or down in the operation. Even numbers are much easier to break than uneven numbers.

Even number of steps (2 or 4): As the columns are in alphabetic order with every second place skipped, only a few letters can come 2 or 4 places above or below a given cipher letter. We start with 2 places up and down: E.g. cipher *"I"* above will become plaintext "J" or "H" (there are exceptions in columns A and Ø). Cipher *"J"* will become plaintext "K" or "I". It is possible quickly to form tables with 2 up or down, and 4 up or down, and it will be obvious which of these is the correct one. The plaintext can then be read in the table. Finding the keyword requires a longer message. If the test for even number of steps does not succeed, uneven steps are probably used.

Uneven number of steps (1, 3 or 5): Here the construction of the table cannot help in the same way. In principle any cipher letter can become any plaintext letter. So we will have to use the Kasiski[2] method to find the length of the keyword, e.g. 5, and then solve the resulting monoalphabetic cipher texts the hard way. However, there is a possibility to find the keyword: You have a good chance to locate "E" in each of the 5 monoalphabetic cipher texts. You can construct a table that for each (cipher) letter shows in which column that letter stands 1, 3 and 5 steps above or below "E". If you combine the "E"-equivalents with that table, you may find which 5 columns (sticks) were used in the encipherment. This gives the keyword and an easy way to read the whole message.

Acknowledgements

I am most grateful to professor emeritus Ole Immanuel Franksen from the Danish Technical University. Mr. Franksen brought the old periodical, "Nær og Fjern", to my attention and kindly allowed me to use his extensive research in the Danish crypto history in this article.

Without the great help of my good colleague, Hans-Erik Hansen, this article would never have been converted to the required format.

The Danish Defence Intelligence Service (DDIS) Technical-Historical Collection owns the Willard hardware, presented to the collection by a former MFA employee. I am the curator (volunteer, unpaid) of the collection.

References

Buonafalce, Augusto, Niels Faurholt and Bjarne Toft. 2006. *Julius Petersen - Danish Mathematician and Cryptologist.* Cryptologia, Vol. 30: 353-360.

Faurholt, Niels. 2006. *Alexis Køhl: A Danish Inventor of Cryptosystems.* Cryptologia, Vol. 30: 23-29.

Johnsen, Erik, Morten Christensen, Ole Immanuel Franksen and Knud Nissen. 1994. *Willard's System.* Matematiklærerforeningen DTU, Lyngby, DK

Kasiski, Friedrich W. 1863. *Die Geheimschriften und die Dechiffrier-Kunst.* E.S.Mittler und Sohn, Berlin

Kjølsen, Klaus and Viggo Sjöqvist. 1970. *Den danske Udenrigstjeneste 1770-1970, Vol. I.* J.H.Schultz, Copenhagen, DK

Petersen, Julius. 1875. *Nær og Fjern*, 154:4-7. Periodical, Copenhagen, DK

[2] The Kasiski method looks after repeated trigrams or longer in the ciphertext, and determines the distances between these. These distances will in most cases be a multiple of the length of the keyword. Once the length of the keyword is found, the cipher message is split into that number of monoalphabetically enciphered texts, that must be solved by frequency analysis.