The Solving of a Fleissner Grille during an Exercise by the Royal Netherlands Army in 1913

Karl de Leeuw
University of Amsterdam / Informatics Institute
Science Park 904, 1098 XH Amsterdam
karl.de.leeuw@xs4all.nl

Abstract

In 1885 the General Staff of the Royal Netherlands Army had adopted a variant of the turning grille devised by Edouard Fleissner von Wostrowitz as a means for encrypting messages, exchanged by telegraph between the General Headquarters and commanders in the field. Some staff members harbored serious doubts about the security of this device, however, and during a military exercise in 1913 it was solved with surprising ease by an army captain. The matter was investigated by a committee of staff officers, concluding that the army lacked the expertise to judge matters like this. It recommended the training of a staff officer for this purpose in particular. The outbreak of the First World War was to speed up the decision process, but – against all odds – the newly trained experts were not drawn from the ranks that had demonstrated their talent for code breaking a year earlier, because these were destined to follow different career paths altogether.

1 Introduction

Kahn (1967) describes the original grille, as conceived by Cardano as:

"a sheet of stiff material, such as cardboard, parchment or metal into which rectangular holes, the height of a line of writing and of varying lengths, are cut at irregular intervals. The encipherer lays this mask over a sheet of paper and writes the secret message through the perforations, some of which will take a whole word, others a single letter, others a syllable. He then removes the grille and fills in the remaining spaces with an innocuous sounding cover message." [1]

[1] Kahn, 144-145

Initially the grille was intended for hiding that a secret message was being sent at all, rather than as a means of encryption. This all changed during the course of the 18th century, when the grille was increasingly used for jumbling the characters in a message by rotating them, according to the holes in the mask. The first description of such use we find by the German mathematician Carl Friedrich von Hindenburg (1796) who was aware that such use could only be made at the expense of a loss in entropy and, therefore, cryptographic strength. The perforation pattern in one quadrant of the mask would automatically limit the possibilities for perforation in all others, because two punch holes could not be allowed to cover the same position after a rotation.

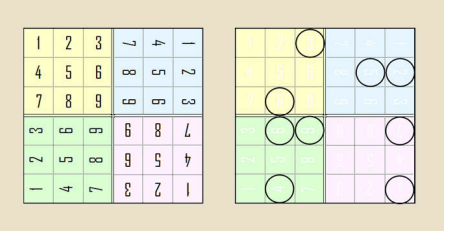

Figure 1: drawing showing how a turning grille can be punched

The appearance of the turning grille in scientific literature only at the end of the 18th century does not mean, however, that it wasn't used before. Karl de Leeuw and Hans van der Meer (1995) have demonstrated that the practice existed already 50 years earlier. The device gained wide popularity much later, after a Austrian Colonel Edouard Fleissner von Wostrowitz (1881) had drawn attention to it in a handbook about military cryptography. Essentially, he proposed the adding of two or more columns with nulls in order to hide the center of rotation of the actual cryptogram. At the eve of

Proceedings of the 1st Conference on Historical Cryptology, pages 49– 54,
Uppsala, Sweden, 18-20 June, 2018

and during the first world war his suggestion was followed widely. Kahn (1967) mentioned the use of turning grilles in different sizes by the Germans during the first months of 1917, only to be solved by French code breakers not much later.[2] The Dutch were no exception. In a circular announcement dated 23 April 1885 the General Staff proscribed the use of the turning grille for telegraph traffic in times of crisis between the General Headquarter and field commanders.[3] Some staff members, however, doubted the cryptographic strength of the device and one of them proposed the enciphering of the original message by means of a addition table, before deploying the turning grille proper.[4] This proposal did not get any follow-up, but the matter became urgent again on 20 June 1913, when another army captain, C.J.H. van der Harst (1876-1938), was able to break an encrypted message from GHQ with surprising ease. This incident caused commander in chief General C.J. Snijders (1852-1939) to appoint a committee to re-examine the use of cryptography by the army.

In this paper I will briefly discuss the military exercise and then show how the message was broken by Captain van der Harst. Subsequently I will analyse the way in which the entire incident was evaluated by the General Staff. In the conclusion, I will assess the viability of the measures taken.

2 The exercise

The Netherlands had been a neutral country since the defeat of Napoleon in 1815. Apart from colonial warfare, mainly in the East Indies and a military expedition to prevent Belgium from gaining its independence in 1830 it had not fought a major war for almost 100 years, when finally war broke out in 1914. The Netherlands managed to stay out of conflict, but were heavily affected by trade embargoes and the flooding of half a million refugees from Belgium. The army was not unprepared. It had to reckon with a military invasion by the British in the south west to liberate Antwerp and with a German attack from the east. The German building of armored flatboats with heavy guns had caused the army much distress, because these could enter the shallow waters protecting the Dutch capital and its surroundings. This clearly indicated that a German attack could not be ruled out, in case war broke out in Western Europe (Klinkert, 2017).

During this exercise, lasting two days in June 1913, a deployment of troops in the IJssel valley was simulated, entailing a movement of troops by train from the western to the eastern part of the country, including the transport of equipment for a field hospital. On the eve of the second day of the exercise – on 20 June – a cable message was sent by the field commander in the western part of country with orders for his troops already present in the eastern part. It was to be intercepted by the party supposedly defending the East, located in the stronghold Cortenoever, overlooking the valley.[5]

The encrypted message was given to Captain C.J.H. van der Harst who was to find out which orders were given for the next day. It consisted of 15 columns and thirty rows filled with letters only, no digits included. Captain van der Harst – who was detached by his regiment with the General Staff – had three advantages: (1) he knew exactly how the turning grille had to be handled according to the guidelines, issued by his colleagues at the General Staff, when it was introduced nearly twenty years before; and (2) he was familiar with the language used by army officers in cables like these; and (3) he was well aware of the limitation in entropy, offered by the turning grille, as he makes a remark about this in his notes.

To start with the first: the use of punctuation marks and digits was strictly prohibited. Numbers were to be represented by the first 10 letters of the alphabet, omitting the "j"; punctuation marks were to be spelled out. The sides of the grille were always indicated by means of the first eight letters of the alphabet. The square in the exact middle of the grille was used to indicate which side had to be placed on top to start with, from that position on every following rotation was to be made clockwise. If the message contained too many letters to fit one cipher block, this procedure was simply repeated. Remaining squares had to be filled in with nulls. The adding of at least two columns with nulls, recommend by Colonel Fleissner von Wostrowitz to hide the rotating center of the cryptogram, was not mandatory for regular use. The

[2] Kahn, 308-309

[3] The Hague, Nationaal Archief, Department van Oorlog, Generale Staf, inv. nr. 82

[4] Ibid., inv. nr. 305: Captain A. van Mens to General C.J. Snijders, Arnhem 1911, January 19. Van Mens wrote his advice on request of the chief of staff, given by mouth five days earlier.

[5] Ibid., inv. nr. 305: handwritten note without date containing instructions for the exercise.

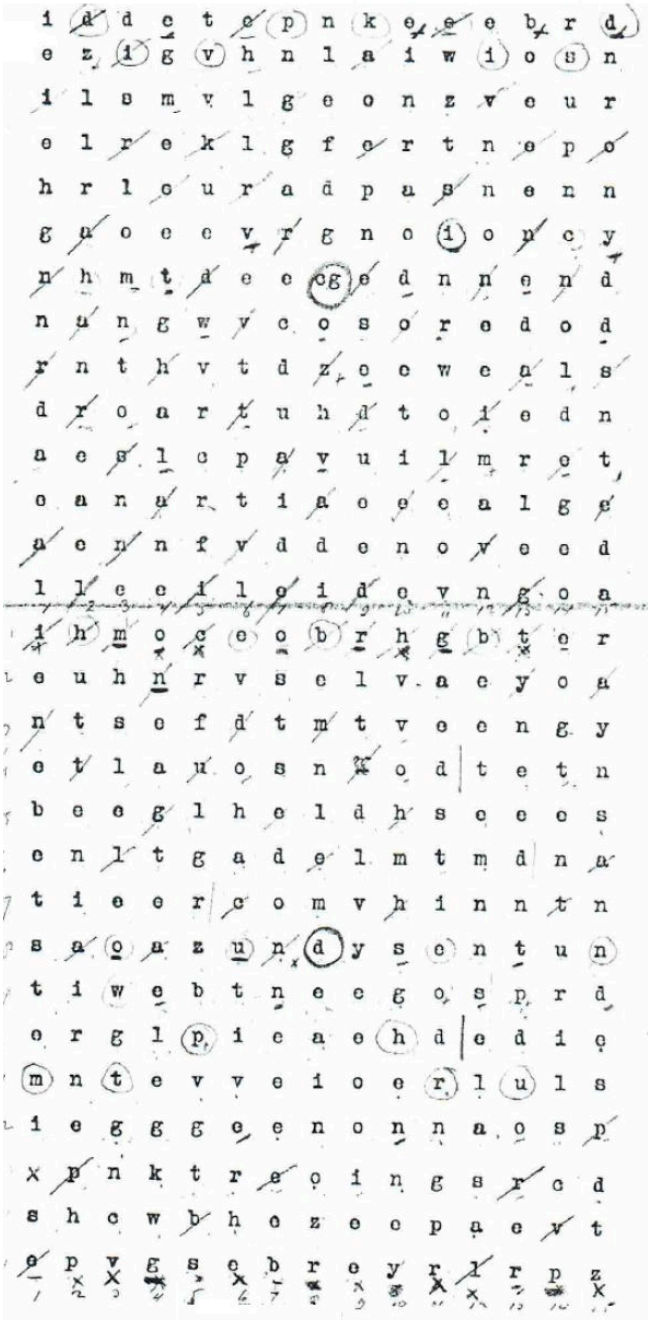

Figure 2: the supposedly intercepted message. Source: Nationaal Archief Den Haag

guidelines did mention this possibility, but only as a complicating measure, to be applied at will. A second complicating measure mentioned was the filling of the mask before rotation with nulls and starting writing the actual message after turning the backside up. This procedure could only be indicated if the center for rotation was filled with two letters: one to indicate the original position of the mask and one to indicate how it had been laid after the backside had been turned up.[6]

3 Reconstructing the grille in use

The approach taken by Captain Van der Harst to solve the cryptogram can be derived from his personal notes, handed over after the exercise to the commander in chief Lieutenant-General Snijders.[7] The captain started his analysis by stating that the size of the letter square, consisting 15 columns and 30 rows, probably indicated a plain use of the turning grille twice, without columns added. This implied that the letter square had to be divided into two halves of 15 rows each and that the punch hole in the exact middle of each letter square would have to contain a letter indicating which side of the grille had to be put on top first.

The square in the middle of the first cipher block contained two letters, however, 'cg', the square in the middle of the second cipher block only one letter: 'd'. Therefore, Van der Harst decided to proceed with the second cipher block.

The captain subsequently asked which words were likely to emerge in the message, words that could be detected easily, because of their spelling that is to say. He mentioned several: 'vyand' (enemy), because the 'y' does not occur very often in Dutch; 'bericht' (message), because the trigram 'cht' is rare; and 'opperbevelhebber' (commander in chief), because this word contained two doublings of consonants: 'pp' and 'bb' which is rare in Dutch also. Generally speaking, Van der Harst expected the message to contain information about troop movements, not yet known to the field commander, orders, or reconnaissance about the enemy.

The first row of the cryptogram contained the letters 'i', 'c'. 'h', and 't', likely constituting the last syllable of the word of 'bericht'; the last row contained 'b', 'e' and 'r', constituting the first syllable of the same word. These letters had to correspond with three punch holes of the mask. Consequently, these squares had to remain black when the grille is turned. The drawing of the mask could now begin. The last row contained one more probable word: 'g', 'r', 'y', 'p', (*attack*). This word is likely to occur in a sentence like this: 'gryp morgen vyand aan' (*attack the enemy tomorrow*). These words can be constituted from letters also to be found in the first and second row, indicating the position of the punch holes when side II is put on top. Another probable grouping of words would be: 'met uwe geheele macht' (*with your entire force*). Detecting of these words makes the unveiling of the second cipher block almost complete. The text occurring in the punch holes when side IV is put on top can now be reconstructed: 'or u vastgestelde stations zijn uitgeladen kondschapsber' (*Railway stations allocated by you reconnaissance mess...*). This implicates that the square is to be used first with side IV being put on top, before side I, II and III are moved to this position, correponding with the letter 'd' in the middle of the second cipher block. The remaining letters occurring when side III is put on top constitute rubbish. The entire text emerging in this cipher block is now clear:

'door u vastgestelde stations zijn uitgeladen volgens kondschapsbericht heeft vyand te helder minstens drie divisies ontscheept gryp morgen vyand aan met uwe geheele macht en werp hem terug opperbevelhebber slot'

(allocated railwaystations are unloaded according to reconnaissance message the enemy has disembarked at least three divisions in helder attack the enemy tomorrow with your entire force and throw him back commander in chief end).

With help of the reconstructed grille, but only after moving the mask in various positions in a process of trial and error, the following message emerged:

Derde divisie, korps RA en vliegafd zullen hedenavond en nacht worden aangevoerd en be-

[6] Ibid., inv. nr. 82: Aanwijzing voor het gebruik van geheimschrift (*Clues for the use of Secret Writing*). It is unclear to me how this recommendation was to be put into practice, if a cable gram was actually sent. After all, all of this depended on the neatly reorganizing the cryptogram in groups of four letters. Clearly, in one way or the other, it had to be indicated that the telegram contained two letters that had to be placed in one square, but how?

[7] Ibid., inv.nr. 305: | Methode van ontcijfering van het geheimschrift (*Method of Deciphering of Cryptogram*). Annex to the letter sent by Lieutenant-General C.J. Snijders to staff captains P. Huizer, E.F. Insinger and P.J. Van Munnekrede, s'Gravenhage, 7 November 1913, GS no 138, Geheim.

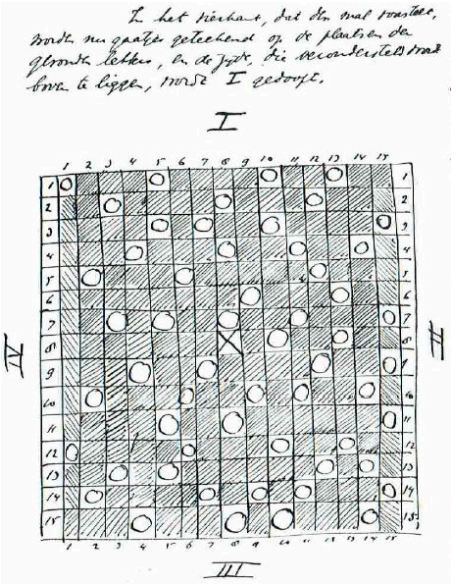

Figure 3: The grille as teconstructed by Van der Harst. Source: Nationaal Archief

halve verpleging en veldhosp afd morgenochtend om zes uur aan de door u vastgestelde stations zijn uitgeladen volgens kondschapsbericht heeft vyand te helder minstens drie divisies ontscheept gryp morgen vyand aan met uwe geheele macht en werp hem terug opperbevelhebber slot'

(third division, royal horse artillery and aircraft unit will be conveyed this evening and night and except for hospital staff and hospital equipment tomorrow morning at six o' clock unloaded at the designated railwaystations according to reconnaissance message the enemy has disembarked at least three divisions in helder attack enemy tomorrow with your entire force and throw him back commander in chief end)

4 The staff report

On 7 November 1913 General C.J. Snijders decided to put the matter before a committee of three staff officers: the captains P. Huizer, E.F. Insinger and P.J. Van Munnekrede. He asked whether the turning grille could be improved or had to be replaced altogether. If the last was to be case, he demanded to pay attention to the question whether the system in use by the Royal Netherlands Navy could be adopted by the Army as well. This would have the advantage that Army and Navy could exchange secret messages without additional effort.[8] He also wanted them to take notice of a system, described recently in a French journal.[9]

Unfortunately, this committee lacked all code breaking experience. It proved, however, to be well versed in the cryptologic literature of the day. It cited among other titles *Les chiffres secrets dévoilées* by E. Bazeries (1901); *Etude sur la cryptographie* by A. Collon (1906); *Kryptographik* by L. Kluber (1809); *Die Geheimschriften im dienste des Geschäfts- und Verkehrslebens*, by H. Schneikert (1905); not to mention of course the well-known *Handbuch der Kryptographie* by E. Fleissner von Wostrowitz (1881).[10] This sufficed, however, to discourage adoption of the cipher system used by the navy, because this consisted of a simple Caesar alphabet to encipher the existing optical signal register whenever needed, offering no genuine protection at all.[11] What is more, according to the committee, a common cipher system for army and navy was unnecessary and even dangerous: unnecessary because army and navy units were not be in direct contact, orders being always given top down; and dangerous, because the distribution of ciphers would become too widespread to offer security any longer. Encryption had to remain limited to messages exchanged between the GHQ and the field commanders.[12]

Surprisingly, a careful examination of the literature had lead the committee to believe that the turning grille was one of the strongest encryption devices available, as no convincing cases were presented of its solution. It did believe, however, that the way in which the system was used in the Netherlands, was ready for improvement.[13] In the view of his colleagues, Captain van der Harst was able to break the cipher, only because he had a some idea what the messages was about; because he was well aware what probable words to look

[8] Ibid., inv.nr. 305: Lieutenant-General C.J. Snijders to staff captains P. Huizer, E.F. Insinger and P.J. Van Munnekrede.s'Gravenhage, 7 November 1913, GS no 138, Geheim.

[9] Génie Civil,XXIII (26), 420.

[10] The Hague, Nationaal Archief, Departement van Oorlog, Generale Staf, inv. nr. 305: Beschouwingen en voorstellen in verband met het bij den Generale Staf in gebruik zijnde geheimschrift. d.d. 30 May 1914. (*Reflections and Propositions with regard to Secret Writing as practiced by the General Staff.*

[11] Ibid., 4.

[12] Ibid., 5-6.

[13] Ibid., 6-7

for; and, last but not least, because no complicating measures, such as the adding of columns to hide the real rotating center of the cipher block were ever taken.[14] Much in line with the original suggestion made by Captain Van Mens in 1911, the committee recommended the enciphering of the original message before putting it under a turning grille by way of a Vigenère, carefully explaining how a Vigenère worked.[15]

The committee did not go into the actual cryptanalysis of the message. It was well aware that it lacked the hands-on experience, needed in an actual war. Therefore, it recommended the appointment and training of an additional staff officer to gain expertise in this particular field. It doubted, however, that this job was suited for a career officer, who had to rotate jobs on a regular basis. The mindset needed was one of patience, perseverance and wisdom: with the possible exception of perseverance attributes difficult to find among people who joined the army in most cases, because they wanted to see action. The committee believed that a reserve officer would be better suited for this task, because he would lack the ambition to make a career in the army to start with. Descent was irrelevant, in this particular case.

5 Conclusion

Less than a month after the committee had completed its report, Archduke Franz Ferdinand and his spouse were murdered and less than two months later war broke out, changing the face of the continent. In this context it should not surprise us that the committee's advice was followed. Henri Koot, a young lieutenant from the colonial army who happened to be in the country to follow a training program, possessed all the required qualities and proved to be able to lay the groundwork for the institution of modern cryptology in the Netherlands, as Karl de Leeuw (2015) has shown. Koot – recognizably of mixed descent – was highly intelligent, but also modest and obedient to the extreme and he had no career expectations outside the colonial army whatsoever. Nor should it, after all that has been said, surprise us, that Van der Harst – who clearly had demonstrated his talent as a cryptologist – wasn't called upon to do the job. He was to rise high in the Royal Netherlands Army, ending his career as a Major General and governor in charge of the Royal Military Academy.

[14] Ibid., 8.

[15] Ibid., Bijlage B.

References

Edouard Fleissner von Wostrowitz. 1881. *Handbuch der Kryptographie*. Seidl & Sohn, Wien, Austria.

Carl Friedrich von Hindenburg. 1796. Fragen eines Ungenannten über die Art durch Gitter geheim zu schreiben. *Archiv der reinen und angewandten Mathematik III*: 347–351, V: 81-99.

David Kahn. 1967. *The Codebreakers. The Story of Secret Writing.* Macmillan Publishing Company, New York, USA.

Wim Klinkert. 2017. 'Espionage Is Practised Here on a Vast Scale'. The Neutral Netherlands, 1914-1940. Floribert Baudet et al., *Perspectives on Military Intelligence from the First World War to Mali. Between Learning and Law.* T.M.C. Asser Press, The Hague, The Netherlands, 23-54.

Karl de Leeuw and Hans van der Meer. 1995. A Turning Grille from the Ancestral Castle of the Dutch Stadtholders. *Cryptologia*, XIX(2), 153-164.

Karl de Leeuw. 2015. 'The Institution of Modern Cryptology in the Netherlands and the Netherlands East Indies, 1914-1935.' *Intelligence and National Security*, 30: 26-46.