The TICOM DF-114 Cryptanalytic Device - A Theory of Operation and Computer Simulation

Magnus Ekhall
magnus.ekhall@gmail.com

Abstract

The M-209 cipher machine was used extensively by the U.S.A. during World War II. It is known that German cryptanalysts under certain circumstances were able to decipher M-209 enciphered messages using pen-and-paper techniques. A German wartime document found by the allies' Target Intelligence Committee (TICOM) in 1947 describes a electromechanical machine that supposedly could be used as an aid when breaking M-209 enciphered messages. The document, designated DF-114 by TICOM, is quite technical but does not describe how the device would work.

This paper suggests a theory of how the device could have been used, and by creating a computer simulation of the device described in DF-114 explores the viability of the theory.

1 The M-209 Cipher Machine

The M-209 is a mechanical cipher machine used by the U.S. military during World War II. Developed by the Swedish company AB Cryptoteknik as C-38, it was licensed to the U.S. military under the designation "Converter M-209". In 1942 national production of M-209 started in the U.S.A. by L. C. Smith & Corona Typewriters Inc. In total more than 140,000 M-209 units were manufactured (Kahn, 1996).

The M-209 has six pin wheels of different sizes: 17, 19, 21, 23, 25 and 26 pins. The pins can be individually set to either an inactive or an active state. For each letter to be enciphered all wheels steps forward one step. Since the sizes of the six wheels are relatively prime, this gives a cycle size of $17 \times 19 \times 21 \times 23 \times 25 \times 26 = 101,405,850$ letters.

Each wheel has a number of letters printed on it corresponding to the number of pins of that wheel. Since the wheels differs in size, the available letters also differs:

Wheel 26:	A-Z
Wheel 25:	A-Z except W
Wheel 23:	A-X except W
Wheel 21:	A-U
Wheel 19:	A-S
Wheel 17:	A-Q

At any time, the six wheels present one pin each to a drum consisting of 27 bars. On each bar two metal lugs can be configured to either a neutral position or to take a position corresponding to one of the six wheels. When the M-209 is enciphering a letter, the drum spins one revolution and all 27 bars are in turn interacting with the pins currently presented by the wheels.

If a lug on a bar meets an active pin, that bar is then activated. Depending on the configuration of the pins and lugs, any number of bars from 0 to 27 could be activated at the end of the revolution. This number of active bars decides what alphabet is used to encipher the letter (Lasry et al., 2016).

A Beaufort reciprocal alphabet is used as a basis for encryption in the M-209:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA
```

With this alphabet letter A would be enciphered to Z, B to Y and so on.

The number of active bars when enciphering a letter changes the alphabet used for enciphering that specific letter: The encryption alphabet is rotated that many steps to the right.

For example, if there are three active bars on the drum, the alphabet used for that letter would look like this:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
CBAZYXWVUTSRQPONMLKJIHGFED
```

Note that it is only possible to create 26 different Beaufort alphabets this way.

In this case letter A would be enciphered to C, B to B and so on. With DF-114 terminology the M-209 in this case is said to have introduced a "skip" of three spaces in the reciprocal alphabet (TICOM, 1948b).

Since the alphabet used is reciprocal, deciphering takes place using the same alphabet as when enciphering and the cipher is thus symmetrical.

Another way to describe the encryption process carried out by the M-209 is that it switches between up to $2^6 = 64$ indexes, depending on the active pins and the lugs on the drum. Each index points to one of the 26 possible Beaufort alphabets. Several of the indexes therefore must point to the same Beaufort alphabet.

1.1 Keys

The cryptographic key of the M-209 consists of two parts: the state of the pins on the wheels and the position of the lugs of the drum. The key was changed at regular intervals, typically daily. The key settings were distributed in advance to all parties that should be able to communicate with each other. Typically each U.S. army division and corps had their own set of keys (Friedman et al., 1950).

When a message was enciphered a procedure was used to set the starting position of the six wheels in a secure manner. The procedure allowed the sender to inform the receiver of the starting position, and also make sure that the starting position is different for each new message. If this procedure is followed, it makes it difficult for an eavesdropper who does not have the correct key to break the cipher.

Different procedures might have been in use, but one that is known to have been used worked as follows (Pokorn, 1945):

1. The operator configures the lugs and pin wheels according to the daily key. This is typically done once per day (or possibly other time period as agreed).

2. The operator **randomly** sets the six wheels and writes down the corresponding letters of the wheel.

3. The operator randomly selects a letter of the alphabet.

4. This letter is encrypted repeatedly with the M-209.

5. The enciphered letters that result from the aforementioned encryption are used to set the six wheels to the real starting position for the encryption of the cleartext message. If a letter is generated that does not exist on that specific wheel, the next encrypted letter is used. This is repeated until viable starting positions for all wheels have been found.

6. The real message is enciphered.

The six letters from point 2 and the random letter from point 3 is part of the message indicator which is transmitted, unencrypted, as part of the message. On the receiving end the operator performs the same operation with the data from the message indicator and will thus decipher the message with the identically configured M-209 as the sender.

By using this procedure every message is enciphered with the six wheels set to a random position. Furthermore it is not easy to obtain the correct starting position for the six wheels from the information in the message indicator alone (Pokorn, 1945).

2 German cryptanalysis of the M-209

A considerable amount of M-209 traffic was broken and read by the Germans during World War II. About 5-10% is an estimate of the amount of traffic read purely by cryptanalytic means. In practice the Germans depended on messages in depth[1] or on M-209 operator errors in order to be able to read the messages (Friedman et al., 1950; TICOM, 1948c). This shows that the procedure outlined in section 1.1 was not strictly followed at all times.

From a broken message it is sometimes possible to deduce the M-209 lug settings, and the sequence of active and inactive pins on the M-209 wheels (Pokorn, 1945). This is called the *relative setting*.

To be able to decipher further messages the *absolute setting* is needed. The absolute setting consists of the additional knowledge of where in the sequence of active and inactive pins the letter "A" is on the circumference of each wheel.

[1] Two or more messages enciphered using the same M-209 settings.

With this information, it is possible to use the message indicator as described in section 1.1, and all messages enciphered with the same key would then be readable. Typically that would be all traffic for one network for one day.

Obtaining the relative setting was estimated to take two to three hours. Obtaining the absolute setting was considerably more difficult, estimated to take between twelve hours and four days (Friedman et al., 1950) and for that, different pen-and-paper techniques were developed (TICOM, 1948a).

3 The TICOM DF-114 document

In 1947 a German document was found dug down in the ground at a camp at Glasenbach just outside Salzburg, Austria. The document was translated into English and got the designation DF-114, document number 2785 by the Target Intelligence Committee (TICOM, 1948b). The title of the document is "Technical Note on machine treatment of AM-1 compromised texts in depth of 5", and it is clear already from the title that the document is related to the M-209 converter which was called "AM-1" by the Germans. Even though the document is translated into English there are some words here and there that are left in German, or sometimes written both in English and in German. The original German title of the document is given as *Techniches Erlaueterung zur maschinellen Bearbeitung von AM-1 Kompromisstextlösung auf 5er Texttiefe*. It is not clear who the original author is or who the target audience for this document is.

The document consists of 13 pages and a TICOM cover page. Of the 13 pages, four are a textual description of an electromechanical apparatus and nine pages are technical drawings of various kinds: electrical schematics, mechanical drawings and an overview.

The text describes what the device consisted of and how the various parts were interconnected. It fails to describe how the device was used: what was the input and what was the output? There are frequent references to the M-209 in the document, so it is clear also from the contents of the document that this design targeted the M-209.

On the cover page, TICOM writes: "From this paper the precise purpose of the device is not clear, neither is the manner in which it is supposed to function."

The document was declassified in 2010 (TICOM, 1948b).

3.1 Theory

The theory that will be investigated in this paper is whether the device can be used to test for possible cribs given an enciphered message and given that you know the pin and lug settings of the day. That is, the relative setting of the M-209 is assumed to be known, but the message that is to be investigated does not need to be in depth.

As mentioned in section 2, the Germans mostly relied on messages in depth, or messages close to being in depth in order to read M-209 traffic.

When having both the cleartext and the ciphertext of a message there were techniques for reconstructing the pin and lug settings: the relative setting (Pokorn, 1945). One remaining problem is that unless there is knowledge of the absolute setting, the rest of the traffic from that day can not be read since it is not possible to use the message indicator as described in section 1.1.

The theory will be described in detail in section 5 but first an analysis of the device described in the DF-114 document is needed.

4 The DF-114 device

This section describes the device as a direct and objective interpretation of the contents of the DF-114 document.

The device described in DF-114 is stated to consist of three main parts and a number of auxiliary parts. The main parts are:

1. Skip box
2. Distributor
3. Switching device

Figure 1 shows the main parts of the DF-114 device and how they are connected.

4.1 Skip box

The skip box (German: *Sprungkasten*) gets its name from the German nomenclature of how the M-209 works. As described in section 1 above, at each position in the message the M-209 introduces a 0 to 27 shift of the reciprocal alphabet used to encipher or decipher the current letter. This shift is called "skip" (German: *Sprung*) by the author of the DF-114 document (TICOM, 1948b).

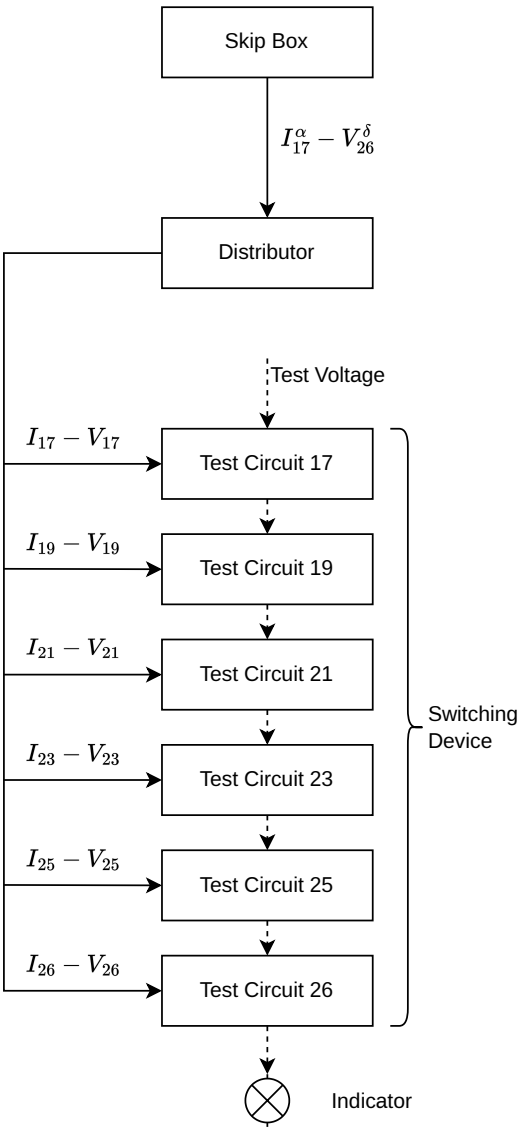

Figure 1: The DF-114 device is described as having three main parts: a skip box, a distributor and a switching device. The switching device consists of six test circuits.

The skip box contains five cylinders. Each cylinder has 26 slots, presumably one slot per letter in the alphabet. Each slot is divided into four sections. One sheet metal plate can be inserted into each section, giving four possible plates in each of the 26 slots of a cylinder. Each metal plate has six teeth that each represent an active or inactive state, depending on whether a tooth is present or has been removed. Each metal plate measures 60 millimeter in width by 15 millimeter in height. In the DF-114 document the teeth are described as "corresponding to the six wheels of the AM-1 or M-209" (TICOM, 1948b).

The five cylinders can be manually rotated independently from each other using a knob on the cylinders. Directly below the cylinders in the skip box are spring loaded electrical switches. Only one of the 26 cylinder slots, the cylinder slot that is facing directly downwards, affects these switches. There is one switch per tooth of a metal plate. So, for one cylinder there are 4×6 electrical switches, which makes $4 \times 6 \times 5 = 120$ in total for all five cylinders.

In DF-114 the five cylinders are denoted with roman numerals from I to V. The four metal plates in a cylinder slot are labeled with Greek letters α to δ, and the six teeth of a metal plate are denoted 17, 19, 21, 23, 25 and 26 which equal the number of pins of the six wheels of the M-209. So for example IV_{19}^{γ} denotes cylinder 4, metal plate 3 and tooth 2 on that metal plate. At all times, only the cylinder slot that is facing downwards and thus affects the electrical switches is considered.

Figure 2 shows a technical drawing from the DF-114 document depicting a cylinder, seen from the side. Figure 3 illustrates how a cylinder is slotted.

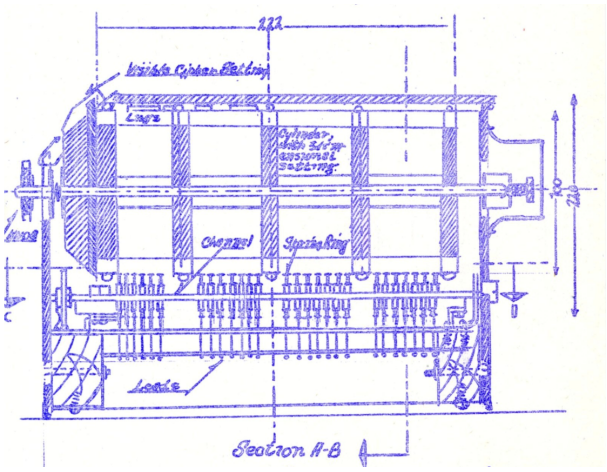

Figure 2: A cross-section of one of the cylinders of the skip box. The spring loaded switches are seen below the cylinder. Source: DF-114.

4.2 Distributor

The distributor (German: *Verteiler*) is connected to the skip box with 120 cables, one for each electrical switch in the skip box. The distributor consists of five wheels, one for each cylinder of the skip box. All cables from skip box cylinder I is connected to wheel I of the distributor and so on. In terms of signal names that means that $I^{\alpha-\delta}$ is connected between cylinder I of the skip box and

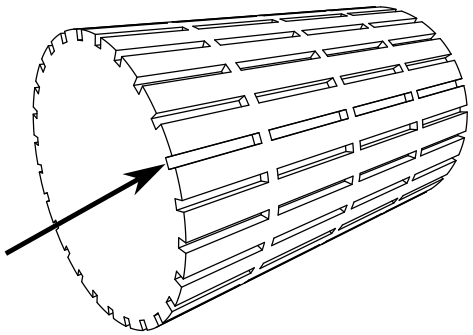

Figure 3: Modern rendition of a DF-114 cylinder. The arrow points to one of the 26 slots which in turn is divided into four sections.

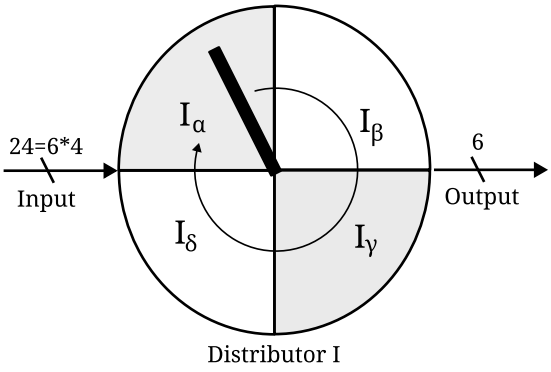

Figure 4: Illustration of the first distributor. The input consists of four groups of six signals from the skip box, denoted α to δ. The output is one of the four groups, but which one changes for every step of the arm.

wheel I of the distributor.

Each distributor wheel has an arm (German: *Zeiger*) that connects the incoming α, β, γ or δ signals to the output of the distributor. That is, each wheel has 4×6 input signals and outputs 6 signals at any time. The wheel or arm can step forward, making the arm connect the next group of signals, (α to δ). In DF-114, wheel I is labeled "low speed", and wheel V is labeled "high speed". This suggests that the five wheels of the distributor moves much like the odometer of a car: once wheel V has iterated through its four inputs, wheel IV will move one step forward. This leads to the distributor, in sequence, outputting all $4^5 = 1024$ different combinations of $I^{\alpha-\delta}$ through $V^{\alpha-\delta}$.

In DF-114 the distributor is described as having "a stepped advance of the five wheels corresponding to the five cylinders" and notes that "the purpose of the distributor is to scan all [4^5] combinations" (TICOM, 1948b).

The total number signals output from the distributor at any time is $5 \times 6 = 30$.

4.3 Switching device

The switching device (German: *Schaltapparat*) consists of six test circuits (German: *Diskussionskreise*). Each test circuit correspond to one of the six teeth of a metal plate and therefore also one of the rotors of the M-209: 17, 19, 21, 23, 25 or 26.

The six test circuits are connected in series, and only if all six circuits produce a positive result is the objective of the whole device is met and the machine stops.

As input, a test circuit has five of the signals coming from the distributor. For example, test circuit 17 is given input from I_{17}, II_{17}, III_{17}, IV_{17} and V_{17}. In addition to this input, a test circuit has a test voltage which comes from the previous test circuit in the series connection or in the case of the first test circuit, a 90 Volt signal. The test voltage is passed through a binary tree implemented with electro-mechanical relays. The relays implement what is nowadays called a demultiplexer, with the output selected by the five control signals from the distributor. A demultiplexer connects one input to one out of several outputs, in our case 32. Since there are five control signals, there are $2^5 = 32$ possible outputs, and only one of these 32 outputs will be connected to the incoming test voltage.

Each of the 32 outputs of the relay circuit is connected to a lamp socket. In a lamp socket there can either be a lamp or not, this is one of the parameters that the operator controls depending on the current job the machine is working on.

After the 32 lamp sockets, the signals are merged into one, and connected to the next test circuit or, in the case of the last test circuit, to a circuit that will halt the machine. When halted the operator can see exactly which six light-bulbs that are shining and then resume the run with the press of a button. Figure 5 illustrates one of the test circuits.

All in all, the switching device has a 90 Volt test voltage as input, $5 \times 6 = 30$ signals coming from the distributor, $32 \times 6 = 192$ lamp sockets and one output for the test voltage.

5 Detailed theory of operation

The previous section is a description and interpretation of what is actually shown and written in the

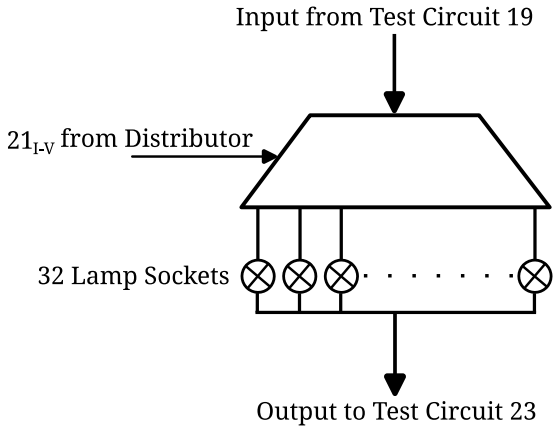

Figure 5: Illustration of one of the six test circuits of the switching device: in this case test cirucit 21 is shown. The five signals 21_{I-V} selects to which of the 32 lamp sockets the input shall be connected. The presence or absence of a lamp in that socket determines if the test signal is passed on to the next test circuit or not.

DF-114 document. What is *not* described in the document is with what data the device should be configured, and what the output of the device is. The following is a theory of one way the DF-114 device could have been used.

As mentioned in section 3.1, the theory investigated here is whether the DF-114 device would be useful as a tool to speed up the process of finding cribs.

The theory is implemented by the following steps:

1. Populate the five cylinders with teethed metal plates according to the known pin and lug setting of the M-209. See section 5.1 below for a detailed description.

2. Put lamps in lamp some of the sockets of the switching device according to the pin settings of the M-209. See section 5.2 below for a detailed description.

3. Assume a five letter cleartext somewhere in the message.

4. Calculate the number of skips the M-209 would have to produce in order for the cleartext letter to be enciphered to the ciphertext letter for each of the five letters.

5. Set the five cylinders so that for each cylinder the right skip is active, according to the calculation done with the crib.

6. Start the device.

When the device is running, the distributor will test all 1024 different combinations of teethed metal plates for the given five skips. In essence, this creates the up to 1024 ways of creating the given ciphertext from the given cleartext.

The switching device will for each of the 1024 combinations test whether the resulting pin sequences are present on all six wheels of the M-209. If that is the case, the machine stops and the operator should investigate this specific setting further. The setting to be investigated can be deduced from the six light-bulbs that are shining (one light bulb from each of the six test circuits of the switching device).

5.1 Cylinder teethed metal plates

The six engaging pins of the M-209 wheels can assume $2^6 = 64$ different combinations. Each of the 64 combinations gets converted to a number of skips in the range $0,\ldots,27$, depending on the lug settings of the M-209. Note that a skip of 26 is equivalent with a skip of 0, and 27 is equivalent with 1, so in practice there are 26 distinct skips: one for each letter of the alphabet. This leads to the fact that some of the 64 pin combinations must result in the same number of skips, since there are only 26 different results. So, for some of the pin combinations the M-209 would encrypt a given cleartext letter to the same ciphertext letter (Pokorn, 1945).

This is the reason why it is possible to have four teethed metal plates in each cylinder slot of the DF-114 device. Each of the 26 slots in the cylinder is populated with the metal plates that generate the same number of skips. If there are more than four metal plates that would generate the same number of skips, the DF-114 document mentions that there is an option to add a fifth skip possibility using "the lead to the switch device". Exactly how this fifth skip possibility would work is not very well described.

Of course, if there is a case where more than five combinations produce the same number of skips this will then potentially lead to missed solutions.

5.2 Lamps of the switching device

As mentioned in section 4.3 each of the six test circuits of the switching device gets as input five signals from the distributor. The theory is that these five signals correspond to a presumed sequence of

Wheel size	Distinct sequences
17	13.67
19	14.82
21	15.90
23	16.90
25	17.86
26	18.29

Table 1: The average number of distinct pin sequences of length five with different wheel sizes. Result of a computer simulation of 1,000,000 samples per wheel size.

five adjacent pins on one of the wheels of the M-209. Each of the $2^5 = 32$ lamp sockets that are part of the test circuit corresponds to one specific five pin sequence. Let `-` denote an inactive pin and `+` denote an active pin: then the pin sequences of the lamp sockets range from `-----`, `----+`, `---+-`, `---++`, and so on, up to `++++-`, `+++++`.

On a M-209 wheel where the pins have been randomly selected there is an expected value of the number of distinct pin sequences of length five over the whole of the wheel. The average number of distinct sequences depends on the length of the wheel and has been determined by computer simulation. The results are visible in table 1.

Given the information in table 1 and the fact that the six test circuits of the switching device are connected in series, it is possible to calculate the probability that a totally random pin sequence would pass through all six test circuits.

$$P = \frac{13.67}{32} \times \frac{14.82}{32} \times \frac{15.90}{32} \times \frac{16.90}{32} \times \frac{17.86}{32} \times \frac{18.29}{32}$$

$$P = 0.0166$$

The probability is thus on average 1.66%.

6 Computer simulation

To test the feasibility of the theory described in section 5 a computer simulation was made of the DF-114 device. The simulation of the DF-114 device was written as a Python program which takes as input the known pin and lug setting (the relative setting), a five letter cleartext word to be tested and the corresponding five letters of ciphertext.

The pin settings for each wheel are used to calculate all distinct pin sequences of length five. This corresponds to which sockets on the test circuits an operator would put light-bulbs into. This data is stored per wheel in an associative list.

Furthermore, the pin and lug settings are used to calculate the number of skips that each of the $2^6 = 64$ wheel pin combinations result in. This corresponds to putting the teethed metal plates in the correct place in the cylinders. Note that while the DF-114 device cylinders are described as having four places for metal plates ($\alpha - \delta$) per skip, the simulation does not have this limitation. For an M-209 key there is a possibility that there will be more than four pin combinations that result in the same number of skips. If this happens then the DF-114 device might not find a solution, but the computer simulation will.

The five letter suggested cleartext letters and the corresponding ciphertext is used to calculate how many skips that must be carried out by the M-209 for each letter for the theory to hold true. This corresponds to what the five cylinders of the skip box would be set to prior to starting the DF-114 device; which of the 26 slots of the cylinders that would be engaging with the electrical switches of the skip box.

This concludes the setting-up part of the simulation and the simulation of the DF-114 device can now be started.

The simulation of a running DF-114 device is done by iterating through the set of skips resulting from the Cartesian product of the active skips from the five cylinders. With each iteration the six test circuits are simulated by looking up whether the produced pin sequences are part of the six corresponding wheels. If all six tests are passed the simulation prints which skips were used to produce the results.

6.1 Example simulation

Assume that there is an M-209 enciphered message where the ciphertext `XEWIR` is believed to correspond to the cleartext `THEZM`[2].

The pin and lug settings are known, and are shown for reference in table 2 and table 3.

The number of skips needed to encipher each of the letters are shown in table 4.

Let S_x denote the set of M-209 wheel pin combinations that produce a skip of length x. With the

[2]The letter Z was used in place of a space between words since the M-209 did not have a specific space character. The plain text message would thus have been “THE M” in this case.

Wheel 17	++-+---+--+--++-+
Wheel 19	-+-+++-++---++-+--+
Wheel 21	--+-++-++---++-+--+++
Wheel 23	++----++-+-+++---++++-+
Wheel 25	+--++-+--+++--+--++-+-+--
Wheel 26	++-+---++-+-++----++-++---

Table 2: Pin settings. A dash denotes an inactive pin, a plus denotes an active pin.

3-0	0-6	1-6	1-5
4-5	0-4	0-4	0-4
0-4	2-0	2-0	2-0
2-0	2-0	1-0	2-0
2-0	2-0	2-0	2-5
2-5	0-5	0-5	0-5
0-5	0-5	0-5	

Table 3: Lug settings on the 27 drum bars of the M-209.

T → X: 17 skips
H → E: 12 skips
E → W: 1 skip
Z → I: 8 skips
M → R: 4 skips

Table 4: Number of skips needed for each letter of the suggested cleartext of the example message.

key used in the example, the sets of interest are shown in table 5.

S_{17}:	+-++-,+--++,-++--,--++++
S_{12}:	+---+-,-++---,----++
S_1:	++++,--+---
S_8:	+--+--,--++-+
S_4:	+-+---,+----+

Table 5: The different wheel pin combinations that produce a certain number of skips.

In this case the number of skip combinations that will be tested is the Cartesian product of the set sizes:

$$|S_{17}| \times |S_{12}| \times |S_1| \times |S_8| \times |S_4| = 96$$

Each skip combination can be seen as a matrix of 6×5 elements. As an example, consider the skip combination consisting of the first member of each of the sets in table 5. This is shown in table 6.

The rows of the matrix in table 6 are M-209 wheel pin combinations that produce the required

+-++-+
+---+-
++++++
+--+--
+-+---

Table 6: One of the 96 skip combinations that are tested.

number of skips. Each column can then be seen as a sequence of active and inactive pins that must be present somewhere on that specific wheel. For example, for the first wheel (size 17), there must be a pin sequence of +++++ somewhere in its pin sequence.

This is looked up by the simulator in the associative per-wheel-list that was calculated earlier. If all six columns exists on their respective wheel the result is positive and the skip combinations are printed. It means that it is possible to encipher the cleartext to the ciphertext with the M-209 key settings given as input.

As seen in table 2 there is no sequence of +++++ anywhere on wheel 17. This particular combination is thus not possible and will not be printed.

7 Results

In order to test the feasibility of this theory of operation the computer simulation was run with different sets of input data: 94 different M-209 keys and three different plaintexts were used for a total of 282 simulations.

All simulations finds the correct solution but also a number of false solutions where the pin patterns happen to exist on the six wheels but it is not the correct solution. In this case the ciphertext would decipher to the correct plaintext, but the rest of the message would not decipher correctly.

From a feasibility perspective it is of interest to see how many false solutions that is expected since each solution had to be investigated further, perhaps on a real M-209 converter. In a perfect situation either the correct solution should be found, or none at all. In practice, the fewer false solutions the better.

Figure 6 shows a histogram of the number of solutions for the simulations. The median number of solutions is 6, and the mean is 8.6.

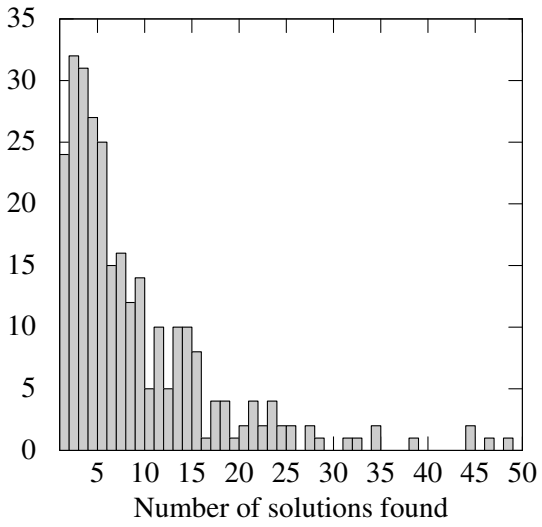

Figure 6: Histogram showing the number of solutions for the 282 simulations.

8 Conclusion

Not much is known of the DF-114 device and neither the device itself nor parts of it have never been found. There exists some evidence which suggests that it has existed and that the use was to speed up the process of finding the absolute setting given the relative setting (Ekhall and Schmeh, 2023). It is not impossible that the DF-114 device is capable of doing so, but it is still not known how the device would be operated in that case.

The theory presented in section 5 is different: it suggests that the DF-114 device can be used to test for cribs given the relative setting.

While the simulation result shows that it is possible to use the DF-114 device in this manner, it also shows that it would sometimes lead to a large number of false solutions which would need to be investigated further. The median number of solutions is six, which perhaps is not terribly bad, but the maximum number of solutions found is 49 and that would lead to considerable manual work. The possibility of a large number of false solutions can be interpreted in two ways:

1. The theory presented in this paper is correct and the DF-114 device would generate a large number of false solutions. The device would thus not have been easy to use and this may explain why there is not a lot of historical records mentioning it. The historical footprint of the DF-114 device is very small, basically limited to the DF-114 document itself and an interview referenced in (Ekhall and Schmeh, 2023).

2. The theory is wrong and there is another, more feasible, way which the DF-114 device would have been used. This is clearly a possible situation and is an area for further research.

Acknowledgments

The author would like to thank the reviewers for their invaluable feedback, which significantly improved the quality of this paper.

References

Magnus Ekhall and Klaus Schmeh. 2023. A WW2 device for breaking the M-209 encryption machine. In *Proceedings of the 6th International Conference on Historical Cryptology HistoCrypt 2023*, HistoCrypt 2023. Linköping University Electronic Press.

W Friedman, B Miller, K Perrin, A Sinkov, F Austin, W Pettengill, and M Lane. 1950. Special conference on M-209 security, minutes of meeting. `https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_371/41755249079440.pdf`. Ref ID: A66657, Folder 371, NSA, William F. Friedman Collection of Official Papers.

David Kahn. 1996. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner.

George Lasry, Nils Kopal, and Arno Wacker. 2016. Ciphertext-only cryptanalysis of Hagelin M-209 pins and lugs. *Cryptologia*, 40(2):141–176.

Alfred Pokorn. 1945. Report by Alfred Pokorn, of OKH/CHI, on M. 209. `https://catalog.archives.gov/id/23890261`. TICOM/I-175. NARA, College Park, NAID: 23890261.

TICOM. 1948a. Determination of the absolute setting of the AM 1 (M-209) by using two messages with different indicators. `https://catalog.archives.gov/id/26466553`. Document T-2795, TICOM/DF-105. NARA, College Park, NAID: 26466553.

TICOM. 1948b. German cryptanalytic device for solution of M-209 traffic. `https://catalog.archives.gov/id/23889821`. Document 2785, TICOM/DF-114. NARA, College Park, NAID: 23889821.

TICOM. 1948c. Report on the solution of messages in depth of the American chipher device

M-209. https://catalog.archives.gov/id/23889823. Document 2794, TICOM/DF-120. NARA, College Park, NAID: 23889823.