Solving a Tunny Challenge with Computerized "Testery" Methods

George Lasry
The DECRYPT Project
george.lasry@gmail.com

Abstract

The Lorenz SZ42, codenamed Tunny, was a teleprinter encryption device used by Germany during WW2 for strategic communications. Its successful cryptanalysis at Bletchley Park (BP) provided the Allies with high-grade intelligence about several fronts, as well as for the preparations for the D-Day landings. The story of Tunny's codebreaking and Colossus is well known, following the declassification of the General Report on Tunny in 2000 (Good et al., 1945), and the publication of several books (Reeds et al., 2015; Gannon, 2014; Copeland, 2010; Roberts, 2017; Mayo-Smith, 2014). The work on Colossus and other machines was carried out in the Newmanry, under the leadership of the mathematician Max Newman.

The work of the Testery, the other Tunny section at BP, is less known. Named after his commander, Major Ralph Tester, the Testery was responsible for the development and application of hand methods, that complemented the work of machines like Colossus. For some reason, the report on the Testery was not declassified until 2018. Following its recent release, it is possible to fully assess the achievements of the Testery cryptanalysts and their key contribution to BP's success against Tunny (Testery, 1945).

The work described in this article is an attempt to determine whether the Testery manual methods can be mechanized with modern computing. The author was able to automate some of the techniques and partially automate some others. With these techniques, the author also succeeded in recovering the key settings and the plaintext of two Tunny challenge messages.

This article is structured as follows: In Section 1, a functional description of the Lorenz SZ42 is given. In Section 2, the contents of the Testery report are surveyed, highlighting the parts that reveal new information. In Section 3, the primary techniques for the cryptanalysis of Tunny are described. In Section 4, a Tunny cipher challenge is introduced. In Section 5, new automated or partially automated versions of the Testery manual methods are described, as well as how they were used to solve the Tunny cipher challenge. In Section 6, the main results of this study are summarized.

1 The Lorenz SZ42 (Tunny)

The history of the Lorenz SZ42 and the details of its design and functioning are documented in the references (Reeds et al., 2015; Gannon, 2014; Copeland, 2010). In this section, only a brief functional description is given.

The Lorenz SZ42 is a teleprinter encryption device. It encodes Baudot teleprinter symbols that consist of five impulses. Each impulse can have one of two states. It can be active, denoted as *cross* according to BP terminology, or **x**. Or it can be inactive, denoted as *dot* or •. The Baudot alphabet, as well as BP's notation for the Baudot symbols, is given in Table 1.

The Lorenz SZ42 functions as a Vernam device. It applies an XOR addition (denoted as $\oplus$) to encrypt plaintext Baudot symbols. The effect of the XOR operation on a pair of impulses a and b is described in Table 2. The XOR operation can also be applied to a pair of Baudot symbols with five impulses each. In that case, it is applied sequentially one impulse at a time. An example is given in Table 3. It should be noted that adding (using an XOR addition) a symbol to itself, results in the symbol ••••• which has only dots, as illustrated in Table 4.

The Lorenz SZ42 generates a keystream K of pseudo-random symbols and performs an XOR ad-

Symbol	BP Notation	Meaning in Letter Shift	Meaning in Figure Shift
•••••	/	null	
••••x	E	E	3
•••x•	4	carriage return	
•••xx	A	A	-
••x••	9	space	
••x•x	S	S	’
••xx•	I	I	8
••xxx	U	U	7
•x•••	3	line feed	
•x••x	D	D	Who are you?
•x•x•	R	R	4
•x•xx	J	J	BELL
•xx••	N	N	,
•xx•x	F	F	%
•xxx•	C	C	:
•xxxx	K	K	(
x••••	T	T	5
x•••x	Z	Z	+
x••x•	L	L	)
x••xx	W	W	2
x•x••	H	H	£
x•x•x	Y	Y	6
x•xx•	P	P	0
x•xxx	Q	Q	1
xx•••	O	O	9
xx••x	B	B	?
xx•x•	G	G	&
xx•xx	5 or +	figure shift	
xxx••	M	M	.
xxx•x	X	X	/
xxxx•	V	V	;
xxxxx	8 or -	letter shift	

Table 1: The Baudot Teleprinter Alphabet

a	b	$a \oplus b$
•	•	•
•	x	x
x	•	x
x	x	•

Table 2: The XOR ($\oplus$) Operation

K	•xxxx
G	xx•x•
K $\oplus$ G	x•x•x

Table 3: XOR ($\oplus$) on the Symbols K and G

G	xx•x•
G	xx•x•
G $\oplus$ G	•••••

Table 4: XOR ($\oplus$) on the Same Symbol

dition on a stream of plaintext P, producing the ciphertext Z, as described in Equation 1, the encryption formula.

$$Z = P \oplus K \tag{1}$$

Encryption and decryption are implemented identically. This is possible since adding (XOR) the keystream K to the ciphertext Z cancels out the effect of the keystream K originally added during encryption, as shown in Equation 2, the decryption formula.

$$Z \oplus K = (P \oplus K) \oplus K = P \oplus (K \oplus K) = P \tag{2}$$

As a result, two machines using identical settings can communicate properly, one side encrypting plaintext and transmitting ciphertext, the other receiving and decrypting the ciphertext.

The functioning of the Lorenz SZ42 is illustrated in Figure 3 in the Appendix. The keystream K is generated by a set of twelve wheels, divided into three functional groups:

- **Five χ wheels, χ_1 to χ_5**: Those wheels have 41, 31, 29, 26, and 23 pins, respectively. Each pin can be set to either an active (cross) or an inactive (dot) state. The χ wheels regularly step after the encryption (or decryption) of each symbol. The stream of Baudot symbols generated by the five χ wheels is denoted as the χ *stream*.

- **Five ψ wheels, ψ_1 to ψ_5**: Those wheels have 43, 47, 51, 53, and 59 pins, respectively. Each pin can be set to either an active or an inactive state. Their stepping is governed by the motor wheels. Either all five ψ wheels step or none of them steps. The actual stream of symbols generated by the ψ wheels is denoted as the ψ' *stream*. It differs from a theoretical ψ *stream*, that would have been generated if the ψ wheels always stepped. The ψ' stream is an extended version of the ψ stream, with symbols duplicated at positions where the ψ wheels did not step.

- **Two motor or μ wheels, μ_1 and μ_2**: Wheel μ_1 has 61 pins, which govern the stepping of wheel μ_2. If the current pin of wheel μ_1 is active (cross), wheel μ_2 steps. Wheel μ_2 has 37 pins, and if its current pin is active, all five ψ wheels step. The single-impulse stream

generated by wheel μ_2 is denoted as the *base motor stream*. In later models of the Lorenz SZ42, various *motor limitations* were introduced to reduce the number of *motor stops*, that is, positions where the ψ wheels are not stepping.[1]

The keystream K consists of the (XOR) addition of two streams, χ, and ψ':

$$K = \chi \oplus \psi' \tag{3}$$

Therefore:

$$Z = P \oplus K = P \oplus \chi \oplus \psi' \tag{4}$$

We define D, also known as the *dechi stream* (or simply, the *dechi*), as:

$$D = Z \oplus \chi \tag{5}$$

The term dechi originates from the fact that we are removing χ from the ciphertext Z, by adding it so that the original contribution of χ cancels out:

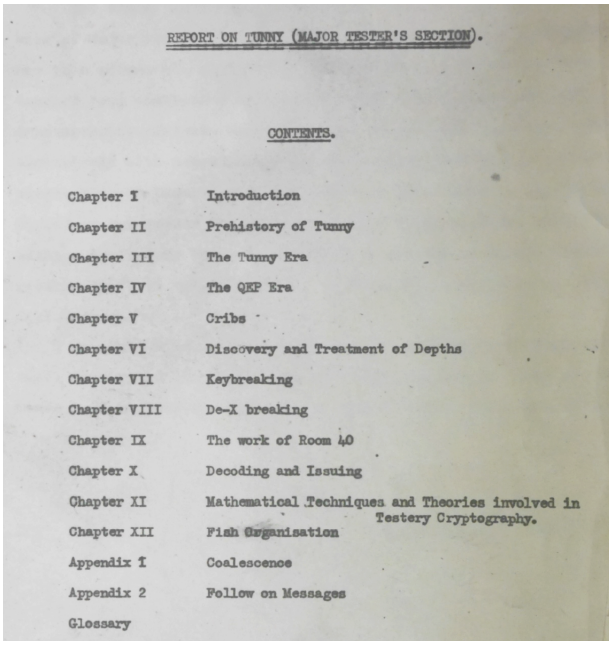
$$D = Z \oplus \chi = P \oplus \chi \oplus \psi' \oplus \chi = P \oplus \psi'. \tag{6}$$

If we add ψ' to both sides of $D = P \oplus \psi'$, it also follows that $P = D \oplus \psi'$.

2 The Testery Report

Each of the two main Tunny sections at BP – the Newmanry and the Testery – wrote a report. The General Report on Tunny with Emphasis on Statistical Methods (GRT) was written in 1945 by I.J. Good, D. Mitchie, and G. Timms from the Newmanry (Good et al., 1945; Reeds et al., 2015). It was declassified in 2000. It describes in detail the work on codebreaking machines such as the Heath Robinson and Colossus in the Newmanry, as well as their mathematical and statistical foundations. While it provides a wealth of technical information, the GRT is not easy to read, and its structure does not always follow a clear logical flow.

[1] A motor limitation forces the ψ wheels to move at positions where the base motor stream is a dot, and the ψ wheels would otherwise not step. Motor limitations are governed by a combination of one or more impulses from the P, χ, and ψ' streams, at previous positions. The combined effect of the μ wheels (the base motor stream) and of the motor limitations is denoted as the *total motor stream*. A description of the various types of motor limitations may be found in (Reeds et al., 2015, Chapter 11B, p. 13). As described in Section 3, most attacks against Tunny take advantage of skewed statistics at motor stop positions. Motor limitations are intended to reduce the number of motor stops, making cryptanalysis more challenging.



REPORT ON TUNNY (MAJOR TESTER'S SECTION).

CONTENTS.

Figure 1: Testery Report – Table of Contents

In some places, it lacks some details or examples necessary to understand some of the key points.

The GRT only briefly mentions the work and methods of the Testery. Those hand methods are also described (in even less detail) in testimonies and books written by Testery veterans (Roberts, 2017; Mayo-Smith, 2014).

The Testery report was not declassified together with the GRT back in 2000. A possible reason is that the Testery report may have contained sensitive information about methods still in use after WW2. This contrasts with a statement by D. Mitchie, one of the GRT authors, who was allowed to review the Testery report, and wrote that *"a good deal of [the Testery report's] content is directly inferable from other sources, including General Report on Tunny. The full Testery report amplifies this knowledge."* (Copeland, 2010, P. 246)

In 2017, at the NSA Symposium on Cryptologic History, the author met the GCHQ historian, Dr. Tony Comer, and inquired about the possible release of the Testery report. In July 2018, the author was pleasantly surprised to receive the following email from Dr. Comer:

"The mills have been grinding slowly since my return from the Symposium, but I am delighted to say that we have transferred HW 25/28 to TNA.[2]*"*

The author soon after traveled to Kew and made of copy of the report at TNA. The report is named

[2] The National Archives, Kew, UK.

Solution of German Teleprinter Ciphers ("Testery") Linguistic Methods (on its cover) and also *Report on Tunny (Major Tester's Section)* in the table of contents page (Testery, 1945). It contains 229 pages. It has twelve chapters, two appendices, and a glossary. Figure 1 shows the table of contents.

From a study of the report, it indeed emerges that most of the contents of the Testery report generally appears in the GRT, but often with significant differences. In contrast with the GRT, the Testery report follows a clearer presentation flow. The cryptanalytic methods are better explained, with useful examples, which were missing from the GRT. For example, a detailed example is given in the Testery report to illustrate the indicator method (Testery, 1945, Chapter II, section 10), and *Turingery*, Turing's method for extracting the χ wheel patterns from a keystream, is described in detail (Testery, 1945, Chapter III, section 2). As a result, the text of the Testery report is more readable. To quote Jim Reeds, one of the authors of the modern edition of the GRT: *"The Testery report was written by grown-ups."*[3]

More importantly, the Testery report contains new material or material that was only briefly mentioned in the GRT. A major example is a description of the operational process for finding cribs to help with cryptanalysis in (Testery, 1945, Chapter V). This work was carried out by Sixta, BP's traffic analysis section. The Sixta History report, like the Testery report, was declassified only in 2018, long after the release of the GRT (Sixta, 1945). It is possible that both the Testery and the Sixta reports were kept classified for a longer period in order not to expose GCHQ's traffic analysis techniques and the role of traffic analysis in assisting cryptanalysis.

From the cryptanalytic perspective, the primary addition of the Testery report, compared to the GRT, consists of more detailed material about the Testery hand methods (Testery, 1945, Chapter VIII), mainly:

- **ψ-Setting**: Finding the ψ wheel settings (i.e., the ψ wheel starting positions) from a dechi stream, when the wheel pin patterns are known.
- **ψ-Breaking**: Finding the ψ wheel pin patterns from a dechi stream, when the patterns are unknown.

While both topics are covered in the GRT (Chapters 28B and 28C), Chapter VIII of the Testery report methodically lays out the rationale for the manual methods, and the various techniques involved. Those techniques take advantage of some features of the German teleprinter language, which may vary according to the traffic on the specific link. For example, some Tunny links may use a different sequence of Baudot symbols to mark a full stop or a comma (e.g., by adding extra spaces or duplicating special symbols such as Figure Shift or Letter Shift). Other techniques rely on German operator habits and mistakes, such as sending messages in depth (encrypted with the same key settings) or "go-backs" – repeating the last 100 symbols of a message at the beginning of the next one (Testery, 1945, Chapter VIII).

The work of the Newmanry on the Colossus, and the role of Colossus in the history of modern computing, have taken center stage in the story of Tunny codebreaking at BP, leaving the achievements of the Testery in the shadow. The Testery report provides a more balanced view, highlighting the critical role played by the Testery in the daily recovery of keys and settings. Repeatedly, when the Germans introduced new security measures, such as motor limitations, the Testery was able to diagnose the modifications and find ways to circumvent them. In other cases, the Testery was often able to find and correct errors in the dechis, the output of the Newmanry's machines. As an illustration of the operational success of the Testery, the following figures are given for April 1945 : Out of 806 dechis provided by the Newmanry, 88% (707) were broken by the Testery. (Reeds et al., 2015, p. 243) (Good et al., 1945, p. 261)

3 Tunny Codebreaking Overview

A complete decryption of the machine and of the hand methods for the cryptanalysis of Tunny, as well as of the multitude of codebreaking scenarios the methods cover, is outside the scope of this paper and may be found in the Testery report and the GRT (Testery, 1945; Good et al., 1945). This section focuses on the main cryptanalytic scenarios.

The most challenging scenario is *breaking*, when the wheel patterns are unknown, there are no messages in depth (encrypted with the same key settings), and no crib is available. Historically, codebreaking for such a scenario included the following steps:

- The recovery by the Newmanry of the χ wheel patterns, using the *rectangling* method devel-

[3] Private conversation with the author, 2019.

oped by Bill Tutte, and later performed with the help of Colossus (Reeds et al., 2015, p. 110-112). After the χ wheel patterns had been recovered, the dechi stream $D = Z \oplus \chi$ was produced by the Newmanry.

- The recovery by the Testery of the ψ' stream from the dechi stream D, using hand methods. From ψ', the ψ wheel patterns could be recovered.
- The recovery of the motor wheel patterns, also by the Testery, from the ψ' stream.
- The decoding of the ciphertext (by the Testery).

For *setting*, when the wheel patterns are known, but the wheel starting positions are unknown for a specific ciphertext, the process was simpler. Historically, χ-setting was done by the Newmanry, and the settings for the ψ and motor wheels were recovered by the Testery.[4]

In case two or more messages in depth were available, their plaintexts could be recovered using linguistic methods, and using segments of plaintext, the keystream $K(= Z \oplus P)$ could also be extracted. From K, the wheel patterns were then recovered by the Testery.[5] A similar process was possible with the help of a long-enough crib.

But unless a crib is available, or plaintext can be extracted from depths, all attacks – for setting and breaking – rely on a major weakness of Tunny, which is described here.

We first introduce the notation Δ, or *differenced* stream. A differenced stream consists of adding (using XOR addition) to each element of an original (undifferenced) stream the value of the element right after it. Differencing can be applied to a single impulse, or to a stream of Baudot symbols, impulse by impulse. An important characteristic of a differenced stream is that if two consecutive symbols are identical, their differenced value is the symbol ●●●●● (all impulses inactive).

In Section 1, Equation 6, it was shown that the dechi stream $D = Z \oplus \chi = P \oplus \psi'$.

We analyze here the frequency distribution of the symbols in the dechi stream D. The ψ wheels may or may not step after each encryption (or decryption), but if they step, they all step together. When the wheels do not step (i.e., a motor stop), the corresponding symbol of ψ' is duplicated, and as a result, the corresponding $\Delta\psi'$ symbol has only dots (●●●●●). This means that at positions where there is a motor stop, $\Delta D = \Delta P$. Therefore ΔD at motor stops has the same frequency distribution as for ΔP.[6] Even though the symbols of ΔD are (roughly) randomly distributed at positions the ψ wheels step, overall, the frequency distribution of ΔD symbols is skewed toward the frequency distribution of ΔP symbols.

This important characteristic can be exploited for setting the χ wheels. While the plaintext for a given ciphertext is unknown, it is possible to compute the distribution of the *expected* differenced plaintext ΔP, using a corpus of the language (e.g., from prior decryptions). To set the χ wheels, we search for the χ wheel positions that result in the symbol distribution of $\Delta D = \Delta Z \oplus \Delta\chi$ being as close as possible to the expected frequency distribution of ΔP in the reference corpus. A similar methodology can be applied for χ breaking, to find the optimal χ patterns, so that the resulting ΔD best matches the expected distribution of ΔP in the reference corpus.

Due to the limits of WW2 technology, those techniques could only be applied to a pair of impulses at a time, e.g., impulses 1 and 2 (the so-called Δ_{1+2} method), rather than to all five impulses at the same time (Reeds et al., 2015, p. 110-112).

The same characteristic of ΔD can be used to recover ψ' from dechi, as described in Section 5.

4 A Tunny Challenge

In 2015, while working on the computerized cryptanalysis of Tunny, the author was able to find several original ciphertexts on the website of the late Tony Sale (www.codesandciphers.org.uk), as well as the relevant wheel patterns and settings. Those included settings and patterns used during WW2 in Tunny links like the one between Berlin and Rome, codenamed *Bream*. To further validate his new computerized methods, the author needed additional ciphertexts for which the patterns and settings were unknown. Frode Weierud, an expert on the history of cipher machines, provided the author with two ciphertexts of unknown origin, together with a set of wheel patterns that might have

[4] For some motor limitations (or if no motor limitation was used), the setting of the ψ and motor wheels could also be performed using the more advanced models of Colossus.

[5] *Turingery*, a method for extracting the χ patterns from K, was developed by Alan Turing.

[6] During cryptanalysis, the positions where there is a motor stop and ψ wheels do not step are unknown.

been used to encrypt the messages. Each ciphertext consists of approximately 5,500 symbols.

The author made several attempts to set the messages using the provided patterns without any success. Next, the author tried to set the messages using patterns found in Tony Sale's website, using a new method which he developed.[7] Setting was successful for the χ wheels, using the Bream link χ patterns from Tony Sale's website (the Bream patterns are given in an appendix at the end of this article).

However, all attempts to set the remaining wheels failed, using the Bream patterns and also trying various motor limitations. To make further progress, there was no choice other than to try and recover the motor and ψ wheel patterns, i.e., to perform motor and ψ-breaking instead of just setting. While the author had also developed new methods for motor and ψ breaking[8], those require at least 10,000-15,000 symbols, many more than the 5,500 symbols in the challenge messages. No further progress could be made on solving the challenges until 2019.

5 Mechanizing the Testery and Solving the Challenge

The main Testery methods are based on the characteristic of ΔD, as described in Section 3. Due to the ψ wheels often not stepping, there are numerous repetitions of consecutive symbols in ψ', and as a result a high frequency of ●●●●● symbols (all impulses inactive) in $\Delta\psi'$.

Due to security measures introduced by the Germans (Reeds et al., 2015, p. 306), there is also a high frequency of **xxxxx** symbols (all five impulses active) in $\Delta\psi'$, at positions where the ψ wheels step.[9] Furthermore, the frequency of $\Delta\psi'$ symbols with a majority of crosses (e.g., ●**xxxx** or ●●**xxx**) is significantly higher than the frequency of symbols with only one or two crosses (e.g., ●**xx**●● or ●●**x**●●). In addition, the probability for a ●●●●● symbol at positions where the ψ wheels are stepping is very low.

Historically, the work of the Testery started after receiving the dechi D, extracted from ciphertext by the Newmanry using mechanized methods. The Testery cryptanalysts tried various possible cribs P at different positions, examining the resulting (putative) $\Delta\psi' = \Delta D \oplus \Delta P$. A putative $\Delta\psi'$ mostly consisting of ●●●●● or **xxxxx** symbols, and the remaining symbols with a majority of crosses, was likely to indicate a correct crib guess. Still, there was always some probability for a wrong guess, especially if the crib was short. This process was labor-intensive and required extensive trial-and-error by the cryptanalysts, who had to memorize the full XOR addition table ($32 \cdot 32 = 1024$ elements) to mentally perform XOR additions (Roberts, 2017; Mayo-Smith, 2014).

For ψ setting, a machine named *Dragon* was developed to "drag" a crib over the whole dechi stream (Reeds et al., 2015, p. 346). For ψ breaking, there was no other choice but to test cribs manually.

After positioning a likely crib, the cryptanalyst would then try to extend it by testing additional symbols inserted before and after the crib, and checking the resulting new putative $\Delta\psi'$. With a long enough-crib and from the resulting ψ' segment ($\psi' = D \oplus P$), it was possible to recover the ψ patterns.

With modern computing, a more efficient process can be implemented. As part of this study, the author has developed a series of new algorithms, which partially automate the Testery manual processes, described in the following sections.

```
Crib P:          89MANNERN89UND89FRAUEN5
Dechi D:         RCPDIIJ/IYZLBMRZQTSEUSX
ψ′:              YRRRRRRRRRYYYYYYGGIIIDI
Δψ′:             8////////8/////K/M//KK
Δψ crosses:      500000005000004030044
```

Figure 2: Example of Crib Hit

5.1 Dictionary Search and Ranking

This new algorithm processes cribs taken from a large dictionary. A space is added before and after the crib, which is tested at all positions of the ciphertext. The results (the crib and their possible positions) are ranked using the resulting putative $\Delta\psi'$, taking into account the number of "good" symbols in $\Delta\psi'$ such as ●●●●● or **xxxxx** symbols, and penalizing symbols with a small (non-zero) number of crosses. The ranked results are manually inspected, and the more likely ones entered into a database of crib hits. Figure 2 shows an example of a particularly good crib hit. In this example, the elements of $\Delta\psi'$ have either no crosses, only crosses, or a majority of crosses (three or

[7] To be described in a separate paper.

[8] To be also described in a separate paper.

[9] To create a seemingly more random output Z as well as ΔZ, each pin on a given ψ wheel was more likely to be followed by a pin in the opposite state.

four).[10] In a more typical case, there will be less "good" symbols, and the ψ wheels are likely to step more often.

The reason the results must be manually inspected is that the algorithm produces a large number of false crib hits, which must be filtered out manually based on the expected traffic contents, or adjacent crib hits. Also, there might be conflicting crib hits at the same position or overlapping.

5.2 Extending Matching Cribs

A manual attempt is then made to extend the most promising cribs, by guessing additional symbols at their beginning and at their end, so that the (longer) putative $\Delta\psi'$ still has good characteristics. With a solid knowledge of the language and of the traffic contents, it is possible to extend the crib further so that a long stretch of ψ' can be obtained. Then, by removing repeated consecutive symbols from ψ', it is possible to obtain the (unextended) ψ stream and from it to extract the ψ wheel patterns. Historically, the Testery cryptanalysts would first recover the ψ patterns as described here, and finally, the motor wheel patterns.

With the current Tunny challenge, due to the author's limited knowledge of the language and the lack of prior information about the traffic contents, he was unable to extend the cribs enough so that the ψ patterns may be recovered.

5.3 Recovering the Motor Wheel Patterns

Instead of first recovering the ψ patterns, as it was done historically, the author had to develop an algorithm to recover the motor wheel patterns based on the crib hits in the database. This new method uses hillclimbing, and it searches for μ_1 and μ_2 patterns that generate an optimal motor stream. Such an optimal motor stream should maximize the number of motor stops at positions with $\Delta\psi'$ being ●●●●●, and minimize the occurrences of motor stops at other positions (where the $\Delta\psi'$ symbol has at least one cross). The $\Delta\psi'$ symbols are obviously examined only at those positions covered by a crib that appears in the database of crib hits.

Using this new algorithm, combined with extensive trial-and-error to rule out some crib hypotheses and to test new ones, the author was able to recover the complete μ_1 and μ_2 patterns for the challenge. The μ_1 and μ_2 patterns turned out to be minor variations of the μ_1 and μ_2 patterns for the Bream link. More importantly, it turned out that no motor limitation was used. A motor limitation would have made the recovery process more challenging.

[10] As shown in Figure 1, in BP notation / represents the ●●●●● symbol, 8 represents **xxxx**, K represents ●**xxxx**, and M represents **xxx**●●.

5.4 Recovering the ψ Wheel Patterns

Knowing the μ_1 and μ_2 patterns, and therefore all the positions where the ψ wheels step (or stop), allows for a more accurate assessment of potential cribs, by applying stricter criteria for valid cribs. Instead of relying on counting the proportion of "good" $\Delta\psi'$ symbols as described above (such as ●●●●● or **xxxxx**), a valid crib should always result in a ●●●●● symbol in $\Delta\psi'$ at motor stops, and in other symbols (with a very high probability) at positions where the ψ wheels step.

In addition to just ranking possible crib hits, it is now possible to rule out most of the wrong hits. This allows for better crib hits to be processed, in order to extend the crib, ultimately increasing the amount of recovered ψ' material. More importantly, since the ψ wheel positions are now known, it is possible to combine disjoint ψ' segments that have been recovered.

The author wrote a program to extract the ψ patterns automatically from such ψ' segments, also checking for possible conflicts. As a result of detecting some conflicts, minor corrections needed to be made to some matching cribs (for example, a particular crib word turned out to be followed by a comma instead of by a wrongly guessed full stop period). The ψ wheel patterns for the challenge were successfully recovered, and surprisingly, they turned out to be the same as those of the Bream link.

5.5 Deciphering the Challenge Messages

Finally, with all the wheel patterns recovered, the ciphertext could be deciphered, and the first challenge message read. After formatting the plaintext, the deciphered message starts as follows:

KRIEGSMASCHINE AUF HOHER SEE DIE U.S.S. LINCOLN ANDRIAN KREYE ANFLUG AUF DEN FLUGZEUGTRAGER U.S.S. ABRAHAM LINCOLN. FUNFUNDNEUNZIGTAUSEND TONNEN ATOMGETRIEBENEN STAHL, DIE GROSSTE KRIEGSMASCHINE IN DER GESCHICHTE DER MENSCHHEIT.

It ends with the following text, which includes the crib *MANNERN UND FRAUEN*:

JEDER QUADRATZENTIMENTER AUF DEM SCHIFF HAT SEINE FUNKTION, JEDER FALSCHE SCHRITT KANN DAS WOHLDURCHDACHTE ZUSAMMENSPIEL VON SECHSTAUSEND *MANNERN UND FRAUEN*, SIEBZIG FLUGZEUGEN UND TECHNISCHEM GERAT FUR MEHRERE MILLIARDEN DOLLAR AUS DEM TAKT BRINGEN.

The second ciphertext was successfully set[11] using the same wheel patterns (but different settings, i.e., different wheel starting positions). The plaintext was identified as an email in English sent encrypted from Frode Weierud to David Hamer. Its ciphertext is given in an appendix and its decipherment is left as an exercise to the reader, who is invited to send the solution to the author. The Bream patterns are also provided for reference.

6 Conclusion

The release of the Testery report has shed new light on the outstanding achievements of the Testery, using hand methods. The work on the mechanization of the Testery techniques and on solving the challenge has enabled the author to fully appreciate the ingenuity and creativity demonstrated by the Testery cryptanalysts. In addition, it is possible to assess the importance of the close cooperation between the Testery and the Newmanry, which was critical to making sure that BP's resources would be fully utilized, and large scale production of strategic intelligence from Tunny traffic could be achieved. Moreover, it is clear that the familiarity of the Testery cryptanalysts with the traffic they processed manually ensured that when the Germans introduced new changes and security measures, those could be promptly diagnosed by the Testery, and the cryptanalytic methods adapted to cope with those changes.

Another conclusion from this study is that the security of the system was greatly reduced by the fact that all five ψ wheels of the Lorenz SZ42 either step or stop together. If the ψ wheel motion had been implemented differently, the vast majority of the mechanized and manual methods developed at BP would have been rendered useless.

[11] The starting positions of the wheels were recovered, allowing for the message to be deciphered.

Acknowledgments

This work has been supported by the Swedish Research Council, Grant 2018-06074, DECRYPT – Decryption of historical manuscripts. In addition, the author would like to thank Dr. Tony Comer for facilitating the release of the Testery Report, and Frode Weierud for providing the challenge messages and reviewing an earlier version of this paper.

References

Jack Copeland. 2010. *Colossus: The Secrets of Bletchley Park's Code-breaking Computers*. OUP Oxford.

Paul Gannon. 2014. *Colossus: Bletchley Park's Last Secret*. Atlantic Books Ltd.

Jack Good, Donald Michie, and Geoffrey Timms. 1945. *General Report on Tunny: With Emphasis on Statistical Methods*. Bletchley Park Report HW 25/4. Kew, London: U.K. National Archives.

Ian Mayo-Smith. 2014. *Eavesdropping on Adolph Hitler: Deciphering the Daily Messages in the Tunny cipher*. Four Pillars Media Group, Connecticut, USA.

James Reeds, Whitfield Diffie, and J.V. Field. 2015. *Breaking Teleprinter Ciphers at Bletchley Park: An Edition of I.J. Good, D. Michie and G. Timms: General Report on Tunny with Emphasis on Statistical methods (1945)*. John Wiley & Sons.

Jerry Roberts. 2017. *Lorenz: Breaking Hitler's Top Secret Code at Bletchley Park*. The History Press, Stroud, Gloucestershire UK.

Sixta. 1945. *The Sixta History*. Bletchley Park Report HW 43/82. Kew, London: U.K. National Archives.

Testery. 1945. *Solution of German Teleprinter Cyphers (Testery) Linguistic Methods*. Bletchley Park Report HW 25/28. Kew, London: U.K. National Archives.

Appendix – Functional Diagram

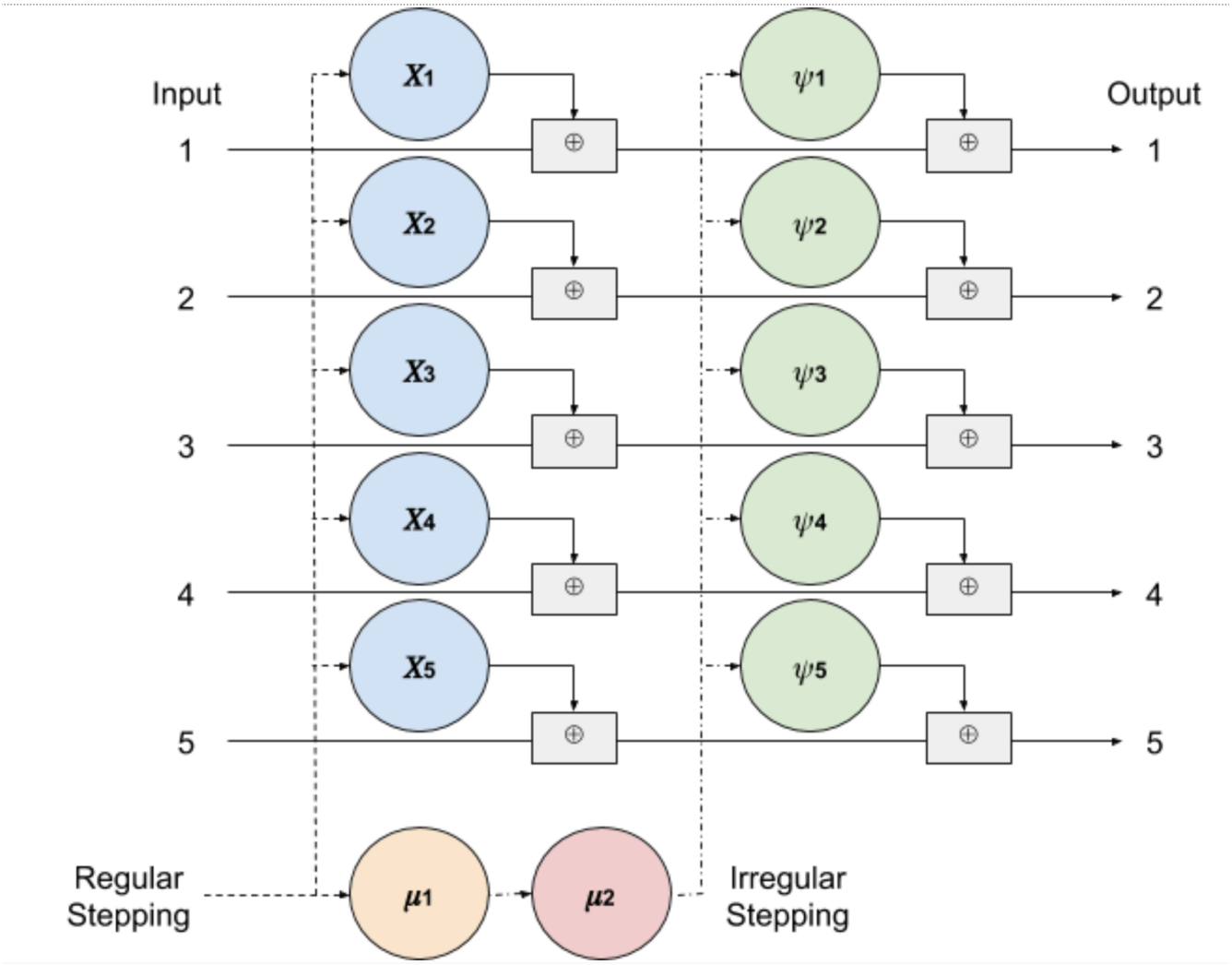


Figure 3: Tunny Lorenz SZ42 – Functional Diagram (Source: The author)

7 Appendix – Second Challenge Ciphertext


```
WGXXAQKD9AT4RYAFD/I4SE8KNDAIDNAYN8APH/MDHAOBM8Z9WRHYYBOZNOMPSVPSVSVJOMYKW+OJ4HJWFA9SRBU4FNUOMFMLWFRM3JGG3JVKHTNZNF4BZWZT4ISZE3/9BMO+
DYSYEGM/UGFWFEKSI8CGOGDIGENS4HREOIJJDKIVJIMT4SB3BAW3+PQJBUC+OYLBET8HKFLKQV+SZD9BI9R4YDBO4OQVEE9WJXCCGGMV3VMB4SUOMY83TLTX8SNQKK4PL8HJ
J8A3JVAI98SHSOKCCMI/HWV/UGYWC4PJVIEKGKJF+SWEXFBZHA9KWGIBZKN3CCL/ASZSPXVNETXPIOFS8P48DBMZBXUANHKGONLCU3V/F+SEORH+ORTATRU4T4WLQQEACGCY
8LIA4+OFVFUZEB/E8+V+NERZVENEH/OXPUUZEJ/UJ+3I4EFTRK8G3ACATNVZNW3FZRS8FNRCOY3QACY9WPFRKSILOIGMMUY+YESI/KPJ+UR/FOBL/G/JGUG3TCDJGJVEVLJI
IUNXCTQLOTAIDIAIPNN4GIX4HC/UCPMBWLXTUHGYCX++ZXDRNVI9KRIAWAND+ML/XFPABBLWFBJCX4BZKMS3EOQEAKDO/F4OBR9V8EJFHFRQPETVKE8VF/4SWB93C/8CMYYI
4C+EW88OXOOAUZXLPFQFM9LCM++TEEMAYBNJH3YIRB9Z4S+OVATHNQSF4WB9UAS94SBMTLZO/FSGHHDBFN+DAYYXFXVQ4AU+NWSJXBQKNHZ+8/KC8ZPHO+UNDPBSJG/8DRHS
ZY+/DF/VPJWVPCW8G9U/+9VUI+IIWO9AEBOX/TZTRFCN3QW3XV8KLFUWWAI4N/OACEUPTALHTTL4JFYDQQVTML8EOEVIYWAS+3APEXPNUBGWO3NJFYVYGAHOL/ELMY43S3PI
K3XYVKXHH+943JV3N+RHLZRHRXESBLYJA/KKLYCQX4TVGCYHFNYHB+UPZ/KB/+M/SE/URJIRIECHTGJDIT98R9HIVXZZSZ4MOKADBH/Z8/DDRLQ4DENYYU8PPJZ3IA3OAWIN
D8OS/8+ZCJZWJOGEL3XMBLZRHBM/YQKYBU8ZL+38L4JA4/O+RBHD4T8MYS9RW3WKE4/C8/GTL84PAB4DFHOUNVHSC8KDZS8AUYXXZT4RN8SFMFJMJLFTAJOXW4YINSKUKX4W
KIOOMQSMGSC9GI+JGLETHABDRERXCKQKEUNWUGEC/HOJPBZ9P4/GZDMYQ9PVWT//MLRFO8AISMPDTRPRM9F8TPGEUL4ZUZ4AVYBPLQL/4PBII8PRCYTJ+ZMEEGBNVPGDFPER
RBFL/GM+XKVSTLIPYEWL/NQAPFT4ABZZBLQ4WY9KF+4X4MVZCBI8MBZFFCNDGC/94/ZH9QG+CLSPJDBMWEAWKVG+AZGN4OC3++LBMDIU/CUDIA+YP8YTDU43VUHC8C/3GLCI
BNU8U4GWROJB/HEVZBLYX9W8NP+YVK9X9TJAWV4HUT/E4UJISKG8SOZUKNRDYBAM/+PLH3ANS4LF4P3UEFHGJ4U+K3XTLFEYAAA4XNHK4ISPSYYEE4LDU38VHFB3LVPFODVJ
+LBPX/GOP+R3F8H9++4LNLIJT4NXH+LM+DM3OE34/DLM//T3S++AZR44AOGLYRA3TWCWAX+OPZUIJ+VLKPWR/+EF+/EH8TJDC+TIIKX38JSJ+HIDTUILOPNEXIG+CRGKJKGT
YJIA++CIDPYU3MEY3/8JYGTXCCT/RNEJGT/S+UHJSGVXFDPIPQUUHNCAZDKO9MLXXCKV/8L3ROOKTEDNHBL4ZPQPS3EVHJW9JYUDP9CS/HP/4/GKAIMT9KKHBB3KNRQOFXTY
RZ9S3RGMMFFDE84SHYIWYE9PC993SYJ4C4XWHCLJ/+D3E4JVC3YEDG+ELGJHRD3PQZB/IRGOWA3DTIQSK3NDJXAGRAFCH/P4E+983MLLRORW9+FPGCVRUVHGKBB/RFY+9GVI
TA+4FNRDI/XDFT44IYWLN/LU9H+KBMJ9O98LR8RYBI9U+/TTZZXKNOETXAW9YUQL4GAEAYBC4NK4FIWEIWK93FPPHJ94U+WZFUW8ZZQPBYI/49+IPZSQKLWB8QTUM/QX+RUU
PRXVMD+VRB/ZNWJVSW9EGHIKDV8OQAZFWOW+SV+P+BCA9RIMEVGIXPP+VHBKB4M3NBJBA3USVC+/ZHXHPKKIHH3CVBQXKKIRBQNYQPBJSPI4EOJK3OOUAHV4J3+N9LVEC3NG
TXVHY+RXRQ3XB/J3CY9/IR4/M/AYV/YQBHQPUXGW4BI9XCEOHKSJVYBEDDNXXNBK3L84TITEMRZPHMX93RYXPJZYDTHVVJTP8XSVS9A8LWAKLUAAKXOJ/FXTOLZ/UDNVH9SG
BWHH+R8LENIAABBQPKBC9WUE4IT4LPX3E9/PXU3QY+FDCBXOT+VTESNPF+T8P3NH3AG8+B9M4ZRSRYRHXGJJEBV4MWWCMKNVV9AGRFBQ89QJAPSVX8+EECQ3DYWGMI/G+SG4
XXTQQI+TKCUIYYTPA+J4JOPM99CAH4TNZHZ/GAYYGLLT/V4DWC4MWYYBHCJWMDTZCZ8GJV88TMCXHTDZSZP3OIR+U8UUFJNPZCBLIROG/8NLZ/JPORMUDDT44U9VZGV/HJBP
MBOHL+3B48IA9/PUJIQIAUTOYOURQD9R/LFQ+APUQJYS+OQ3WTD8ZDPHFTYXIWPV4I/FRWXE8LMU9KUDJ9ZYMQMGNOXYCZWFLSJ49WDHBHQVJT33YFNSMJTRJDMKSOUXPCVK
+F+3XS89GWN4UPGQJ4HCQPW4YKQL9AZLT+YON/QABQUTK+ZH3/GBQUBTSSKVHOX8JPDWIB9RDBLOBGMKJN8K9ZUUNNSHRWZ/3TCKXBLZLEK9I/AUOJ8JBTHQWR3OQLDV+PCJ
9HMQIVPWXO+JR3V3EF8GXTXP8MR/AAI4ZPFCAGLZ4YZP8NL+9PSSP+TS+P/+QHUEFJ8RV3N8AX49E84QK43JYQT88U8UIC+UIOWSHW89AICN+FYGMS9GDFUYWM4G//TILINC
CCYWXCRDX9EBLE/8ER/IJGLLDDOJNESZTIJDFMWXZ9LLLM+XMTBV8BMXNCWZWF9LF+DW9WHRNFATBW+M+UWPHDUWUZPMMZHDA3OXAYBV8FJ8++4RPWUTMQRUREREZUAK4ZGV
P+JDZEHL3XNATMVNEHZPRJFU9MGGKPUFYC9N9PY9VFSB8+3PLUYR/M+TKMRO/JX9HMUKL8PZINB+H8TS/W/Q33YJB+GUCFTXHPX+E/9DGMTLCS48NFKGB34CIX4VEUGAMAQL
K4M3D+UBLVG8TU3W+TY9XP4JC3MLG9MX+KPKF9/QEDPS9NYYHZVL4ECYZ+Y43ASND++GQQJXLVGGOEYZF+XK8XMK9TN+YAMYE9LQNNY48SSW9HX4SSIOQXM9XBSIFW4FMQNL
SZ3GB8P/JDN3TP+XX/8SJIGKDLU3H9KQTELCDWXUX4RBINO3DRXMZISPG9DJQ4IKEBDAYWTBI43/4DENES8VOQAHQWXDQHHECD49ZPLPMBQ4+WOW9NW98VQHRKDV/OZHCSII
YNKDXGXYM3BWHHJ4BFKLW+GZDYBAUVPXGNMHSVQHDVEU/ZULZABCTRR9Q9PPK+SMCBH+TISZZJ/F4/ARA4QL+FOBYU/S+J9WBOCY3YX/NFIMB9IFXP/D99CSWOA9BOOPDZDV
L8IUSNKFL+STSFGV/KPXGLOGRJRJ3XCS8HJHEJJOPRXZRS9XZL+ORVOJAP4P/4GM4BW4XY8L/JVEQYZU/R4+F4NRX4GWHOGS3JBAAGVRRMII4YEEPVJZHYR9JZ/8RZRNC/L/
LOKWL8OW/M3VAUZXI4VJKLBPWM9ODLAAOXCZVGMXQ3I+JNJLRDD/3HUMMGSEIBFUTEUGP9X/BJX/3+VZL3/MR4MGP43IRRRITLPKFKRM/DC4ZNERP+DTOYB+B3N9+NK8M8W8
RBB3SSQDCIJQN+NUOEE9Z+O/SSCEM4FDKEMCJZ4TCIO/WRYELWIYJNW8BSVFMNVFBG8TR8Q9JS3HWCXNRORWLZ3M+BFBBAZTR3X3OHNDEVB+LSQUNASYOFRXBVPAZCOCL+XB
LWKT+NMNU44TVBCFEURH4LNGWQYHNQTHSNSTGZFNFGNF4ESNLHFCTBRATPTK/NK3BWVTJ4+AGQZR4C/TK39Y/HIE3MU8UNRUROG9DKMPHNVPHCOUQRMJSZA93H4HZN8MO/AY
PPTX8KN3C4YLC9W8M9LSH9YAPMCP/9MULFWGW/4SPHLKUSEIP+VX8IXY38HSHJ4M8VRBJ4LME4S3A9SPBQMGTCW+EU+BRX8JJ39LFAGNSQGFEHD8OUHU9QGPESLHXHJ+JGH4
+CPI38JVEDQXLAKKXKRLZ448OBRRE+NMW3GV/ZWN9XXFRLSYKZY+JVJTOQZUUWYX/RGSBO9DFPB4NAVKNP3NAFMQB/GWW4R83PDZS3HUI89MFRZ+QMDAITAQPMTKMEKPBQNJ
4VOAHQNA/CHTXRQKY49XKTFLUWUD84VTHWJFSV/KL8I3S3Z4R8YLLN8+ATWCLPECZNDRDGXLGK+APCHGYJGLENGIEYYLBRI4UT+RTAKNEKUXHUICMUNNXN9AVDUNEXGUDN//
PPWAZR8KNEP3UXQQ93FYQW3IHKVPUFGNFT9BIDE9KPP/9HGT+L3FG//YCLXYDYXP83LWU98UTOLVBJJPGQMOIGVZMRPLJ4SL4XMOMQBNI48PZO/F/LEQVCFH+CXRUERGOGXN
/YG+ISV8INOQMFTNLGG9VTXY8TZN4P+DDJOLNTAX/ZNYBFV8PVWUVQBR9/JGSIY/YFCXKFYU/48YP8MWUIZHZZEMVWMNZ3OS3BRCAXFNHNMKU4OVD9SXT3C9N94GFISDWHJ+
IWHKU4HHSIQI4PGY3SFCXW4Z4IPMNNFGTQCI4HVXPWJIJY4WN3KLQMDIHZLZMICBBSQSCBMT/AHY8NCDVCML4XQ4BX+9S3BUYDDZAYJZX8W4+8IVH3LSFS4QWB3Z9NMJUY4/
MQCDQFSPTA9QFK4FKSJ9K/ELBCRFOWNPGWVT9T9TOHNNSD4FQAMAMDFSD9CTR3W3WBGQL8C+FETSHKJO8E+UJ3ZVZDOSIG938N9MF/PTPSXKEZICSN/EECD84++TM4XGWZCF
Z9AGF8PMUNNTMYCFT8PQSKEZG3Y8HXPFJDZISVEHZ9J9MIREP8K+CC+8/8Y3WIMLUQ+/GQQSZEUJ9JUZ9KDWV9BJWNTHKLX9GIGQ/BAJJRZGLTZN8ELB8JFLLMF
```


Bream wheel patterns:[12]

χ_1 ●●●XXXXX●●●●XX●●●●X●XX●●X●●XX●X●XX●X●XXXX●

χ_2 XX●●XXX●XX●●●X●X●XX●●●X●●●XXX●

χ_3 ●●XXX●XX●●X●●●●XXX●●XX●XX●●XX

χ_4 ●●XX●●X●XX●●X●●XX●●X●●XXXX

χ_5 ●X●●●X●XX●●X●●●XXX●XXX●

ψ_1 ●●X●X●X●X●●X●●●X●XX●XX●X●X●●XX●XXX●●XXX●●●

ψ_2 ●●X●XX●X●X●X●X●XX●●XX●X●●X●XXXX●●●●●XXX●●X●XX

ψ_3 X●X●X●X●X●X●X●●X●●XX●X●X●XXXX●●●●●XXX●●●●XXX●XX●●X●●X

ψ_4 X●X●●XX●X●X●X●X●X●XX●X●●●●XX●●XX●●XX●XXXXX●X●●X●●●●X●

ψ_5 ●X●X●X●X●XX●●●X●X●X●●XXX●XXXX●XX●X●●●●X●●●X●●XX●XX●●XX●●X●X●X

μ_1 XXX●X●XX●●XX●●XX●●●XXXXX●X●XX●XX●●●XX●●●●XXXXX●XX●●XX●●●XX●●●●X

μ_2 X●XXX●X●X●X●X●●X●X●XXX●X●X●X●X●X●X●X●

[12] While the Bream patterns for the χ and ψ wheels were used to encrypt the challenge original plaintexts, the μ wheel patterns used for encryption are slightly different from the μ wheel patterns given here.