The Unbreakable Nazi Code and How it Was Broken

Robert A. Beeler, Ph.D.
East Tennessee State University

A Brief Intro to the Enigma

- Also known as German E-Code.
- The Enigma was a poly-alphabetic rotor-based cipher machine.
- Several similar machines were developed between WWI and WWII.
- The Enigma was the most famous of these because of its use by the German Military during World War II.

Some Disclaimers

- There were several variants of the Enigma used by the German military during World War II. For instance, the Naval Enigma was more complicated than the Army Enigma.
- To complicate matters, the Germans changed procedures several times. For example in 1938 the Army began selecting three rotors from five (instead of from three).
- I've had a hard time determining some of the details on how the cryptanalysis took place.
- All versions of the Enigma operate in essentially the same manner.
- My pronunciation on several names will likely be off.

Quick Outline

Frank Gorshin as

The Riddler, a.k.a, E. Nygma

- Intro to Cipher Systems in general
- Design and operation of the Enigma
- How it was broken
- Legacy

Cipher Systems

- A *cipher system* is a way of disguising a message in such a way that if it is intercepted, it can not be easily read by an “adversary.”

- We should assume that the adversary has intercepted the ciphered. Further, we should assume that the adversary knows the general method used to create the ciphered message.

- Hence, the objective should be to make it difficult or at least very time consuming for the adversary to decipher the message.

The Message Key

- Additional security is dependant on creating a *message key* which is the specific details as to how a particular message was ciphered. Thus, without knowing the message key, the intercepted message is of little value.
- In general, the higher the number of possible message keys, the higher the security of the system.
- Thus, the adversary would not be able to decipher the message by guessing.

Earliest Ciphers

- The earliest (and simplest) ciphers are *substitution ciphers*. A substitution cipher simply replaces every letter with another letter.
- Basically, a substitution cipher is just a permutation on the alphabet.
- For all cipher systems, the message being transmitted is called the *plain text.* The encrypted message is called the *cipher text.*

Caesar Cipher

- The *Caesar Cipher* is a substitution cipher in which every letter is replaced by the letter *k* units away.
- Example: If *k*=*5*, then ‘A’ is replaced by ‘F’, ‘B’ is replaced by ‘G’,…, ‘U’ is replaced by ‘Z’, ‘V’ is replaced by ‘A’,…, and ‘Z’ is replaced by ‘E.’
- The advantage of the Caesar Cipher is that it is easy to remember. All one needs to remember is the specific key *k* being used.

Ceasar Cipher (Continued)

- If each letter *x* is thought of as a integer modulo 26, then the Caesar cipher can be described as $x+k=y \pmod{26}$, where *k* is the shift being used (i.e., the message key) and *y* is the resulting cipher text.
- This can be deciphered using the equation $y-k=x \pmod{26}$.
- Of course, the adversary need only try 26 different *k* to decipher the message.

Random Permutation

- Another type of cipher system involves replacing ever letter with a *random* letter.
- For example, in the below cipher, each letter is replaced with the one directly below it.
- Unfortunately, the intended recipient must know what each letter has been replaced with.
- At first glance, this would seem to be more secure. There are now 26! or over $4*10^{26}$ possible message keys.

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

Random Permutation (Continued)

- Unfortunately, this is not actually that secure and can be broken using common sense.
- For example, in an English message of sufficient length: ‘E’ is 12.7% of the letters, ‘T’ is 9.1% of the letters, ‘A’ is 8.2 of the letters, ‘O’ is 7.5% of the letters, and ‘S’ is 6.3% of the letters.
- Thus it can be often be defeated by doing a frequency analysis of the cipher text letters.
- The most common two letter combinations are TH, HE, IN, ER, AN, RE, ED, ON, ES, and ST (in decreasing order).
- The most common three letter combinations are THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, and ETH.

Vigenere Cipher

- Appeared in a 1553 book by Bellaso, but misattributed to Vigenere (right) in 19th century.
- Example of a *polyalphabetic cipher.* That is, the substitution changes with each letter.
- Suppose that we choose period *n* for the Vigenere cipher. For i=1,…,n every ith letter is enciphered with $y=x+k_i \pmod{26}$. The k_i is a shift similar to that of the Caesar Cipher.
- $k_1,\ldots, k_n$ is the *key word.*
- Number of possible message keys is limited only to number of key words.
- French called it “le chiffre indéchiffrable.”

Vigenere Example

- Suppose our message is “ENCRYPTION” (5,14, 3, 18, 25, 16, 20, 9, 15, 14) and key word “MATH” (13, 1, 20, 8).
- Break the plain text into blocks of four (as math is a four letter word).
- The first block is enciphered 5+13 = 18 (mod 26), 14+1=15 (mod 26), 3+20 = 23 (mod 26), 18+8=0 (mod 26).
- Entire message is enciphered as (18, 15, 23, 0, 12, 17, 14, 17, 2, 15) or ROWZLQNQBO.

Breaking the Vigenere Cipher

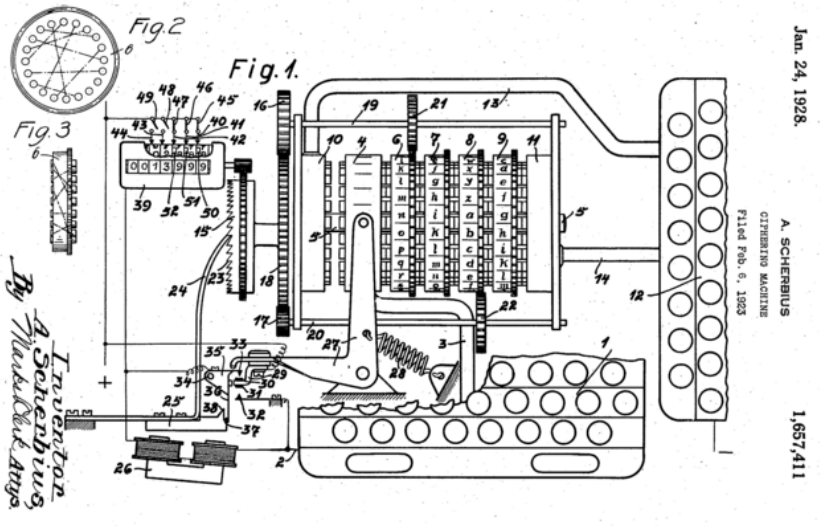
- Charles Babbage (1791-1871) broke the Vigenere Cipher in 1854, but did not publish his method.
- General method for breaking the Vigenere Cipher published by Friedrich Kasiski (1805-1881) in 1863.
- If the message is sufficiently long (relative to the key word), then the Vigenere Cipher can be broken by using frequency analysis on all possible block lengths.
- If the message is short (relative to the key word) then the Vigenere cipher can be broken by making educated guesses about what the plaintext may contain. For example, guessing that the message begins with “the.”
- It is also possible that the key word is some common phrase.

One-Time Pad

- Note that if the message key for the Vigenere Cipher is as long as the message, is a sequence of random characters, and is used only once, it is completely unbreakable.
- This is the basis for the one-time pad (right).

```
ZDXWWW EJKAWO FECIFE WSNZIP PXPKIY URMZHI JZTLBC YLGDYJ
HTSVTV RRYYEG EXNCGA GGQVRF FHZCIB EWLGGR BZXQDQ DGGIAK
YHJYEQ TDLCQT HZBSIZ IRZDYS RBYJFZ AIRCWI UCVXTW YKPQMK
CKHVEX VXYVCS WOGAAZ OUVVON GCNEVR LMBLYB SBDCDC PCGVJX
QXAUIP PXZQIJ JIUWYH COVWMJ UZOJHL DWHPER UBSRUJ HGAAPR
CRWVHI FRNTQW AJVWRT ACAKRD OZKIIB VIQGBK IJCWHF GTTSSE
EXFIPJ KICASQ IOUQTP ZSGXGH YTYCTI BAZSTN JKMFXI RERYWE
```

The Enigma Machine

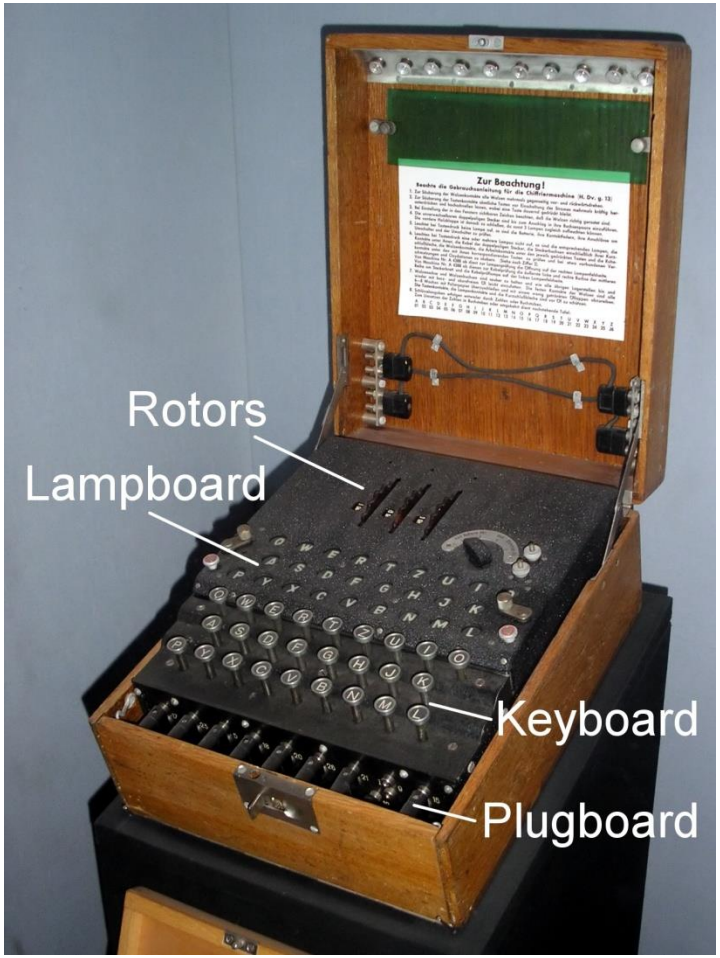


- The Enigma Machine is based on a complicated polyalphabetic cipher.
- Uses electrical components to substitute letters.
- Uses mechanical components to change the cipher system.
- Invented by Arthur Scherbius (1878-1929) in 1918.
- In its day, it was the world's most formidable practical cipher.
- Adjusting for inflation, each Enigma machine cost as much as $30,000.

Enigma Machine (continued)

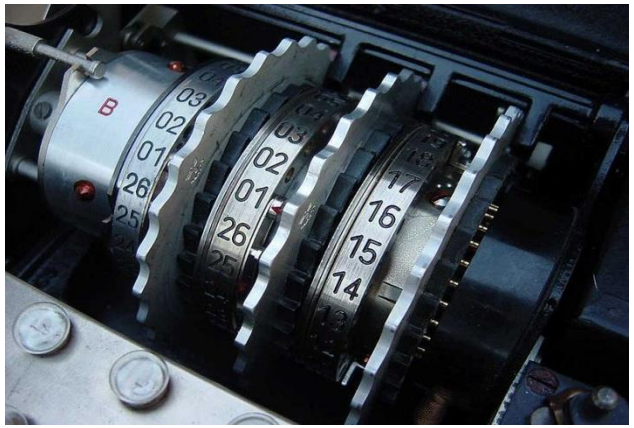
- Originally, the German military was not interested in the machine as they believed it to be too costly.
- Further, they (wrongly) believed that their ADFGVX cipher from WWI was still secure.
- In 1923, Britain published several histories of WWI. These detailed the importance of their intelligence and the failure of the German cipher system.
- German Navy began using Enigma in 1926. Subsequently adopted by the rest of the German military.
- Germans believed that Enigma was unbreakable until the end of WWII.

Components of the Enigma

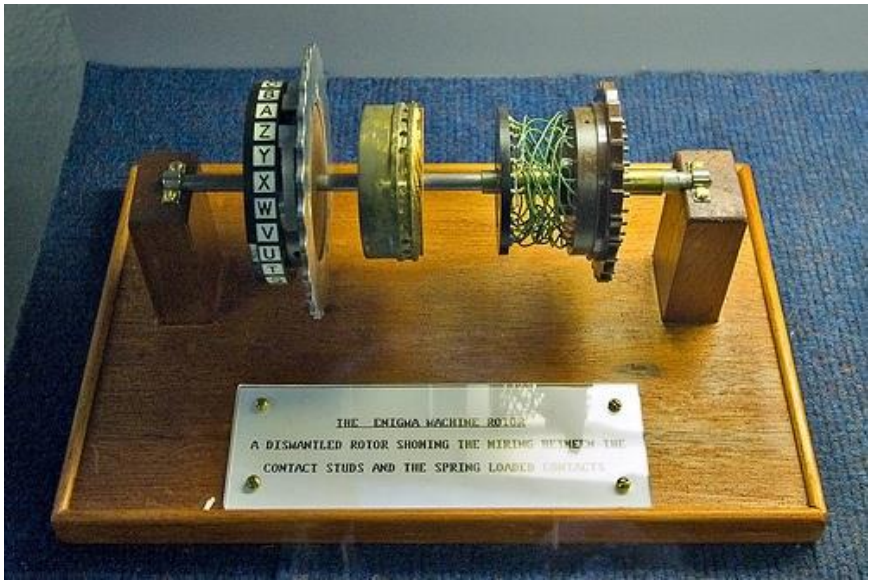


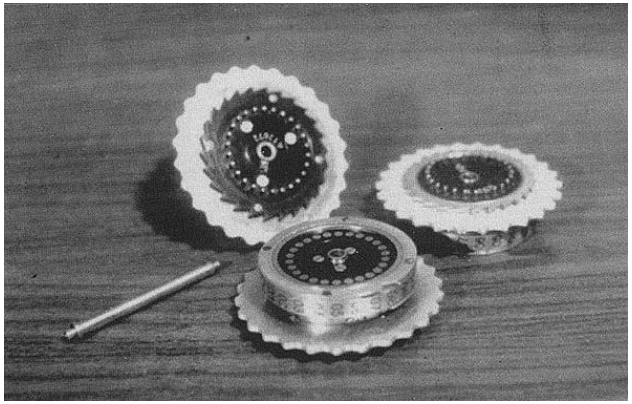
- The (military) Engima consists of a set of three interchangeable rotors, a reflector, a plugboard, a keyboard, and a set of labeled lamps.
- The operator would type the message into the key board. The lamps would illuminate the ciphered text.
- When a message was received, the operator would type in the cipher text. The lamps would then illuminate the plain text letters.
- Two operators were usually necessary. One operator would key in the message. The second would read the lamps.
- Some models of the Enigma included a printer.

The Rotors



- Each rotor had internal wiring that would enable the substitution.
- The rotors (typically labeled I,I,III, and later IV, V) were interchangeable.
- Each day, it was specified which rotors would be used and in which order.





What the rotors would do

- Let's say that the three rotors would respectively do the three substitutions below.
- So, if the letter 'G' is pressed, the first rotor would map it to 'C'. The second rotor would map 'C' to 'D.' Then the third rotor would map 'D' to 'F'

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

The Reflector

- Patented feature of the Enigma.
- The reflector would affect another permutation. This permutation would inter-change pairs of letters. The reflector would then send the signal back through the rotors.
- Note that when the signal is sent back through the rotors, the rotors use the inverse permutations.

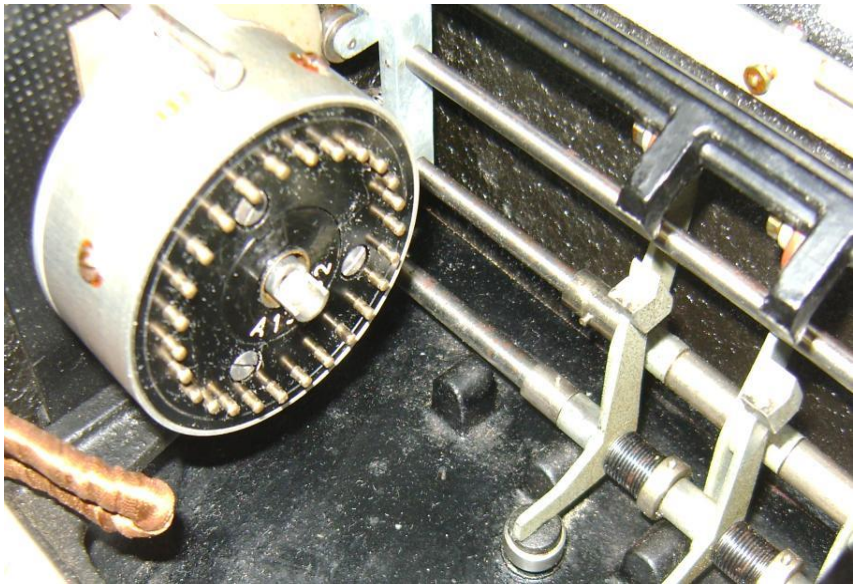
Example – Continued.

- Suppose that the action of the reflector is given by the permutation below. The remaining permutations are the inverses of the above example (in reverse order).
- Recall that ‘G’ had been mapped to ‘F’ by the rotors. The reflector then maps ‘F’ to ‘S’. The third rotor (inverse) maps ‘S’ to ‘S.’ The second rotor (inverse) maps ‘S’ to ‘E.’ Finally, the first rotor (inverse) maps ‘E’ to ‘P.’
- So after all that, the Enigma maps ‘G’ to ‘P.’

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

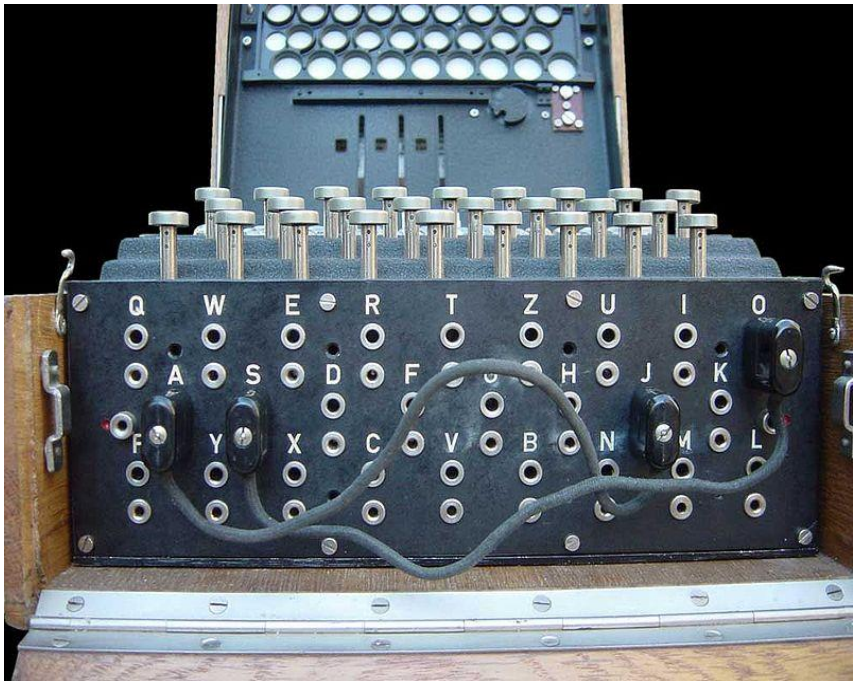
The Reflector (Continued)

- The advantage of the reflector is that it enabled a single Enigma machine to function for both encryption and decryption.
- In other words, the Enigma is self-inverse.
- This means that no letter was ever mapped to itself. This weakened the Enigma and was a valuable tool to the cryptologists trying to break the cipher.

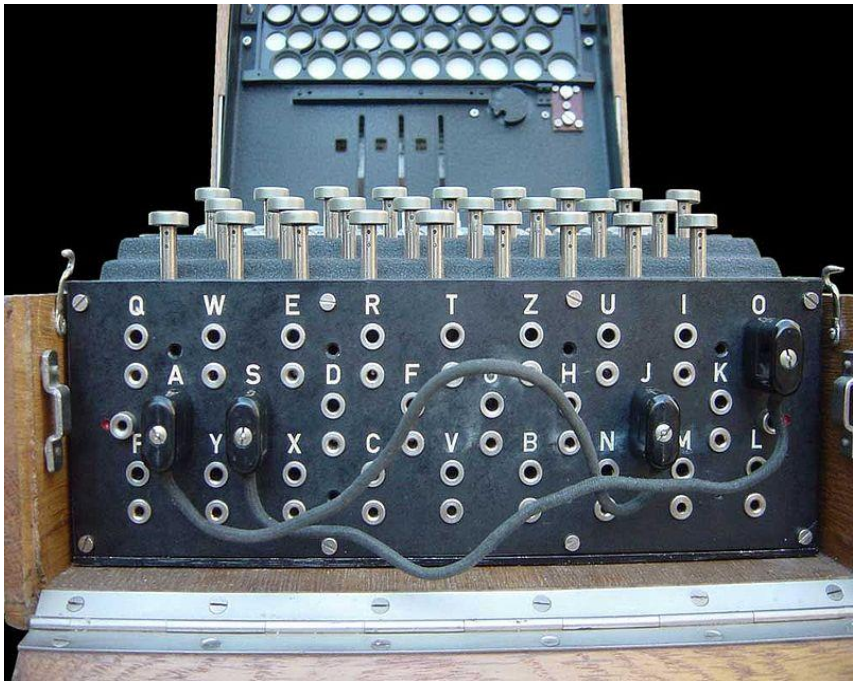


The Plugboard

- Feature of the military Enigma that greatly increased its security.
- Enigma machines without plugboards could be broken “by hand.”
- The plugboard (shown on the right) would swap pairs of letters before sending the information to the rotors or to the lamps.
- Up to thirteen pairs could be swapped. In practice, six (and later ten) pairs were usually swapped.



Plugboard (Continued)



- Suppose that the plugboard makes the swaps A<->G and T<->P (among others).
- Suppose the operator presses A. The plugboard swaps with G which is sent to the rotors. The rotors/reflectors change G to P (as described above). The plugboard then changes P to T. T is then illuminated by a lamp.
- All of this happens at the speed of electricity.
- Pairs of letters that were swapped by the plugboard were called “steckered.”

Composing Permutations

- The rotors, reflector, and plugboard each do a different permutation on the set of letters.
- Thus the combined effect of the plugboard, the three rotors, the reflector, the inverses of the three rotors (in reverse order), and the plugboard again can be thought of as a composition of nine permutations. This can be denoted

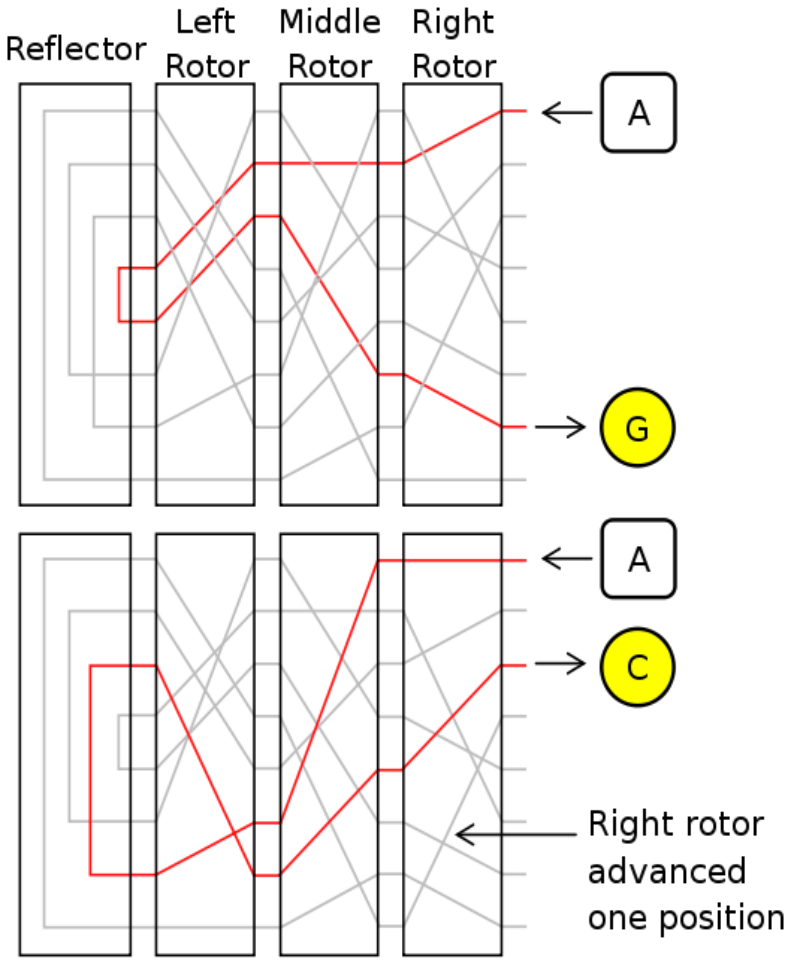
$$PRMLUL^{-1}M^{-1}R^{-1}P$$

- The composition of nine permutations is still just a permutation. Thus the result is an alphabetic substitution. So why was the Enigma more difficult to break than any other substitution cipher?

The Stepping Motion

- To prevent the Enigma machine from simply being a complicated way of doing a substitution cipher, each time a key was pressed one or more of the rotors would advance.
- This resulted in a new substitution cipher with each key stroke. In other words, the Enigma would mechanical do a polyalphabetic cipher.
- With each key stroke, the first rotor would advance one position. When the first rotor had advanced 26 positions, the second rotor would advance one position. When the second rotor advanced 26 positions, the third rotor would advance one position.

A Simple Example



- Suppose that a message begins with AA.
- On the first key stroke, the result is G.
- The first rotor then advances one position.
- When A is pressed the second time, the result is C because of the new substitution being used.

Enigma Applet

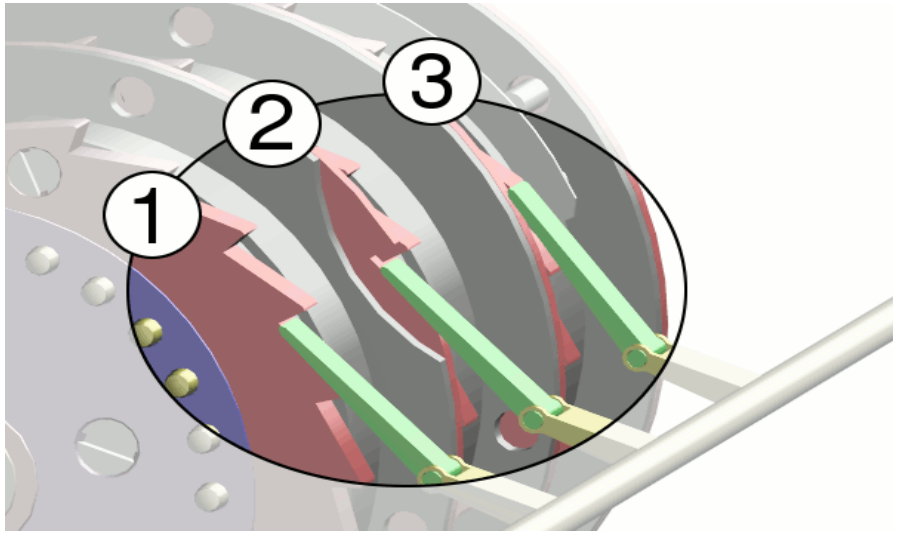
- An excellent Applet that simulates the Enigma is located at:

http://russells.freeshell.org/enigma/

- Note that the Enigma works as both encryption and decryption. So by returning the rotors to their original positions and typing in the cipher text, you get back the original message.

Double-Stepping

- If the stepping motion was all the Enigma did, it would result in an odometer style period.
- Instead, the Enigma featured *double-stepping.*
- If the second rotor advanced rotor three, the second rotor would advance again on the subsequent keystroke (i.e., two consecutive steps).



The Period

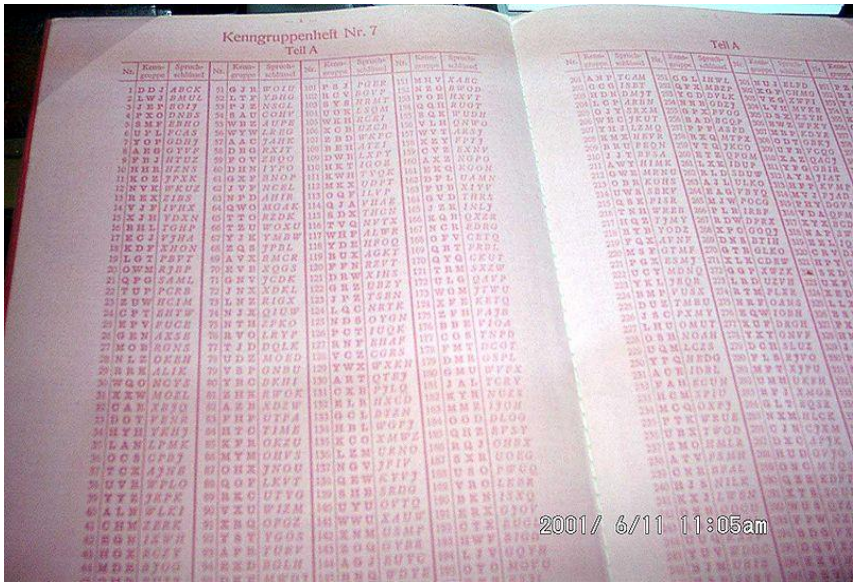
- Because of the double-stepping motion of the Enigma, the same combined rotor positions would only be achieved every 26*25*26=16,900 keystrokes. This is the period of the polyalphabetic cipher.
- Usually, the longer the period, the more secure the polyalphabetic cipher.
- Messages were limited to less than a thousand characters.
- Longer messages were parsed into two or more messages.
- Thus there was no chance of repeating the same combined rotor positions in a single message.

The Ring Setting

- The Enigma also included a *ring setting*.
- Two “rings” were placed in the Enigma. One was placed between the first and second rotor. The second was placed between the second and third rotor.
- Adjusting the rings changed when the rotors would advance relative to the previous rotor.
- So for instance you could set the ring so that the second rotor would advance when the first rotor had ‘A’ in the top position.
- Though the period remained the same, it was less predictable.
- Least vital component of the Enigma. We will largely ignore the ring setting for the remainder of the talk.

The Daily Settings

- It was necessary to insure that all military units used the same settings for the rotors and the plugboard.
- Thus each unit with an Enigma was provided with a table of settings (on right) that dictated these positions.



Geheim!

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppe
31.	I V III	06 20 24	UA PF RQ EO NI EY BG HL TX ZJ	jeu nyq aqm
30.	V II III	01 07 12	GF KV JM IB UW LX TD QS NA ZH	azs zds kck
29.	IV I V	11 17 26	CI OK PV ZL HX NB AW DJ FE ST	kap gwh lyx

A Bit of Combinatorics

- Suppose that we do not know the wiring of the rotors or the reflector. Further, we do not know the procedures in place (i.e., using six plugboard cables). However, we do know how the Enigma works.
- The number of possible combinations is then:

$$\left(\sum_{p=0}^{13}\frac{26!}{2^p(26-2p)!\,p!}\right)\left(\frac{26!}{2^{13}13!}\right)(26!)(26!-1)(26!-2)(26^3)(26^2)\approx 3.28*10^{114}$$

- To put in comparison, there are only about 10^{80} atoms in the known universe. No wonder the Germans believed the Enigma to be unbreakable.

A Bit More Combinatorics…

- Note that if we tried to break the Enigma by brute force (i.e., trying all possible combinations), this would be impossible (or at least VERY impractical) - even with modern computers.
- We can reduce the number of combinations by knowing the wiring of the rotors and the reflector. We can also reduce the number by knowing the German procedure of using six cables.
- Suppose that we know the above information. The number of possible settings is then:

$$\left(\frac{26!}{2^6 14!6!}\right) * 3! * 26^3 * 26^2 \approx 7.16 * 10^{18}$$

Yet More Combinatorics…

- Later in the war, Germans began using ten plugboard cables. Further, they began selecting (and ordering) three rotors from a pool of five.
- We still know the wiring and the German procedures.
- The number of possible message keys is then:

$$\left(\frac{26!}{2^{10}6!10!}\right)(5*4*3)\left(26^3\right)\left(26^2\right)\approx 1.07*10^{23}$$

- *If a man were able to adjust, day and night, a new key every minute, it would take him 4000 years to try all those possibilities one after another.* - Enigma Sales Brochure.

Sending a Message with Enigma

- Set Enigma according to the daily settings.
- Select a three letter *operator setting*. This is keyed in twice (as an error check). The operator notes the illuminated lamps – this forms the preamble.
- Reset the rotors based on the cipher of the three letter operator setting.
- Key in the message to be set.
- The preamble and the ciphered message is then transmitted.
- The operator setting meant that only a small portion of each message was encoded with that day's key.

Weaknesses of the Enigma

- In theory, the Enigma was practically unbreakable. However, various aspects allowed it to be broken.
- Machines, rotors, tables, and manuals were captured by the Allies.
- The Enigma functioned as both an encryption and a decryption device. Hence if `A' is mapped to `K,' then 'K' is mapped to `A.'
- No letter is mapped to itself.
- The true weakness of the Enigma lay in the procedures for using it and in operator error.
- Without this human error, it is thought that the Enigma would not have been broken.

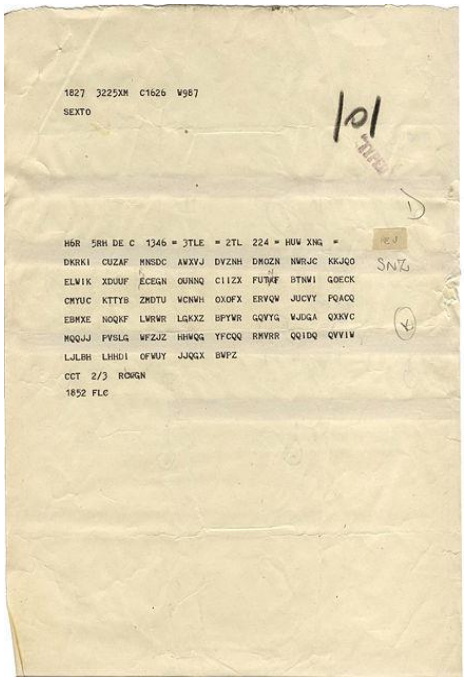
Operational Shortcomings

- Operators were supposed to select a *random* three letter operator setting. However, humans *rarely* choose things randomly.
- Some of the most common three letter settings were *HIT, LER, BER, LIN,* and *ABC.* One operator would always select *CIL* – for his girlfriend Cecilia.
- Operators would often select three letters that were adjacent on the keyboard.
- Other times, they would select three letters that would be close to the rotor setting. This would reduce the amount of work necessary to turn the rotors before sending the message.

Procedural Shortcomings

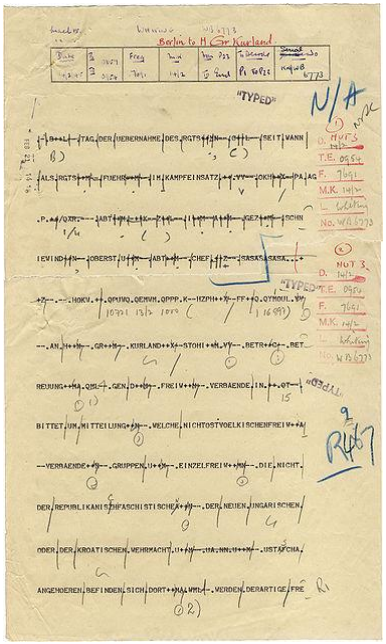
- Number of plugboard cables was always six (later ten). By varying the number of connections, the Germans could have greatly increased the number of possible message keys.
- Improvements in the Enigma and its procedures were made incrementally. For instance, when new rotors and a new reflector were introduced, messages were sent using both the old system and the new system. This would give the Allies time to determine the wiring of the new components.
- Similarly, messages were often transmitted on a less secure cipher.
- The Germans introduced several odd policies at various times that reduced the number of possible message keys (thus reducing security):
  - No rotor order was used twice in the same month.
  - No rotor would be in the same position it was on the previous day.
  - No letter was connected to its neighbor. So ‘S’ would not be connected to ‘R
- Settings from previous month were often reused.

To Decrypt the Enigma



- To decrypt the Enigma, an adversary would need the following:

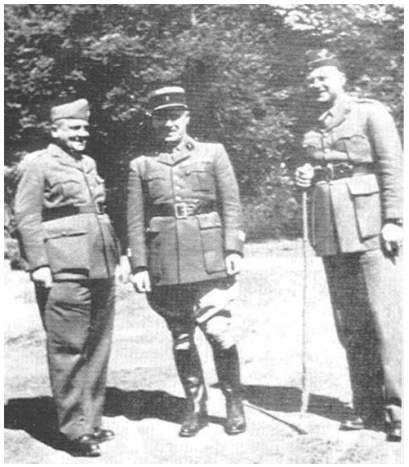
1. An understanding of the basic workings of the Enigma. This could be obtained by studying the commercial Enigma.
2. The wiring of the rotors and the reflector.
3. The daily settings.



Agent Asche

- Agent Asche (top) was the code name given to Hans-Thilo Schmidt (1888-1943).
- Sold Enigma manuals and daily settings to the agents of French Captain Gustave Bertrand (1896-1976, bottom center).
- The French believed that the Enigma was unbreakable, so provided these materials to Gwido Langer (1894-1948, bottom left) of the Polish Cipher Bureau.

Figure 41 Hans-Thilo Schmidt.



The Polish Mathematicians

- Because of the mechanical nature of the Enigma, it was believed that a scientific mind would have better luck than a linguist.
- In 1929, a secret cryptology course was organized by the Polish Cipher Bureau.
- Only selected German speaking mathematics students were selected.
- Of those students selected, only Marian Rejewski, Henryk Zygalski, and Jerzy Rozycki were successful.

Marian Rejewski (1905-1980)

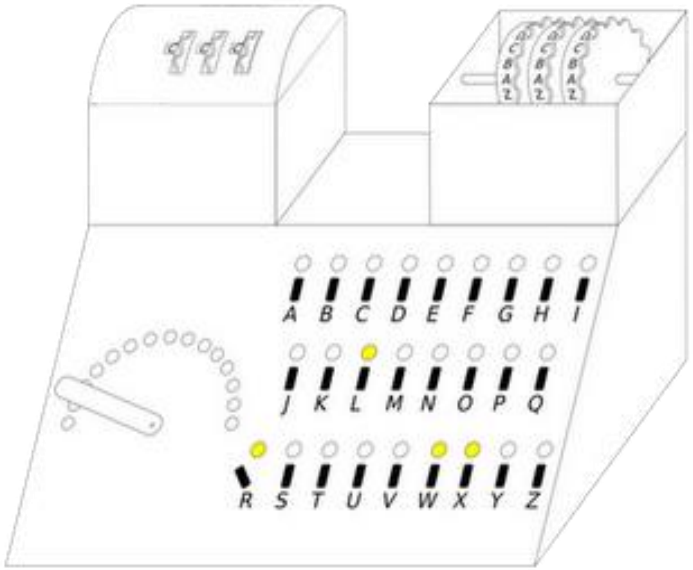
- Was provided daily settings for September and October and the Enigma operational manual by Langer.
- At this time, the Germans only changed rotor order every quarter. Since September and October are in different quarters, this was invaluable.
- By studying four letter cycles in the preamble, a few lucky guesses, and the material supplied by Bertrand and Langer, Rejewski was able to deduce the internal wiring of the rotors and the reflector.
- Also developed several methods to determine the daily settings.

Cycles in the Preamble

- Rejewski's method only worked provided that the second rotor was stationary during the initial six permutations.
- Suppose that we have a large enough number of Enigma messages for a given day. As noted earlier, the first and fourth letter of the cipher text correspond to the same plain text letter. This relation is given below.
- In this case, there are four cycles (A,X, Y,T, N,V,U,J,Q,W,O,D), (B,F), (C,E,R,K, I,H,L,G,S,M), and (P,Z). These are cycles of length 12, 2, 10, and 2, respectively.
- Though the letters in each cycle were changed by the plugboard, the cycle patterns (in this case 12, 2, 10, 2) were not.
- Allowed for the development of the cyclometer.

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

The Cyclometer



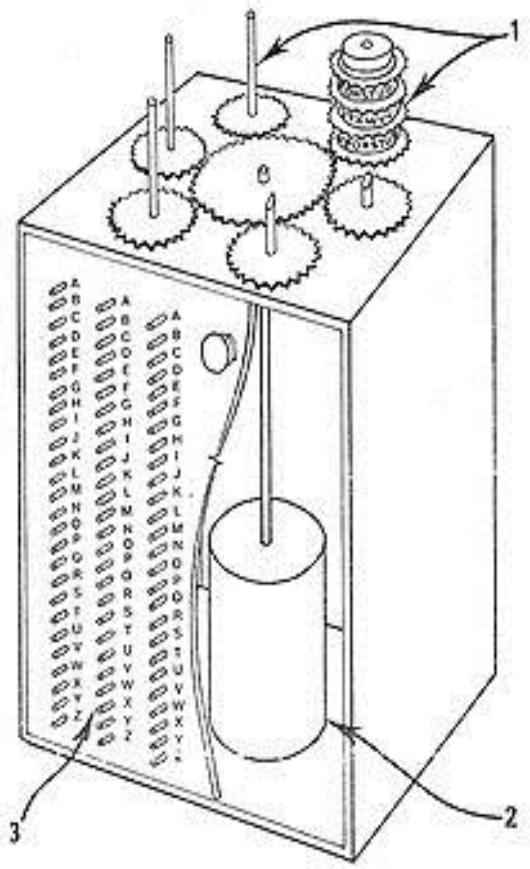
- Developed by Rejewski in 1934 or 1935.
- Mechanically determined the number and length of cycles generated by rotors in the Enigma Machine.
- Consisted two sets of Enigma rotors. The first was set to the rotor positions (say ABC), the second to three positions later (i.e., ABF).
- Independent of the plugboard settings.

Card Catalog

- The card catalog was a list of possible cycle patterns and the corresponding rotor settings.
- Reduced the $7*10^{18}$ settings to merely 105,456.
- Took nearly a year to construct.
- Once card catalog was constructed, daily settings could be determined in under 20 minutes.
- When the Germans changed the reflector, card catalog had to be reconstructed from scratch.

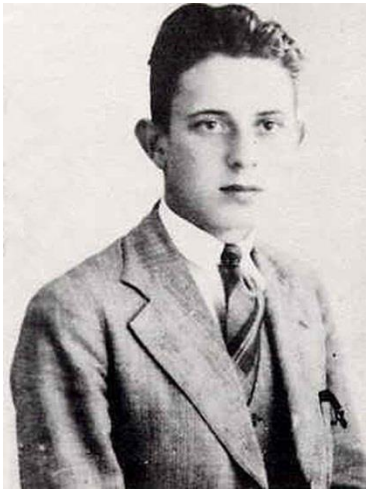
The Polish Bomba

- Developed by Rejewski in 1938.
- Six machines were used simultaneously.
- Used brute force to go through all rotor settings.
- Worked independent of the plugboard connections.
- Could reconstruct daily settings in about two hours.



Henryk Zygalski (1908-1978) Jerzy Rozycki (1909-1942)

- Zygalski (top) developed a manual method for determining the daily settings.
- Rozycki (below) developed a “clock” method to determine which of the machine’s rotors was in the right most position.



Zygalski Sheets

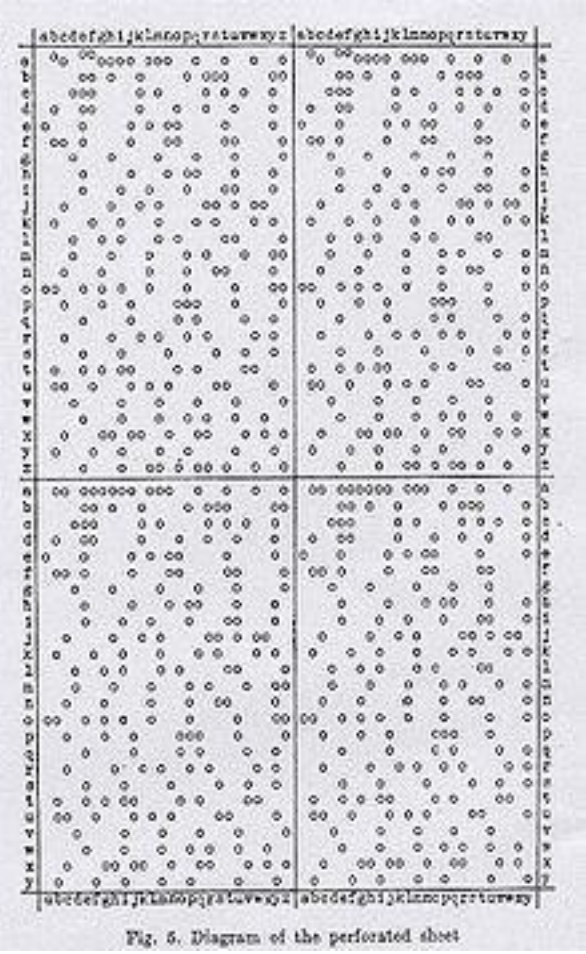


Fig. 5. Diagram of the perforated sheet

- The Zygalski Sheets were perforated sheets used six at a time (one for each of the possible permutations of the rotors).
- For security concerns, these were hand made by the mathematicians.
- 26X26 matrix represented the 676 possible starting states of the left and middle rotors.
- Used to determine the starting position of the left most rotor. As this is this is the slowest moving rotor, this starting position would be used for most of the cipher.

Changes in the Enigma

- Polish Cipher Bureau was breaking Enigma ciphers in December 1932.
- Germans changed the reflector in November 1937, rendering the “card catalog” obsolete.
- In December 1938, the Germans introduced two new rotors. This meant that there were ten times as many combinations for the daily settings. Effectively, this meant that ten times as many Zygalski sheets had to be produced. Further, it meant ten times as many bombas were necessary.
- In July 25, 1939, the Poles divulged their intelligence on the Enigma to their French and British allies.

Moving on…

- Rejewski and Zygalski were evacuated from Poland to France shortly after Germany invaded Poland on September 1, 1939.
- Moved from France to England shortly after the French surrendered in June 1940.
- Began working with the English at Bletchley Park.
- The Poles were years ahead of their Allies who had made very little progress on the problem of Enigma.
- Peripherally involved with Project Ultra in Britain.
- Ultra was most often associated with the breaking of Enigma messages.
- Despite their groundbreaking work on the Enigma, the Poles were rarely trusted with anything important – they were often relegated to more menial tasks.

Project Ultra

- Codename of the high-level intelligence gathered by Britain's Government Code and Cipher School.
- Based at Bletchley Park (below) an estate near Buckinghamshire.
- Winston Churchill - "It was thanks to Ultra that we won the war."
- Harry Hinsley – Ultra shortened the war "by not less than two years and probably by four years."

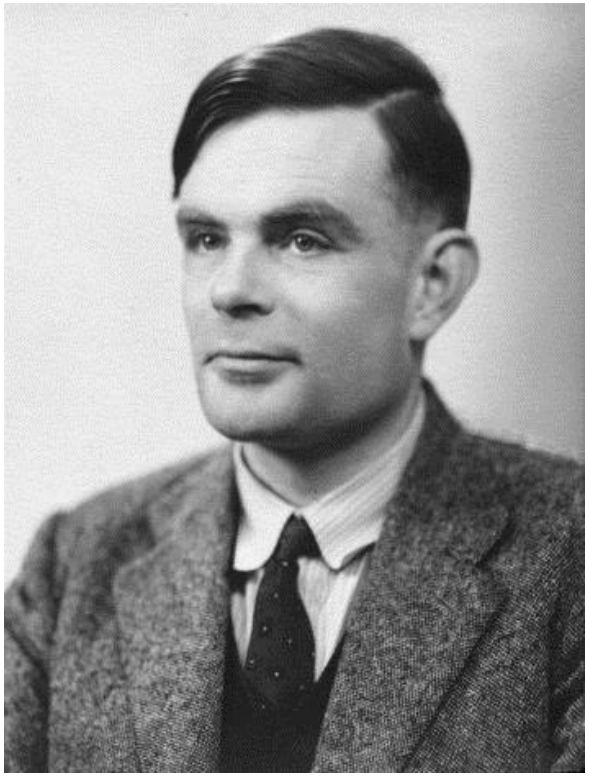
Project Ultra (continued)

Hut 6, where the Air Force Enigma decryption was housed.

- Employed not only mathematicians but linguists, chess masters, and crossword experts.
- Problems were often passed around the room to find someone with the skill set to tackle it.
- Actually used a difficult crossword in the newspaper to find potential recruits.

Alan Turing (1912-1954)

- Head of section responsible for German naval cryptanalysis.
- Developed the *bombe* with the aid of Gordon Welchman in 1938.
- In 1939, solved the essential part of the naval indicator system.
- Developed a method to decrypt Enigma messages *without* relying on the three letter operator setting.

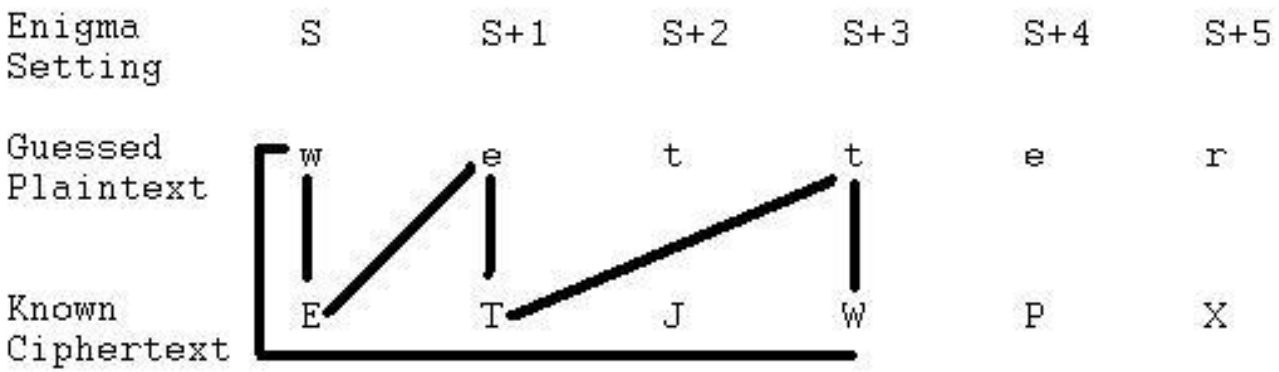


Crib-based decryption

- A *crib* is any plaintext or suspected plaintext in the ciphertext.
- Common cribs included military ranks.
- The word “EINS” (German for “one”) occurred in 90% of all messages.
- Weather stations would begin with “Today’s weather in…”
- In the case of parsed messages, the second message would begin with “Continued from…”
- Hemorrhoids were a problem in desert regions. Transmissions from those regions would often include that word.
- Allies would sometimes allow themselves to be spotted by German units. Those units would then report the sighting using that day’s key. This was a technique known as *gardening*.
- “Nothing to Report” was also a common crib.

Loops within Cribs

- Suppose that we are looking for the crib “wetter” (German for “weather”).
- Turing realized that certain types of cribs would contain loops connecting plaintext and ciphertext letters.
- An example of such a loop is below.

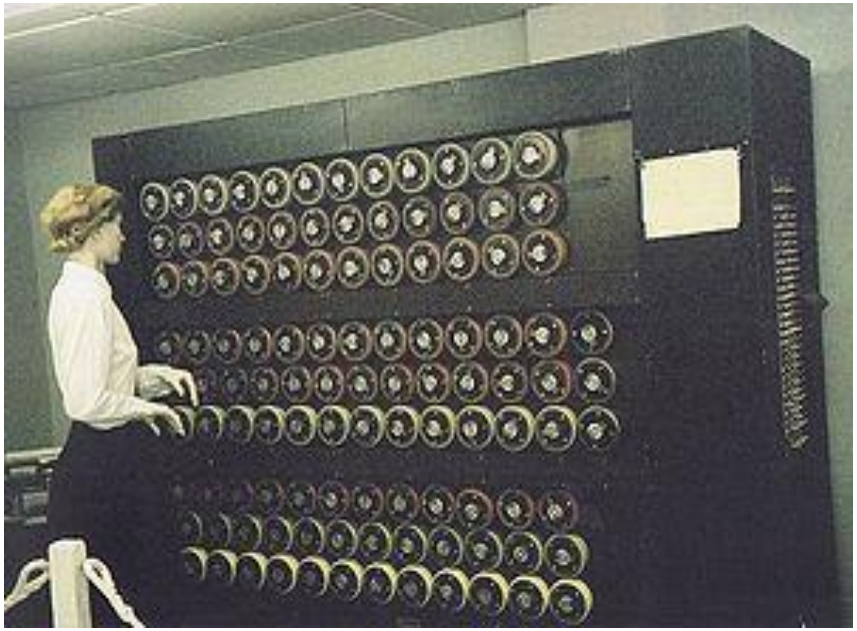


Finding Cribs

- Knowing what cribs to look for would be insufficient. You also needed to know *where* in the ciphertext the crib occurred.
- Cribs could often be located in the ciphertext using the fact that the Enigma *will never* cipher a letter into itself.
- Basically, can rule out locations for a potential crib.

Guessed Plaintext (1)			W	E	T	T	E	R	N	U	L	L	S	E	C	H				
Guessed Plaintext (2)				W	E	T	T	E	R	N	U	L	L	S	E	C	H			
Known Ciphertext	I	P	R	E	N	L	W	K	M	J	J	S	X	C	P	L	E	J	W	Q

Turing's Bombe



- Based on the Polish Bomba, however was substantially faster.
- Essentially 108 Enigma rotors.
- Used *cribs* and *logical deductions* to reduce the number of possible rotor settings.
- Brute force analysis of the remaining rotor settings.
- Also determined the plugboard partner for a specified letter.
- Basically a primitive computer that paved the was for the Colossus.

“Dilly” Knox (1884-1943)
Gordon Welchman (1906-1985)

- Alfred Dillwyn “Dilly” Knox (top) was a British codebreaker. Developed a linguistic technique known as *rodding* for breaking Enigma codes that did not have a plugboard.
- Welchman (bottom) was a British-American mathematician. Developed a *diagonal board* that increased the efficiency of Turing’s bombe. Suggested to Turing to look for cribs.

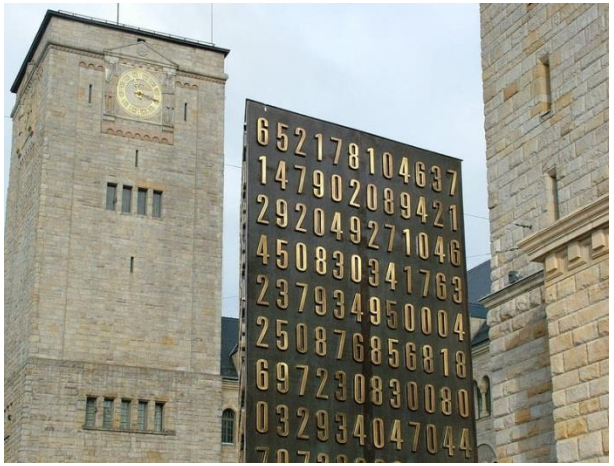
Safeguarding Sources

- In order to keep the Germans from realizing that their unbreakable code had been broken, they were careful to safeguard their sources.
- Spotter ships and aircrafts were sent before attacks on Axis supply ships. Search missions were simultaneously sent to areas with no Axis ships. Fake messages were also sent signaling the sighting of U-boats.
- Sent radio messages to a fictitious spy in Naples. Thus the Germans believed that leaks were due to espionage rather than codebreaking.
- Allies made judicious and careful use of Ultra intelligence. Winterbotham claims that Britain allowed the Coventry Blitz (below) on November 14, 1940 to occur in order to safeguard Ultra.

Legacy of the Enigma

- Per Allied orders, captured Enigma machines were often destroyed at the end of WWII.
- Many of the surviving Enigma machines are in museums in U.S. and Europe. Others are in private collections. Complete Enigma machines have sold for over $100,000.
- Britain sold several Enigma machines to developing countries. They also gave several to former colonies.
- The Enigma (and other rotor based cipher systems) were largely rendered obsolete by computers.

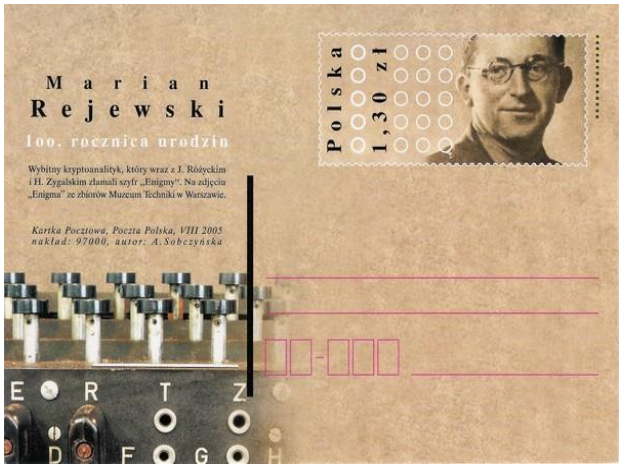
Legacy of the Poles



- The contribution of the Polish mathematicians was not widely known until 1974.
- Bronze monument (top) erected in 2007 in front of Poznan Castle.
- Plaque in front of Bletchley Park (below) placed in 2002.
- All three posthumously awarded Grand Cross of the Order of Polonia Restituta.

Legacy of Rejewski

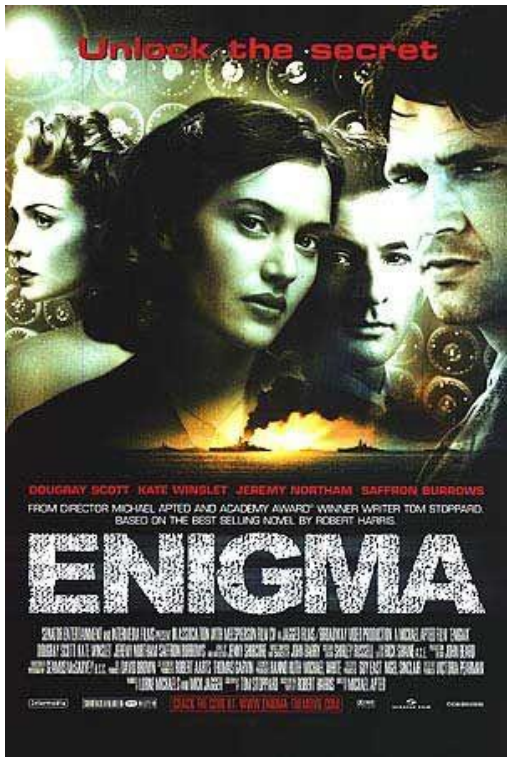
- Rejewski in particular is remembered as a national hero in Poland.
- Buried with full military honors at Warsaw's Powazki Military Cemetery.
- Memorial (top) unveiled in 2005 at his birthplace.
- A prepaid Polish postcard featuring Rejewski (below) released in 2005.

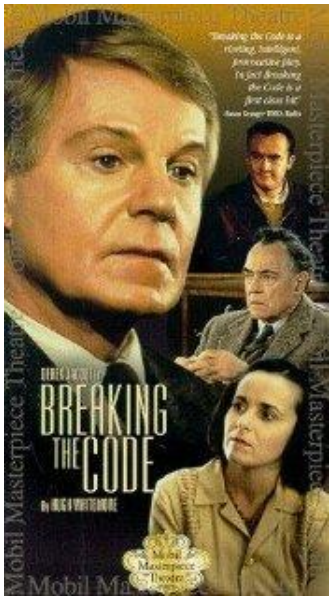


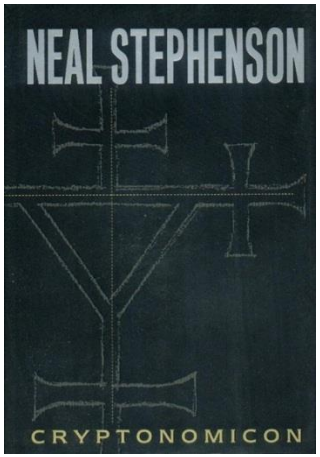
Turing's Legacy

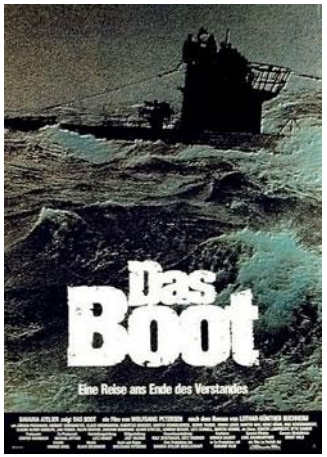
- Remembered as "The Father of Computer Science."
- In 1952, convicted of indecency. Opted for chemical castration rather than imprisonment.
- Committed suicide in 1954 by eating a cyanide laced apple.

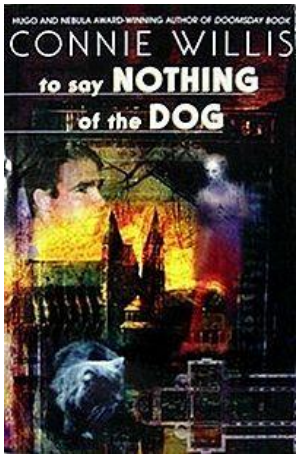
The Enigma in Popular Culture











Internet Sites

- Many of the images in this presentation were “borrowed” from various sites on the internet.
- Bletchley Park’s Official Page: http://www.bletchleypark.org.uk/
- Enigma Applet: http://russells.freeshell.org/enigma/
- Tony Sale’s Codes and Ciphers page on Enigma: http://www.codesandciphers.org.uk/enigma/
- National Cryptologic Museum: http://www.nsa.gov/about/cryptologic_heritage/museum/
- National Security Agency: http://www.nsa.gov

References

- Chris Christensen. “Polish Mathematicians Finding Patterns in Enigma Messages.” *Mathematics Magazine.* **80**, No. 4, (2007), 247-273.
- Josef Garlinski. *The Enigma War: The Inside Story of the German Enigma Codes and How the Allies Broke Them.* Schribner: 1983.
- F. H. Hinsley and Alan Stripp. *Codebreakers: The Inside Story of Bletchley Park.* Oxford university Press: 2001.
- David Kahn. *Seizing the Enigma: The race to break the German U-boat codes 1939-1943*. Barnes and Noble, New York: 1991.
- Wladyslaw Kozaczuk and Jerzy Straszak. *Enigma: How the Poles Broke the Nazi Code.* Hippocrene Books, New York: 2004.
- Marian Rejewski. “An Application of the Theory of Permutations in Breaking the Enigma Cipher.” *Applicaciones Mathematicae.* **16**, No. 4, (1980), 543-559.
- Hugh Sebag-Montefiore. *Enigma: The Battle for the Code.* Wiley: 2004.
- Simon Singh.*The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Anchor Books, New York: 1999.
- Douglas R. Stinson. *Cryptography: Theory and Practice, Second Edition.* Chapman & Hall/CRC, Boca Raton: 2002.
- Brian J. Winkel, Cipher Deavers, and David Kahn. *The German Enigma Cipher Machine: Beginnings, Success, and Ultimate Failure.* Artech House: 2005.
- F. W. Winterbotham. *The Ultra Secret.* Orion Paperbacks: 2000.