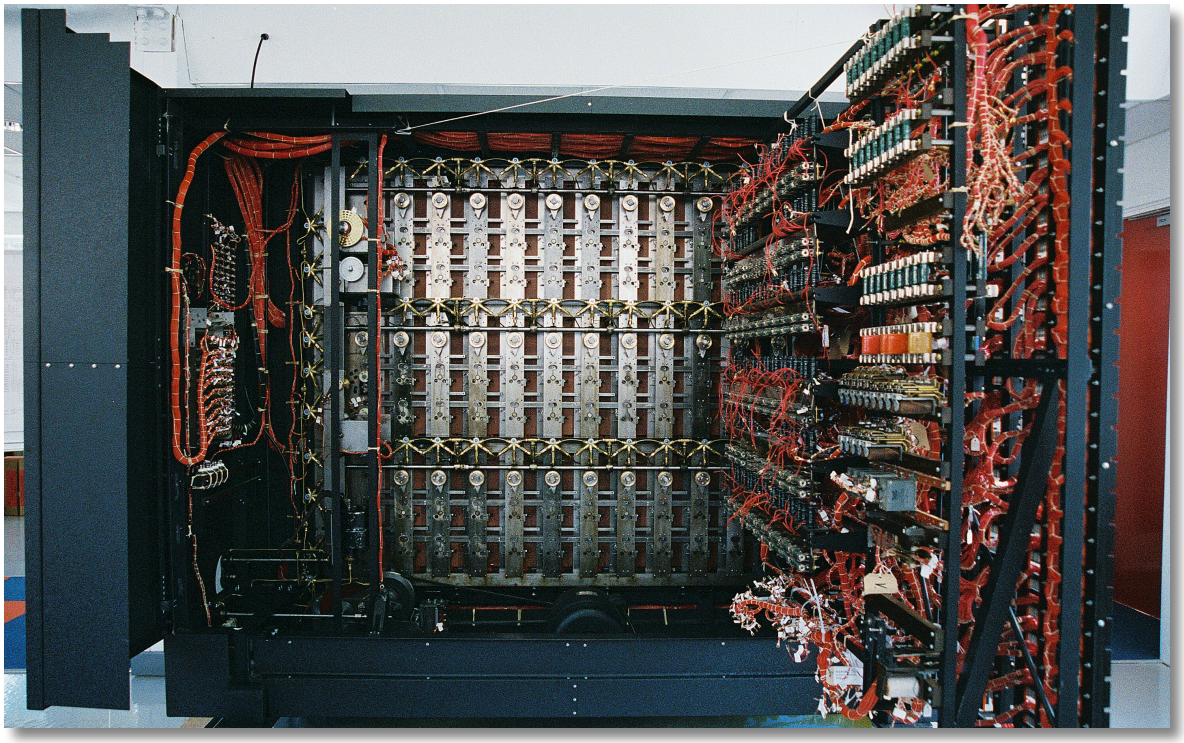
Breaking Enigma



Leqi Wang

July 2017

Math 190s Duke University

Breaking Enigma

Abstract

Enigma is a machine widely used by Nazi German military, an abominable enemy of the Allies in WWII (the second world war). One Enigma machine has 159 million million million settings, which takes people 20 million years to break. However, if the settings of Enigma could not be solved, the Allies would never know the meaning of the messages floating in the air. Therefore, the work of breaking Enigma was essential for Allies in the war. This paper will go through the contribution made by Polish mathematicians and navigate deeper into the secret work in Bletchley Park: the Bombe Machine designed by Alan Turing and Gordon Welchman — the precursor of Colossus computer and the birth of computer science.

I. Background

1. History

After WWI (the first world war), the statutes of the Treaty of Versailles made the German Empire (Deutsches Kaiserreich), the defeated nation, lose their priority before the war. “Of the many provisions in the treaty, one of the most important and controversial required ‘Germany [to] accept the responsibility of Germany and her allies for causing all the loss and damage’ during the war.”[1] “The treaty stripped Germany of 25,000 square miles (65,000 km^2) of territory and 7 million people. It also required

[1] https://en.wikipedia.org/wiki/Treaty_of_Versailles

Germany to give up the gains made via the Treaty of Brest-Litovsk and grant independence to the protectorates that had been established.” [2] … …

The massive slash weakened the German community and put British on a highly unwary state. The English Channel had put too much sense of safety in the British mind. When the first commercial Enigma (with no plugboard) first emerged in 1918, British had known its existence and openly bought some for studying. Soon, since they found out that the rotor settings were almost unbreakable, they gave up trying. After all, Enigma belonged to their defeated opponent, which made British think it was unnecessary to solve this seemingly invincible machine. Eight years after that, in 1926, the German Navy started to equip Enigma. The British knew it, but they took their chances to ignore it because of their arrogance and accomplished nothing during these eight years. Along with them was the Allies of World War I — French and Americans whose over-confidence also made them disregard the potential which Enigma may possess in the future.

Still, there was a community who noticed Enigma —- the Poles.

figure1: Poland in 1919

[2] https://en.wikipedia.org/wiki/Treaty_of_Versailles#Territorial_changes

“In the Aftermath of the war, following the collapse of the Russian, German and Austro-Hungarian Empires, Poland became an independent republic in Nov11th, 1918.” New Poland valued its grave crisis. In May8th, 1919, Polish government had established its own intelligence office and until 1926, their capacity of breaking German and Soviet secret code remained a high position. It was what happened in 1926 really freak them out —- they could not break any German code anymore. Throughout the experience Polish had in breaking German and Soviet code in the old days, they could not even find one clue of how to break new German message. Still, the Poles did not give up like their went along in England. They did the first and most important contribution, a huge break through, in the history of cryptography —- they replaced linguistics with mathematicians. And since then, progress had been made in the code breaking work.

II. The Polish

1. Cryptography of Enigma

If we want to break Enigma code, there are few things have to know beforehand:

(a) The structure of Enigma, including internal circuit of each rotor. And to achieve this, a German spy named Hans Schmidt, who was wrecked should took all the credit. “Hans-Thilo Schmidt (13 May 1888 – 19 September 1943) codenamed Asché or Source D, was a spy who, during the 1930s, sold secrets about the Germans' Enigma machine to the French."But French did not have any clue and were

too lazy to solve the puzzle, so they transmit this machine to the Poles. " …thereafter the Poles were able to read a large proportion of Enigma-enciphered traffic."

(b) German Army operation code — their encryption order. And this term was also achieved by Polish excellent agents work: the operators would first encipher the text-key using the daily key (from the code brochures they got at the beginning of the month) twice. And this enciphered daily key would be put at the beginning of each message. For example, if the daily key is XYZ (window setting in Enigma) , the sender will randomly come up with three letters , such as QWE, as the text-key or the index group. (These three letters cannot be adjoining or repeating.)

A —>C1
T—>C2
X—>C3
A—>C4
T—>C5
X—>C6

And the message Poles received, should be:

C1C2C3C4C5C6，… …

Since Enigma is self-reciprocal, the receiver just have to set the window to XYZ, and input C1C2C3C4C5C6, then they can get two groups of ATX, which is the text-key of the whole passage. Then he or she should set the window to ATX, then input the content, the letters, in the ciphertext.

(c) The daily settings of Enigma, which involves the order of the rotors, window setting (or rotor settings) and plugboard settings. This part, the default settings, was what Polish mathematicians had to work out.

“Now we had the machine, but we didn't have the keys and we couldn't very well require Bertrand to keep on supplying us with the keys every month ... The situation had reversed itself: before, we'd had the keys but we hadn't had the machine — we solved the machine; now we had the machine but we didn't have the keys. We had to work out methods to find the daily keys.” —- Marian Rejewski.

2. Marian Rejewski.

figure2: Marian Rejewski

“In 1929, while studying mathematics at Poznań University, Rejewski attended a secret cryptology course conducted by the Polish General Staff's Cipher Bureau (*Biuro Szyfrów*), which he joined in September 1932. The Bureau had had no success in reading Enigma-enciphered messages and set Rejewski to work on the problem in late 1932; he deduced the machine's secret internal wiring after only a few weeks. Rejewski and his

two colleagues then developed successive techniques for the regular decryption of Enigma messages. His contributions included the cryptologic card catalog, derived using the cyclometer that he had invented, and the cryptologic bomb." “ Until just before the Second World War a small Polish team of three mathematician-cryptologists, headed by the brilliant Marian Rejewski, had been happily breaking the German military cipher machine, the Enigma for many years.” What he did was to use group theory and matrix permutation establish the theoretical solution, and designed a machine called “Bomba”, an electrically powered aggregate of six Enigmas, which solved the daily keys within about two hours. This machine greatly inspired Alan Turing’s Bombe machine afterward.

The mathematical process was too complex and too abstract. Still, there was a principle Rejewski developed to work on —- six-letter index group.

a) Break rotor settings:

If we set the changing process of text-key to ciphertext as function (A), the time rotor rotate represented as footnote 0,1,2… …(A0, A1,A2… …), then we have:

$$X(A0) = H$$

$$Y(A1) = G(\text{the rotor has rotated once after the operator taps})$$

$$Z(A2) = A$$

$$X(A3) = B$$

$$Y(A4) = L$$

$$Z(A5) = E$$

(let XYZ represent three random non-repeated and non-adjoining letters)

Notice, letter H and letter B are transformed from one letter X. And letter X(A0) happens when the first rotor remains default state. This is an essential information for directly shows the default settings of Enigma.

Because of the reciprocal quality of Enigma, we have:

$$X(A0)(A0) = X$$

Therefore:

$$X(A0)(A0)(A3) = B$$

We've already know H = X(A0), so:

$$H(A0)(A3) = B$$

Until now, the letter X is eliminated. And this was also what Rejewski discovered — the relationship between ciphertext B and H is irrelevant to the plaintext X. So if we want to find the default rotor settings of Enigma, we just have to find 26 different telegraph text with non-repeating first letter and the forth letter to find one word substitution table.

For instance, we find the first letter in these 26 message pieces to be:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

And the forth letter in these 26 message pieces to be:

FQHPLWOGBMVRXUYCZITNJEASDK

And then we can construct one table:

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

b) Break the plugboard

From the table above, we can discover:

A = F = W = **A**;

B= Q = Z = K = V = E = L = R = I = **B**;

C = H = G = O = Y = D = P = **C**;

J = M = X = S = T = N = U = **J**;

each table will give us several loops.

And Rejewski notice that though people put on the plugboard of letter A and B, the chain would only become:

B = F = W = **B**;

A= Q = Z = K = V = E = L = R = I = **A**;

C = H = G = O = Y = D = P = **C**;

J = M = X = S = T = N = U = **J**;

Plugboard would not change the length of the chain and the number of the chain under the same window setting of Enigma. (He used strict mathematics to prove it.) So the effect of plugboard can since be canceled.

The work of making letter substitution table took Polish almost a year. But finally, Polish mathematicians ripped off the Encryption mechanism in 1933.

c) Flaw

"The Polish cryptologic bomba (Polish: bomba kryptologiczna; plural bomby) had been useful only as long as three conditions were met. First, the form of the indicator had to include the repetition of the message key; second, the number of rotors available had to be limited to three, giving six different "wheel orders" (the three rotors and their order within the machine); and third, the number of plug-board leads had to remain relatively small so that the majority of letters were unsteckered.[dubious – discuss] Six machines were

built, one for each possible rotor order. The bomby were delivered in November 1938, but barely a month later the Germans introduced two additional rotors for loading into the Enigma scrambler, increasing the number of wheel orders by a factor of ten. Building another 54 bomby was beyond the Poles' resources. Also, on 1 January 1939, the number of plug-board leads was increased to ten. The Poles therefore had to return to manual methods, the Zygalski sheets." And not long after that, in Sep 1939, German and Soviet Union invaded Poland. In Oct 6th, 1939, Warsaw capitulated.

III. Bletchley Park

figure3:Bletchley Park pictured in 1926. (Evening Standard/Getty Images)

Since the Poles withdrew from the historical arena, the British had already experienced the frightful Enigma code.

"Some people thought we were at war with the Germans — incorrect. We were at war with the clock. Britain was literally starving to death. The Americans sent over

100,000 tons of food every week. Every week the Germans would send our desperately needed bread to the bottom of the ocean."

Bletchley Park, therefore, was a institution set up by authority — British government itself — to gather the most brilliant mind in the world and solve the hardest puzzle at then — Enigma. At the beginning of WWII, there were only about 200 people in the Bletchley park. However, at the end of the war, there were near 7000. "These people had a variety of backgrounds – linguists, chess champions, and crossword experts were common, and in Knox's case papyrology. The British War Office recruited top solvers of cryptic crossword puzzles, as these individuals had strong lateral thinking skills." Winston Churchill referred to them as " *my geese that laid the golden eggs and never cackled*".

"On the day Britain declared war on Germany, Denniston wrote to the Foreign Office about recruiting 'men of the professor type'.Personal networking drove early recruitments, particularly of men from the universities of Cambridge and Oxford." These people were distributed in 15 different houses, or "huts". And Alan Turing, the man who designed the original form of Bombe machine, happened to work in one of them, hut8, specializing in breaking German Navy Enigma code.

IV. British Bombe machine

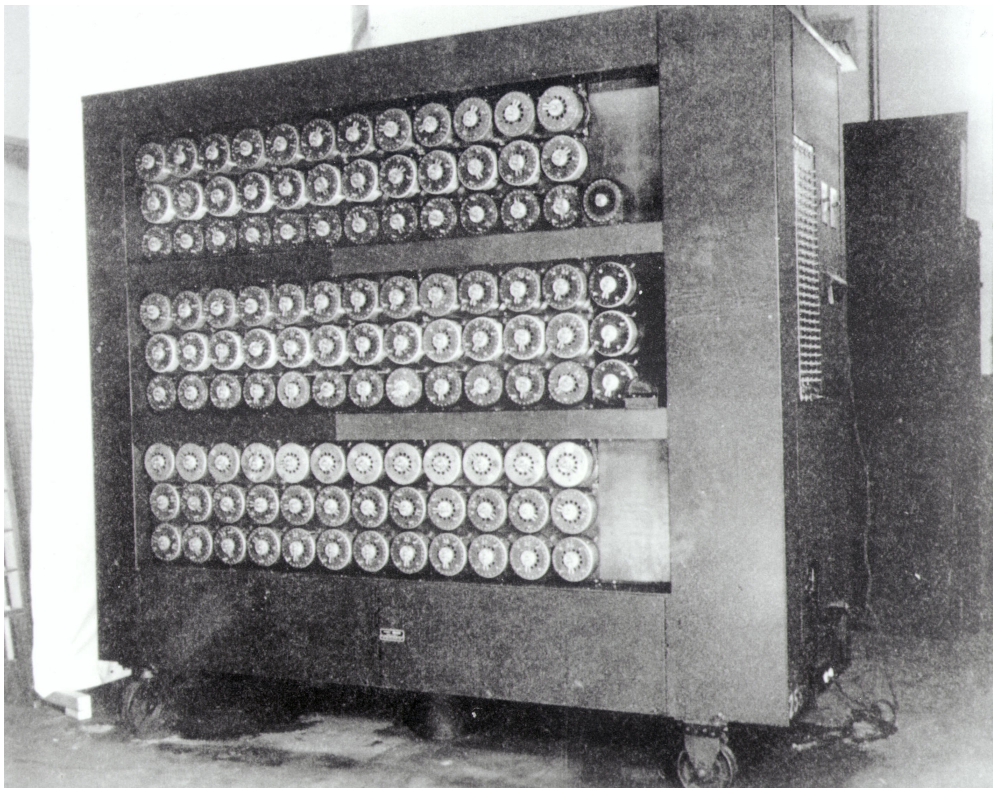


figure4:Front of bombe code-breaking machine at Bletchley Park, 1943.

"Enigma is an extremely well-designed machine. Our problem is that we are only using men to try to beat it. What if only a machine can defeat another machine?"

—The Imitation Game

-Turing's machine

Enigma machine mechanized the enciphering process. I have mentioned that Polish invented a machine called Bomba to defeat Enigma. Unfortunately, the lack of

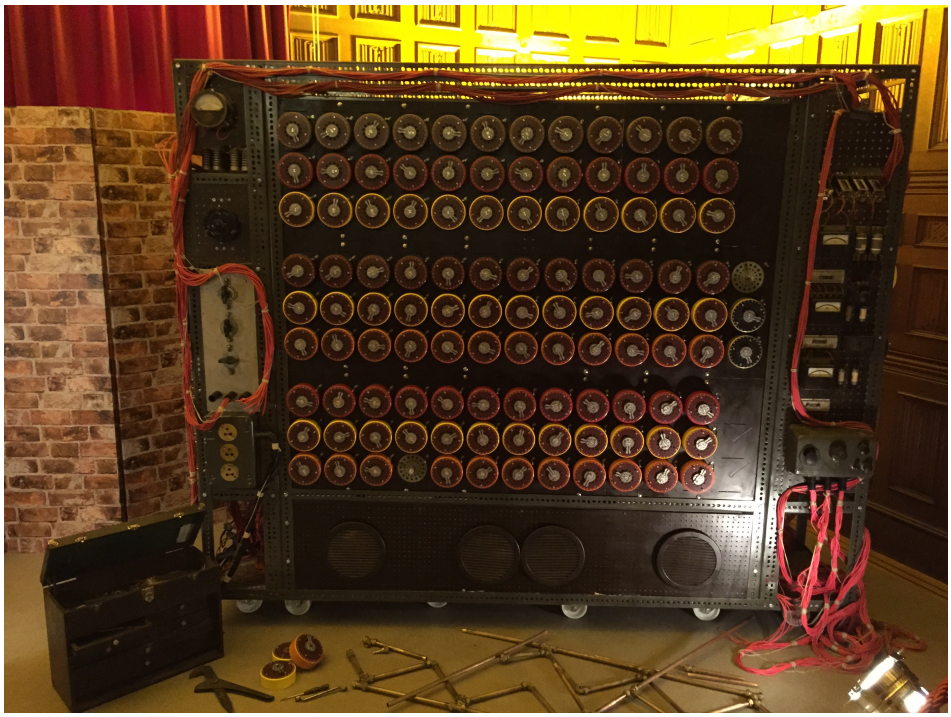


figure5: Modern replicate of British Bombe machine. (there were no Bombe machine left after the war because of its ultra confidentiality in the government.

funding and technical supporting finally could not make Bomba keep up with the upgrading Enigma design. However, Turing's research subject (those flexible and full-functional Turing's machine) and his research train of thought (universal machine, digital computers) brought hope for the gradually losing Allies.

He was inspired by what Rejewski did previously:

a) Intercept the message and use the first 6 letters (index group) to create loops.

b) Conceive permutation matrix and diminish plugboard influence.

c) Using Bomba to calculate possible settings in scrambler part (rotors settings).

d)Using other mechanisms recover plugboard settings.

But the technique Rejewski used was rather wasteful — they only used the first 6 letters in a whole ciphertext. Besides, after the Germans add two rotors in to the

scrambler, this method became inoperable. Therefore, Turing comes up with a new idea:

	Rejewski	Turing
purpose	find connection	find connection
range	first 6 letters	whole message
basis	same index group is enciphered twice	one on one substitution between plaintext and ciphertext
principle	ciphertext-ciphertext connection	ciphertext-plaintext connection
method	creating loops + brute force cracking	creating loops + brute force cracking
application	3-rotor Enigma	all Enigma

Notably, once in Bletchley Park, interceptors always received one message at 6:05a.m everyday. These messages were short and very punctual. And a female staff in the Park, Margaret Rock, made an accurate guess — these message were all weather report. So what index could a weather report tell us?

Sunny or rainy

Clouds amount

The wind

Temperature

Maybe in some area, there would be ocean temperature or the storm condition.

So from the Cryptanalysis perspective, we can cracking this weather message from following angle:

1. statistics angle: in a weather report, it should not involve too many datas in one plaintext, not to mention these plaintext have to appear in a certain order.

2. Comparative Interpretation/Contrast cracking: If we know this message is towards what part on the ocean, we can use our own weather report to make contrast and deduce the data-containing letters in the message.

3. By guessing the right correspondence in plaintext and ciphertext, then make exclusion of the wrong key.

The last principle is not only suitable for weather report but for all kinds of Enigma code. And Bombe machine, Turing's machine, was also based on this last principle.

For example, if we intercept a message at 6:05 a.m:

Q P L U D O E T Q W K Y O F I X Z M D F

Now we've already know that this is a weather report, whose correspondence in German is "wetter". And we know that every words' ciphertext cannot be itself (reflector). Then we can make a guess that "wetter" corresponds to ETQW KY:

```
Q P L U D  O E T Q W  K Y O F I  X Z M D F
           | | | |    | |
           W E T T    E R
```

And if we start to create a loop, we have:

```
W  E2 T2 T3 E R
|  |  |  |  | |
E1 T1 Q  W K Y
```

in order to create a loops, we should make

(W-E1-E2-T1-T3-W)

as one loop

which represents the relation of

plaintext - ciphertext - plaintext - ciphertext - plaintext - ciphertext

Set the position of the plaintext letter on the ciphertext position x as P(X), the next enciphered letter should be P(X+1). Since “wetter” has 6 letter in it, we have P(1)~P(6).

Then Turing carried out his most adept logic: each move of the enciphering, he imagines it as a working machine. If we set this independent machine as T(n), we have:

T(1)	T(2)	T(3)	T(4)	T(5)	T(6)
W	E2	T2	T3	E	R
|	|	|	|	|	|
E1	T1	Q	W	K	Y

Remember, the enciphering order of Enigma is:

Plaintext —> plugboard —>3rotors —> plugboard —> ciphertext

So T(n) also represents:

Plaintext—> Ciphertext

T(1): W— >E1

T(2): E2— >T1

T(4): T3— >W

In each Turing’s machine, it has:

Plaintext —> plugboard —>3rotors —> plugboard —> ciphertext

so the relationship among cipher texts and plaintext as a whole become:

T(1):W —>plugboard —>C1—>rotors—>C2—>plugboard—>E1

—>T(2):E2—>plugboard —>C3—>rotors—>C4—>plugboard—>T1

—>T(3):T3 —>plugboard —>C5—>rotors—>C6—>plugboard—>W

—>T(1):W

We have known that the function of the plugboard is to reverse two letters to create larger possibility. So we have:

C2 = C3;
C4 = C5;
C6 = C1;(loop)

And the plugboard between these letters cannot create impact any longer.

T(1):W —>~~plugboard~~ —>C1—>rotors—>C2—>~~plugboard~~—>E1

—>T(2):E2—>~~plugboard~~ —>C3—>rotors—>C4—>~~plugboard~~—>T1

—>T(3):T3 —>~~plugboard~~—>C5—>rotors—>C6—>~~plugboard~~—>W

—>T(1):W

Alan Turing's Bombe machine connects 36 Enigma machines in series to diminish all the effect plugboards have. And it can find all possible settings of rotors by method of exhaustion (brute force).

Conclusion

Unlike Bomba using the substitution letter table to work out all the settings, Bombe machine used some unchangeable underlying flaws in Enigma to decipher the code. Turing's team built 2 machines in 1940 and deciphered over170 messages. At the end of WWII, British made nearly 200 Bombe machines. Though Bombe machine did not represent one notable advance in computer technology since it was made up by relay switches and mechanical rotors, its upgraded edition — the Colossus Computer, made up by electrical circuit and vacuum tube and used to break Nazi Lorenz cipher — became the precursor of modern computer and the representative of computer science.

Reference

Yanfeng Zhao. (2008).Legends of Enigma. Beijing, China: Science publishing house.

Andrew Hodge. Counting the Possible Plugboard Settings.https://www.codesandciphers.org.uk/enigma/steckercount.htm(Accessed July 22nd, 2017)

https://www.highbeam.com/doc/1P2-37646813.html

https://www.zhihu.com/question/28397034

https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#Polish_breakthroughs

https://en.wikipedia.org/wiki/Bombe#Bombe_menu

https://movie.douban.com/subject/10463953/questions/34393/

https://freewechat.com/a/MzI5MzIwNDI1MQ==/2650115543/5

https://en.wikipedia.org/wiki/Colossus_computer

http://www.cryptomuseum.com/crypto/bombe/

https://sites.google.com/site/bomberebuilt/rebuild1-htm

http://www.ellsbury.com/bombe1.htm