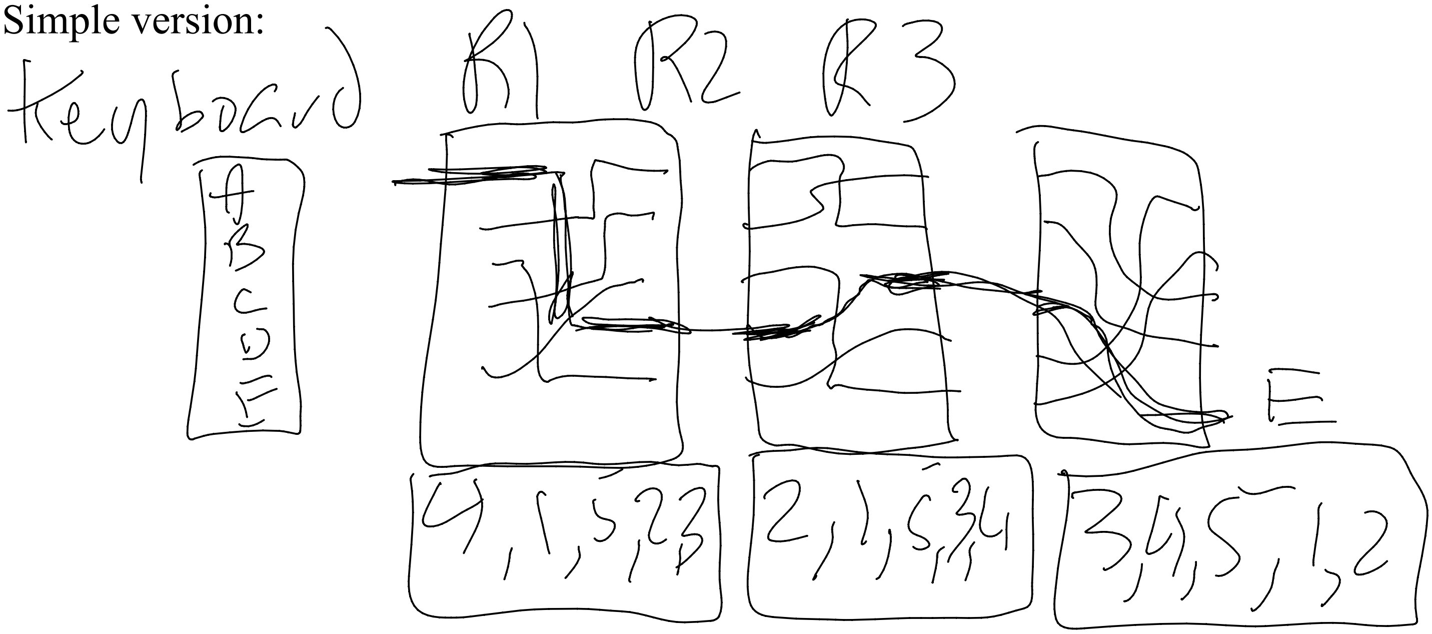
Enigma

Friday, September 18, 2020 11:32 AM

Before Computers.
But it was a machine that looked like a typewriter.

Around 1920 or so, Germans were looking for a machine to do encryption. They decided to use something created by a civilian, Arthur Scherbius (1918 founded their company)

Simple version:



If we just kept the rotors where they are, this is exactly a random substitution cipher!!!

AFTER ONE LETTER IS ENCRYPTED, ROTOR 3 ROTATES BY ONE SLOT. (EXACTLY LIKE THE ODOMETER ON A CAR.)

As an example, the permutation 2,1,5,3,4 represents this function:

1-->2
2-->1
3-->5
4-->3
5-->4

Rotate everything by one spot and we get:

1-->5
2-->3
3-->2
4-->1
5-->4

So this is a different mapping.

So each time we rotate a rotor, the substitution performed is different!!!

We rotate R3 26 times before it gets back to it's original position, and when this occurs, we rotate R2 once, much like on an odometer wen we get to 009, the next setting is 010. Then, when R2 rotates 26 times, R1 will rotate once…like 099 going to 100.

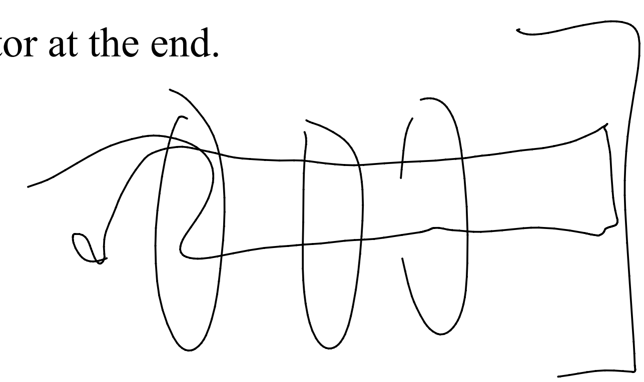
This means there are 26^3 = 17,576 different substitution keys that the machine can do!!!

This is extraordinary!!!
In Vigenere we use about 10 different shift ciphers, for say 10 bins of letters. (of course not always 10 just whatever the keyword length is)

Here, we create 17,576 bins, and for each bin, instead of just doing a shift, we do an arbitrary substitution!!!

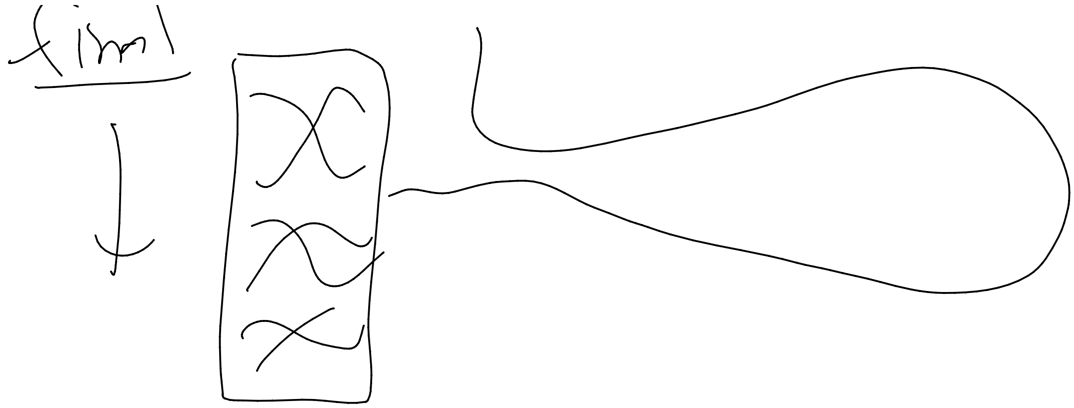
In addition to this craziness, Enigma had the following:

1) Reflector at the end.



2) Plug board, where at the very end, some pairs of letters were swapped.

Final



3) The rotors could be pulled out of the machine and reordered, so we could have the rotors in the orders (R1, R2, R3),(R1, R3, R2), (R2, R1, R3), (R2, R3, R1), (R3, R1, R2) or (R3,R2, R1), so this multiplies the # of substitution ciphers used by 6.

Without the plug board, we have 6 x 17576 = 105456 different settings on the machine.

So many different bins that most messages won't even put two letters in a single bin!!!

How the German's used this machine

Each day there was a day code. A sheet paper had the day codes for each day of the year. A day code would be three letters long and contain a rotor order, specifying the order of the rotors and their initial position when sending a message for the day.

Day Code: RYT 3, 1, 2 (Put rotor 3 in first, rotor 1 in second, rotor 2 in third), then shift rotor 3 to position R, shift rotor 1 to position Y, and shift rotor 2 to position T. (Set for the full day.)

For each message, there was a message code. This is just three letters, no change in the rotor settings. The operator was allowed to choose a random 3 letter message code. So, say they chose "MQZ"

So, the first six letter of the plaintext would be MQZMQZ, and this would be encrypted using the day code setting. (Message code repeated twice.)

M will be encrypted with the setting RYT 312
Q will be encrypted with the setting RYU 312
Z will be encrypted with the setting RYV 312
M will be encrypted with the setting RYW 312
Q will be encrypted with the setting RYX 312
Z will be encrypted with the setting RYY 312

After that, the operator will CHANGE the rotor settings to MQZ.

Let's say the beginning of the message was "HOWARE"

H will be encrypted with the setting MQZ 312
O will be encrypted with the setting MRA 312
W will be encrypted with the setting MRB 312
A will be encrypted with the setting MRC 312
R will be encrypted with the setting MRD 312
E will be encrypted with the setting MRE 312

In terms of frequency info, ONLY 6 letters were encrypted with the day code each message, and then for the rest of the message, each letter is encrypted by a set of substitutions that are in a different part of the setting of the machine.

Germans enjoyed no one reading their messages in the 1920s.
The French were suspicious of the Germans and wanted to see what they were up to.
In 1929, the French set up a secret agent to try to find out how Enigma worked. He had some gov't money…he could bribe someone…

Hans Thilo Schmidt (a little disgruntled, probably didn't make a ton of money), secret agent offered him 10,000 francs (lots of money) if Hans would temporarily steal a copy of the Enigma blueprint from his office and allow the secret agent to take pictures of it.

French had a peacetime information sharing pact with the Polish. Polish acquired the blueprints for Enigma.

Polish were also suspicious of the Germans…with good reason…

So, they tried to break Enigma, and gave more effort than the French.

Marian Rejewski…a very good mathematician…noticed some patterns about Enigma.

A letter could never encrypt to itself (because of how the reflector worked).

More importantly, he realized some really interesting patterns about the encryption of the message code.

The reason the Germans sent it twice is just in case there was a transmission error. But, this is precisely what Rejewski exploited…

M-->R
Q-->T
Z-->A
M-->Q
Q-->B
Z-->M

M first encrypted as R, then M encrypted as Q
Q first encrypted as T then Q encrypted as B
Z first encrypted as A, then Z encrypted as M

M-->Q-->K-->Y-->M (a loop of size 4)
All 26 letters would be parts of different loops
So, for this ONE day code setting, for positions 1 and 4, we could put together this loop information

MQKY(M) -- 4
BJ(B) -- 2
etc.
4, 2, 10, 3, 7 (all the loop sizes)

For each different setting of the machine, the loop sizes were different.

So, for over a year, Rejewski, went through all 105,000+ settings of the machine, encrypting stuff over and over again, to get all of these looping lengths.

Then, he made a huge book with a two way look up table, loop sizes to rotor setting, rotor setting to loop sizes.

Then, to break Enigma, the Polish would intercept messages, and eventually catalog the loop sizes for that day. Then, their look up table would tell them what the day code was. Then, they could go back and read all of the messages, since they had a copy of the machine and knew exactly how to set it to read each message code for the day, and then set the machine to read the messages also.

Unfortunately, right around 1939 (if you look at history some important stuff happened then), the Germans added rotor 4 and rotor 5. Now, instead of 3 x 2 x 1 = 6 settings, the rotors could be placed in 5 x 4 x 3 = 60 ways. (It took Rejewski 1 year to catalog 6 settings, at the same pace, it would take him 9 more years to account for the new rotors. Which was too much time to be useful…)

By 1940, the Polish shared their work on Enigma with the British and the Allied forces. British were stunned at the amazing work the Polish did!!!

The British, with the knowledge of what Rejewski did, aimed to mechanize the process of making these large look up tables. Turing helped design the machines that sped up the time to create the necessary look up tables.

Some other things the British exploited
----

1. Germans always sent a weather report in the morning at the exact same time and in that particular message, the plaintext "wetter" (German for weather) appeared in the exact same spot. (With known plaintext in some locations, decryption was much easier.)
2. Some operators would always use the same exact message codes and when messages were sent, some of the Allied forces could tell which operator sent it because they had a unique "fist" (pulsing of the signals was distinct for some operators)
3. The fact that a letter can't encrypt to itself was also helpful.

Without the plug board, the # of different settings of the machine is 26^3 times the number of rotor settings (which rotor goes in which location).

If you were to count the plug board…

(26 choose 2) (24 choose 2) (22 choose 2)…(8 choose 2)/10!

n choose 2 = n*(n-1)/2

We did this in python and it's a really big number:

150738274937250

But linguists could handle figuring out which letters were swapped at the end…