Fall 2006
Chris Christensen
MAT/CSC 483

Machine Ciphers

Polyalphabetic ciphers are good ways to destroy the usefulness of frequency analysis. Implementation can be a problem, however. The key to a polyalphabetic cipher specifies the order of the ciphers that will be used during encryption. Ideally there would be as many ciphers as there are letters in the plaintext message and the ordering of the ciphers would be random – an one-time pad. More commonly, some rotation among a small number of ciphers is prescribed. But, rotating among a small number of ciphers leads to a period, which a cryptanalyst can exploit. Rotating among a "large" number of ciphers might work, but that is hard to do by hand – there is a high probability of encryption errors. Maybe, a machine.

During World War II, all the Allied and Axis countries used machine ciphers. The United States had SIGABA, Britain had TypeX, Japan had "Purple," and Germany (and Italy) had Enigma.

SIGABA
http://en.wikipedia.org/wiki/SIGABA

A TypeX machine at Bletchley Park.

From the 1920s until the 1970s, cryptology was dominated by machine ciphers.

What the machine ciphers typically did was provide a mechanical way to rotate among a large number of ciphers. The rotation was not random, but the large number of ciphers that were available could prevent depth from occurring within messages and (if the machines were used properly) among messages.

We will examine Enigma, which was broken by Polish mathematicians in the 1930s and by the British during World War II. The Japanese Purple machine, which was used to transmit diplomatic messages, was broken by William Friedman's cryptanalysts. It appears that SIGABA and TypeX were never broken.

Enigma

Although Enigma was only one of a family of machine ciphers, it has attracted the most interest because of the exciting stories of the "duels" between the machine and, first, the Polish and, then, the British codebreakers. The story of Enigma began to become visible in 1974 with the publication of *The Ultra Secret* by F. W. Winterbotham. Since that time much has been written about Enigma and the duel. Because of the secret nature of military cryptography and cryptanalysis, the story of Enigma is often muddled and contradictory, but there is a clear trail from Arthur Scherbius' 1918 patent of a machine designed to protect commercial communications to the German military Enigma of World War II.

A commercial Enigma on display at the NSA's National Cryptological Musuem. Notice that this machine does not have a plugboard.

If you have no good coding system, you are always running a considerable risk. Transmitted by cable or without wire, your correspondence will always be exposed to every spy, your letters, to being opened and copied, your intended or settled contracts, your offers and important news to every inquisitive eye. Considering this state of things, it is almost inconceivable that persons interested in those circumstances should delay securing themselves better against such things. Yet, ciphering and deciphering has been a troublesome art hitherto. … Now, we can offer you our machine "Enigma", being a universal remedy for all those inconveniences.

Mid-1920s Enigma sales brochure reprinted in July 2001 *Cryptologia*

Here is how Enigma works. The Enigma machine consists of four visible components: a keyboard, a plugboard, a rotor system, and a lampboard.

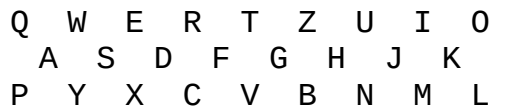
A 3-rotor Enigma machine. The plugboard is at the bottom of the picture. The keyboard is above the plugboard. The lampboard is above the keyboard. The three rotors are under the windows at the top of the picture. Display at the British Intelligence Museum Chicksands.

The same Enigma machine with the top open revealing the three rotors and the lamps.
Display at the British Intelligence Museum Chicksands.

Enigma has both electronic and mechanical parts. The executive summary of its operation is that the operator pushes a plaintext letter on the keyboard and the corresponding ciphertext letter is lighted on the lampboard.

Forget for a moment about the mechanical part of Enigma and follow the electrical action from the keyboard to the lampboard.

First, notice that the arrangement of the keys on the keyboard is slightly different than on a keyboard today.



Enigma keyboard

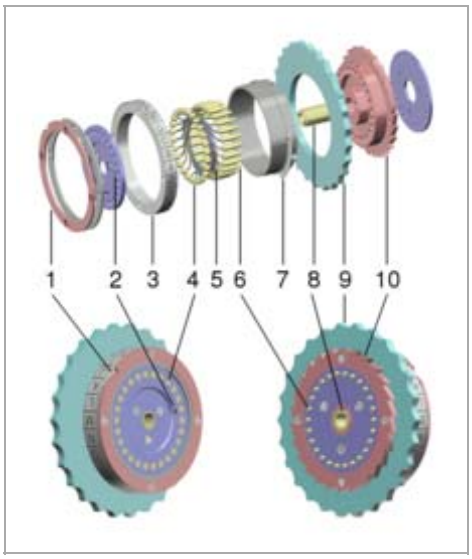
When the operator pushes a key on the keyboard (O is the key in the diagram), an electrical current passes from the key to the plugboard. The plugboard looks like an old telephone switchboard. There are 26 sockets – one for each letter of the keyboard.

Throughout the war, the Enigma machine evolved and the methods for using it changed. Different branches of the German military used it differently at the same time. So, a description of how Enigma operated is dependent on who was using it and when they were using it. This description applies to the Enigma that the Polish mathematicians were attacking in 1932.

When the Polish mathematicians began their attack on Enigma, six plugs were in use. Each plug would connect (in a way prescribed by the key) one letter on the plugboard to another. The effect of the plugboard was to swap 6 pairs of letters and let the remaining 20 letters pass through unchanged. The plugboard permutation consisted of 6 transpositions; 20 letters were fixed by the plugboard permutation. Latter in the war, more plugs (often 10) were used. In the diagram, the plugboard permutation includes the transposition (ON); so, O is replaced by N by the plugboard. (Not all versions of Enigma had a plugboard.)

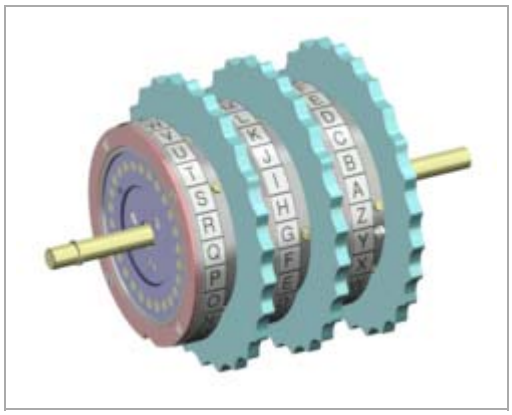
After passing through the plugboard, the electrical charge passed into the rotor system.

Exploded view of an Enigma rotor



1. notched ring
2. marking dot for "A" contact
3. alphabet tyre
4. plate contacts
5. wire connections
6. pin contacts
7. spring-loaded ring adjusting lever
8. hub
9. finger wheel
10. ratchet wheel

Three rotors in sequence



http://en.wikipedia.org/wiki/Enigma_machine

In 1932, the rotor system consisted of three rotors and a reflector. Each rotor permuted the letters of the alphabet. The right-hand side of each rotor had 26 spring-loaded input terminals arranged around the disk; the left-hand side had 26 flat circular output terminals. Each input was internally wired to an output. The wiring determined the permutation. At the time that the Polish mathematicians began attacking Enigma, the machine had only 3 rotors; later the machine had as many as 8 rotors from which either 3 or 4 were installed depending on the type of Enigma in use.

The rotors were numbered using Roman numerals; these numbers do not correspond to the positions of the rotors in the machine. The permutations accomplished by the 3 rotors are:

Rotor I	(aeltphqxru)(bknw)(cmoy)(dfg)(iv)(jz)(s)
Cycles	10 4 4 3 2 2 1

Rotor II	(a)(bj)(cdklhup)(esz)(fixvyomw)(gr)(nt)(q)
Cycles	8 7 3 2 2 2 1 1

Rotor III	(abdhpejt)(cflvmzoyqirwukzsg)(n)
Cycles	17 8 1

Following the diagram, the electrical charge enters the rotor system as N. N enters the right-hand rotor and exits as Z, Z enters the middle rotor and exits as X, X enters the left-hand rotor and exits as B, and then B enters the reflector at the left of the rotor system.

The reflector was “half a rotor.” There were 26 contacts on the right-hand side of the reflector. Internally, the 26 contacts were joined in pairs by wires to create a permutation consisting of 13 disjoint transpositions. At the time that we are considering, Enigma had just one reflector (reflector A). It creates the following permutation:

Reflector A (ai)(bm)(ce)(dt)(fg)(hr)(jy)(ks)(lq)(nz)(ox)(pw)(uv)

In the diagram, B enters the reflector and exits as F.

Then the electrical charge passes backwards through the rotor system. F enters the left-hand rotor, passes backwards through it, and exits as E. E enters the middle rotor, passes backwards through it, and exits as B. B enters the right-hand rotor, passes backwards through it, and exits as Y.

Y then passes through the plugboard where it is changed to Q, and lamp Q lights. The operator would substitute ciphertext Q for plaintext O.

This is an unduly complicated way to do a single permutation, but the point of the process is that the mechanical portion of Enigma allows for the generation of a long sequence of different permutations. Each time that a letter on the keyboard is pressed, before enciphering begins, the right-hand rotors turns one letter forward. The output side of the right-hand rotor has a notch that causes the middle rotor to turn forward. Like the odometer of a car, the middle rotor will turn forward one letter once during every 26 turns of the right-hand rotor. Similarly, there is a notch on the output side of the middle rotor that causes the left-hand rotor to turn forward one letter once during every 26 turns of the middle rotor. The theoretical maximum of $26^3 = 17576$ permutations is not actually achieved by Enigma because the mechanical movement of the rotors is such that the middle rotor can "double step" – it can rotate forward on two subsequent presses on the keyboard. So, $26 \times 25 \times 26 = 16900$ keys can be pressed on the keyboard before the rotor system returns to the initial permutation. For a given setup of Enigma, 16900 permutations are generated in an order; 16900 substitution ciphers are generated in order.

Setting up Enigma

Two Enigma operators could communicate only if their Enigma machines were set up using the same key. Commonly Enigma keys were changed daily, but there are instances of more frequent changes. Keys were provided to the operators in a book, for example, for a month at a time. There were several settings which made up the Enigma key. In 1932, the following made up the key.

Plugboard: The key specified which 6 pairs of letters were to be connected on the plugboard. For example, CO DI FR HU JW LS.

Rotor order: The key specified the order in which the rotors were placed in the rotor system (from left to right). For example, I III II.

Ring setting: There was a ring around the circumference of each rotor on which the letters of alphabet A, B, …, Z or the numbers 01, 02, … 26 were engraved. This ring could be rotated around the circumference and then held in place with a pin. The ring setting of the key indicated the letter of the alphabet on the ring that corresponded to the position of the pin. For example, P K M. One effect of the ring setting was to set the letters on the ring with respect to the internal wiring of the rotor. The permutations that were given earlier for each rotor assume that the ring setting for each is A. Another effect was to position the turnover notch. The notch was in a fixed position on the left side of each rotor. Changing the ring setting changed the position of the turnover with respect to the internal wiring of the rotors.

Groundsetting: This portion of the key specified the position of each rotor at the beginning of sending or receiving a transmission. The groundsetting indicated which letter on each ring should be visible in the windows above the 3 rotors. For example, A L V.

These settings made up the key.

The Number of Enigma Keys

[If] a man were able to adjust, day and night, a new key at every minute, it would take him 4000 years to try all those possibilities through on after another.
Mid-1920s Enigma sales brochure reprinted in July 2001 *Cryptologia*

The security of Enigma depends on its having a large key space. The size of the keyspace equals the number of possible plugboard settings × the number of possible rotor orders × the number of possible ring settings × the number of possible ground settings.

The number of possible plugboard settings: Assume that *n* plugs are being used. There are

$$\frac{[26\times 25]\times[24\times 23]\times[22\times 21]\times\ldots\times[(26-2n+2)\times(26-2n+1)]}{2^n\times n!}$$

ways to connect *n* plugs into the plugboard. Here is a table which shows the number of connections for each of the possible number of plugs.

Number of cables n	Number of connections	Number of cables n	Number of connections
0	1	7	1,305,093,289,500
1	325	8	10,767,019,638,375
2	44,850	9	53,835,098,191,875
3	3,453,450	10	150,738,274,937,250
4	164,038,875	11	205,552,193,096,250
5	5,019,589,575	12	102,776,096,548,125
6	100,391,791,500	13	7,905,853,580,625

When the Poles began to attack Enigma, 6 plugs were in use. So, there were 100,391,791,500 ways to connect the 6 plugs into the plugboard. Later the Germans used 10 plugs.

The number of possible rotor orders: There are 6 ways to arrange the 3 rotors in order in the rotor system.

The number of possible ring settings: Only the positions of the notches on the right-hand and middle rotors contributed to the cryptographic security of Enigma. So, we will say that there are $26^2 = 676$ possible ring settings.

The number of possible groundsettings: There are $26^3 = 17576$ choices of the letters to appear in the windows.

So, effectively, the number of possible keys was

$$100{,}391{,}791{,}500 \times 6 \times 676 \times 17576 = 7{,}156{,}755{,}732{,}750{,}624{,}000$$

which would seem to be secure enough.

Every Enigma permutation is self-reciprocal – if `a` enciphers to `T`, then `t` enciphers to `A`. This enables to both encipher and decipher without adjustment to the machine.

But, being self-reciprocal can also be a weakness because no Enigma permutation enciphers a letter as itself. The latter was useful information for British cryptanalysts. The cryptanalysts who attacked Enigma would know, for example, that ciphertext `T` did not correspond to plaintext `t`. The same rule usually applies to cryptograms that appear in newspapers (so-called "aristocrats") – no letter ever substitutes for itself. With such a rule, we would know, for example, that the trigraph `JFE` could not represent plaintext `the`.

Mathematicians to the Rescue

Prior to the outbreak of World War II [Poland was attacked by Germany on September 1, 1939], fearing invasion, Poland was intercepting German radio transmissions, but the Poles were stumped by the encryption.

> In the years that followed the First World War, the British cryptanalysts in Room 40 continued to monitor German communications. In 1926 they began to intercept messages which baffled them completely. Enigma had arrived, and as the number of Enigma machines increased, Room 40's ability to gather intelligence diminished rapidly. The Americans and the French also tried to tackle the Enigma cipher, but their attempts were equally dismal, and they soon gave up hope of breaking it. …
>
> … in the wake of the First World War the allies no longer feared anybody. Germany had been crippled by defeat, the Allies were in a dominant position, and as a result they seemed to lose their cryptanalytic zeal. Allied cryptanalysts dwindled in number and deteriorated in quality.
>
> One nation, however, could not afford to relax. After the First World War, Poland re-established itself as an independent state, but it was concerned about threats to its new-found sovereignty. To the east lay Russia, a nation ambitious to spread its communism, and to the west lay Germany, desperate to regain territory ceded to Poland after the war. Sandwiched between these two enemies, the Poles were desperate for intelligence information, and they formed a new cipher bureau, the Biuro Szyfrów [BURE-oh SHIF-roof]. … [Their monitoring of German communications was] effective until 1926, when they too encountered the Enigma messages.
>
> At first sight [Enigma] seemed to be impregnable, but the Polish cryptanalysts were undaunted. They were prepared to explore every avenue in order to find a weakness in the Enigma machine … . Foremost in the battle against Enigma was a new breed of cryptanalyst. For centuries, it had been assumed that the best cryptanalysts were experts in the structure of language, but the arrival of Enigma prompted the Poles to alter their recruiting policy. Enigma was a mechanical cipher, and the Biuro Szyfrów reasoned that a more scientific mind might stand a better chance of breaking it. The Biuro organized a course on cryptography and invited twenty mathematicians, each of them sworn to an oath of secrecy. The mathematicians were all from the university at Poznán. Although not the most respected academic institution in Poland, it had the advantage of being located in the west of the country, in territory that had been part of Germany until 1918. These mathematicians were therefore fluent in German.
>
> Three of the twenty demonstrated an aptitude for solving ciphers, and were recruited into the Biuro. The most gifted was Marian Rejewski … .

> [Rejewski had a mathematical breakthrough that enabled the Poles to read German communications.] Poland was not at war with Germany, but there was a threat of invasion, and Polish relief at conquering Enigma was nevertheless immense. …
>
> The Polish success in breaking the Enigma cipher can be attributed to three factors: fear, mathematics, and espionage. Without the fear of invasion, the Poles [like the British, the French, and the Americans] would have been discouraged by the apparent invulnerability of the Enigma cipher. Without mathematics, Rejewski would not have been able to analyze [the cipher]. And without [Hans-Thilo] Schmidt, [a German who became a French informant], code-named 'Asche', and his documents, the wiring of the scramblers would not have been known and, cryptanalysis could not even have begun. …
>
> The Poles successfully used Rejewski's technique for several years.
>
> …
>
> In 1938 Polish interceptions and decipherments had been at their peak, but by the beginning of 1939 the new scramblers and extra plugboard cables stemmed the flow of intelligence. …
>
> The new invulnerability of Enigma was a devastating blow to Poland, …, it was at the heart of Hitler's blitzkrieg strategy. (Singh, Simon, *The Code Book: The evolution of secrecy from Mary Queen of Scots to quantum cryptography*, Doubleday, 1999.)

Seeing the likelihood of invasion by Germany, the Poles provided Britain and France with the results of their work on the Enigma machine. The Poles proved to the British and French that the Enigma machine was breakable, and the Poles also demonstrated the value of using mathematicians as cryptanalysts. British cryptanalytic efforts had concentrated on using linguists as codebreakers; now they began to employ mathematicians and scientists.

Bletchley Park

The train station at Bletchley.

British cryptanalytic efforts were located at Bletchley Park, a Victorian country estate at a railway stop 50 miles northwest of London (and the midpoint on the train route between Oxford and Cambridge).

In September 1939, it became the location of the Government Code and Cipher School (GC&CS).

The Bletchley Park Mansion.

GC&CS grew out of the First World War Admiralty's Room 40 that had broken a number of German codes. During the 1920s and 1930s, GC&CS recruited heavily from the universities (mainly Cambridge and Oxford) and formed useful contacts with mathematicians and linguists.

The Admiralty in London.

The work at Bletchley Park began with about 30 people – “old-time professionals” from the First World War Admiralty and new recruits from chess masters, mathematicians, professors, and linguists, most from Cambridge University.

The entrance to Bletchley Park.

Naval Commander Alastair Denniston was the director of Bletchley Park.

Two of the leading mathematicians were Alan Turing and Gordon Welchman. Another familiar name is Ian Fleming.

Much of the early work was done in temporary huts and the designations stuck throughout the war even though the locations of the sections changed.

Hut 3: German Army and Air Force intelligence; German scholars who translated the messages and decided what the messages meant.

Hut 6: German Army and Air Force cryptanalytical section; mathematicians who broke the codes. Gordon Welchman worked in Hut 6. He the author of *The Hut Six Story*.

Hut 4: German Navy intelligence. The mansion is on the right.

Hut 6 (on the left), Hut 1 (on the right; the BP wireless station), and (in the background) Hut 8 -- German Navy Enigma cryptanalysts.

Hut 8 -- German Navy Enigma cryptanalysts. This is where Alan Turing worked.

Hut 4 – German Navy intelligence.

By the end of the War, over 7000 people were working at Bletchley Park

See: Hinsley, F.H., and Stripp, Alan (eds), *Codebreakers: The inside story of Bletchley Park*, Oxford, 1993.