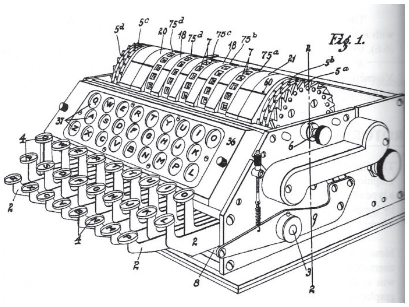
Rotor Machines and Enigma



Eduard Hebern's *Electric Code Machine* (U.S. Patent 1673072)

Contents:

1. The Introduction of Rotor Machines.
2. Arthur Scherbius and the Enigma Machine.
3. The Principles of Enigma.
4. Interwar Poland, and the Biuro Szyfrów.
5. Marian Rejewski, and Breaking Enigma.
6. Alan Turing, and the British Effort.

1. The Introduction of Rotor Machines.

Doing encryption by hand is obviously error-prone.

Cryptographers have always invented various mechanical devices to both speed up the encryption process, and also help make it more reliable.

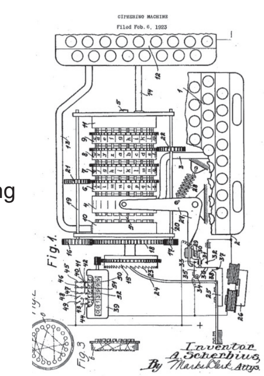
For a monoalphabetic substitution cypher:
— aligning plain/cypher letter pairs on a ruler, at least stops you forgetting;
— putting plain/cypher letter pairs on two concentric rings, able to rotate with respect to each other, not only stops you forgetting, but also gives you 26 different monoalphabetic substitution cyphers, by altering the orientation of the disks.

Cypher disks were invented by Leon Battista Alberti (1430's). But the small number of monoalphabetic cyphers available made analysis easy enough as time progressed.

Rotor machines combined several disks into a single device which had a much larger number of monoalphabetic cyphers, enough to defeat statistical analysis in principle.

Eduard Hebern invented the first, and many similar ones soon followed.

2. Arthur Scherbius and the Enigma Machine.



Arthur Scherbius invented his Enigma machine in 1918.

It was the first of a number of models, which gradually improved over the next few years.

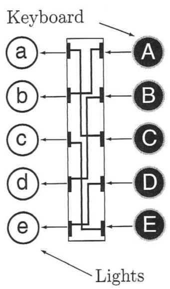
U.S. Patent 01657411 was granted for Enigma in 1928.

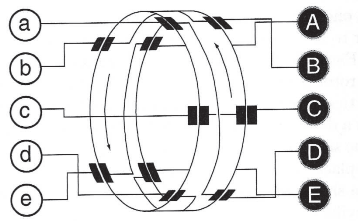
His big breakthrough was due to the mortification felt by the German High Command after WWI, caused by finding out that the Allies had routinely broken German cyphers all through WWI. They decided to buy the best devices for encryption that they could. Scherbius was the right man at the right time, since Enigma was German made.

Enigma went into mass production. Eventually about 30,000 Enigma machines were bought by the German military. Scherbius got rich from Enigma. But he died in 1929, and did not live to realise that Enigma would be broken in WWII, just like the German cyphers had been in WWI.

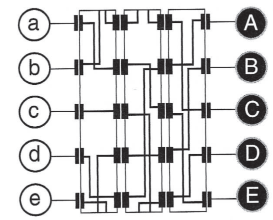
3.The Principles of Enigma.

Enigma was a rotor machine. In a rotor machine, each rotor implements a mono-alphabetic substitution cypher, rather like the cypher disks of Leon Battista Alberti.





Of course a single disk is very little use.
You need several.



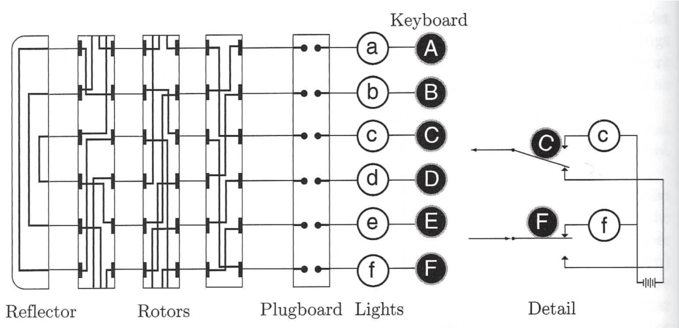
The output of one disk is fed into the input of the next. By itself, this does not help, since several fixed disks compose to give just a single permutation — *but if after each letter the disks move relative to one another*, then a huge range of different substitutions are generated — too many to analyse by the usual statistical techniques.

Enigma worked in *odometer* mode. After a full turn of the fast disk, the medium disk turned one step. After a full turn of the medium disk, the slow disk turned one step.

Because of the huge range of permutations, you have to be able to use the same machine backwards for decryption.

Enigma had two additional features: the first, the plugboard, increased even further the huge number of permutations; the second, the reflector, enabled decryption to be done by the same process as encryption — these latter two features proved to be the Achilles Heel of Enigma.

Enigma Schematic



The plugboard enabled arbitrary sets of pairs of letters to be swapped.

The reflector meant that if pressing C caused F to light up, then pressing F caused C to light up — encryption and decryption were the same process — very convenient in the stress of battle.

Original Enigma Rotor and Reflector Settings

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

B	AY	BR	CU	DH	EQ	FS	GL	IP	JX	KN	MO	TZ	VW
C	AF	BV	CP	DJ	EI	GO	HY	KR	LZ	MX	NW	TQ	SU
B thin	AE	BN	CK	DQ	FU	GY	HW	IJ	LO	MP	RX	SZ	TV
C thin	AR	BD	CO	EJ	FN	GT	HK	IV	LM	PW	QZ	SX	UY

Enigma Operation

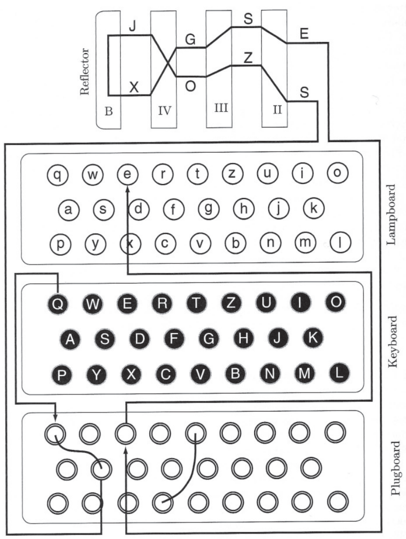
1. Select number of plugboad cables.
2. Set plugboad cables.
3. Select rotors to be used.
4. Select rotor slots.
5. Select rotor initial settings.
6. Select reflector.

Items 1-6 constitute the Enigma key.

Encode the message by pressing keys on the keyboard and observing the lamps that light up.

Decode the cyphertext by pressing keys on the keyboard and observing the lamps that light up.

After each key press, one or more disks would rotate, changing the substitution being used.



The Enigma Keyspace

Three fixed rotors implies $26^3 = 17{,}576$ rotor positions, so that many permutations.

Testing 1 trial key per minute, working $24/7$, you need $17{,}576 / (24 \times 60) = 12.2$ days to try all keys. Not very secure. Build 12 replica machines and you only need one day.

More rotors increases security by 26 per rotor. Not enough really.

With N exchangeable rotors you increase security by $\binom{N}{3} \times 3!$ If $N = 8$ you get 336.

The plugboard increases this dramatically. First cable can be set in $\binom{26}{2}$ ways, the second in $\binom{24}{2}/2!$ ways, etc. At first there were 6 cables, later 10. This helps a lot.

Finally, there are 4 reflectors to choose from.

It all looks pretty impressive.

4. Interwar Poland, and the Biuro Szyfrów.

After WWI, Britain and France were complacent. They had won. They were in charge. Like all nations at the top of the heap, they got into the mindset that they didn't have to try too hard. They knew all about the German Enigma and the vicious complexity of its keyspace. On the face of it, it looked impossible to analyse. They didn't even bother trying.

Poland was in a completely different situation. Since 1795 it had completely ceased to exist as an independent nation, having been dismembered in a succession of three *Partitions* by the Prussians (i.e. Germans), Russians, and Austrians. The Prussians and Russians were brutal occupiers, suppressing Polish language and culture. Polish patriotic feelings burned fiercely during the next 120 years, and helped to fuel the widespread nationalistic tendencies that came to the fore after WWI.

At the end of WWI, these nationalistic tendencies brought about the creation of many new nations in Europe. Poland was recreated, this being helped by the defeat of Germany and Austria and the chaos in Russia following the Bolshevik revolution.

Polish territory before WWI

Poland after WWI.

It wasn't as easy as just bringing WWI to an end.

Although the Versailles Peace Conference instituted the new Polish state, many more issues, such as its eastern borders, were left unresolved. In fact, in Poland, WWI was followed by more fighting: the Polish-Lithuanian War, the Polish-Ukrainian War and the Polish-Russian War. That the brand new nation came through all this was due in no small part to the leadership of the revered[1] Jósef Piłsudski. Things finally settled down in about 1922.

Moreover, the Germans greatly resented the loss of their eastern territories. The Poles constantly feared attack from the west (ultimately they were proved right of course). It was vital to know what the Germans were up to. For the Poles then, complacency about Enigma was not an option.

1. 'Revered' is no exageration. Pilsudski lived in the Belweder district of Warszawa (Warsaw), a few streets away from the seats of government of the Polish state, from where he was closely involved in the running of the country, despite the vagaries of various political systems, for most of the interwar period. He made the journey every day on foot, accompanied by a single bodyguard. He could have been assassinated at any time. Yet, despite the political squabbling that afflicted the new nation, and the fashion for political violence in Europe at that time, there was never a single attempt on his life.
Nowadays, if you visit Kraków (Cracow), you can go to the Zamek Wawelski (Wawel Castle), and descend into the cathedral crypt, where most of Poland's kings and queens lie buried. You pass by a series of increasingly elaborate stone and marble tombs, in line with the increasingly sophisticated burial technology employed by European royalty through the centuries. Just before you exit, you see a chamber on your right. It is bare aside from a plain riveted copper coffin resting on a simple wooden trestle. It is the last resting place of Jósef Pilsudski. A lone veteran keeps vigil. It is very moving.

The Biuro Szyfrów (Bureau of Cyphers) had been established, and had been breaking pre-Enigma traffic successfully. Then came Enigma. It was a different kettle of fish.

In 1931, a dissatisfied German employee, Hans-Thilo Schmidt, sold Enigma design documents to the French. Since (see above) the French were complacent, they did not try to break the design — it looked too difficult. Because of a military co-operation agreement with Poland (and because the French believed the information useless), the Enigma documentation reached the Poles — who were not complacent.

In charge of decyphering German messages at the Biuro Szyfrów was Maksymilian Ciężki (literal translation: Max the Heavy). He knew that Enigma required a different combination of skills than hitherto, and recruited several mathematicians from the University of Poznań to try to attack Enigma.

The most outstanding proved to be Marian Rejewski. After much effort, he eventually found the way to break Enigma, relying on the specific way the Germans used it.


Marian Rejewski

5. Marian Rejewski, and Breaking Enigma.

The Germans used hardcopy books of day keys which said what the settings for each day were, one month's worth of keys per book. (Major Gwido Langer, the boss of the Biuro, regularly got these from Schmidt, but left Rejewski to sweat it out, reasoning that one day the supply was bound to dry up, as of course it did.)

Using the day code, the Germans would decide on a message key (a different set of rotor settings for each message), and then put the message key twice at the beginning of the message — twice, to ensure that radio interference did not introduce errors. Once the message key had been sent (using the day key), the rotors were reset to the message key, and the rest of the message was sent.

Rejewski's breakthrough was to realise how the double encypherment of the message key could be used to decouple the effects of the rotors from those of the plugboard. Since there were only three rotors originally, the total number of settings was 105,456. Not small, but not hopeless for exhaustive search.

The main idea was to look for cycles arising from the 1st and 4th, 2nd and 5th, 3rd and 6th letters of the cyphertext.

Suppose four messages start with **FWIKMS , KWPANB , IUQSDJ , WDLMYF** .

Then **F/K** both encypher the first letter of the key, similarly **K/A** , **I/S** , **W/M** etc.

A series of links builds up.

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
					K			S		A												M			

As messages come in, the table of 1st and 4th links gets filled (similarly for the tables of 2nd and 5th, and the 3rd and 6th links).

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

With a full table, we can analyse the loop structure.

(3) $\mathbf{A} \to \mathbf{F} \to \mathbf{K}$
(7) $\mathbf{B} \to \mathbf{T} \to \mathbf{E} \to \mathbf{Q} \to \mathbf{N} \to \mathbf{J} \to \mathbf{X}$
(9) $\mathbf{C} \to \mathbf{W} \to \mathbf{M} \to \mathbf{L} \to \mathbf{P} \to \mathbf{G} \to \mathbf{I} \to \mathbf{S} \to \mathbf{Y}$
(5) $\mathbf{D} \to \mathbf{Z} \to \mathbf{H} \to \mathbf{O} \to \mathbf{V}$
(2) $\mathbf{R} \to \mathbf{U}$

The number of cycles and their lengths is independent of the plugboard.

Why ?

In a cycle, when you encypher a letter, you exit via a given swap (of the plugboard), and immediately encypher the next letter using the same swap again. The same swap twice is equivalent to *no swap at all* ... *so it doesn't matter what the swap was*.

So each rotor setting would be characterised by a particular loop structure, eg.:

Letters 1 and 4: 5 loops, lengths 3, 7, 9, 5, 2.
Letters 2 and 5: 4 loops, lengths 9, 2, 5, 10.
Letters 3 and 6: 5 loops, lengths 4, 7, 6, 2, 7.

The Biuro built a dictionary that matched rotor settings and loop structures.

Every day they would collect messages till the tables filled up, consult the dictionary, and extract the rotor settings.

They still had the plugboard to contend with. But that was a lot easier, with the rotor manipulations removed from the cyphertext. Now, the real plaintext differed from the candidate plaintext just by letter swaps (no more than six swaps initially). These could often be guessed from a knowledge of the German language.

Mock example. Suppose the candidate plaintext came out as:

`tregges nie mich morges gruch im ubliches platz heisrich`

Knowing the German language ...

`heisrich` was probably supposed to be **`Heinrich`**, so **`s/n`** was a likely plugboard setting.

This gives **`treggen`** from **`tregges`**, and **`treggen`** was probably supposed to be **`treffen`** (meet), so **`f/g`** was a likely plugboard setting. Soon you get to

`treffen sie mich morgen fruch im ublichen platz heinrich`

i.e. “meet me at the usual place Heinrich”.

The Germans improved security by changing their procedures. The dictionary became useless.

Rejewski fought back by designing an Enigma-like machine that could mechanically deduce the day key by examining all the possibilities. It was termed a “bombe” (maybe because it ticked as it went along trying various settings, or maybe because Rejewski was sitting eating a bombe (a hemispherical shaped kind of ice cream) when he had the idea). Six were used in parallel to deduce the day key in a couple of hours.

This worked well for a while.

The Germans improved security by going from three rotors to five. Rejewski and the Biuro realised they would need ten times as many bombes to do the job. This was utterly beyond the financial resources of the Biuro.

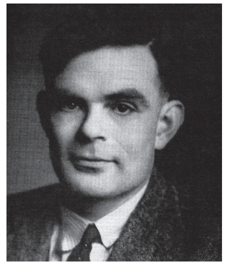
Poland now knew that war was unavoidable. In order not to lose what was known, the Poles decided to tell the other Allies. Two weeks before the war started, a meeting was held in Warszawa to which the British and French cypher experts were invited. Open mouthed (since both the British and the French believed Enigma to be impregnable), they viewed the work of the Biuro. The equipment was handed over and was secretly shipped over the Channel. A few weeks later, following attacks by the Germans from the west and the Russians from the east, Poland once more ceased to exist.

6. Alan Turing, and the British Effort.

Somewhat startled, the Brits got to work. Encryption and decryption was the job of “Room 40”. With the onset of war, its activities were greatly expanded, and for reasons of safety and space, it was moved to Bletchley Park (near Milton Keynes).[1]

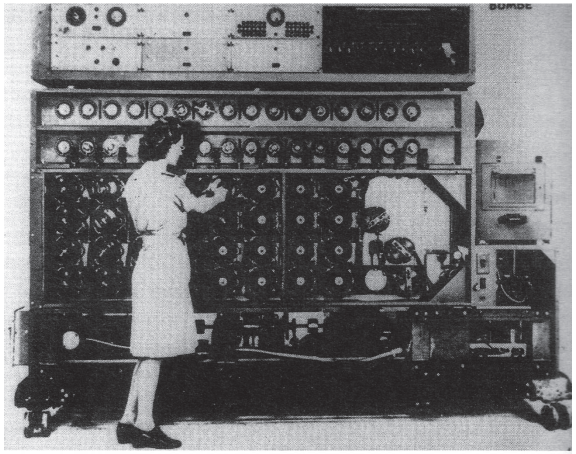
The Bletchley Park team grew from 200 to over 7000 during the war. It included crossword experts, linguists, mathematicians, logicians etc. One figure stood out as identifying Enigma's weaknesses, and thus contributed to defeating it, more than most: Alan Turing (who later came here, to the University of Manchester).

The Brits had the resources that the Poles lacked to build Enigma-cracking machines. Turing and his team designed the much bigger bombes needed to tackle the increasingly sophisticated German procedures.



Alan Turing

1. Nowadays, you can go and visit.



A Bletchley Park Bombe

Turing attacked the way that Enigma was being used in the field.

— operators often reused keys that had been used before,
— operators often used keys derived from family names etc.,
— operators often used keys that were simple patterns on the keyboard.

In addition:

— no rotor was allowed to be in the same position on consecutive days,
— plugboard cables were not allowed to connect adjacent keyboard letters,
— etc.

All of these cut down the number of possible keys, and/or, suggested “things to try first”. These were called cillies. It worked surprisingly often.

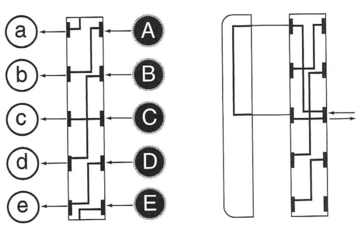
Turing and his colleagues were terrified by the fact that one day, the Germans were bound to stop repeating the message key twice at the beginning of the message. What then?

Turing noticed that many decrypted messages had a predictable structure:

— eg. there was a weather report each day at about 6.10 am.
— eg. many messages contained predictable words, often in similar places in the plaintext.

He developed the idea of *cribbing*, i.e. guessing that a certain word or phrase would occur, and then using that insight to break the cypher.

Fact. Because of the reflector, no letter could be encrypted to itself. This cuts down the possibilities significantly.



The “no self encryption” property is very useful.

Suppose you believe that the word

`fuehrerhauptquartier`

was in the plaintext (i.e. **`fuehrerhauptquartier`** is your crib). Then the cyphertext substring corresponding to this could not:

— have **`F`** as its 1st letter,
— have **`U`** as its 2nd, 10th, 14th letter,
— have **`E`** as its 3rd, 6th, 19th letter,
— etc.

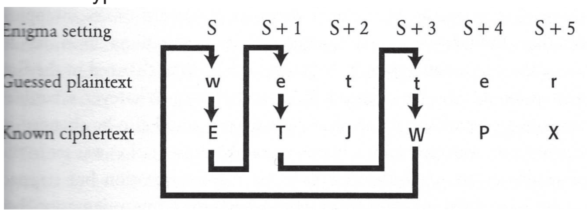
Only cyphertext substrings that *satisfied all these tests* could be encriptions of **`fuehrerhauptquartier`** . This excluded a huge number of possibilities.

The plaintext was slid along the cyphertext, place by place. Any time there was a match of a letter anywhere along the plaintext/cyphertext pair, you could discard that pairing as invalid. This was part of the Achilles Heel of Enigma at work.

Sometimes the Allies made certain millitary moves specifically to provoke messages with a given word in the plaintext.

Using a Crib

Inspired by Rejewski, Turing looked to use cribs to eliminate the plugboard. He looked for loops in the crib/cyphertext.



Suppose there is a loop like this. Guess a rotor setting S. Your hypothesis is then:

S encrypts **w** to **E** ,
$\mathrm{S}+1$ (i.e. the odometer setting 1 step after S) encrypts **e** to **T** ,
$\mathrm{S}+3$ (i.e. the odometer setting 3 steps after S) encrypts **t** to **W** .

Connect three Enigmas in series, set to S, $\mathrm{S}+1$, $\mathrm{S}+3$.
Press **w** . If **W** comes up on the third, you're in business.

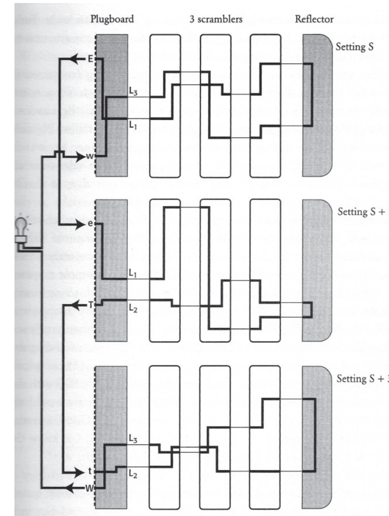
Turing designed new bombes to do this. Much better to do it electronically of course, than mechanically.

Each bombe had 12 Enigmas in series. Given the **wetter** crib, you connect three of them in the S, $\mathrm{S}+1$, $\mathrm{S}+3$, configuration (for an initial S), and you looked for the lamp to light up.

You eliminate the plugboard by ignoring *which* letters are the cyphertext letters of of the encyphered crib cycle. You just look for the lamp to light up.

In the picture, the fact that **w** loops back to **W** (with the correct plugboard settings) is equivalent to the fact that L_1 loops back to L_1 without any plugboard.

If the lamp does not light up, you change S to the next setting and try again.



One day the dreaded event occurred — the Germans stopped repeating the message key twice at the beginning of the message.

The new bombes didn't quite work initially. After a frantic few weeks though, working versions were produced, and the Allies were back in business.

You still needed cribs and loops in cribs to get going though, so it wasn't all automatic.

Other facts:

- The German army, airforce and navy all used different systems.
- The army and airforce codes were broken fairly readily.
- Admiral Doenitz, in charge of the navy, was much more cautious; the navy codes could not be broken. He used eight-rotor machines, and varied his procedures frequently. So there was a dreadful toll on Allied shipping in the North Atlantic.
- Only when German naval code books were captured from a submarine which didn't sink as its captain had assumed, did the Allies get a handle on the naval codes, and the tide turned in the North Atlantic.
- Doenitz could not bring himself to imagine that his ultracareful procedures had been compromised, so carried on as before. The rest is history.

The information that was obtained by breaking Enigma was codenamed ULTRA.

After the war, the Allies confiscated all the German Enigma machines that they found.

Gleefully, the British handed them out to the governments of their colonies (Britain still had its empire then), describing them as furnishing an unbreakable means of keeping their communications secret ... and carried on listening to all their secret comms traffic for the next several decades.

Not till the early 1970's, when one of the Bletchley Park insiders who was now close to death decided to write his memoirs (which would contravene official secrecy), and strong computer based cryptanalysis became much more widely known (which made Enigma truly obsolete), did the facts relating to Enigma emerge into the public domain.

Pictures taken (with appreciation) from:
D. Salomon, Data privacy and Security
S. Singh, The Code Book
A. Konheim, Computer Security and Cryptography.