Part XIV

History of cryptography

HISTORY of CRYPTOGRAPHY

PROLOGUE

- As information becomes an increasingly valuable commodity, the encryption is the only way to protect our privacy and guarantee the success of the e-business.

- Some groups, for example businessmen and civil libertarians, require strong cryptography.

- The forces of law and order are pressing governments to restrict the use of cryptography.

- What to value more? Personal freedom or the order and law?

WHO are CODEBREAKERS

The vision of codebreakers has changed through the history, depending on the tools used for encryption and cryptanalysis.

Before computer era views: Codebreakers or cryptanalysts are linguistic alchemists, a mystical tribe attempting to conjure sensible words out of meaningless symbols.

Current view: Codebreakers and cryptanalyst's are artists that can superbly use modern mathematics, informatics and computing super-technology.

Three views of the history

- First World War was the war of chemists (deadly gases).
- Second World War was the war of physicists (atomic bombs)
- Third World War would be the war of informaticians (cryptographers and cryptanalysts).

HISTORY of CRYPTOGRAPHY - SUMMARY

The history of cryptography has been the story of centuries-old battles between codemakers and codebreakers, an intellectual arms race that has had a dramatic impact on the course of history.

It has been the ongoing battle between codemakers and codebreakers has inspired a whole series of remarkable scientific breakthroughs.

History is full of codes. They have decided the outcomes of battles and led to the deaths of kings and queens.

- At the beginning of 4-th century BC, Kautylia in India wrote a book. Arthasastrta, that contains suggestions for diplomat to use cryptanalysis to obtain secret information about trades.
- Kamasutra (4-th/5-th century AD) lists cryptography as the 44-th and 45-th of 64 arts people should use.
- In 1474 Citto Simonetta wrote, in Pavia, the first book devoted solely to cryptography.
- In 1555 Pope established of Cipher Secretary of Pontiff.
- Around 1585 Matteo Argenti wrote a 135-pages book on cryptography that is considered as the highlight of the renaissance cryptography.

POLYALPHABETIC CRYPTOSYSTEMS

- Such cryptosystem was first clearly explained by Leon Battista Alberti around 1467.
- The French cryptographer Blaise de Vigenere devised a practical polyalphabetic cryptosystem which bears now his name.
- Such cryptosystems were not much used for 200 years because they were considered too complicated.
- A method to break polyalphabetic cryptosystem developed first Charles Babbage during Crimean war.
- The method was redeveloped and and published later by The Prussian Friedrich Kassiski.

OLD GOLDEN TIMES of CRYPTOGRAPHY

- Golden times of Islamic culture (from 9th till 12th century). Islamic culture had very efficient administration that relied on secure communication through encryption. (For example tax records were protected by encryption.)

- By the fourteenth century the use of cryptography had become widespread, with alchemists and scientists using it to keep their discoveries secret.

- By the fifteenth century, European cryptography was a burgeoning industry.
  For example, each ambassador of (many) of the Italian states had a crypto-secretary.

EXAMPLES of "UNBREAKABLE CODES"

- GREAT CIPHER of LOUIS XIV (created around 1630) was used to encrypt letters of Louis XIV.
- GREAT CIPHER was broken around 1890 by Bzeries.
- BEALE CODE, published in 1885, should contain encryption of the place where a treasury worth of 20 mil. of dolars is hidden.

BEALE CODE

- In 1885 a paper was made public that contains three pages of codes that should describe a place where a treasury has been hidden that is worth of 50 millions of dollars and what to do with it.

- Many people spent a lot of time, some whole their life, to decode it.

- One page could be decoded using an article about American indeoendence.

- The key part describing exctly place treasury is hidden has not been decrypted yet.

92   *The Code Book*

When, in the course of human events, it becomes [10] necessary for one people to dissolve the political bands which [20] have connected them with another, and to assume among the [30] powers of the earth, the separate and equal station to [40] which the laws of nature and of nature's God entitle [50] them, a decent respect to the opinions of mankind requires [60] that they should declare the causes which impel them to [70] the separation.

We hold these truths to be self-evident, [80] that all men are created equal, that they are endowed [90] by their Creator with certain inalienable rights, that among these [100] are life, liberty and the pursuit of happiness; That to [110] secure these rights, governments are instituted among men, deriving their [120] just powers from the consent of the governed; That whenever [130] any form of government becomes destructive of these ends, it [140] is the right of the people to alter or to [150] abolish it, and to institute a new government, laying its [160] foundation on such principles and organizing its powers in such [170] form, as to them shall seem most likely to effect [180] their safety and happiness. Prudence, indeed, will dictate that governments [190] long established should not be changed for light and transient [200] causes; and accordingly all experience hath shewn, that mankind are [210] more disposed to suffer, while evils are sufferable, than to [220] right themselves by abolishing the forms to which they are [230] accustomed.

But when a long train of abuses and usurpations, [240] pursuing invariably the same object evinces a design to reduce them [250] under absolute despotism, it is their right, it is their [260] duty, to throw off such government, and to provide new [270] Guards for their future security. Such has been the patient [280] sufferance of these Colonies; and such is now the necessity [290] which constrains them to alter their former systems of government. [300] The history of the present King of Great Britain is [310] a history of repeated injuries and usurpations, all having in [320] direct object the establishment of an absolute tyranny over these [330] States. To prove this, let facts be submitted to a [340] candid world.

Figure 24 The first three paragraphs of the Declaration of Independence, with every tenth word numbered. This is the key for deciphering the second Beale cipher.

BLACK CHAMBERS

By 1700 cryptanalysis was industrialized, with teams of of cryptanalysts working in so called BLACK CHAMBERS established by most powerful governments.

For example, BLACK CHAMBER in Vienna used to encrypt about 100 letters daily.

FAMOUS CRYPTOGRAPHERS of pre COMPUTER ERA

- Girolamo Cardano (1501-1576) - father of probability theory
- De la Bigotiere Viete (1540-1603) - father of modern algebra.
- Antoine Rosignol (known as Father of Cryptology for France)
- John Wallis (1616-1703) (known as Father of Cryptology for England)
- Thomas Jefferson (1743-1826) - known as Father of American Cryptography
- Charles Babbage (broke Vigenere cryptosystem - the inventor of the first universal computer).
- Allan Turing (helped to brake ENIGMA, designed BOMBS, developed a technique to determine positions of German submarines).
- John Nash (Nobel price for game theory and economics)

THOMAS JEFFERSON (1743-1826)

- The first draftsman of the Declaration of Independence of the United States.

- The second vice-president of USA

- The third president of USA

- Inventor of cryptographic device called Wheel Cypher or Jefferson Wheel

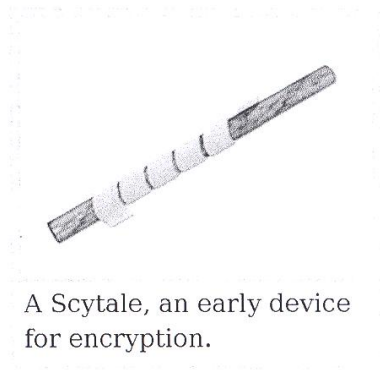# FROM "BLACK MAGIC" to "SCIENCE" VIEW OF CRYPTOGRAPHY

- Cryptography has been practices already for centuries.
- Cryptography is needed in all situations involving long-distance communication (in time/space) where secrecy and (mis)trust are key factors.
- Till 20th century most of cryptography has been practice and understood as "black magic" rather than as a science.
- The advent of computers and development of computational complexity has changed situation.
- Achieving this progress has required formalization of some notions - such as randomness, knowledge, in-distinguishibility and proof - whose mathematical formalisation seems very elusive.

CRYPTOGRAPHY in JAPAN

- Cryptography in Japan seems not to have been used till 1510.
- Advanced techniques were not known till about 1860 - until after the opening country to the west.
- During 1920's Polish naval officers assisted the Japanese military with cryptography developments.
- During WW2 US Navy cryptographers broke several Japanese Navy cryptosystems.
- The break into system JN-25 led to the US-victory in the Battle of Midway.
- US Army group managed to break the highest security Japanese cryptosystem called *PURPLE* even before beginning of WW2.

HISTORY of CRYPTOGRAPHIC MACHINES

FIRST KNOWN DEVICES - SCYTALE

■ Spartans used transposition cipher device called scytale . It was a tapered wooden staff around which a strip of parchment (or leather or papyrus) was spirally wrapped, layer upon layer. The plaintext was written on the parchment lengthwise down the staff. Then the parchment was unwrapped and sent. Text on parchment had no sense until re-wrapped around a staff of equal proportion. (One use of the scytale was documented to occur around 475 BC).

A Scytale, an early device for encryption.

ENCRYPTING DISCS

Leon Battista Alberti (1401-1472) developed an encrypting disk to be used for polymorphic substitution.

They were used for several centuries to speed up the use of CAESAR cryptosystem.

Encryption disks could also be called **scramblers**.

JEFFERSON's WHEEL

For an interested reader, [Ka] contains a description of the wheel in Jefferson's own words.

Jefferson's wheel consists of a cylinder mounted on an axis. 26 straight lines, parallel to the axis and at equal distances from each other, are drawn on the cylinder. The cylinder is then cut into 10 smaller cylinders of equal height. The smaller cylinders are referred to as *disks*. Thus, we have 10 disks free to rotate independently about the common axis. Moreover, each of the disks is divided into 26 boxes of equal size on its circumference. On each disk, the 26 boxes are now filled with the 26 letters of the English alphabet. The order of the letters is chosen arbitrarily and varies from disk to disk.

A particular Jefferson wheel is depicted in Fig. 1.7. The same wheel will be used in Example 1.7, where also the individual disks are described in detail, that is, also the parts not visible in the figure.

Fig. 1.7

It should be added that Jefferson used 36 disks. We have chosen the smaller number 10, for clarity of presentation.

Both the sender and the receiver possess identical wheels, that is, the cyclic order of the letters is the same on each disk. To encrypt an English plaintext, the sender first divides it into blocks of 10 letters each. A block is encrypted by first rotating the disks in such a way that the block can be read from one of the 26 letter sequences parallel to the axis, and then choosing any of the 25 remaining letter sequences as the cryptotext.

To decrypt, the legal receiver rotates the disks of the Jefferson wheel in such a way that the cryptotext can be read from one of the 26 letter sequences. The plaintext then appears as one of the 25 remaining letter sequences. It will be obvious which one: with an extremely high probability, only one of the letter sequences can be a part of a meaningful English text. Thus, it is not necessary to agree in advance how many lines in the wheel will be advanced in the encryption process. It can be any number between 1 and 25, and the number can vary from block to block.

The situation is slightly different if the plaintext is "nonsense." Then the encryption distance in the wheel must be agreed upon in advance. For instance, if the encryption distance is 3 then the plaintext AAAAAAAAAA will be encrypted as ESYMTRHUEE according to the wheel of Fig. 1.7.

CRYPTOGRAPHY of the FIRST WORLD WAR

BEGINNING of FIRST WORLD WAR

The advent of radio and First World War intensified the need for effective encryptions.

One of the most famous cryptosystems of the First World War was German ADFGVX cryptosystem (selected from a variety of candidates and considered to be unbreakable) introduced on March 5, 1918.

By the beginning of June 1918, the German artillery was only 100 km from Paris. The only hope for allies was to break ADFCVX cryptosystem to find where Germans were planning to make their final attack. Georges Painvin cracked for the first time an

ADFGVX message on June 2.

It is estimated that French intercepted 100 million words of German communications during First World War.

ADFGVX CRYPTOSYSTEM

A combination of substitution and permutation cryptosystems introduced on **March 5, 1918**, to provide German army with an **unbreakable cryptosystem**. Each key had two parts:

- **A** 6×6 **blackboard filled with 26 letters and 10 digits**. It was used for the first encoding similarly as at the Playright cryptosystem.

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	i	t	4	0	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	g	e	y	0	1	q

plaintext **attack at 10 pm**

is encrypted: **DV DD DD DV FG FO DV DD AY XG AD GX**

- **A short permutation**, say of m elements. It was used for writing first cryptotext into rows of length m, then permuting columns and writing final cryptotext row by row.

M	A	R	K
D	V	D	D
D	D	D	V
G	G	F	D
D	V	D	D
A	V	X	G
A	D	G	X

A	K	M	R
V	D	D	D
D	V	D	D
G	D	F	F
V	D	D	D
V	G	A	X
D	X	A	G

First important ADFGVX message was cracked by French G. Painvin on **June 2, 1918**.

ROOM 40

- **Room 40** was a section of British Admiralty with task to decrypt German messages.
- Room 40 was formed in October 1914 and deactivated in 1919.
- It is expected that they decrypted about 15 000 German messages.
- Their success was to a large part due to the fact that several German codebooks could be obtained from destroyed ships.
- On August 26, 1914 Russians seized from German cruiser Magdeburg the German naval codebook **SKM Signalbuch der Kaiserlichen Marine** and gave one copy to British. Codebook had 34 000 instructions for coding and decoding.
- On October 11, 1914 British captured from the German steamer Hobart a codebook **HVB - Handelsschiffsvkehrsbuch** used by German warships, zeppelins and U-boats.
- HVB code used 450 000 possible four letter groups which allowed alternative representations of the same meaning, plus an alternate 10 letter grouping for use in cables.
- On November 30 British recovered from the sunken German destroyer S-119 Verkehrsbuch (VB) - the code used to communicate with embassies and warships
- The code consisted of 100 000 groups of 5 digit numbers each with a particular meaning.
- Several other codebooks were captured in years 1918-1919.

The Mechanization of Secrecy 111

ralty's cipher bureau, named after the office in which it was initially housed. Room 40 was a strange mixture of linguists, classical scholars and puzzle addicts, capable of the most ingenious feats of cryptanalysis. For example, the Reverend Montgomery, a gifted translator of German theological works, had deciphered a secret message hidden in a postcard addressed to Sir Henry Jones, 184 King's Road, Tighnabruaich, Scotland.

ZIMMERMAN TELEGRAM - STORY
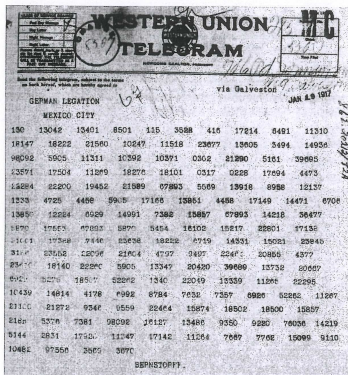
- The most important contribution of Room 40 was decryption of so called "Zimmerman telegram.'

- It was a telegram sent on January 17, 2017 from the German Foreign Office via Washington to its ambassador in Mexico.

- In the telegram German Foreign Minister Arthur Zimmerman offered to Mexico United States territories of Arizona, New Mexico, and Texas as an enticement to join the war as a German ally.

- Motto of telegram was "Make war together and then make peace together". Germens also promised Mexico "Generous financial support:.

- This telegram convinced president Roosevelt, who believed in negotiations with Germany, that it is necessary to declare the war to Germany, what then happened on 6 April 1917.

- Mexican president did not accept German's proposal because he consider their claim about financial support as empty and a war with very strong US as very dangerous for Mexico.

CRYPTOGRAPHY of the SECOND WORLD WAR

BATTLE OF ATLANTIC

- For allies it was of the key importance during WW2 to achieve that Germans do not conquer UK.
- UK was not able to fight against Germans without a very intensive help of USA, concerning food and arms.
- US tried to help UK by sending supplies using convoys of ships.
- Germans tried to destroy these convoys using their U-boats.
- Once a U-boat discovered a convoy informed other U-boats and then they gathered and made a surprising and coordinated attack.
- Between June 1940 and June 1941 Allies lost an average 50 big ships each month and about 50 000 seamen died.
- German submarines (U-boats) were able to sink in total 2780 supply ships from USA
- To make convoys with supply ships to get safely to England it was very important to find out where U-boats were, that had their docks in France.
- It was of key importance for Allies to break communication code of U-boats created by special navy Enigma machines.
- During the period September 1941 and September 1845 US built 2710 big identical ships called "Liberty ships".

STORY of ENIGMA

ENIGMA – its PRINCIPLES

In 1918 Arthur Scherbius invented an encryption machine, called **ENIGMA**, that played an enormous role in the World War Two.

Main components of the Enigma cryptomachine:

- **Keyboard**
- n **scramblers**, $n \geq 3$. At each position a scrambler could implement a CAESAR cryptosystem. After encoding one letter it moved one position. After making full completion, next scrambler was moved one position.
- **Reflector** - to allow to use the same technique for encryption and description.
- **Plugboard** – to realize several transpositions of letters
- **Lampboard**

Number of keys with three scramblers:

- Scramblers orientations 26^3 settings.
- Scrambler arrangements $3! = 6$
- Plugboard settings: 100 391 791 500

Total number of keys is $\approx 10^{16}$.

About 30 000 Enigma machines have been produced.
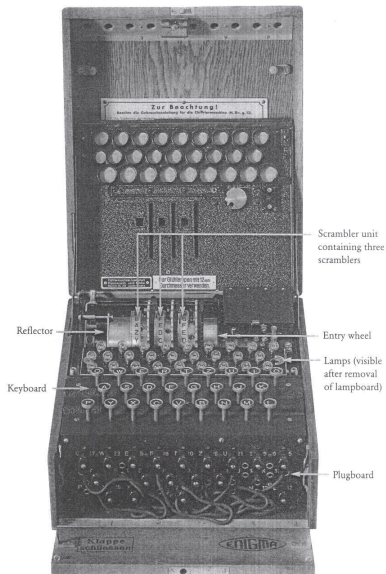
Figure 40: An Enigma machine with the inner lid opened, revealing the three scramblers

IMPACTS of a two SCRAMBLER

The following picture shows how one moving scrambler causes that the same letter - "B" in this time, may be differently encoded if several times are encoded.
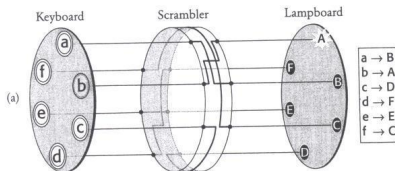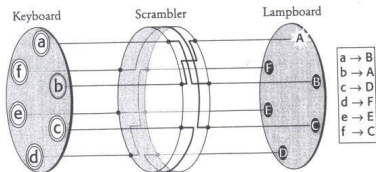
IMPACTS of two SCRAMBLERS

The following picture shows how two moving scramblers cause that the same letter - "B" in this time, may be differently encoded if several times are encoded.

Keyboard   2 scramblers   Lampboard

(a)

(b)

The following picture shows basic structure of ENIGMA with lampboard, keyboard, plugboard, three scramblers and reflector.
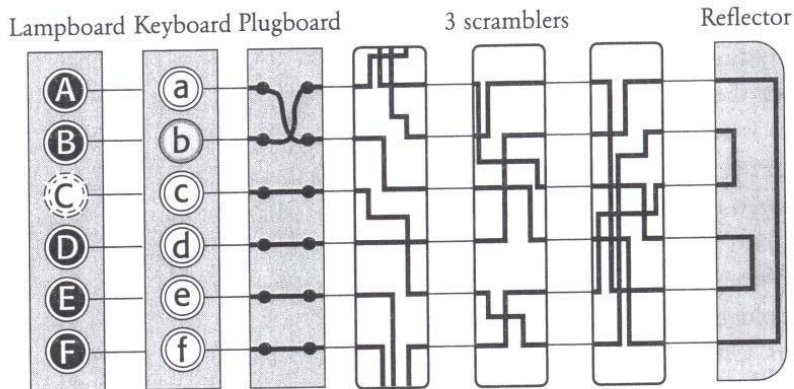
CRACKING of ENIGMA

Of up most importance for the victory of Allies in the Second World War was the fact that they were able to break ENIGMA.

Key events in breaking ENIGMA.

- On November 8, 1931 German Hans-Thilo Schmidt handed to French documents allowing to deduce wirings inside the scramblers.
- Rejewski in Warsaw was able to design methodology and technology to break first ENIGMA using handed documents and a clever idea how to make use of the fact that in addition to having a **daily key** each message encrypting started with sending a 3-letter message key encrypted using twice the day key.
- Alan Turing anticipated that Germans will stop using old message keys and developed method and technology (BOMBS) to make encryptions. One of the key point was clever using of **cribs** – clever guesses that some words were parts of the message (for example **WETTER**).
- Allies were able to still some codebooks.

DAY KEYS versus MESSAGE KEYS I

Day-key components:

Plugboard setting: A-L, P-R, T-D, B-W, K-F, D-Y
Scrambler orientation: Q - C - W
Scramblers ordering: 2 - 3 - 1

- Day-keys were distributed for the whole month.
- A day-key was used only to encode, **TWICE**, randomly chosen message keys - scramblers orientation

Example: PGHPGH –> KIVBJE
Message key PGH is encoded as KIVBJE

CRACKING ENIGMA – BASIC INSIGHT

Rajewski observed that dependencies between letters caused at the decryption of message keys using a daily key form cycles and their number and length dependent only on the scrambler settings.

Example:

1st message	L	O	K	R	G	M
2nd message	M	V	T	X	Z	E
3rd message	J	K	T	M	P	E
4th message	D	V	Y	P	S	X

Cycles

$A \rightarrow F \rightarrow W \rightarrow A$

$B \rightarrow Q \rightarrow Z \rightarrow K \rightarrow V \rightarrow E \rightarrow L \rightarrow R \rightarrow I \rightarrow B$

$C \rightarrow H \rightarrow G \rightarrow O \rightarrow Y \rightarrow D \rightarrow P \rightarrow C$

$J \rightarrow M \rightarrow X \rightarrow S \rightarrow T \rightarrow N \rightarrow U \rightarrow J$

Within one year Rajewski's group created a catalogue of cycles lengths for all 105 456 possible scrambler settings.

Afterwards, each morning they first determined cycles imposed by the that day setting of scramblers (what took few hours), then found in catalogue the proper scramblers setting and then they could easily decrypt messages of that day.

Later they mechanized this decryption process using machines called *bombs*.

DAY KEYS versus MESSAGE KEYS II

- Rajewski enormously simplified the task of finding the day key by separating the problem of finding the scrambler setting from the problem of finding the plugboard setting.
- Finding the plugboard setting was relatively easy task because meaningful German messages were encrypted.
- To find the plugboard setting Rajewski did first decoding without paying any attention to plugboard connections.

Example if the cryptotext was decrypted as

allieinbelrin

this suggested that the transposition

$$L - -R$$

was used.

- Naval Enigma had eight scramblers (three more than the usual Enigma) and its reflector could be set in any of 26 orientations.
- In total Naval Enigma had 156 times more keys to consider than the "usual Enigma".
- Breaking Naval Enigma was extremely important task needed to make see channel between US and England reasonable safe. Without that Allies could have no idea about positions of German submarines and could not plan safe see routes.
- Between June 1940 and June 1941 the Allies lost an average of 50 ships each month, and they were in danger not to build new ships quickly enough to replace

STORY of BLETCHEY PARK

BLETCHEY PARK

The key role in breaking ENIGMA-codes during the Second World War played the team of codebreakers at *Bletchey park* in England.

- Up to 7000 people worked finally in the Bletchey park.
- Team of top codebreakers consisted of people of various professions. To hire new people a crossword was once used to test applicants.
- Work of people in Bletchey park was kept secret till 1974.
- The most difficult problem and most important task was to break navy ENIGMA. (In 1940 and 1941 Allies used to lose about 50 ships per moths that were sink by German submarines.)
- Sophisticated techniques were used to make sure that Germans do not realize that their "unbreakable ENIGMA" was broken.
- Main techniques used were: brains, technology, intelligence, luck.

CRIBS

Combination of three basic cryptographic discoveries/techniques were behind main successes of British crypto-analysis during WW2.

1. Discovery of cribs in encrypted messages - what was an art - that allowed dramatically to reduce the number of potential day keys that needed to be explored. (A crib is a guessed encryption of some frequently used word as Wetter.)

2. Discovery that one can separate encryptions due to scramblers from description caused by transposition of letters due to plugboard again helped dramatically to reduce number of potential keys that needed to be explored.

3. Design of special key testing machines, called bombs, suggested by Turing, allowed to check fast, in few hours, a huge number of potential keys. At the end of war 44 Bombs were in operation.

Success of WW2 cryptanalysis was therefore due to a proper combination of art, science and technology.

TURING's ROLE in BLETCHEY PARK

- In Bletchey park Turing first helped to refine design of the code breaking machines called Bombes. First such machine worked in Bletchey park in March 1940.
- It took 18 minutes to test all possible wheel settings of ENIGMA that was used for encoding.
- Later Turing developed a much labor intensive method based on Bayesian approach how to reduce burden of Bombes.
- The idea was to use "cribs" - likely encodings of known words. They had a catalogue of 17000 ways "ein" could be encrypted.
- Turing's group started to break naval ENIGMA on 27.5.1941, exactly in day where British succeeded to sank the largest German battleship. Next 23 days no supply ship was destroyed.
- Germans then added one wheel to ENIGMA and for four months British were not able to decrypt their messages. In August and Septemeber 1942 German were able to sink 47 ships.
- In order to quantify quality of guesses he developed a measure of it called "ban" - and defined it as the smallest change in weight of evidence that is directly perceptible to human intuition. One ban represented odds of 10 to 1 in favour of a guess. Normally he work with decibans and centibans - smaller units.

BOMBS
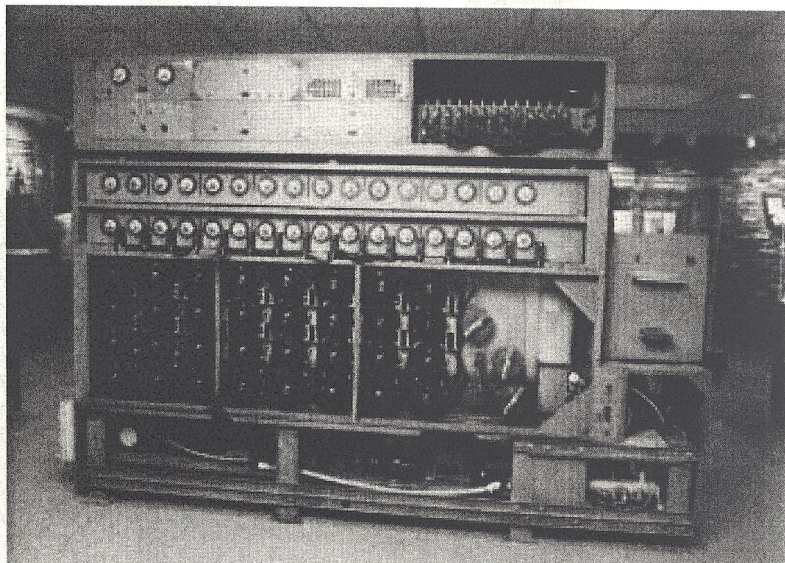
LORENZ SZ40 and COLOSSUS

LORENZ SZ40

- Lorenz SZ40 was an electromechanical encryption machine, far more complicated than Enigma that was used to encrypt telegraphic messages between German High Command and their army commands in Europe.
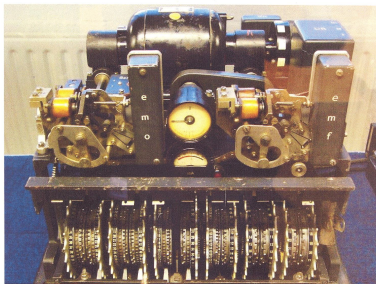

age:Lorenz-SZ42-2.jpg - Wikipedia, the free encyclopedia

http://en.wikipedia.org/wiki/Image:Lorenz-SZ4

Image:Lorenz-SZ42-2.jpg

From Wikipedia, the free encyclopedia

- Image
- File history
- File links

Size of this preview: 800 × 595 pixels
Full resolution (1,141 × 848 pixels, file size: 146 KB, MIME type: image/jpeg)

This is a file from the Wikimedia Commons. The description on its **description page there** is shown below. Commons is a freely licensed media file repository. You can help.

A Lorenz SZ42 cipher machine on display at Bletchley Park museum.

- To encrypt a message with Lorenz, the 5-bit plaintext symbols were combined with a stream of key characters.
- The keystream was generated using 12 pinwheels:

COLLOSUS TECHNICAL DETAILS
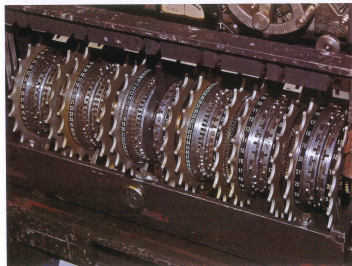
- Colossus was the world's first electronic, digital, fixed-program, single purpose computer with variable coefficients.
- Colossus used vacuum tubes to perform Boolean operations and calculations.
- Colossus was used in Bletchey park during WW2 to help in the cryptanalysis of the Lorenz cipher.
- Colossus was used to find possible Lorenz key settings rather than to decrypt particular cryptotexts.
- The cryptotext was read at the high speed from a paper tape and the other stream was generated internally as a simulation of outcomes of the Lorenz machine
- If the count for the setting was above a certain

- The logical structure of the Lorenz machine was diagnosed at Bletchey park without the machine being seen.!!!!!!!
- First John Tiltman, a very clever cryptanalyst, derived a key stream of 4000 symbols from a German operating blunder in August 1941.
- Bill Tute, a newly arrived member of the cryptanalysts team, used this key stream to work out the logical structure of the Lorenz machine.
- Tute determined that Lorenz had 12 wheels in two groups of five, called χ=wheels and ψ-wheels and 2 special μ-wheels.
- The χ wheels stepped regularly with each symbol that was encrypted; ψ wheels stepped irregularly; under the control of motor wheels μ.

# COLOSSUS - DECRYPTION of LORENZ

- In order to read a message two tasks had to be performed.
- **Wheel breaking** - to discover pin patterns for χ wheels.
- Once the patterns were set up they were used for a while.
- **Wheel setting** that could be attempted once pin patterns are known.
- Each message encrypted with Lorenz was encrypted with a different start position of the wheels.
- Tute discovered, on the basis of the fact that different letters have difference occurence statistic, that trying two impulses of the χ-stream against the cryptotext would produce a statistic that was not random.
- The process of *wheel setting* found the start position for a message.
- Initially Colosus was used to work out the start positions of χ wheels, but later also to determine the wheel breaking.

DESIGN of COLOSSUS

- To break Lorenz encryption at first a counting machine "Heath Robinson" was designed.
- However, its electromechanical part was too slow and it was difficult to synchronize two streams - on two paper tapes.
- Tommy Flowers, a senior researcher at the Post Office's Research Centre, suggested to design a better machine, called **Colossus**, with 1500 electronic valves on to do the job, but his proposal was rejected by Max Newman, head of Section, because the idea that so many electronic valves could work reliably was considered as unrealistic and more "Heah Robinson machines" were ordered..
- However, Flowers got some support elsewhere and work on it in Post Office Laboratory.
- On December 8, 1943 Colossus Mark 1, with 150 valves, was working and was operational in Bletchey Park on February 5, 1944.
- An improved version, 5 times faster with 2400 valves, called Colossus Mark 2 first worked on 1 June 1944, just in time for Normandy landing. (ENIAC had 17, 468 valves)
- Ten Colossus computers were in use by the end of the war.
- After the WW2 Colossus computers were destroyed, at the order from Churchil. Moreover, Tommy Flowers was ordered to destroy also blueprints of Colossus and he did so on 8 June 1945 (!?!?!?!?!?!?!)

COLOSSUS - DETAILS
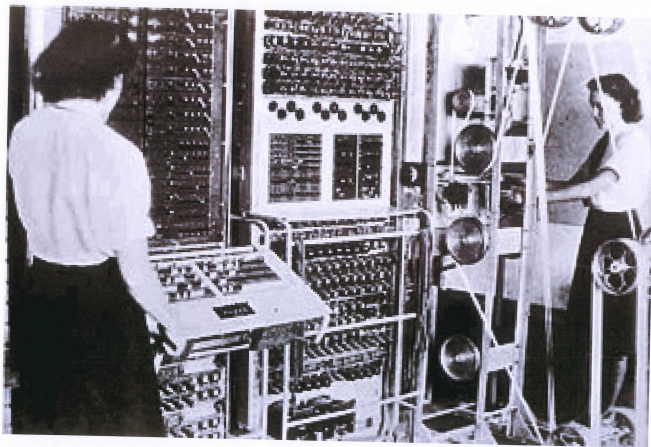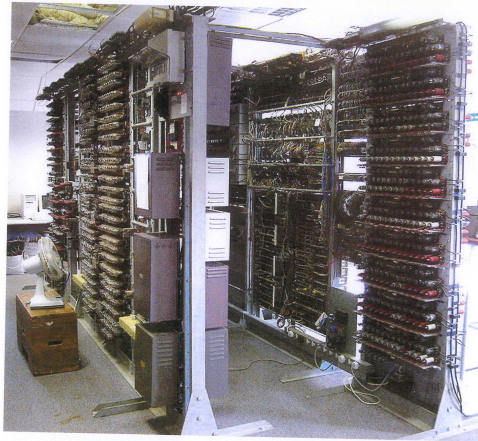
- Each of ten Colossi was 2.3 m high, about 14 m long and occupied one room.
- Colossus reduced the time to break Lorenz messages from weeks to hours.
- Colossus was built just in time for the deciphering of messages which gave vital information prior to D-Day of 2WW. They showed that Hitler swallowed the deception campaign about the area of landing of Allies.
- By the end of 2WW 63 millions of characters of top secret German messages were decrypted
- In 1994 attempts started to redesign Colossus for a museum. A functioning replica was completed in 2007 and is on display at the *National museum of computing*

- Collosus was not "Turing complete" - it was not a general purpose (universal) computer.
- At that time it was not realized that "Turing completeness" is of large importance.
- To set up Colossus for a new task the operators had to set up plugs and switches to alter wiring.

STORY of ENCRYPTION MACHINES

- British were able to break ENIGMA only because it was used with various unproper restrictions and because it was used for stereotypical messages that resulted in "cribs".

- US crypto analysts were also successful in breaking Japanese encryption machine called Purple.

- On the other hand, encryption machines "Typex" used by British army and air force, and machine SIGABA used by US army have never been broken during second world war.

- However, all these machines could not really been used in such fighting as on Pacific islands in jungles.

- A new ingenious idea was to use Navajo Indians for communication because no Japanese could understand it.

NAVAJO CODE

- One of the most useful encryption ideas during WW2 was to assign to American army units Navajo Indians who a given message first translated to the Navajo language and then transmitted using the usual radio waves.

- Main problem with this idea was how to deal with words that had no equivalent in Navajo languages.

- This way of transmitting messages secretly was 100% successful.

- More than 800 Navajo Indians served this way successfully in American Army.

STORY of RSA

HISTORY of RSA

- Diffie published his idea of asymmetric cryptosystem in summer 1975, though he had no example of such a cryptosystem.
- The problem was to find a one-way function with a backdoor.
- Rivest, Shamir and Adleman, from MIT, started to work on this problem in 1976.
- Rivest and Shamir spent a year coming up with new ideas and Adleman spent a year shooting them down.
- In April 1977 they spent a holiday evening drinking quite a bit of wine.
  At night Rivest could not sleep, mediated and all of sudden got an idea. In the morning the paper about RSA was practically written down.

HISTORY of RSA REVISITED

- Around 1960 British military people started to worry about the key distribution problem.
- At the beginning of 1969 James Ellis from secrete Government Communications Headquarters (GCHQ) was asked to look into the problem.
- By the end of 1969 Ellis discovered the basic idea of public key cryptography.
- For next three years best minds of GCHQ tried to unsuccessfully find a suitable trapdoor function necessary for useful public-key cryptography.
- In September 1973 a new member of the team, Clifford Cock, who graduated in number theory from Cambridge, was told about problem and solved it in few hours. By that all main aspects of public-key cryptography were discovered.
- This discovery was, however, too early and GCHQ kept it secret and they disclosed their discovery only after RSA has been shown very successful.

ATTACKS on RSA

RSA can be seen as absolutely secure. However, this does not mean that under special circumstances some special attacks can not be successful. Two of such attacks are:

- The first attack succeeds in case the decryption exponent is not large enough.
  Theorem (Wiener, 1990) Let $n = pq$, where p and q are primes such that $q < p < 2q$ and let (n, e) be such that $de \equiv 1 (\mod \phi(n))$. If $d < \frac{1}{3} n^{1/4}$. then there is an efficient procedure for computing d.

- **Timing attack** P. Kocher (1995) showed that it is possible to discover the decryption exponent by carefully counting the computation times for a series of decryptions. Basic idea: Suppose that Eve is able to observes times Bob needs to decrypt several cryptotext s. Knowing cryptotext and times needed for their decryption, it is possible to determine decryption exponent.

PRETTY GOOD PRIVACY

In 1991 Phill Zimmerman developed and released PGP (Pretty Good Privacy) and by that he made use of the RSA cryptosystem very friendly and easy and, consequently, by that he made strong cryptography widely available.

Starting February 1993 Zimmerman was for three years a subject of FBI and Grand Jury investigations, being accused of illegal exporting arms (strong cryptography tools).

William Cowell, Deputy Director of NSA said: "If all personal computers in the world – approximately 200 millions – were to be put to work on a single PGP encrypted message, it would take an average an estimated 12 million times the age of universe to break a single message".

Heated discussion whether strong cryptography should be allowed keep going on. September 11 attack brought another dimension into the problem.

Even in 2004 former FBI director in his Congress inquiry asked for a new law against public use of encryptions.

HISTORY of QUANTUM CRYPTOGRAPHY

- Around 1970 Stephen J. Wiesner developed, but did not published, the concept of quantum secret money.
- In 1984 Charles Bennett and Gilles Brassard published BB84 protocol.
- In 1989 Bennett at all made first cryptography experiment with photon transmission of photons at the distance 32 cm
- In 1990 unconditional security of the BB84 protocol has been shown.
- In 1991 Eckert published his entanglement based protocol E91 for unconditionally secure generation of classical shared key,
- In 1993 Bennett et al. developed the protocol for quantum teleportation.
- In 1995 quantum key generation using optical cable for distance 22.5 km was demonstrated
- In 1997 it was shown that unconditionally secure quantum bit commitment is impossible.
- In 1998 quantum teleportation was experimentally confirmed.
- In 2004 an open air absolutely secure photon transmission for the distance 27 km was shown, from one Alp's peak to another.
- In 2008 an open air absolutely secure photon transmission was demonstrated for distance 147km on Canary Islands.

EPILOGUE

- **Military success of Allies during World War II was partly due to great outcomes of cryptanalysts.**

- **Because of that cryptography was highly estimated during the Cold War and cryptography was considered as a war weapon in many countries, especially in USA. As a consequence cryptography production, products, use and export were regulated in the corresponding way as for other arms.**

USEFUL OBSERVATIONS

- Very secure systems are rarely used in a massive way in practice due to efficiency problems.

- Cryptographic systems that are used in practice look pretty safe when they are introduced, but after few years they are usually shown not to be safe anymore.

- Because of that it has not much sense to teach about current standards - they will likely be replaced by new ones in few years.

- Beautiful and deep mathematics is usually needed to create safe cryptographic systems - any tools that work are fine for breaking cryptosystems.