

5



Encryption

- "All we need to be secure is good encryption and that will take care of everything." That is the refrain that used to be heard.
- Encryption is certainly an important security tool.
- Encryption mechanisms *can* help with confidentiality, integrity, and accountability.
- Encryption mechanisms are probably the most widely used security mechanisms
- Not all ciphers are used for communication with others: records and reminders may be kept in cipher for use of the author alone.

6




Encryption

- Encryption by itself is not the answer.
- Encryption mechanisms can and should be a part of a comprehensive security program.
- Encryption system can be broken. Encryption is only a delaying action.
- It is just that the length of time and the resources required to gain access to the information being protected by the encryption *are* both significant. Thus the attacker may try some other weakness in the overall system.

Encryption

7




Basic concepts

- Encryption is simply the obfuscation of information in such a way as to hide it from unauthorized individuals while allowing authorized individuals to see it.
- Individuals *are* defined as authorized if they have the appropriate key to decrypt the information.
- This is a very simple concept; the "how" of doing it is where the difficulty lies.
- The intent with any encryption system is to make it extremely difficult for an unauthorized individual to gain access to the information, even if he has the encrypted information and knows the algorithm used to encrypt it.

Encryption

8



Basic concepts

- As long as the unauthorized individual does not have the key, the information should be safe.
- Encryption can be used in three security services:
 - **Confidentiality:** Encryption *can* be used to hide information from unauthorized individuals, either in transit or in storage.
 - **Integrity:** Encryption can be used to identify changes to information either in transit or in storage.
 - **Accountability** Encryption *can* be used to authenticate the origin of information and prevent the origin of information from repudiating the fact that the information came from

9



Encryption Terms

- Plaintext: The information in its original form. This is also known as cleartext.
- Ciphertext: The information after it has been obfuscated by the encryption algorithm.
- Algorithm: The method of manipulation that is used to change the plaintext into ciphertext.
- Key: The input data into the algorithm that transforms the plaintext into the ciphertext or the ciphertext into the plaintext.
- Encryption: The process of changing the plaintext into ciphertext.

10

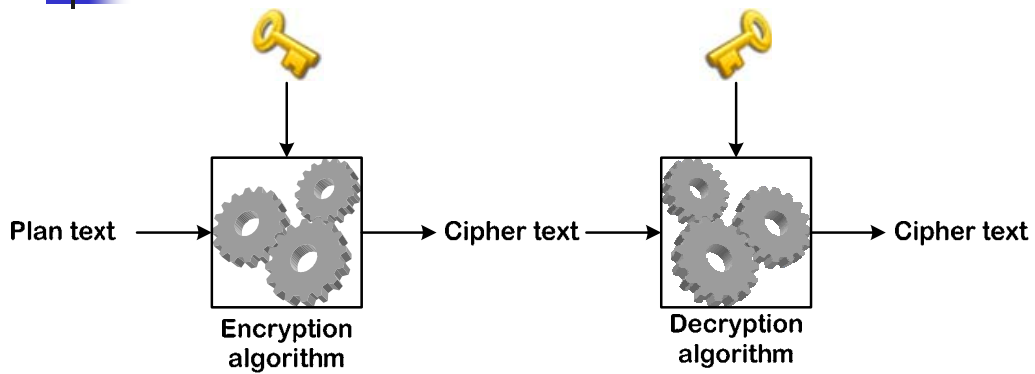


Encryption Terms

- Decryption: The process of changing the ciphertext into plaintext.
- Cryptography: The *art* of concealing information using encryption.
- Cryptographer: An individual who practices cryptography.
- Cryptanalysis: The *art* of analyzing cryptographic algorithms with the intent of identifying weaknesses.
- Cryptanalyst: An individual who uses cryptanalysis to identify and use weaknesses in cryptographic algorithms.

11

Basic Encryption operation



12

Attacks Against Encryption

- Encryption systems can be attacked in three ways:
 - Through weaknesses in the algorithm
 - Through brute force against the key
 - Through weaknesses in the surrounding system

13



Attacking Encryption Algorithm

- When an algorithm is attacked, the cryptanalyst is looking for a weakness in the way that the algorithm changes plaintext into ciphertext so that the plaintext may be recovered without knowing the key.
- Algorithms that have weaknesses of this type are rarely considered strong enough for use.
- This is because a known weakness can be used to quickly recover the original plaintext.
- The attacker will not be forced to use significant resources.

14



Brute Force Attckes

- Attempts to use every possible key on the ciphertext to find the plaintext
- On the average, an analyst using this method will have to try 50% of the keys before finding the correct key.
- The strength of the algorithm is then only defined by the number of keys that must be attempted.
- Long key → large number of keys → large number of keys to be tried until the correct key is found → longer time to break encryption.

15



Brute Force Attckes

- Brute-force attacks will always succeed eventually if enough time and resources are used.
- Therefore, algorithms should be measured by the time the information is expected to be protected even in the face of a brute-force attack.
- An algorithm is considered computationally secure if the cost of acquiring the key through brute force is more than the value of the information being protected.

16



Attack through weaknesses in the surrounding system

- It is usually easier to attack the surrounding system than it is to attack the encryption algorithm.
- Example:
 - An algorithm is strong and has a long key that will require millions of dollars of computer equipment to brute force in a reasonable period of time.
 - The organization using this algorithm sends the keys to its remote locations via regular mail.
 - If an intruder know when the key will be sent, it may be easier to intercept the envelope and gain access to the key that way.



Attack through weaknesses in the surrounding system

17

- Example 2
 - An encryption package uses strong encryption algorithms
 - The encryption used cannot be easily attacked through the algorithm or by brute force.
 - However, the user's key is stored in a file on his computer.
 - The file is encrypted with a password.
 - It is significantly easier to guess or brute force the user's password than it is to brute force the user's key.
- The lesson here is that the surrounding system is just as important to the overall security of encryption as the algorithm and the key.



History

18

- Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption) — conversion of messages from a comprehensible form into an incomprehensible one, and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely, the key needed for decryption of that message).
- The earliest forms of secret writing required little more than local pen and paper analogs, as most people could not read.
- More literacy, or opponent literacy, required actual cryptography.

19



Now

- Confidentiality
- Message integrity checking,
- sender/receiver identity authentication,
- digital signatures,
- interactive proofs,
- secure computation,.

20



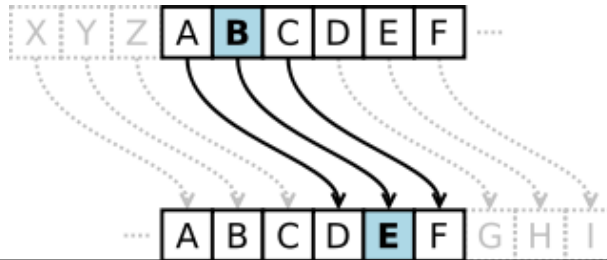
classical cipher types

- Transposition ciphers:
 - rearrange the order of letters in a message
 - in a trivially simple scheme 'help me' becomes 'ehpl em'
- Substitution ciphers,
 - systematically replace letters or groups of letters with other letters or groups of letters
 - 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the alphabet

21

Caesar cipher

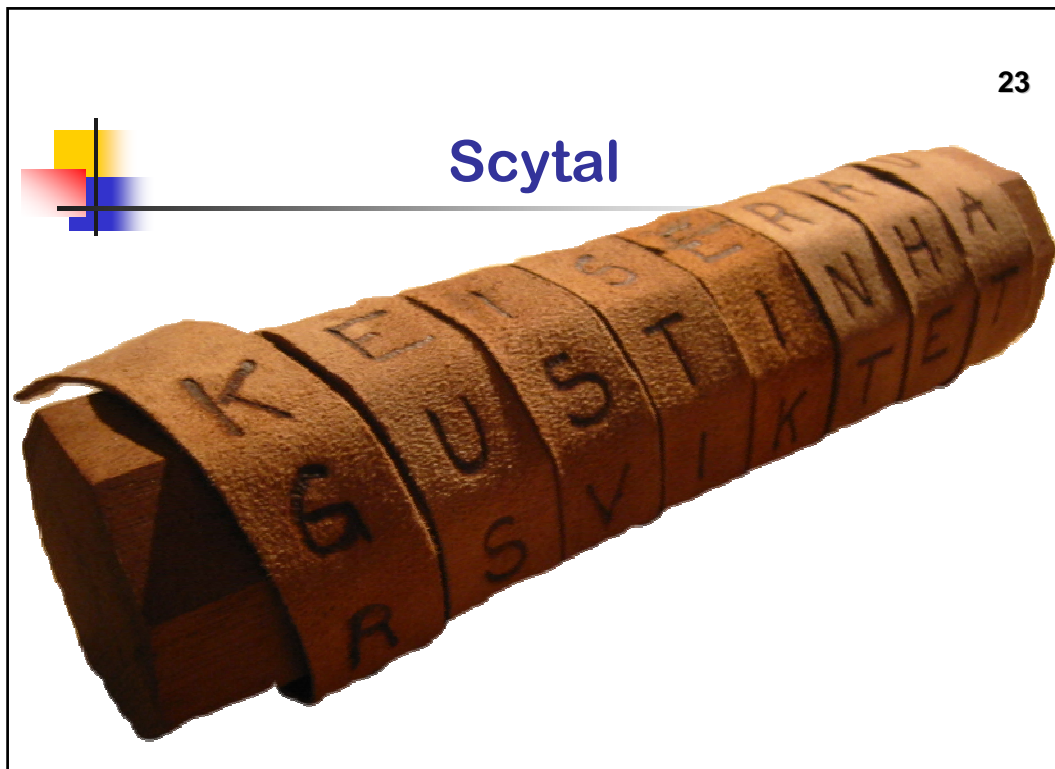
- Named after Julius Caesar who is reported to have used it,
- An early substitution cipher
- Each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet.
- Caser used a shift of 3, to communicate with his generals during his military campaigns.



22

scytale

- Rhymes with Italy, skytale, Greek, a baton
- A tool used to perform a transposition cipher, consisting of a cylinder with a strip of leather wound around it on which is written a message.
- The ancient Greeks, and the Spartans in particular, are said to have used this cipher to communicate during military campaigns.
- The recipient uses a rod of the same diameter on which he wraps the paper to read the message.
- It has the advantage of being fast and not prone to mistakes



24

scytale

- It can be easily broken.
- Since the strip of paper hints strongly at the method, the ciphertext would have to be transferred to something less suggestive, somewhat reducing the advantage noted.

25



Rail Fence Cipher

- A form of transposition cipher that gets its name from the way in which it is encoded.
- In the rail fence cipher, the plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom.
- The message is then read off in rows.

26



Rail Fence Cipher Example

- Using 4 "rails" cipher the message of 'WE ARE DISCOVERED. FLEE AT ONCE',

W
E
A
R
E
D
I
S
C
O
V
E
R
E
D
F
L
E
E
A
T
O
N
C
E

W I E E E
E D S R E E A C
A E C E D L T N
R V F O

27

Grille cipher

- A technique for encrypting a plaintext by writing it onto a sheet of paper through a pierced sheet (of paper or cardboard or similar).
- The earliest known description is due to Cardano in 1550.
- His proposal was for a rectangular stencil allowing single letters, syllables, or words to be written, then later read, through its various apertures.
- The written fragments of the plaintext could be further disguised by filling the gaps between the fragments with words or letters.
- Steganography??

28


Cipher Grille

B	I	H	J	T	K
D	P	A	Q	U	2
N	3	U	N	9	G
F	E	O	I	I	8
V	E	A	O	7	T
O	M	R	6	S	L

A cardboard grille with eight single-letter apertures.

29

Cipher Grille

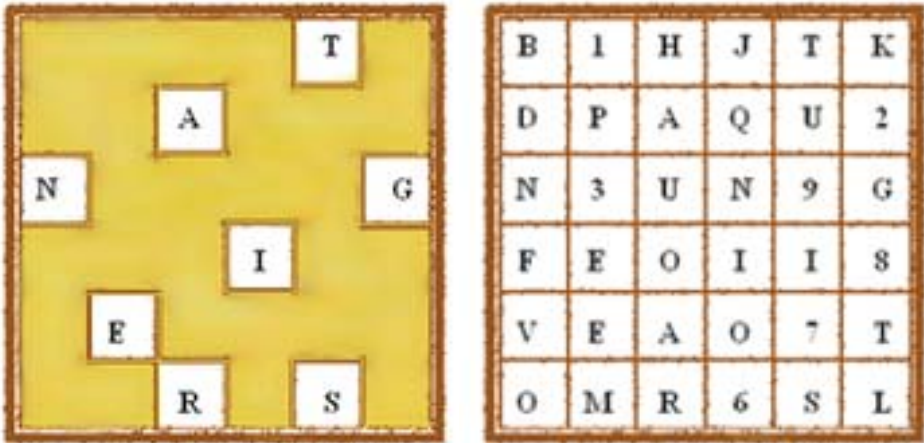


A yellow cardboard grille with eight white rectangular apertures. The apertures are arranged in a pattern and contain the following letters: T (top right), A (top center), N (left), G (right), I (center), E (bottom left), R (bottom center), and S (bottom right).

A cardboard grille with eight single-letter apertures.

30

Cipher Grille



A yellow cardboard grille with eight white rectangular apertures, identical to the one on slide 29. To its right is a 6x6 grid of letters:

B	I	H	J	T	K
D	P	A	Q	U	2
N	3	U	N	9	G
F	E	O	I	I	8
V	E	A	O	7	T
O	M	R	6	S	L

A cardboard grille with eight single-letter apertures.

31



Single-letter grilles

- The grille in the example has eight irregularly placed (ideally randomly) holes – equal to the length of a key word TANGIERS.
- The grille is placed on a gridded sheet and the letters written in from top to bottom.
- A grid filled with random letters and numbers surrounding a key word entered from a grille.
- Removing the grille, the grid is filled with random letters and numbers.
- Then, one hopes, only the possessor of the grille or a copy can read out the hidden letters or numbers

32



Single-letter grilles

- The grille and the grid are kept separately.
- If there is only one copy of the grille and one of the grid, the loss of either results in the loss of both.
- Clearly, in the case of communication by grille cipher, both sender and recipient must possess an identical copy of the grille.
- The loss of a grille leads to the probable loss of all secret correspondence encrypted with that grille.
- Either the messages cannot be read (ie, decrypted) or someone else (with the lost grille) may be reading them.

33



Single-letter grilles

- A further use for such a grille has been suggested: it is a method of generating pseudo-random sequences from a pre-existing text.
- A grille is easily usable for protection of brief information such as a key word or a key number in such a use.

34



Trellis (chessboard) ciphers

- In a chessboard like grid, each successive letter of the message is written in a single white square.
- If the message is written vertically, it is taken off horizontally and vice versa.
- After filling in 32 letters, write on the black squares
- Shorter messages are filled with null letters (each square must be filled up)
- Messages longer than 64 letters require another turn of the board and another sheet of paper.

Trellis (chessboard) ciphers

- Send Money with all speed to our friend Jack in a Ntwerpat the Golden Innx

	M		H		D		I
S		Y		S		U	
	O		A		T		E
E		W		P		R	
	N		L		O		N
N		I		E		F	
	E		L		O		D
D		T		E		R	

J		T		H		L	
	I		P		L		I
A		W		E		I	
	N		A		D		N
C		E		G		O	
	A		T		E		N
K		R		O		N	
	N		T		N		X

Trellis (chessboard) ciphers

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

- JMTHHDLISIYPSLUIAOWAETIEENWAPD
ENENELGOONNAITEEFNKERLOONDDNT
TENRX

37



Trellis ciphers

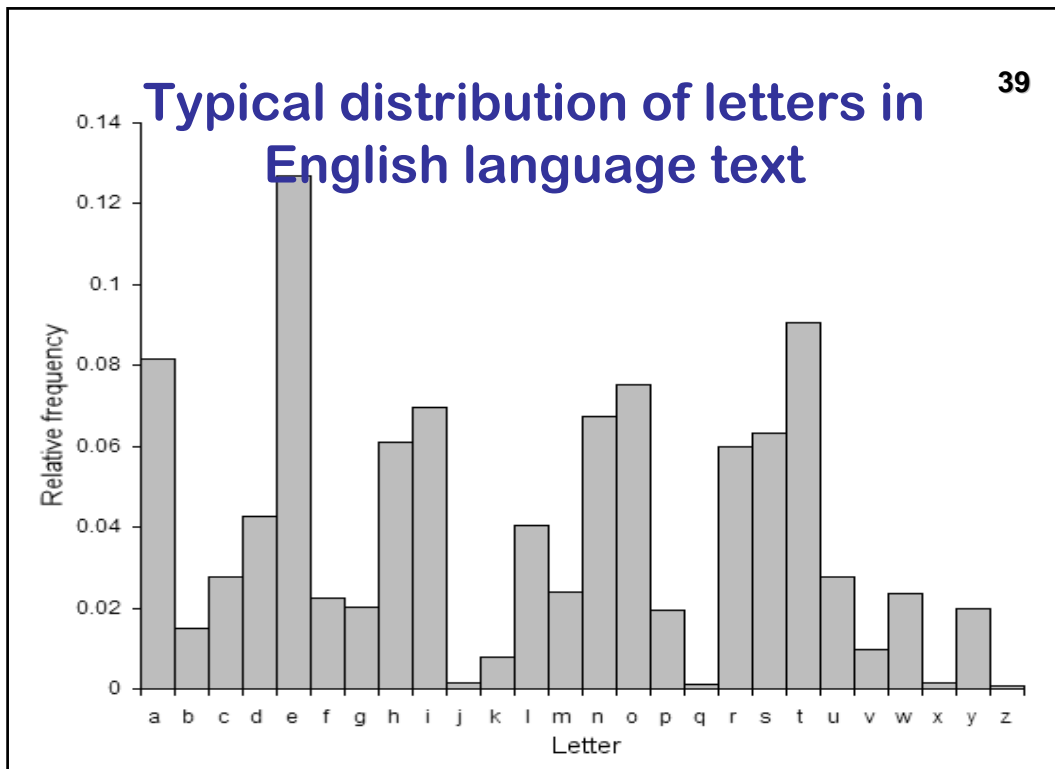
- This transposition method produces an invariant pattern and is not satisfactorily secure for anything other than cursory notes.
- A second transposition is needed to obscure the letters.
- Following the chess analogy, the route taken might be the knight's move.
- Some other path can be agreed upon, such as a reverse spiral, together with a specific number of nulls to pad the start and end
- Grilles can be constructed in various sizes.
- Some grille with code name:- 5x5 ANNA; 6X6 BERTA; 7X7 CLARA; 8X8 DORA; 9X9 EMIL; 10X10 FRANZ.

38




Classical cipher

- Ciphertexts produced by classical ciphers (and some modern ones) always reveal statistical information about the plaintext
- After the Arab discovery of frequency analysis (ca 1000CE), nearly all such ciphers became more or less readily breakable
- Such classical ciphers still enjoy popularity today, as puzzles
- Although frequency analysis is a powerful and general technique, encryption was still often effective in practice; many a would-be cryptanalyst was unaware of the technique.
- Breaking a message without frequency analysis essentially required knowledge of the cipher used.



40



Poly alphabetic cipher

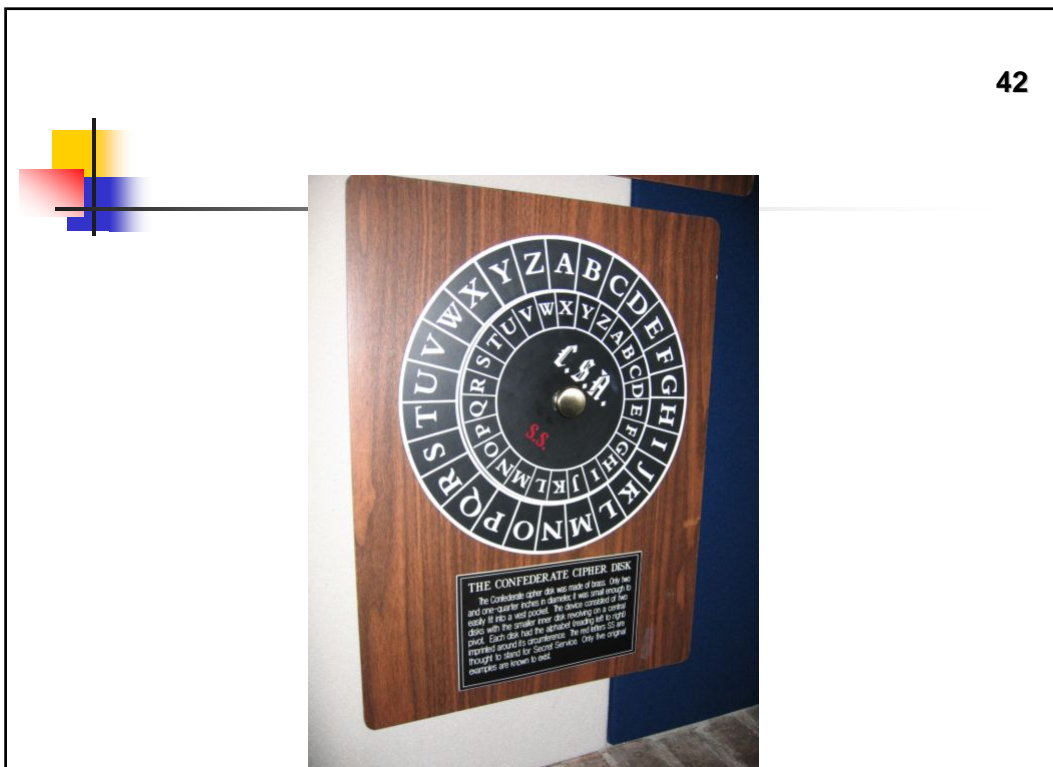
- The Enigma machine is more complex but still fundamentally a poly alphabetic substitution cipher.

41

Poly alphabetic cipher

- A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
- The first published polyalphabetic cipher was invented by Leon Battista Alberti around 1467.
- Alberti used a Caesar cipher to encrypt a message, but he would switch to a different alphabet, indicating that by capitalizing the first letter encrypted with the new alphabet.
- Alberti also invented a decoder device (encryption disk)
- The disk has two alphabets, one on a fixed outer ring, and the other on the rotating disk.

42



43

Poly alphabetic cipher Johannes Trithemius

- Switched alphabets for each letter of the message.
- Start with a tabula recta, a square with 26 alphabets in it
- Each alphabet was shifted one letter to the left from the one above it, and started again with A after reaching Z
- Trithemius's idea was to encipher the first letter of the message using the first shifted alphabet, so A became B, B became C, etc.
- The second letter of the message was enciphered using the second shifted alphabet, etc.
- Trithemius' cipher was trivial to break,

44

Tabula recta

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



polyalphabetic

- The principle (particularly Alberti's unlimited additional substitution alphabets) was a major advance
- The most significant in the several hundred years since frequency analysis had been developed.
- A reasonable implementation would have been vastly harder to break.
- Although Alberti is usually considered the father of polyalphabetic cipher, based on a recently discovered ancient script, the Arab scintests knew the polyalphabetic ciphers 500 years before Alberti.



فاما اسم الالف والهمزة في بعض النسخ فاحذفها من كل ما فيها من الالف والهمزة من غير ان
 يحذف الالف من غير الهمزة والهمزة من غير الالف من غير ان يحذف الالف من غير الهمزة والهمزة
 من غير الالف من غير الهمزة والهمزة من غير الالف من غير الهمزة والهمزة من غير الالف
 من غير الهمزة والهمزة من غير الالف من غير الهمزة والهمزة من غير الالف من غير الهمزة
 والهمزة من غير الالف من غير الهمزة والهمزة من غير الالف من غير الهمزة والهمزة من غير
 الالف من غير الهمزة والهمزة من غير الالف من غير الهمزة والهمزة من غير الالف من غير
 الهمزة والهمزة من غير الالف من غير الهمزة والهمزة من غير الالف من غير الهمزة والهمزة

تم التمام في شهر رجب سنة ١٠٤٠

في سنة ١٠٤٠ من الهجرة النبوية في شهر رجب سنة ١٠٤٠ من الهجرة النبوية في شهر رجب سنة ١٠٤٠
 من الهجرة النبوية في شهر رجب سنة ١٠٤٠ من الهجرة النبوية في شهر رجب سنة ١٠٤٠ من الهجرة
 النبوية في شهر رجب سنة ١٠٤٠ من الهجرة النبوية في شهر رجب سنة ١٠٤٠ من الهجرة النبوية في شهر رجب
 سنة ١٠٤٠ من الهجرة النبوية في شهر رجب سنة ١٠٤٠ من الهجرة النبوية في شهر رجب سنة ١٠٤٠ من الهجرة
 النبوية في شهر رجب سنة ١٠٤٠ من الهجرة النبوية في شهر رجب سنة ١٠٤٠ من الهجرة النبوية في شهر رجب

47

polyalphabetic

- The Arabic scientist Abu Yusuf Al-Kindi authored a book on cryptology the "Risalah fi Istikhrāj al-Mu'amma" (Manuscript for the Deciphering Cryptographic Messages) circa 750 AD.
- Al-Kindi introduced cryptanalysis techniques (including those for polyalphabetic ciphers), classification of ciphers, Arabic Phonetics and Syntax and most importantly described the use of several statistical techniques for cryptanalysis.
- His book antedates other cryptology references by 300 years.
- It also predates writings on probability and statistics by Pascal and Fermat by nearly 800 years.

48

Enigma



49



Enigma

- A cipher machine used to encrypt and decrypt secret messages.
- More precisely, Enigma was a family of related electro-mechanical rotor machines — comprising a variety of different models.
- The Enigma was used commercially from the early 1920s on, and was also adopted by the military and governmental services of a number of nations—most famously by Nazi Germany before and during World War II.
- The German military model, the Wehrmacht Enigma, is the version most commonly discussed.

50



Enigma

- Enigma machine is a combination of mechanical and electrical systems.
- The mechanical mechanism consists of
 - keyboard;
 - set of rotating disks called rotors arranged adjacently along a spindle;
 - stepping mechanism to turn one or more of the rotors with each key press.

51



Enigma machine's initial state

- Wheel order (Walzenlage) — the choice of rotors and the order in which they are fitted.
- Initial position of the rotors: — chosen by the operator, different for each message.
- Ring settings (Ringstellung) — the position of the alphabet ring relative to the rotor wiring.
- Plug settings (Steckerverbindungen) — the connections of the plugs in the plugboard.
- In very late versions, the wiring of the reconfigurable reflector.

52



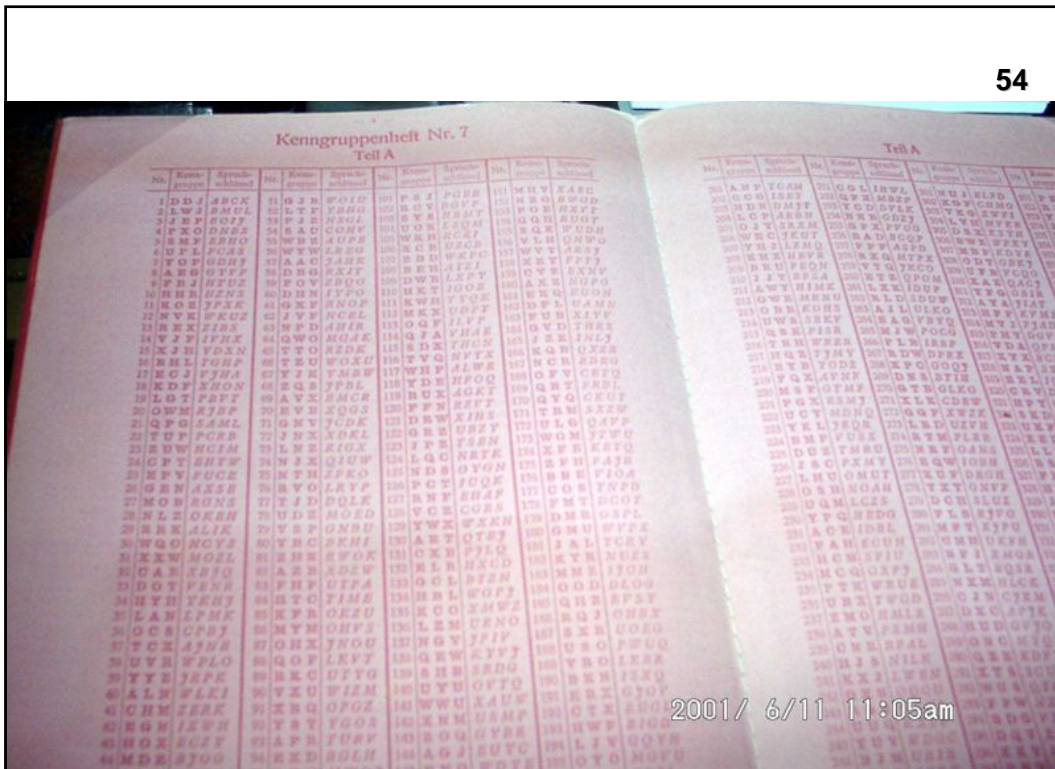
Enigma

- The exact mechanism varies, but the most common form is for the right-hand rotor to step once with every key stroke, and occasionally the motion of neighboring rotors is triggered.
- The continual movement of the rotors results in a different cryptographic transformation after each key press.
- In German military usage, communications were divided up into a number of different networks, all using different settings for their Enigma machines.
- These communication nets were termed keys at Bletchley Park, and were assigned codenames, such as Red, Chaffinch and Shark.



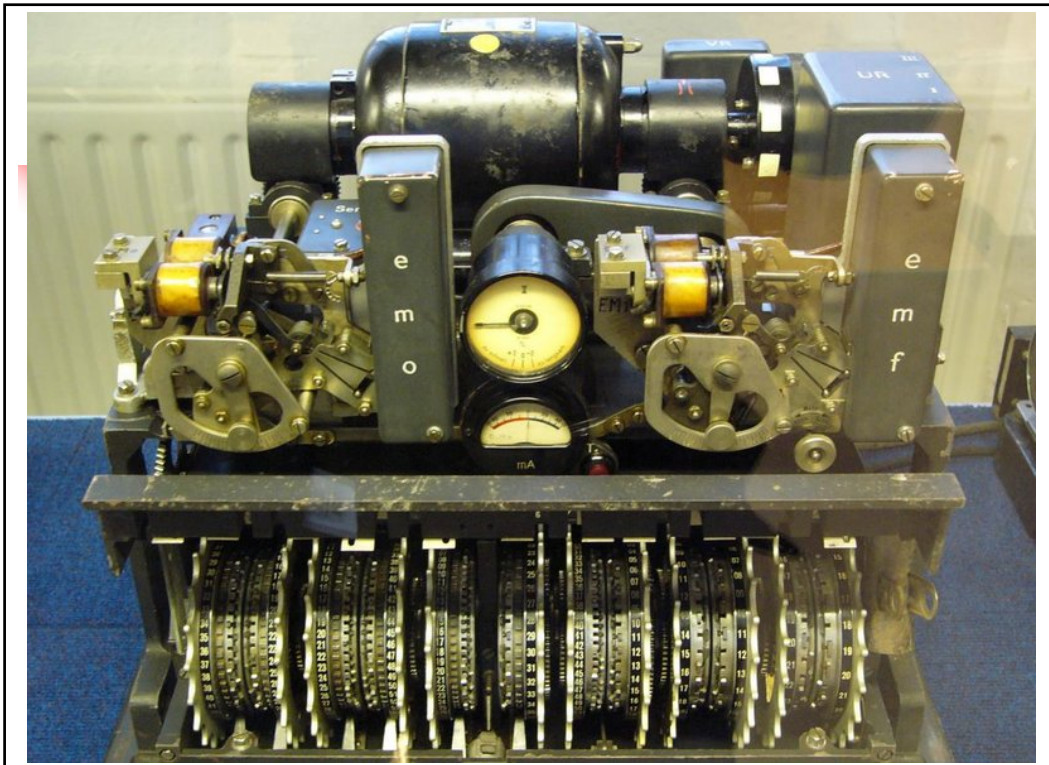
Enigma

- Each unit operating on a network was assigned a settings list for its Enigma for a period of time.
- For a message to be correctly encrypted and decrypted, both sender and receiver had to set up their Enigma in the same way; the rotor selection and order, the starting position and the plugboard connections must be identical.
- All these settings (together the key in modern terms) must have been established beforehand, and were distributed in codebooks.



Lorenz cipher

- The Lorenz, German cipher machines used during World War II for teleprinter circuits.
- While the Enigma was generally used by field units, the Lorenz was used for high-level communications which could support the heavy machine, teletypewriter and attendant fixed circuits.
- The machine itself measured 51cm × 46cm × 46cm (20in × 18in × 18in), and served as an attachment to a standard Lorenz teleprinter.
- The machines implemented a stream cipher.



57



Lorenz cipher

- The teleprinters output each character as five parallel bits on five lines, typically encoded in the Baudot code or something similar.
- The Lorenz machine output groups of five pseudorandom bits to be XORed with the plaintext.
- The pseudorandom bits were generated by ten pinwheels, five of which stepped regularly, termed the χ ("chi") wheels, and five of which were stepped irregularly, termed the ψ ("psi") wheels.
- The stepping of the ψ wheels was determined by two more pinwheels, termed the "motor wheels".

58



Lorenz cipher

- Apart from the stepping of the five irregular pinwheels (which either all stepped together, or all stayed together), the Lorenz machine is actually five parallel pseudorandom generators;
- There is no other interaction between the five lines.
- The numbers of pins on all the wheels were relatively prime.

59



Lorenz cipher

- British cryptographers deduced the operation of the machine because of a mistake made by a German operator.
- A 4,000 character message was transmitted; however, the message was not received correctly at the other end
- The recipient sent an unencoded request for retransmission, which let the codebreakers know what was happening
- The message was retransmitted with the same key settings — a forbidden practice.
- Moreover, the second time the operator made a number of small alterations to the message, such as using abbreviations.

60



Lorenz cipher

- From these two related ciphertexts, John Tiltman was able to recover both the plaintext and the keystream.
- From the keystream, the entire structure of the machine was reconstructed by W. T. Tutte.



SIGABA

- ECM Mark II was a rotor machine used by the United States from World War II (WWII) until the 1950s.
- The machine was also known as the SIGABA or Converter M-134 by the Army, or CSP-888/889 by the Navy, and a modified Navy version was termed the CSP-2900.
- Like many machines of the era it used an electromechanical system of rotors in order to encipher messages.
- No successful cryptanalysis of the machine during its service lifetime is publicly known.



TypeX

- Typex machines were British cipher machines used from 1937.
- It was an adaptation of the commercial German Enigma with a number of enhancements that greatly increased its security.
- Typex came in five-rotor machines (as opposed to three or four in the Enigma) with a non-rotating reflector.
- An improvement the Typex had over the Enigma was that the rotors in the machine contained multiple notches that would turn its neighbouring rotor.
- On some models, operators could achieve 20 words a minute, and the output ciphertext or plaintext was printed on paper tape.



65

Mark III


- Portable version of TypeX,




66

M209







M94


67

- Consisted of 25 aluminum discs attached to a 4.5" rod
- Each disc containing the 26 letters of the Roman alphabet in scrambled order around its circumference (with the exception of the 17th disc, which began with the letters "ARMY OF THE US").
- Each wheel had a different arrangement of the alphabet, and was stamped with an identifying number 1 to 25
- The wheels could be assembled on the rod in any order; the ordering used during encoding comprised the key.
- There were $25!$ (25 factorial) = 15511210043330985984000000 possible keys, which can be expressed as about an 84-bit key size.



M94


68

- Messages were encrypted 25 letters at a time.
- Turning the discs individually, the operator aligned the letters in the message horizontally.
- Then, any one of the remaining lines around the circumference of the cylinder was sent as the ciphertext.
- To decrypt, the wheels were turned until one line matched a 25 letter block of ciphertext.
- The plaintext would then appear on one of the other lines, which could be visually located easily, as it would be the only one likely to "read."

