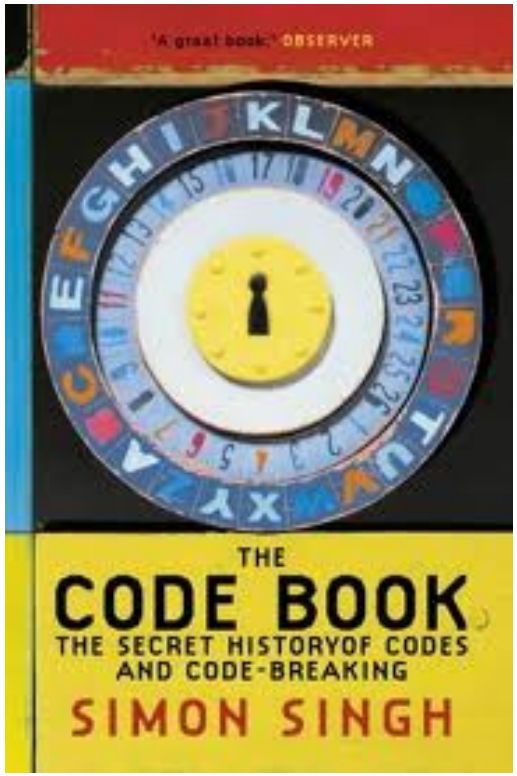
Turing Trilogy 圖靈三部曲
Part 2
The Code War
密碼戰爭

By Cambridge Wong
黃劍翹

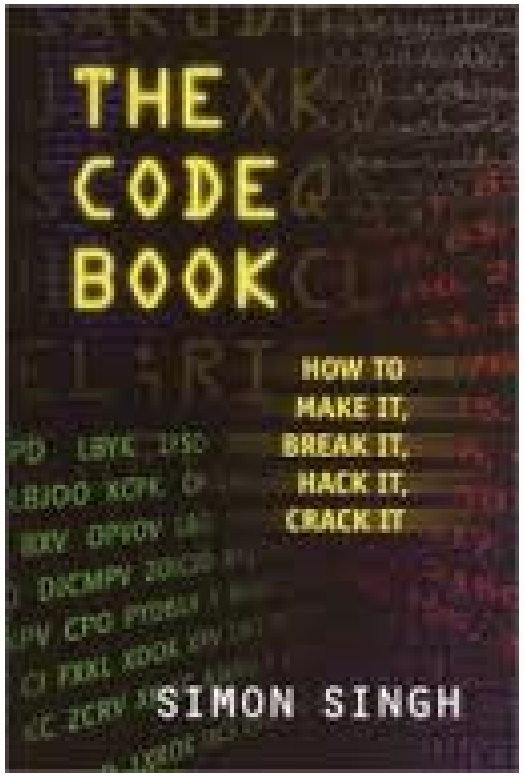
香港中文大學讀書會

22 Jun 2012
Co-hosted by CUHK Book Club
And Hong Kong Computer Society

HONG KONG COMPUTER SOCIETY



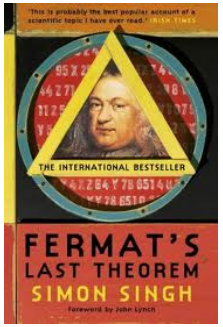
1999 version



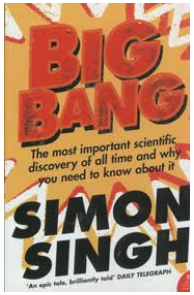
2001 simplified version

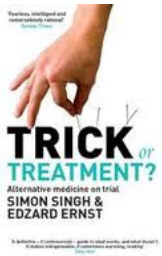
Author – Simon Singh

http://simonsingh.net/



1. Fermat's Last Theorem – the epic quest to Solve the World's Greatest Mathematical Problem (2007)
2. The Code Book (1999)
3. Big Bang - about the Big Bang theory and the origins of the universe (2005)
4. Trick or Treatment? Alternative Medicine on Trial - about complementary and alternative medicine (2008)

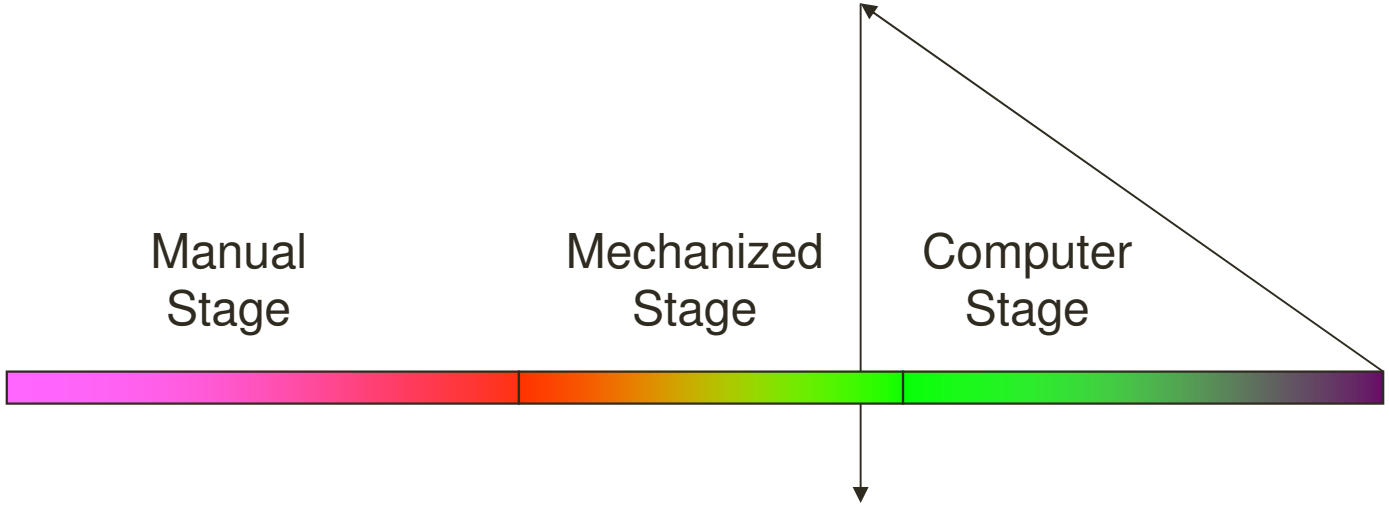




The Book (simplified version)

- The history of cryptography
  - Chapter I – The birth
  - Chapter 2 – The development
  - Chapter 3 – The mechanization in WWII
- Side Track
  - Chapter 4 – Breaking through the language barrier
- Entering the modern days
  - Chapter 5 – Public/Private key (Modern days)
  - Chapter 6 – PGP, the future and the unresolved

My story telling approach

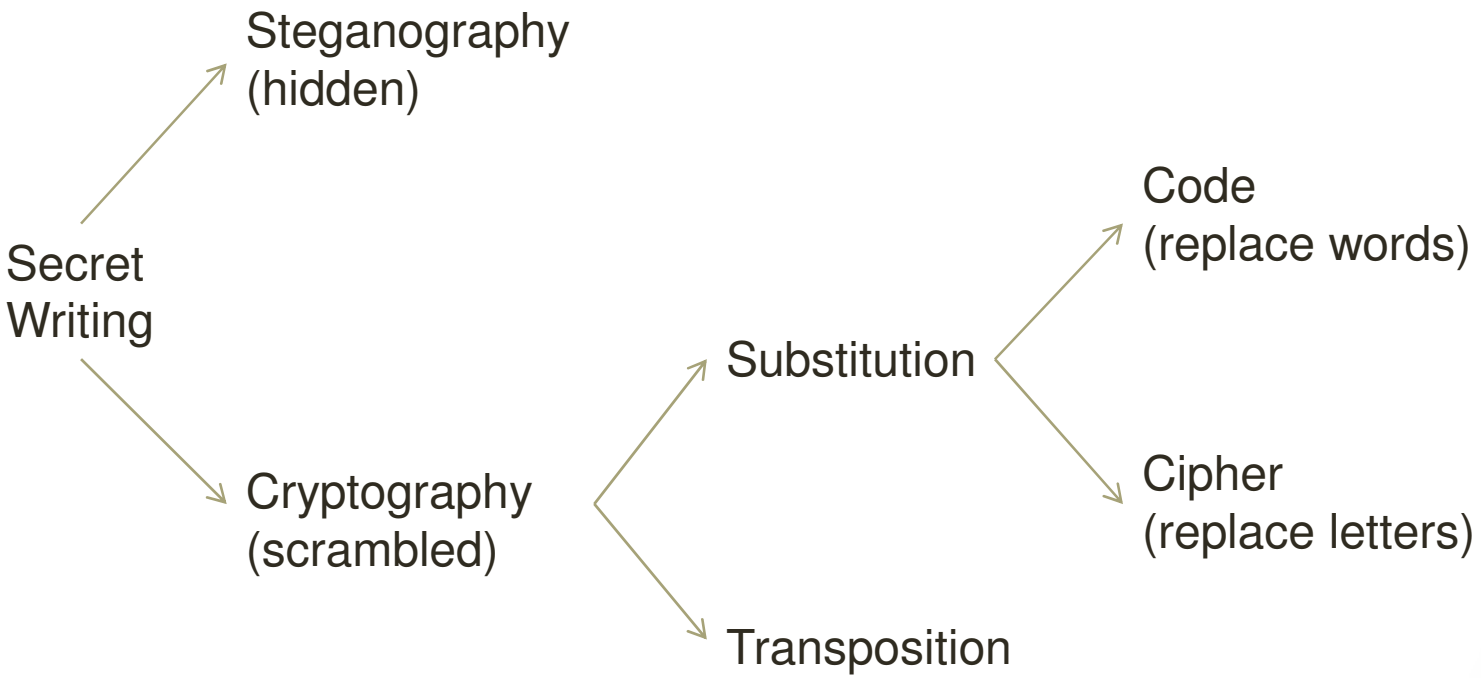


The Enigma Story

Alan Turing

The Greatest Code Breaker

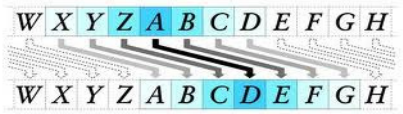
The family tree of encryption



Manual Stage

- Ancient time till early 20th century
- Encryption Techniques
  - Transposition
    - Rail Fence
    - Scytale

  - Substitution



    - Caesar shift (numerical shift, monoalphabetic)
    - Keyphrase substitution (key shift, monoalphabetic)
    - Vigenere cipher (1553, polyalphabetic), unsolvable for centuries

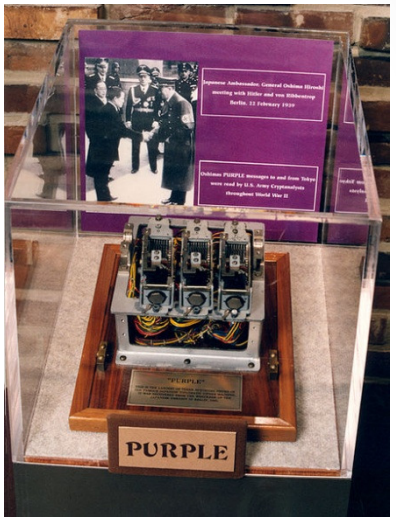
Manual Stage

- Decipher techniques: Frequency Analysis
  - La Disparition (Georges Perec)
  - A Void (Gilbert Adair)
  - Lipogram (constrainted writing)
- Interesting stories
  - The Babington Plot, Mary Queen of Scots
  - Charles Babbage vs the Vigenere cipher
  - Beale treasure
  - Zimmermann telegram (WWI)

Mechanized Stage

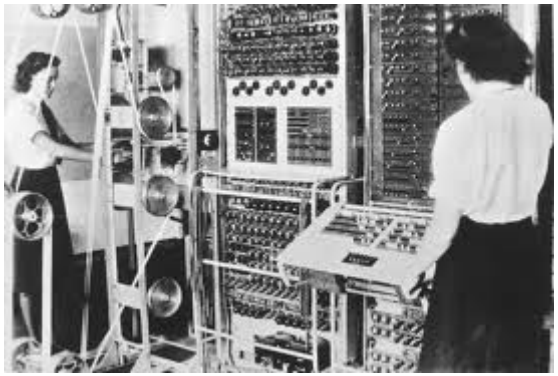
German Enigma

German Lorenz



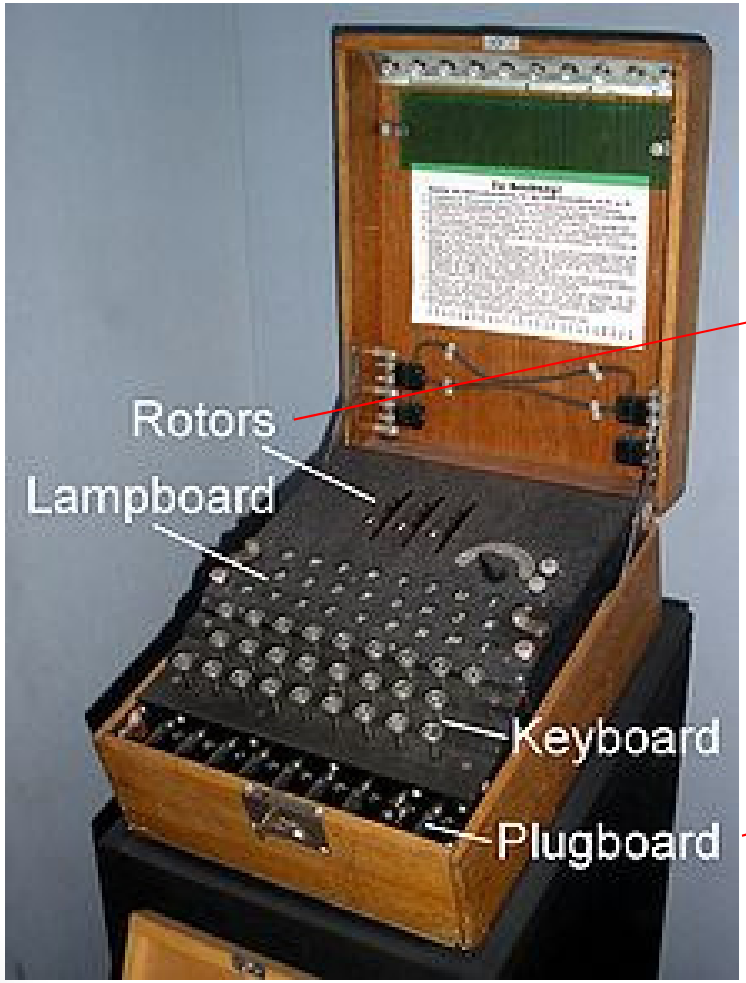
Japanese Purple

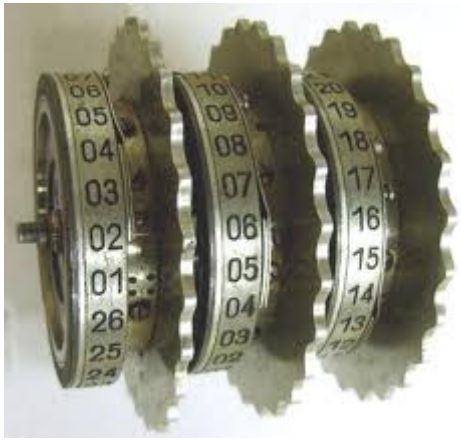
Bomba/Bombe

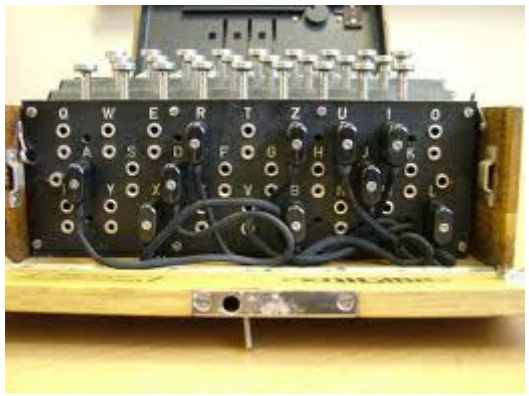


Ultra's Colossus

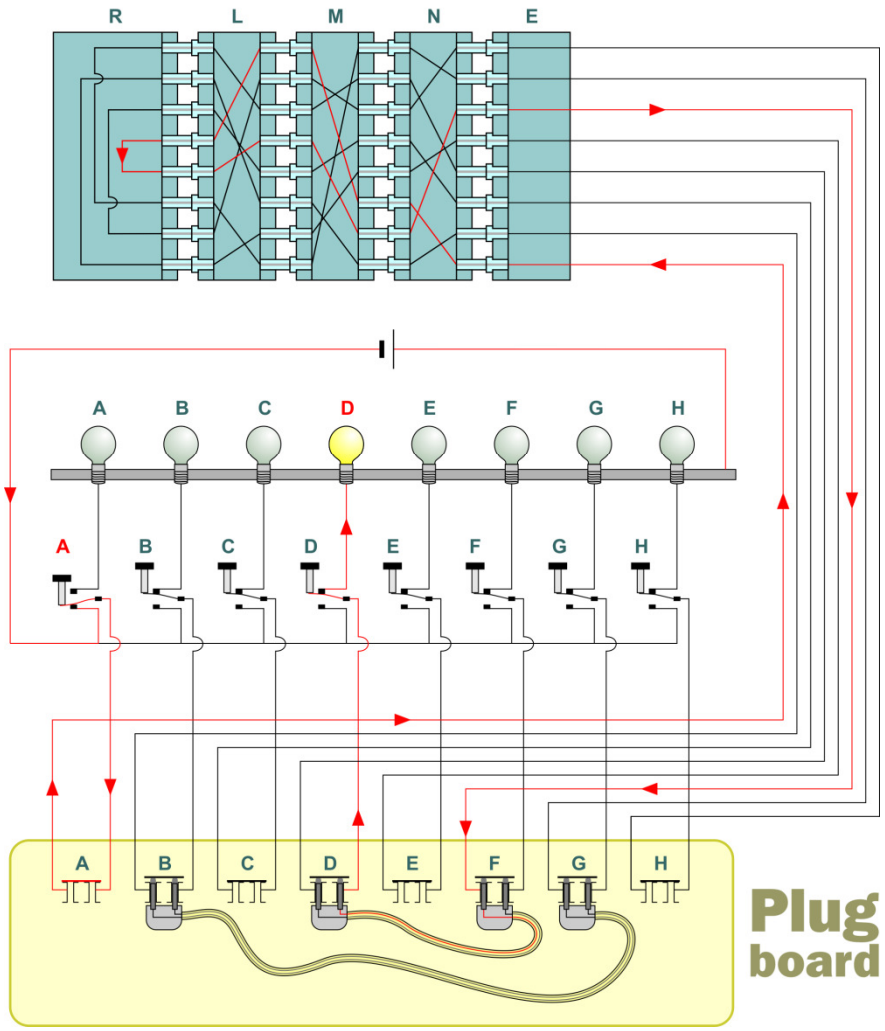
Enigma Machine



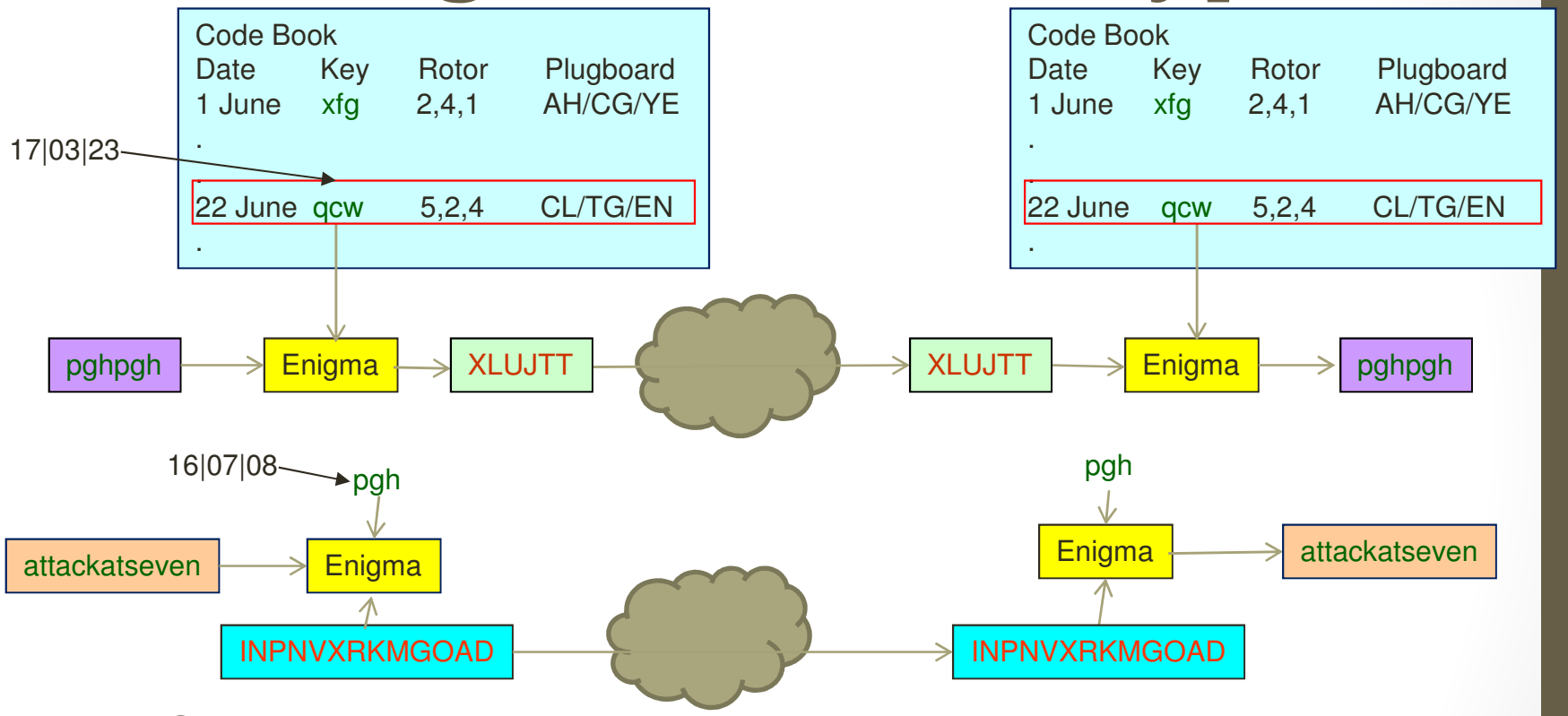




The Enigma Circuit



How Enigma do the encryption



Sender
picks a message key
e.g. PGH in this case

Today is 22 June

Receiver

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

Complexity of Enigma

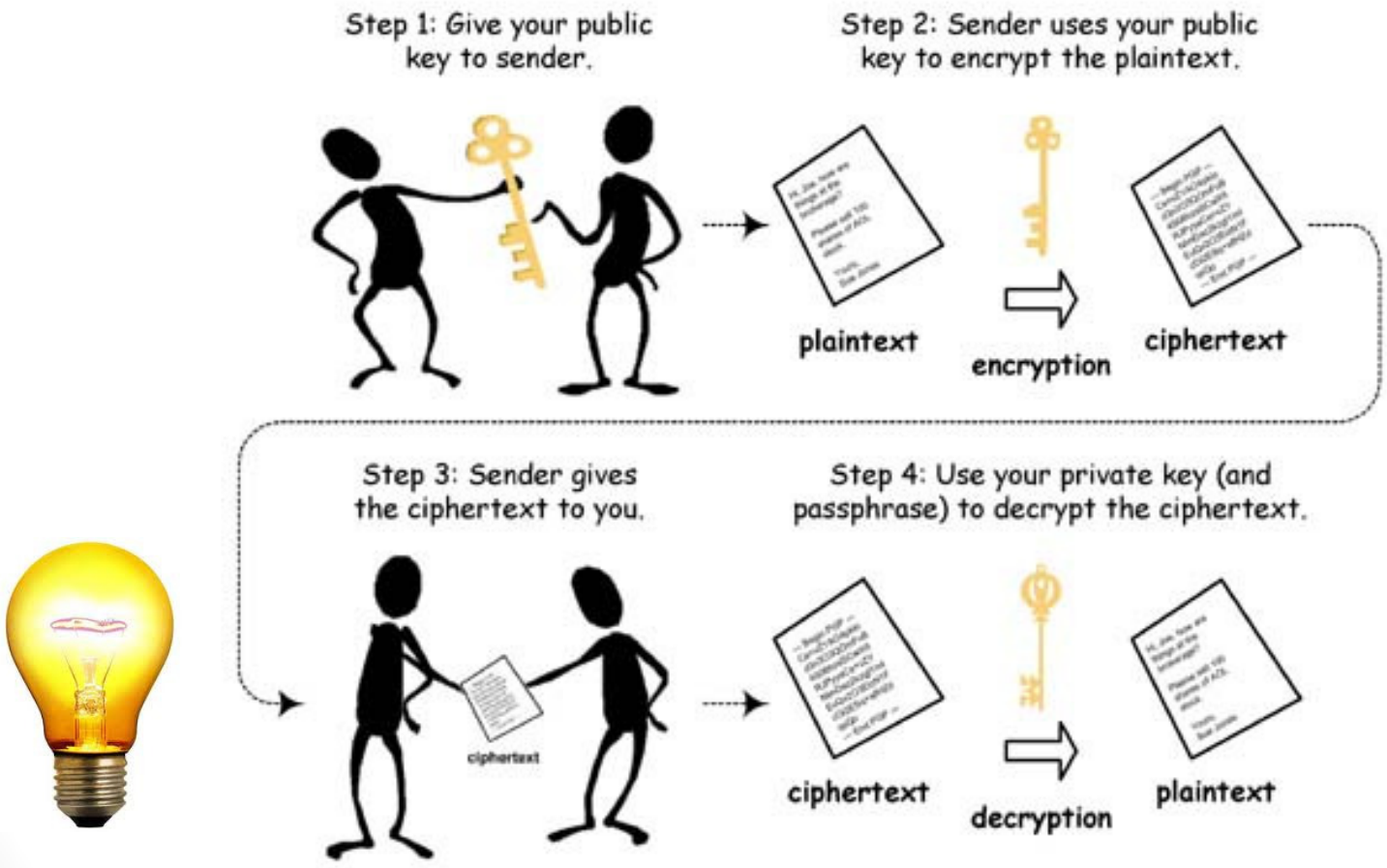
	Before the war	During the war
Rotor arrangement	3 out of 3	3 out of 5
	${}_3P_3 = 6$	${}_3P_5 = 60$
Rotor initial setting	26 x 26 x 26	26 x 26 x 26
	17,576	17,576
Plugboard	6 pairs of letters	10 pairs of letters
	100,391,791,500	150,738,274,937,250
Possible arrangement	About 10^{16}	About 10^{20}

Assume to use 1 min. to try one setting, it will take longer than the age of universe (ie. 13.7B years) to try all settings

Computer Stage

- Major problem: key distribution
- Breakthrough in 1975 by Whitfield Diffie and Martin Hellman at Stanford
- Concept of public key/private key invented that solve the key distribution problem
- Practical solution is invented by 3 MIT scientists: Rivest, Shamir and Adleman (RSA) by another 2 years
- Based on one way function of factorization of two very large prime numbers

Public Key/Private Key



A. Public key holder can send encrypted message to Private key holder
B. Private key holder can issue signed message to Public key holder

Public/private key security

- Private key consist of two very large prime number: p & q
- Public key consist of N which is the product of p & q
- Very Easy to get N if you have p & q
- Very difficult to find p & q if you have N
- eg. N (order of 10^{129}) = 114,381,625,757,888,867,669,235,779, 976,146,612,010,218,296,721,242,362,562,561,842,935,706, 935,245,733,897,830,597,123,563,958,705,058,989,075,147, 599,290,026,879,543,541
- It took a team 600 people, 17 years to find p & q
- p = 3,490,529,510,847,650,949,147,849,619,903,898,133,417, 764 ,638,493,387,843,990,820,577
- q = 32,769,132,993,266,709,549,961,988,190,834,461,413, 177,642,967,992,942,539,798,288,533

The secret and the future of public key encryption

- GCHQ has invented the non-secret key (ie. Public/Private key) 4 years earlier
- Concept is invented by James Ellis
- Practical solution is invented by Clifford Cocks using one night
- The RSA future success lies on P vs NP (1 of the 7 millennium problems)
- Quantum cryptography based on Uncertainty Principle

The Enigma Story

- Developed by Arthur Scherbius (1918) as commercial product
- Adopted by German military service (1926)
- Schmidt's treachery (1931)
- Polish breakthrough before the war (Fingerprint & Bomba)
- Reveal its work to French & Britain just before the war (1939)
- Several setbacks by Enigma version upgrade
- Air force Enigma code is broken at early stage
- Navy Enigma code is the hardest to break, finally broken by luck, bravely, tricks and the genius of Alan Turing
- Hilter's Lorenz code is broken by Ultra's Colossus programmable machine by Tommy Flowers based on Turing's ideas in 1936 (Universal Turing Machine)

Luck, Bravely and Tricks

- Treachery
- Procedural flaws
- Operator mistakes
- Rigidity of military protocol
- Seizing the codebook from U-boat
- Minimizing tell-tale signs
- ‘Ping Pong’ technique

The Polish Breakthrough

- French gives up and passes all the Enigma information to Poland under a military corporation agreement (early 30)
- Rejewski discovered the weakness of the repeated message key
- Repetition leads to pattern
- The message key encrypted twice jeopardize Enigma

Marian *Rejewski*

Exploiting the Engima weakness

	1st	2nd	3rd	4th	5th	6th
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	Z	X

1st Letter A B C D E F G H I J K L M N P O P Q R S T U V W X Y Z
4th Letter P M R X

After enough messages are collected, the complete relationship is found:

1st Letter 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

4th Letter F Q H P L W O G B M V R X U Y C Z I T N J E A S D K

A → F → W → A	3 Links
B → Q → Z → K → V → E → L → R → I → B	9 Links
C → H → G → O → Y → D → P → C	7 Links
J → M → X → S → T → N → U → J	7 Links

Exploiting the Enigma weakness

- Rejewski found that the chain length is independent of the plugboard setting
- Thus, the chain length is the signature (fingerprint) of the rotor setting
- Number of rotor setting = 6 x 26 x 26 x 26 = 105,456
- Manageable
- Prepare a catalogue of chain length (in one whole year)
- Invented Bomba to speed up the searching process
- Predictable message key called Cillies also help speeding up the search of day key

German Naval Enigma

- No repeated message key
- Cannot produce the fingerprint
- Other cryptanalysts have already given up breaking the naval enigma code
- Alan Turing took up the problem on his own, thus he broke the German Naval Enigma code single-handedly

"It is always difficult to say that anyone is absolutely indispensable but if anyone was indispensable to Hut 8 it was Turing. The pioneer work always tends to be forgotten when experience and routine later make everything seems easy and many of us in Hut 8 felt that the magnitude of Turing's contribution was never fully realized by the outside world."

Hugh Alexander "History of Naval Enigma"

Alan Turing statue at Bletchley Park

Turing genius ideas

- Studied library of decrypted messages and noticed a rigid structure in most messages
- He could predict part of the contents of un-deciphered message
- eg. ‘wetter’ appears in all messages intercepted at 6:05am
- Plain text associated with cipher text, the combination is called ‘Crib’
- Another Enigma weakness: will not encipher a letter as itself, a feature of the reflector
- That helps speed up the location of the crib in the cipher text
- Designed Bombe to check thousands of the rotor settings

Lorenz and Colossus

- Lorenz cipher was used to encrypt communications between Hilter and his generals
- Lorenz SZ40 was far more complicated than Enigma
- One weakness was discovered (not to be discussed here)
- Breaking Lorenz required searching, matching, statistical analysis and careful judgment
- Based on Alan Turing ideas on his 1936 paper, Max Newman (teacher of Alan Turing) designed the Colossus but Blatchley's officials shelved the project to build it
- Tommy Flowers ignored the decision and built it by himself
- Colossus is programmable
- Probably the first modern digital computer
- All Colossus machines and design document were destroyed after the war

Alan Turing Year in HK