Week 3 :Classical & Mechanical Ciphers

When and how long it was begun?
Why?

History of Cryptologic Research(1/3)

1900BC : Non-standard hieroglyphics

1500BC : Mesopotamian pottery glazes

50BC : Caesar cipher

1518 : Trithemius’ cipher book

1558 : Keys invented

1583 : Vigenere’s book

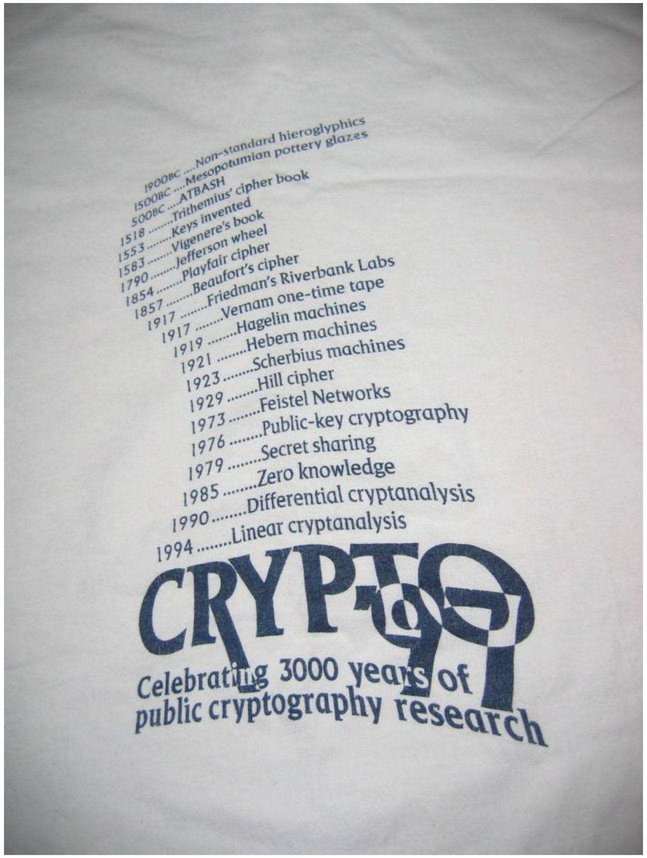
1790 : Jefferson wheel

1854 : Playfair cipher

1857 : Beaufort’s cipher

1917 : Friedman’s Riverbank Labs

1917 : Vernam one-time pads



History of Cryptologic Research(2/3)

Modern Cryptography

1919 : Hegelin machines

1921 : Hebern machines

1929 : Hill cipher

1949; Shannon's Theory

1973 : Feistel networks

1976 : Public key cryptography (Diffie-Hellman)

1977: DES

1978 : RSA

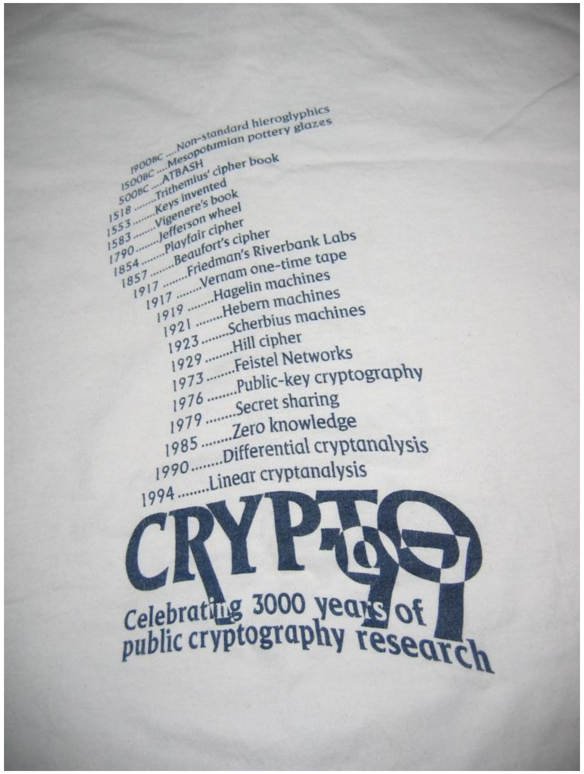
1985 : ECC

1990 : Differential cryptanalysis

1994 : Linear cryptanalysis

1997 : Triple-DES

1998 ~ 2001 : AES



History of Cryptologic Research (3/3)

	Period	Features	Examples
Classical Cipher	ancient ~ 1920	Substitution Transposition (Easy & Simple)	Scytale, Caesar, Vigenere, Beaufort (USA)
Mechanical Cipher	1920 ~ 1950	Using rotor machine	Enigma (Germany in 2^{nd} WW) M-209 (USA in 2^{nd} WW)
Modern Crypto.	1950 ~ current	Shannon's theory Using computer (Difficult & Complicated)	DES, SEED, AES RSA, DH, ElGamal, ECC, DSA, KCDSA, etc

Classical Encryption Techniques

- Basic building blocks of all encryption techniques
  - Substitution: replacement
  - Transposition: relocation, permutation

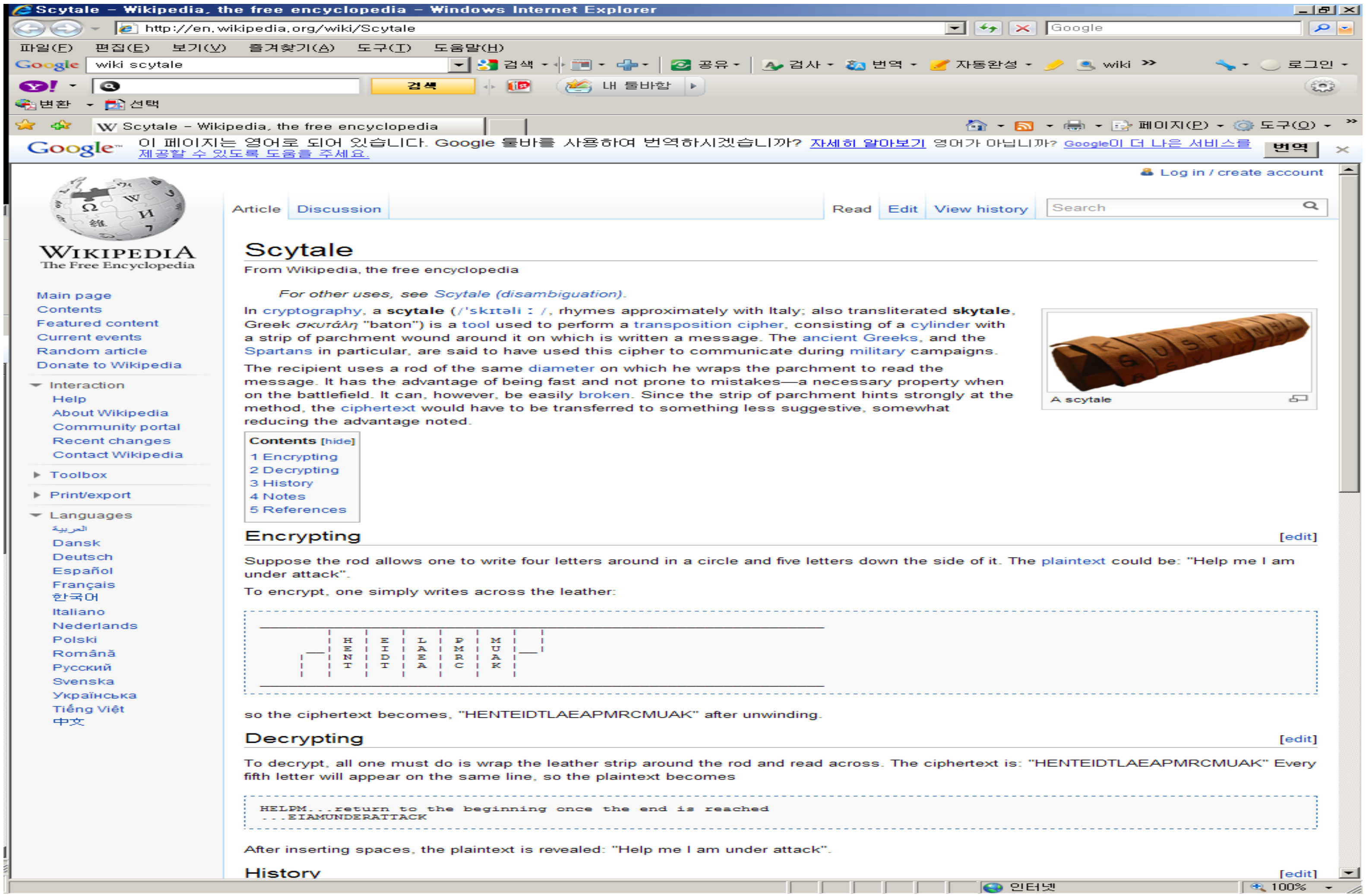
- Transposition ciphers
  - Rotor machines: Enigma, Purple

- Substitution ciphers
  - Caesar cipher
  - Monoalphabetic ciphers
  - Playfair cipher
  - Hill cipher
  - Polyalphabetic ciphers: Vigenere cipher
  - Vernam cipher/One-time pad: perfect cipher

Transposition Ciphers

- Scytale cipher
- Rotor machines
  - Enigma
  - Purple
  - M-209

Scytale (1/2)



Scytale – Wikipedia, the free encyclopedia – Windows Internet Explorer

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

Log in / create account

Article | Discussion | Read | Edit | View history | Search

Scytale

From Wikipedia, the free encyclopedia

For other uses, see Scytale (disambiguation).

In cryptography, a **scytale** (/ˈskɪtəli ː /, rhymes approximately with Italy; also transliterated **skytale**, Greek σκυτάλη "baton") is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment 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 parchment to read the message. It has the advantage of being fast and not prone to mistakes—a necessary property when on the battlefield. It can, however, be easily broken. Since the strip of parchment hints strongly at the method, the ciphertext would have to be transferred to something less suggestive, somewhat reducing the advantage noted.

A scytale

Contents [hide]

Encrypting [edit]

Suppose the rod allows one to write four letters around in a circle and five letters down the side of it. The plaintext could be: "Help me I am under attack".

To encrypt, one simply writes across the leather:

```
       |   |   |   |   |   |  |
     __| H | E | L | P | M |__|
    |  | E | I | A | M | U |
    |  | N | D | E | R | A |
    |  | T | T | A | C | K |
```

so the ciphertext becomes, "HENTEIDTLAEAPMRCMUAK" after unwinding.

Decrypting [edit]

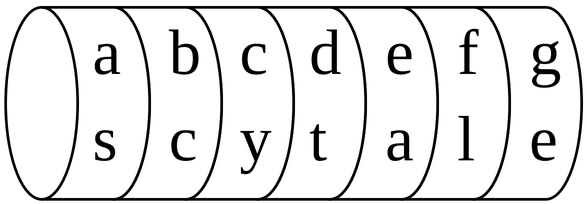
To decrypt, all one must do is wrap the leather strip around the rod and read across. The ciphertext is: "HENTEIDTLAEAPMRCMUAK" Every fifth letter will appear on the same line, so the plaintext becomes

```
HELPM...return to the beginning once the end is reached
...EIAMUNDERATTACK
```

After inserting spaces, the plaintext is revealed: "Help me I am under attack".

History [edit]

Scytale (2/2)



as bc cy dt ea fl ge

Why don't you try to encrypt your message using this cipher ?
What is key?

Transposition Ciphers

- Rearrange characters of plaintext to produce ciphertext
- Frequency distribution of the characters is not changed by encryption

- Example:

Encryption permutation

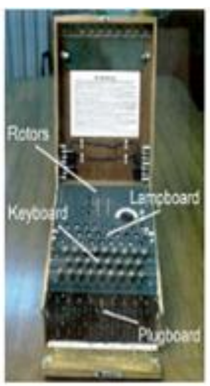
1	2	3	4	5	6
3	5	1	6	4	2

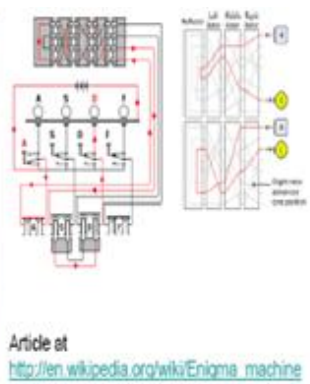
Decryption permutation

1	2	3	4	5	6
3	6	1	5	2	4

plaintext	i n f o r m a t i o n s e c u r i t y x y z a b
ciphertext	F R I M O N I N A S O T U I E T R C Y A Y B Z X

Enigma(German) *vs*. Purple (Japan)@WWII





Do you want to watch video of Engima?

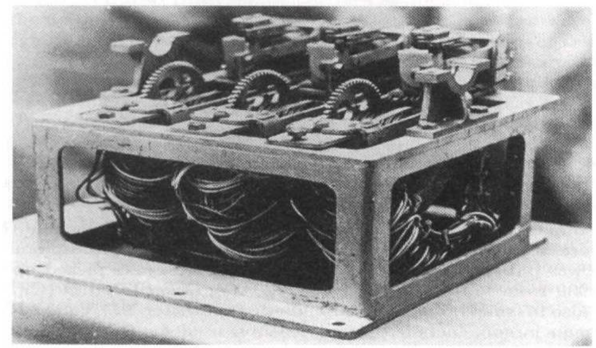


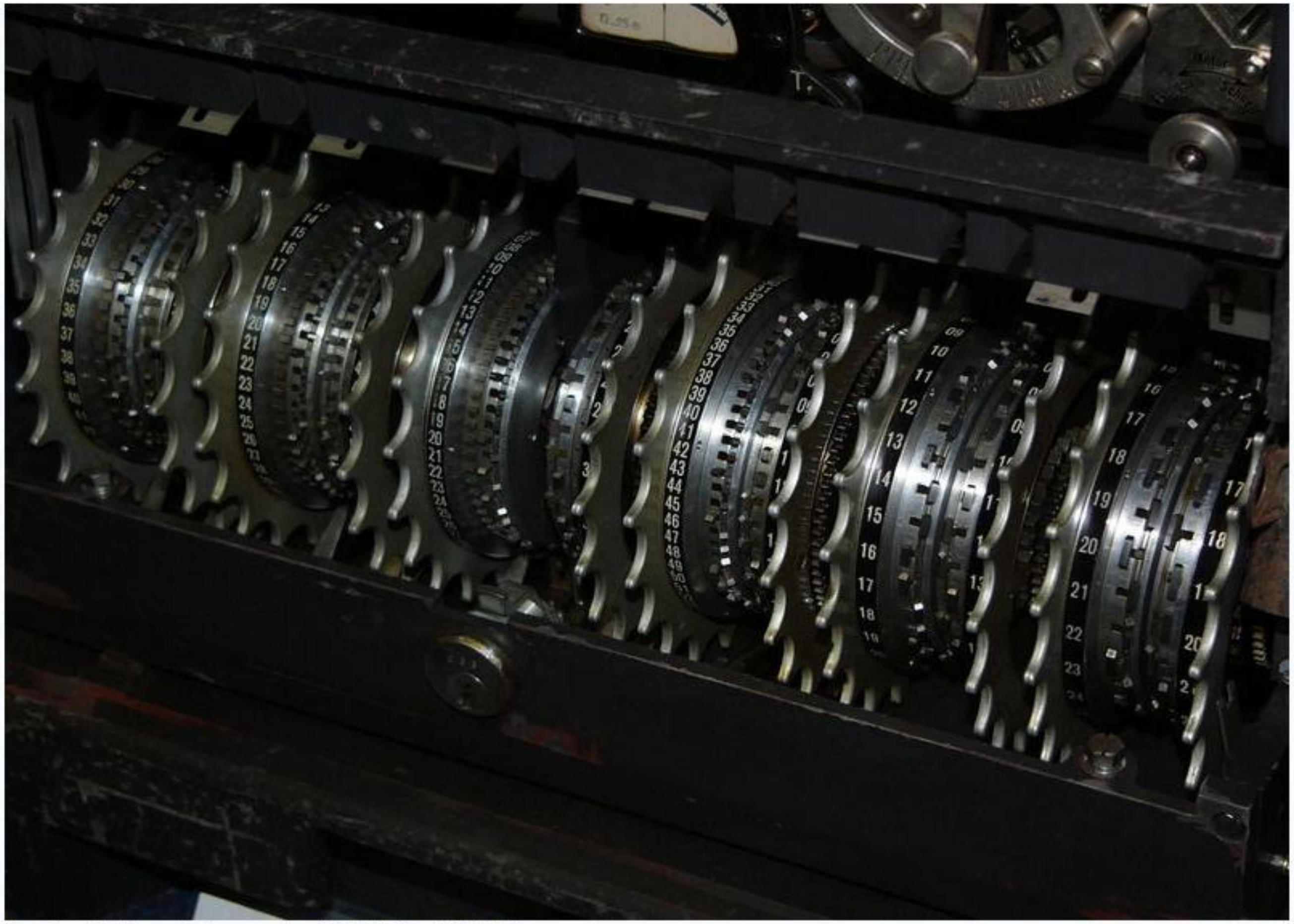
Fig. 68. Stepping switch bank of the Japanese PURPLE machine

US Military classified the success of breaking Purple during WWII.

Kerckhoff's Principle

- **Auguste Kerckhoff, 1883**
  - ***A cryptosystem should be secure even if everything about the system, except the key, is public knowledge*.**
  - **Eric Raymond extends this principle in support of open source software, saying "Any security software design that doesn't assume the enemy possesses the source code is already untrustworthy; therefore, never trust closed source".**
  - **The majority of civilian cryptography makes use of publicly-known algorithms. By contrast, ciphers used to protect classified government or military information are often kept secret . Why ?**

Lorenz SZ42 Cipher Machine



Substitution Ciphers

- Caesar ciphers
- Affine ciphers
- Hill cipher
- Monoalphabetic substitution cipher
- Homophonic substitution cipher
- Polyalphabetic substitution cipher
- Vigenere cipher
- One-time pad

Caesar Cipher (1/2)

Julius Caesar, the Roman emperor
Also known as *shift cipher*

Mathematically assign unique number to each alphabet like below

a	b	c	d	e	f	g	h	i	j	k	...	z
0	1	2	3	4	5	6	7	8	9	10	...	25

Caesar cipher :

Encryption : $C = E_K(M) = M + K \mod 26$
$K = 3$ e.g., $E_K(a) = d$

Decryption : $M = D_K(C) = C - K \mod 26$
$K = 3$

Caesar Cipher (2/2)

Define transformation as:

a	b	c	d	e	f	g	h	i	j	k	…	z
D	E	F	G	H	I	J	K	L	M	N	…	C

Encryption example

i	**n**	**f**	**o**	**r**	**m**	**a**	**t**	**i**	**o**	**n**
L	**Q**	**I**	**R**	**U**	**P**	**D**	**W**	**L**	**R**	**Q**

Weakness

- **Key space is too short – only 26 possible keys**
- **Brute force search**

Example: Break “L ORYH BRX"

Design of Affine Cipher

Generalization of Caesar cipher

Encryption

$$C = E_K(M) = K_1 M + K_2 \bmod 26$$

$$\gcd(K_1, 26) = 1$$

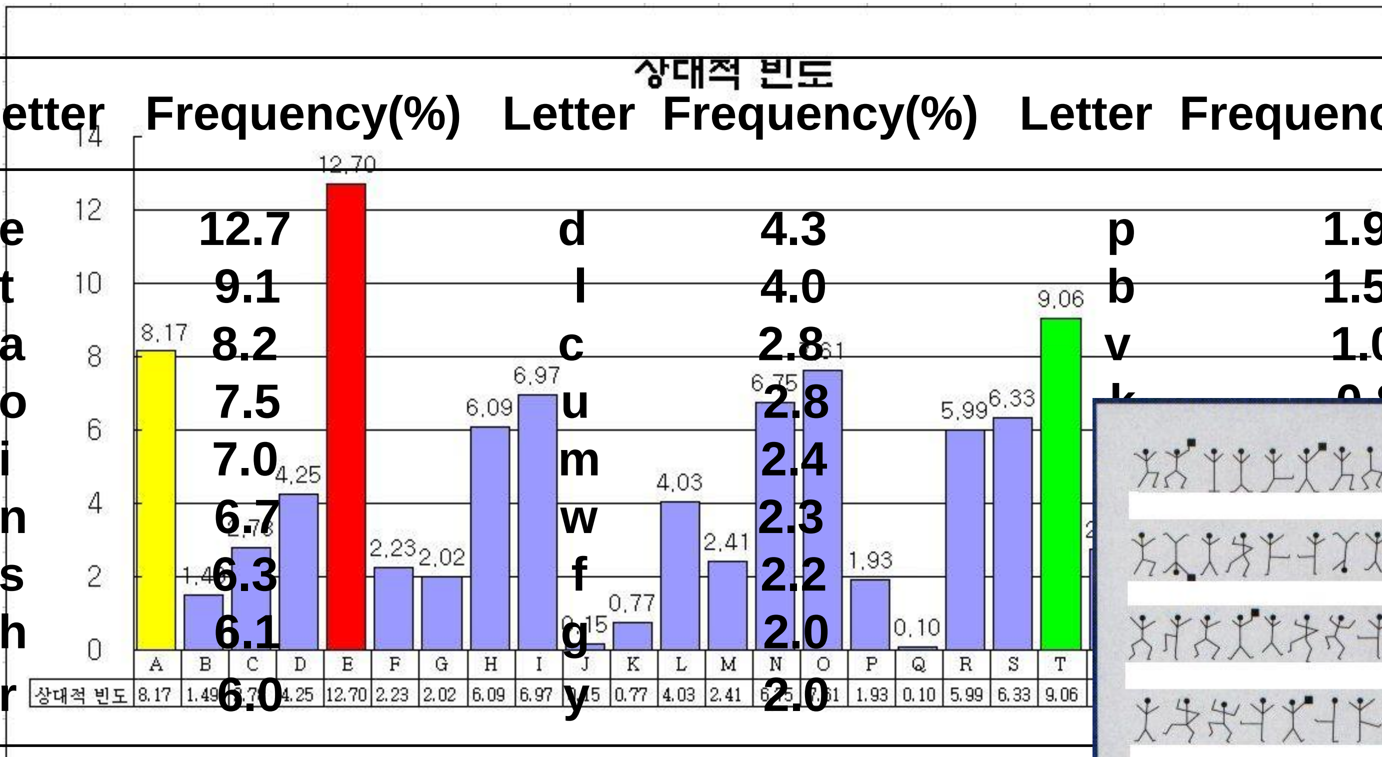
Decryption

$$M = D_K(C) = (C - K_2) K_1^{-1} \bmod 26$$

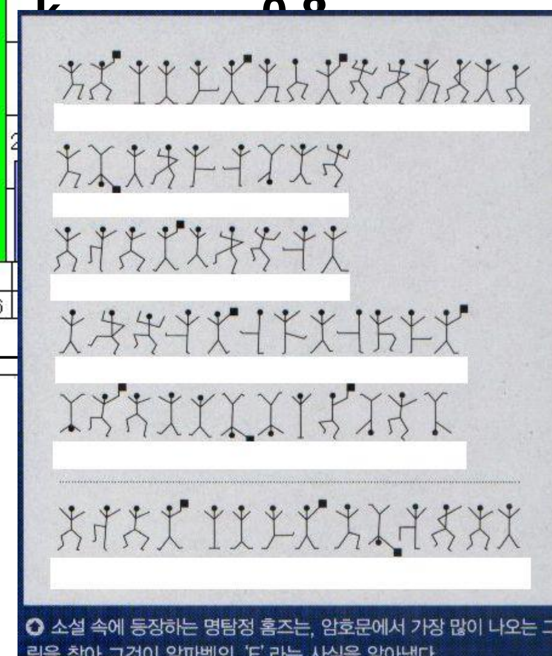
Mathematical Term: Multiplicative inverse

Quiz: How many possible keys in affine cipher?

Breaking of Affine Cipher



Letter	Frequency(%)	Letter	Frequency(%)	Letter	Frequency(%)
e	12.7	d	4.3	p	1.9
t	9.1	l	4.0	b	1.5
a	8.2	c	2.8	v	1.0
o	7.5	u	2.8	k	0.8
i	7.0	m	2.4		
n	6.7	w	2.3		
s	6.3	f	2.2		
h	6.1	g	2.0		
r	6.0	y	2.0		



(1) Pr(e) = 0.12, (2) Pr(t,a,o,i,n,s,h,r) = 0.06 ~0.09
(3) Pr(d,l) = 0.04 (4) Pr(c,u,m,w,f,g,y,p,b) = 0.015~0.023
(5) Pr(v,k,j,x,q,z) <= 0.01

Polyalphabetic Substitution Ciphers

Hide the frequency distribution by making multiple substitutions.
Apply *d* different permutations.

$$m = m_1, m_2, \ldots, m_d, m_{d+1}, m_{d+2}, \ldots, m_{2d}, \ldots$$

$$E_K(m) = \pi_1(m_1), \pi_2(m_2), \ldots, \pi_d(m_d), \pi_1(m_{d+1}), \pi_2(m_{d+2}), \ldots, \pi_d(m_{2d}), \ldots$$

Vigenère Ciphers

- **Multiple Caesar cipher**

$$k = (k_1, k_2, \ldots, k_d), \left|k\right| = 26^d$$

$$c = E_k(m_1, m_2, \ldots, m_d) = (c_1, c_2, \ldots, c_d) = m_i + k_i \bmod 26 \quad \text{for } i = 1, \ldots, d$$

$$m = D_k(c_1, c_2, \ldots, c_d) = (m_1, m_2, \ldots, m_d) = c_i - k_i \bmod 26 \quad \text{for } i = 1, \ldots, d$$

Beauford ciphers (used in US civil war)

$$k = (k_1, k_2, \ldots, k_d), \left|k\right| = 26^d$$

$$c = E_k(m_1, m_2, \ldots, m_d) = (c_1, c_2, \ldots, c_d) = k_i - m_i \bmod 26 \quad \text{for } i = 1, \ldots, d$$

$$m = D_k(c_1, c_2, \ldots, c_d) = (m_1, m_2, \ldots, m_d) = k_i - c_i \bmod 26 \quad \text{for } i = 1, \ldots, d$$

Vigenère Ciphers

Plaintext	t h i s c r y p t o s y s t e m i s n o t s e c u r e
Keyword	S E C U R I T Y S E C U R I T Y S E C U R I T Y S E C
Ciphertext	L L K M T Z R N L S U S J B X K A W P I K A X A M V G

One-time Pad (Vernam cipher)

- **Use a random key as long as the message size and use the key only once**
- **Unbreakable**
  - **Since ciphertext bears no statistical relationship to the plaintext**
  - **Since for any plaintext & any ciphertext there exists a key mapping one to other**
- **Have the problem of safe distribution of key**

Ex) Binary alphabet

P :	o	n	e	t	i
P’:	01101111	01101110	01100101	01110100	01101001
K :	01011100	01010001	11100000	01101001	01111010
C :	00110011	00111111	10000101	00011101	00010011

Perfect Cipher : p (x|y) = p(x) for all $x \in P$, $y \in C$

Impossible COA

One-time pad of Russian origin, small enough to fit in the palm of a hand. The typewritten numbers have figures in Russian style.

Product Ciphers

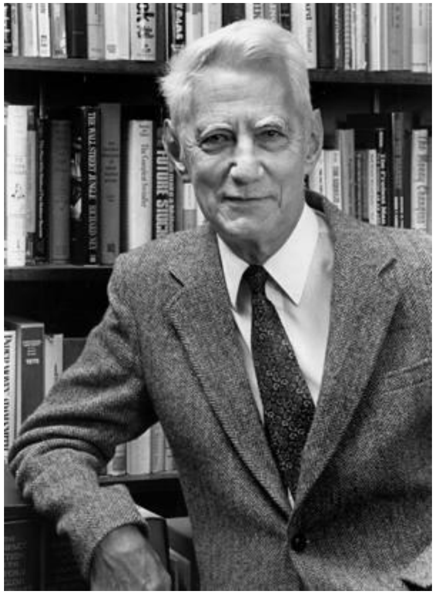
- Shannon
- Mixing Transformation
- SP Network
- Feistel Network

Shannon's Idea (1/2)

- C. Shannon, "*Communication Theory for Secrecy Systems", ***1949**
  - Compose different kind of simple and insecure ciphers to create complex and secure cryptosystems → called "product cipher"
  - Incorporate confusion and diffusion
  - Substitution-Permutation Network

http://www.bell-labs.com/news/2001/february/26/1.html

http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html



Claude Shannon

Shannon's Idea (2/2)

- **Confusion (substitution) :**
  - **The ciphertext statistics should depend on the plaintext statistics in a manner too complicated to be exploited by the enemy cryptanalyst**
  - **Makes relationship between ciphertext and key as complex as possible**

- **Diffusion (permutation) :**
  - **Each digit of the plaintext should influence many digits of the ciphertext, and/or**
  - **Each digit of the secret key should influence many digits of the the ciphertext.**
  - **Dissipates statistical structure of plaintext over bulk of ciphertext**

SP Network (1/2)

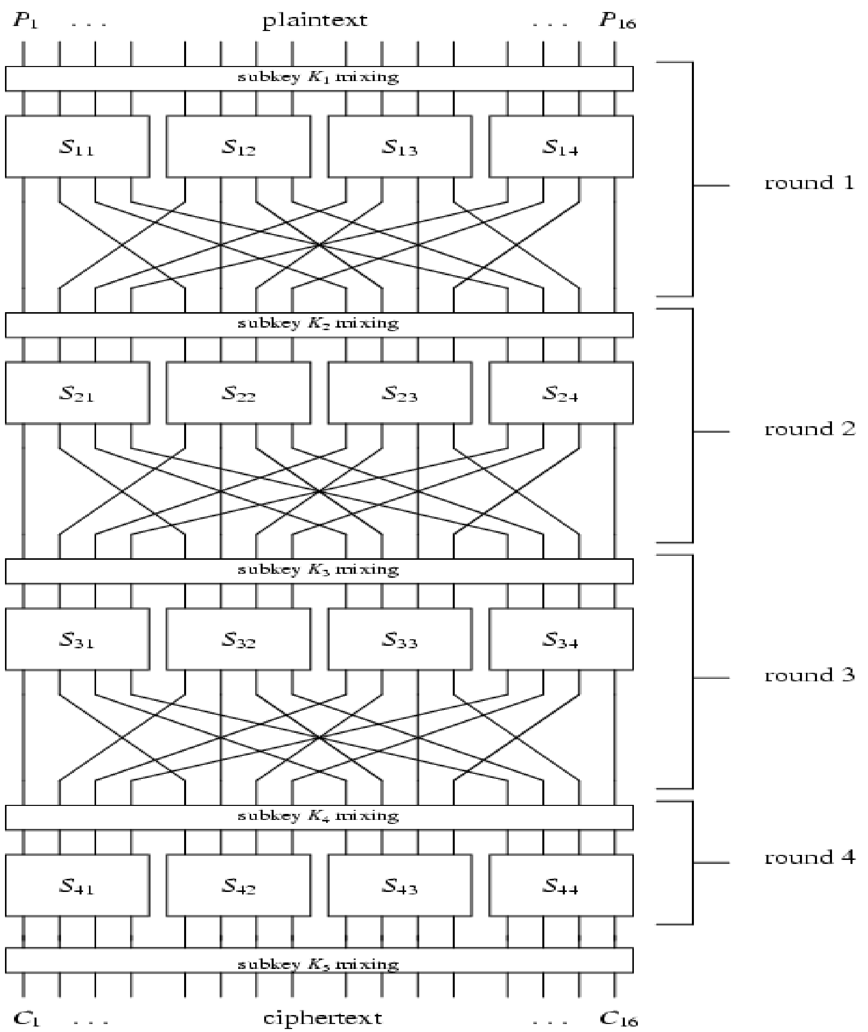
- **Substitution-Permutation network**
  - **Substitution (S-box) : secret key is used**
  - **Permutation (P-box) : no secret key, fixed topology**

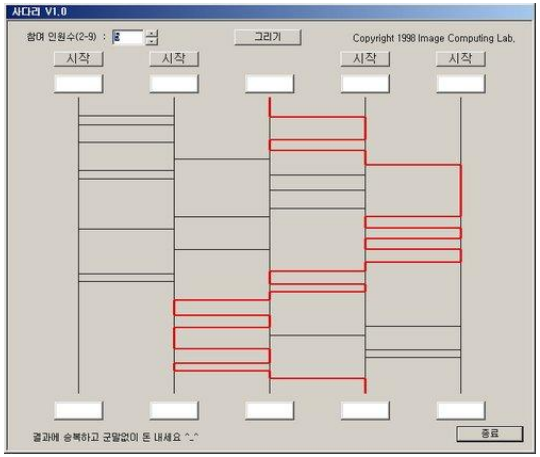
- **Provide Confusion and Diffusion**

- **S-P networks are expected to have**
  - **Avalanche property: a single input bit change should force the complementation of approximately half of the output bits**
  - **Completeness property: each output bit should be a complex function of every input bits**

- **Theoretical basis of modern block ciphers**

SP Network(2/2)





How many rounds?

Using Cryptography

- Before modern crypto : limited usage
  - National security, diplomatic, military purpose
  - Researched by limited people (underground, closed)
  - Communication Security

- Current crypto : widely open, standardize
  - Research and development by anyone
  - Network Security, Computer Security, Cyber Security
  - Protecting your personal data too