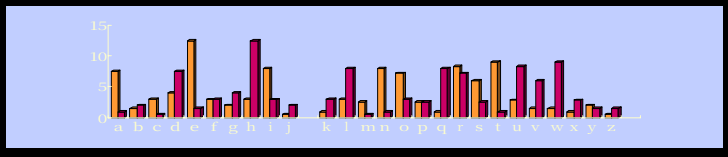
❑ 암호의 역사

- ❑ **고대**
  - Egypt, Greeks, Rome : 상형문자, **Scytale 암호**, **Caesar 암호**
- ❑ **중세 ~ 근대 (19세기 초반)**
  - 고전적 암호시스템 (Classical Cipher)
- ❑ **1/2차 세계대전**
  - ROTOR Machine, **ENIGMA**, COLOSSUS
- ❑ **현대**
  - C. Shannon, **정보이론**(Information Theory)
  - DES, RSA, DSA, etc
  - 국방, 외교, 민간분야
  - IACR(International Association of Cryptographic Research)
  - Crypto, Eurocrypt, Asiacrypt, Auscrypt, 한국통신정보보호학회 (1990)

❑ Mono-alphabetic Substitution Cipher

- ❑ **CAESAR CIPHER**
  - $E_k(m) = (m + k) \bmod n$
- ❑ **MONOALPHABETIC CIPHER**
  - permutations of alphabet
- ❑ **DEDUCTION BASED ON GUESS**
  - WKLV PHVVDJH LV QRW WRR KDUG WR EUHDN
- ❑ **FREQUENCY ANALYSIS**
  - e.g. $E_k(m) = (m + k) \bmod n$,where $k = 3$



❑ Poly-alphabetic Substitution Cipher

- ❑ **MONO. CIPHER의 단점**
  - 암호문에서의 각 문자의 빈도가 평문에 그대로 반영.
- ❑ $M = m_1 m_2 ... m_d\, m_{d+1} ... m_{2d} ...$
  - Mono. $E_k(M) = f(m_1)f(m_2)...$
  - Poly. $E_k(M) = f_1(m_1)f_2(m_2)...f_d(m_d)f_1(m_{d+1})f_2(m_{d+2})...$
  - period = d
- ❑ **VIGENERE CIPHER**
  - $K = k_1 k_2 k_3 ... k_d$,
  - $f_i(m) = (m + k_i) \bmod n$
  - e.g. $d=4$, $K = k_1 k_2 k_3 k_4$
    = BAND

```
M = RENA ISSA NCE
K = BAND BAND BAN
C = SEAD JSFD OCR
```


❑ Poly-alphabetic Substitution Cipher

- ❑ **KASISKI METHOD**
  - period "d"를 결정하는 방법
  - if we know "d", $c_1 c_2 ... c_d\, c_{d+1} ... c_{2d}\, c_{2d+1}$
    $\{c_1, c_{d+1}, c_{2d+1}, ...\}\ \{c_2, c_{d+2}, ...\}\ \{c_3, c_{d+3}, ...\}$
  - (예)

```
K = TUFBN      TUFBN
M = THEREISNOOTHERMATTER
C = MBJS       MBJS
```

  - distance = 10 = 2*5
  - period = 2 or 5
- ❑ **VERNAM CIPHER**
  - $C_i = M_i +_2 K_i$, where $+_2$ is binary EX-OR operation
  - random key generation
  - **One-Time Pad**

❑ Hill Cipher

Hill 암호는 d개의 암호문 문자를 생성하기 위해서 d개의 평문 문자에 대해 선형 변환(linear transformation)을 가하는 다중 대체암호이다. $d = 2$이고 $m = m_1m_2$인 경우에 암호문 $c = E_k(m) = c_1c_2$는 다음과 같이 생성된다.

$$c_1 = (k_{11}m_1 + k_{12}m_2) \bmod n \qquad c_2 = (k_{21}m_1 + k_{22}m_2) \bmod n$$

$k_{11}, k_{12}, k_{21}, k_{22}$는 비밀키가 되고 n은 평문 문자들의 총개수이다. 평문 m과 암호문 c를 열 벡터(column vector)로 표현하면, 즉 $M = (m_1, m_2)$, $C = (c_1, c_2)$이면 위의 식은 아래 식과 같이 표현될 수 있다.

$$E_K(M) = C = KM \bmod n \quad \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \end{bmatrix}$$

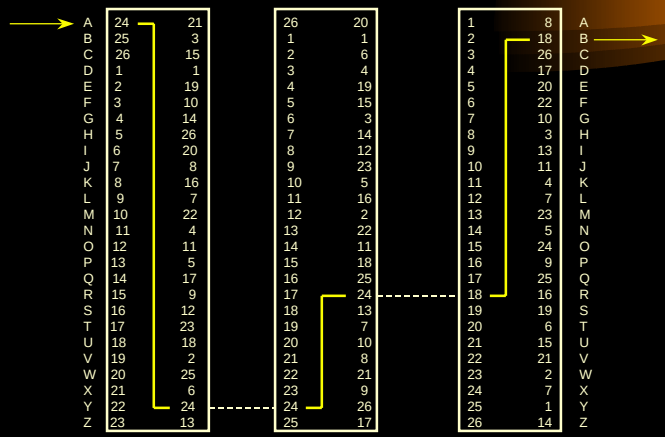
복호화는 다음 식과 같이 역 행렬(inverse matrix) K^{-1}를 통해서 행해진다.

$$D_K(C) = K^{-1}C \bmod n = K^{-1}KM \bmod n = M$$

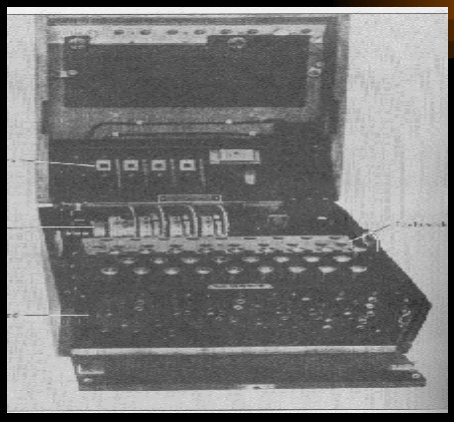
위의 식에서 I가 2×2 항등 행렬일 때 $I = K^{-1}K$가 된다. 하지만 *Hill* 암호는 암호화 함수가 선형의 성질을 지니고 있기 때문에 알려진 평문 공격(known-plaintext attack)을 통해서 쉽게 적용된 비밀키 K를 도출해 낼 수가 있다. 즉, 알려진 평문 M이 가역 행렬(invertible matrix)의 성질을 가지고 있다면 $K = CM^{-1} \bmod n$를 구할 수가 있게 된다.

암호이론과 보안 고전적 암호시스템

❑ ROTOR Machine, ENIGMA



❑ ROTOR Machine, ENIGMA



❑ Transposition Cipher

- ❑ **SIMPLE TRANSPOSITION**
  - permutation
  - e.g. i = (1,2,3,4) M = RENA ISSA NCES
    $f(i)$ = (2,4,1,3) C = EARN SAIS CSNE
  - keyword 사용,
    e.g. COMPUTER = $f(i)$ = (1,4,3,5,8,7,2,6)
- ❑ **NIHILIST CIPHER**
  - M = Y O U R B O O K S
    K = C A N = (2,1,3)
- ❑ **CRYPTANALYSIS**
  - important to know the period "d"
  - 각각의 period 내에서 다시 rearrange

	C	A	N	
C	O	Y	U	
A	B	R	O	
N	K	O	S	→ BROOYUKOS

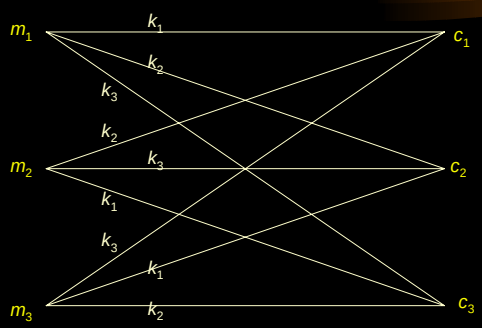
❑ Transposition Cipher

- "LDWEOHETTHSESTRUHTELOBSEDEFEIVNT"

  - *d*=2 LD WE OH ET TH SE ST RU HT EL OB SE DE FE IV NT
  - *d*=3 LDW EOH ETT HSE STR UHT ELO BSE DEF EIV NT
  - *d*=4 LDWE OHET THSE STRU HTEL OBSE DEFE IVNT
  - *d*=5 LDWEO HETTH SESTR UHTEL OBSED EFEIV NT
  - *d*=6 LDWEOH ETTHSE STRUHT ELOBSE DEFEIV NT
    - "THESET" or "TTHESE"
    - The possible permutations are
      (316245) (361245) (516243) (561234)
      (612354) (412356) (621354) (421356)

- "WE HOLD THESE TRUTHS TO BE SELF EVIDENT"

❑ Perfect Secrecy (완전 비밀성)



❑ Perfect Secrecy (완전 비밀성)

key	복호화된 평문
0 :	YMNXHNUMJWNXGWTPJS
1 :	XLMWGMTLIVMWFVSOIR
2 :	WKLVFLSKHULVEURNHQ
3 :	VJKUEKRJGTKUDTQMGP
4 :	UIJTDJQIFSJTCSPLFO
5 :	THISCIPHERISBROKEN
6 :	SGHRBHOGDQHRAQNJDM
.....	.....
25 :	ZNOYIOVNKXOYHXUQKT