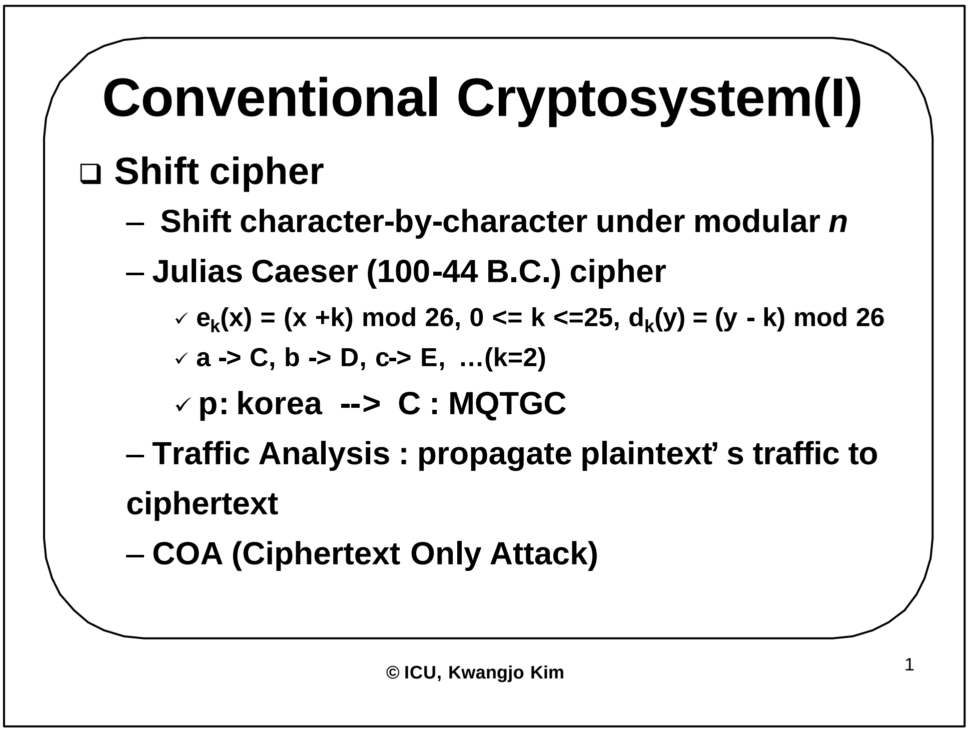
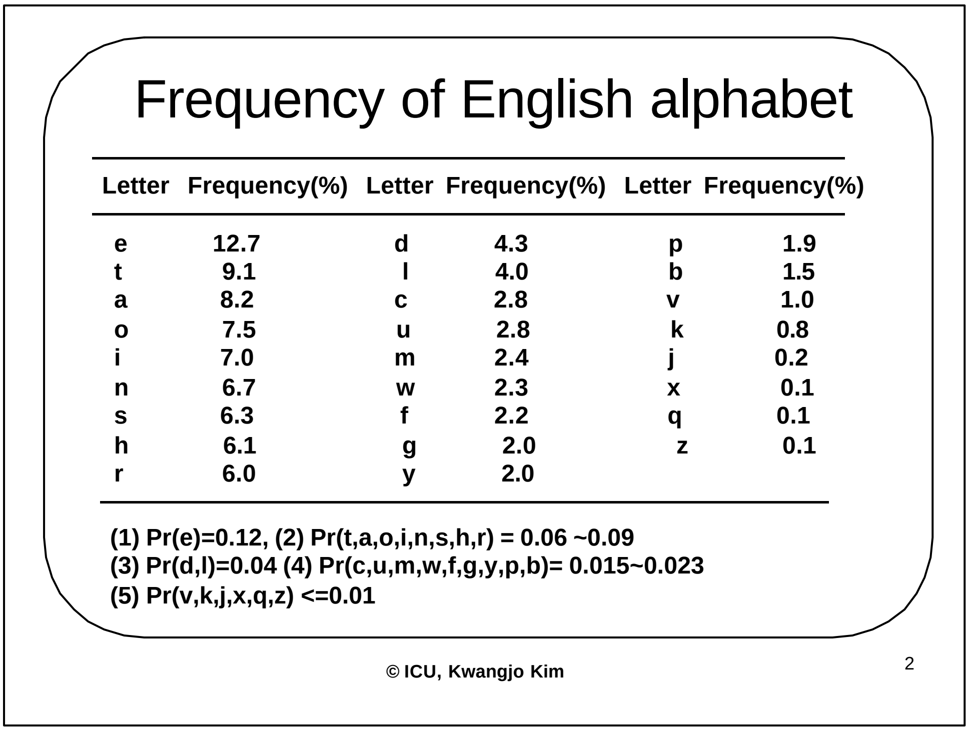


Conventional Cryptosystem(I)

❑ **Shift cipher**

- – Shift character-by-character under modular *n*
- – Julias Caeser (100-44 B.C.) cipher
  - ✓ $e_k(x) = (x + k) \bmod 26, 0 <= k <= 25, d_k(y) = (y - k) \bmod 26$
  - ✓ a -> C, b -> D, c-> E, …(k=2)
  - ✓ p: korea --> C : MQTGC
- – Traffic Analysis : propagate plaintext’ s traffic to ciphertext
- – COA (Ciphertext Only Attack)



Frequency of English alphabet

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	j	0.2
n	6.7	w	2.3	x	0.1
s	6.3	f	2.2	q	0.1
h	6.1	g	2.0	z	0.1
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

Mathematical Background(I)

- ❑ (Def) a =b mod m if m | b-a
  - – a is congruent to b modulo m
- ❑ Z_m = {0,1, ..,m}, (+, x)
  1. + is closed, for any a,bÎ Z_m a+b Î Z_m
  2. + is commutative, for a,b Î Z_m , a+b = b+a
  3. + is associative, for a,b,c Î Z_m , (a+b)+c = a +(b+c)
  4. 0 is additive identity , for a Î Z_m , a+0=0+a=a
  5. Additive inverse of any a Î Z_m is m-a, a+(m-a)=(m-a)+a=0
  6. x is closed, for any a,bÎ Z_m ab Î Z_m
  7. x is commutative, for any a,b Î Z_m ,ab = ba
  8. x is associative, for any a,b,c Î Z_m , (ab)c = a(bc)
  9. 1 is multiplicative identity, for any a Î Z_m , a x 1 =1 x a = a
  10. x distributes over +, for any a,b,c Î Z_m , (a+b)c=(ac)+(bc), a(b+c)=(ab) + (ac)

© ICU, Kwangjo Kim

3

Mathematical Background(II)

- ❑ Algebraic structure
  - – P1,P3-P5 : Group, (Z_m, +)
    - ◆ and +P2 : commutative (Abelian) group
  - – P1-P10 : Ring, (Z_m ,+, x), Ex : Z, polynomial
  - – Commutative ring in which all non-zero elements have multiplicative inverses : Field, Ex : ($Z_p^{*,}$ +,x)
- ❑ Number theory
  - – (Th) ax = b mod m has an unique solution x Î Z_m for every b Î Z_m iff gcd(a,m)=1.
  - – (Def) Euler phi-function j (m) : number of relative prime to m. If m=$P_{i=1}^{n}$ $p_i^{e_i}$, j (m)=$P_{i=1}^{n}$($p_i^{e_i}$ - $p_i^{e_i -1)}$
  - – (Def) a Î Z_m, multiplicative inverse of a is a^{-1} Î Z_m s.t. aa^{-1}=a^{-1}a=1 mod m

© ICU, Kwangjo Kim

4

Conventional Cryptosystem(II)

❑Substitution cipher

– 1 to 1 mapping random of a word

– single /multi characters

– single/multi/random table

– Ex) Substitution table

	0	1	2	3	4	5	6	7	8	9
2	ㄱ	ㄴ	ㄷ	ㄹ	ㅁ	ㅂ	ㅅ	ㅇ	ㅈ	ㅊ
3	ㅋ	ㅌ	ㅍ	ㅎ	ㅏ	ㅑ	ㅓ	ㅕ	ㅗ	ㅛ
4	ㅜ	ㅠ	ㅡ	ㅣ						

P : 대한민국 -> C : 22 34 43 33 34 21 24 43 21 20 40 20

– COA

Frequency of English Words

Word	Frequency(%)	Word	Frequency(%)	Word	Frequency(%)
the	6.41	a	2.092	i	0.945
of	4.028	in	1.778	it	0.930
and	3.15	that	1.244	for	0.770
to	2.367	is	1.034	as	0.764

Conventional Cryptosystem(III)

❑ Affine Cipher

- K = {(a,b) Î Z_{26} x Z_{26} : gcd(a,26)=1}
- $e_k(x)$ = ax +b mod 26
- $d_k(y) = a^{-1}(y\text{-}b)$ mod 26
- Ex : $e_K(x)$ = 7x + 3, $d_K(y)$ = 15(y-3) = 15y -19
- Propagate of Plaintext' s Traffic
- COA
- a variation of Substitution cipher

Conventional Cryptosystem(IV)

❑ Vigenere Cipher

- Improve weakness of Ceaser cipher
- Use different Shift per each word
- Ex) repetition use of key word
  - ✓ P : vig ene res cip her
  - ✓ K : key key key key key
  - ✓ C : FME ORC BIQ MMN RIP
- Cryptanalysis (Kasiski, 1863) : Index of Coincidence
  - ✓ Step 1: search of a length of a key word
  - ✓ Step 2: search a key

Conventional Cryptosystem(V)

❑ **Hill Cipher**

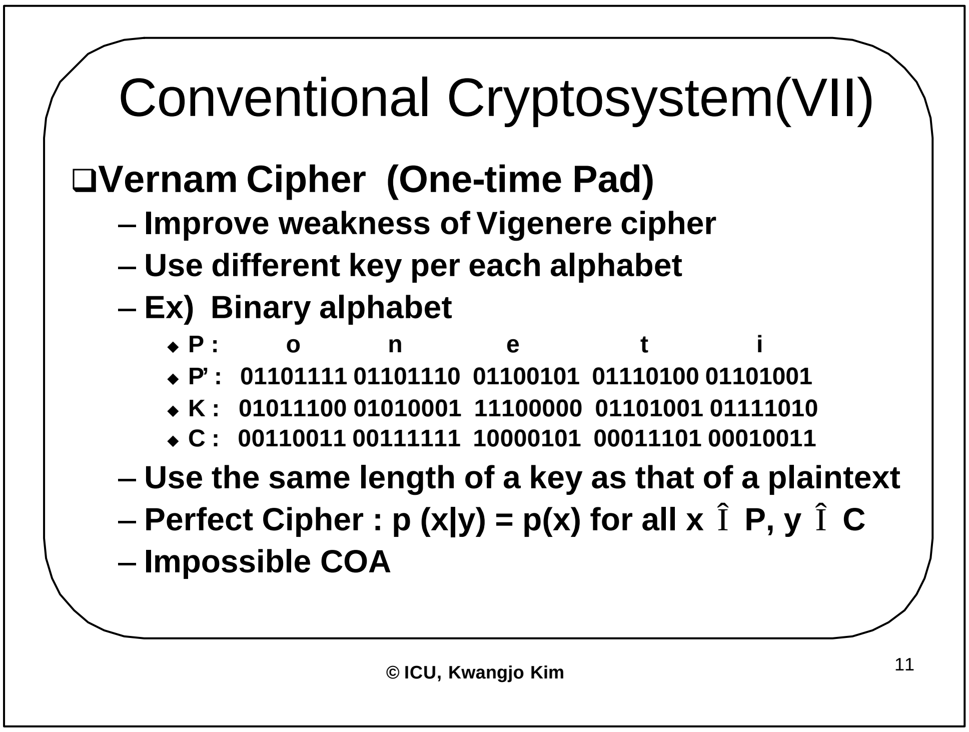
$e_K(x)$: $(y_1,y_2, ..,y_m)$ =$(x_1,x_2, ..,x_m)$ K where K is *m* x *m* matrix and gcd(det K, 26) =1

- **$d_K(y)$ = y K^{-1}**
- **(Ex) K = (11 8) K^{-1} = (7 18)**
  (3 7), (23 11)
  - ✓ **x : july, (j,u)= (9,20), (l,y) = (11,24)**
  - ✓ **(9,20) K = (3,4) = (D,E), (11,24) K = (11,22) = (L,W)**
- **KPA**

Conventional Cryptosystem(VI)

❑**Permutation (or Transposition) cipher**

- **m=6, p = (3,5,1,6,4,2), p^{-1}= (3,6,1,5,2,4)**
- **(Ex)**
  x= shesellsseashellsbytheseashore
  x= shesel|lsseas|hellsb|ythese|ashore
  y= EESLSH|SALSES|LSHBLE|HSYEET|HRAEOS
- **special case of Hill cipher**



Conventional Cryptosystem(VII)

❑Vernam Cipher (One-time Pad)

- Improve weakness of Vigenere cipher
- Use different key per each alphabet
- 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
- Use the same length of a key as that of a plaintext
- Perfect Cipher : p (x|y) = p(x) for all x Î P, y Î C
- Impossible COA