

CSS322 – Classical Encryption Techniques Notes

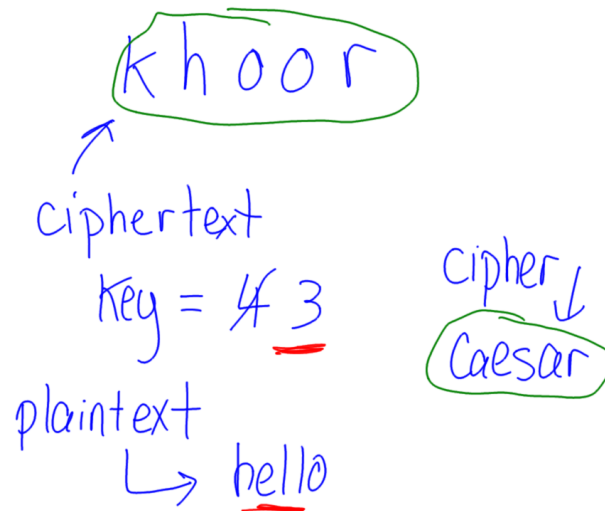


Figure 1: Caesar cipher decryption; Lecture 01

$C = abmdm$ Caesar

$k=0$: $P = abmdm$ X
(a)

$k=1$ (b) : $P = zalc l$ X

$k=2$ (c) : $P = yzkbk$ X

↓

$k=8$ (i) :

↓

$k=25$ (z) : P $P = (C - k) \bmod 26$

C	a	b	m	d	m
	0	1	12	3	12
$k=i, 8$	8	8	8	8	8
	-8	-7	4	-5	4
	18	19	4	21	4
	s	t	e	v	e
	$\underline{-1} \times 26 + \underline{18} = -8$				
	+ve				

Figure 2: Attack on Caesar cipher; Lecture 02

$P: a b c d e \dots x y z$

$C: L H E R I \dots T A Q$

$26 \times 25 \times 24 \times 23 \times 22 \times \dots \times 3 \times 2 \times 1 = 26!$

~~a b~~

L L

$C = L$ $P = ?$

Figure 3: Key length of a monoalphabetic cipher; Lecture 02

keyword = thailand P = hello

t	h	a	i	l
n	d	b	c	e
f	g	k	m	o
p	q	r	s	u
v	w	x	y	z

he → LD lx → AZ lo → EU
 C = LDAZEU

P = helxlo
 C = LDAZEU

Figure 4: Encryption with Playfair cipher; Lecture 03

i	n
8	13
5	i
18	8
A	V
0	21

Figure 5: Encryption with Vigenere cipher; Lecture 03

ieeenoenpitan
 nrtcogsdpcis
 3 tnthliaalao

ieeenoenpitanrtcogsdpcistnthl
 iaalao

Figure 6: Rail Fence Transposition cipher; Lecture 03

3 1 5 6 2 4
 s e c u r i
 t y a n d c
 r y p t o g
 r a p h y x
EYVA RDOYSTRR ICGXCAPPUNTH

Figure 7: Rows Columns Transposition cipher; Lecture 03

$$C_i = (P_i + k_i) \pmod{26} \quad \text{English lowercase}$$

$$P = p_1, p_2, p_3 \dots p_i \dots p_n$$

$$K = k_1, k_2, k_3 \dots k_i \dots k_n$$

$$C = c_1, c_2, c_3 \dots c_i \dots c_n$$

$$C_i = (P_i + k_i) \pmod{2} \quad \text{Binary}$$

P_i	k_i	$C_i = P_i \oplus K_i$
0	0	0
1	0	1
0	1	1
1	1	0

OTP : $C = P \oplus K$

Figure 8: One Time Pad in Binary; Lecture 04

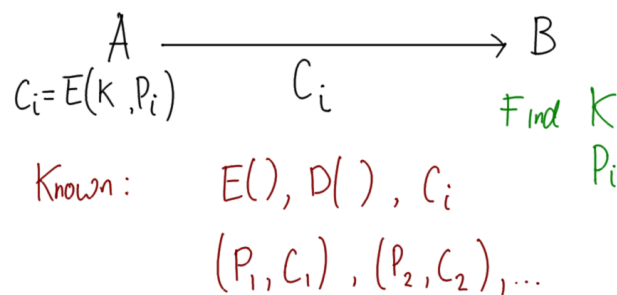


Figure 9: Example of Known Plaintext; Lecture 04