

CSS441 – Classical Encryption Techniques Notes

Ciphertext : p r q g d b
 Cipher : Caesar Key = 3 or d
 Plaintext : m o n d a y

Figure 1: Caesar Cipher Example; Lecture 01

Ciphertext : a b m d m
 K=0, a P= a b m d m x
 K=1, b P= z a l c l x
 K=2, c P= x
 ⋮
 K=8, i P= s t e v e ✓
 Actual : 9 decrypts
 Best : 1 decrypt
 Worst : 26 decrypts
 Average : 13 decrypts

Figure 2: Brute Force Attack on Caesar Cipher; Lecture 01

$$\begin{array}{r}
 \text{Ciphertext : } \quad a \quad b \quad m \quad d \quad m \\
 \quad \quad \quad C \quad 0 \quad 1 \quad 12 \quad 3 \quad 12 \\
 \text{Key} = 8, i \quad k \quad 8 \quad 8 \quad 8 \quad 8 \quad 8 \\
 \quad \quad \quad C-k \quad -8 \quad -7 \quad 4 \quad -5 \quad 4 \\
 (C-k) \bmod 26 \quad 18 \quad 19 \quad 4 \quad 21 \quad 4 \\
 \quad \quad \quad \quad \quad s \quad t \quad e \quad v \quad e \\
 \underline{-1} \times 26 + \frac{18}{+ve} = -8
 \end{array}$$

Figure 3: Caesar Cipher with Equation; Lecture 01

$$\begin{array}{r}
 \text{User A} \qquad \qquad \qquad \text{User B} \\
 a b c d e \dots x y z \\
 L H E R I \quad T A G \\
 26 \times 25 \times 24 \times 23 \times 22 \times \dots \times 3 \times 2 \times 1 = 26! \\
 P = \text{dead} \qquad \text{Average brute force} \\
 C = \text{RILR} \qquad \frac{26!}{2} \approx 2 \times 10^{26} \\
 \text{Try } 10^{12} \text{ decrypts/sec} : 63941 \text{ centuries} \\
 \qquad \qquad \qquad \times 10^6 \qquad \qquad \qquad 6.3 \text{ years}
 \end{array}$$

Figure 4: Brute Force Attack on Monoalphabetic Cipher; Lecture 01

Keyword = thailand P = hello

t	h	a	i	l	he → LD
n	d	b	c	e	lx → AZ
f	g	k	m	o	lo → EU
p	q	r	s	u	C = LDAZEU
v	w	x	y	z	

Figure 5: Playfair Cipher Example; Lecture 03

P: i n t e r
 8 13 19
 K: s i r i n
 18 8 17
 P+K: 26 21 36
 (P+K) mod 26: 0 21 10
 C: A V K

Figure 6: Vigenere Cipher Example; Lecture 03

i e e n o e n p i t n
 n r t c o g s d p c i s
 t n t h l i a a l a o

C = ieeenoenpithnnrtcogsdpcistnthliadao

k=2 isedepecn
 k=3 internet

Figure 7: Rail Fence Cipher Example; 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	← padding

C = E M P A R D O Y S T R R I C G X C A P P O N T H

Figure 8: Rows Columns Cipher Example; Lecture 03