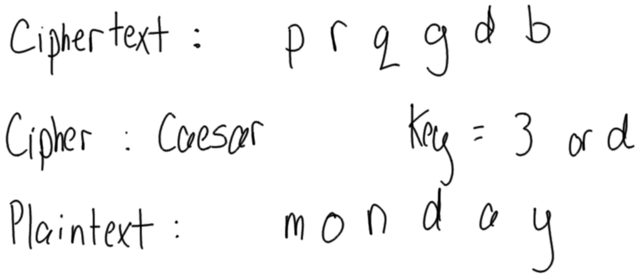
CSS441 – Classical Encryption Techniques Notes

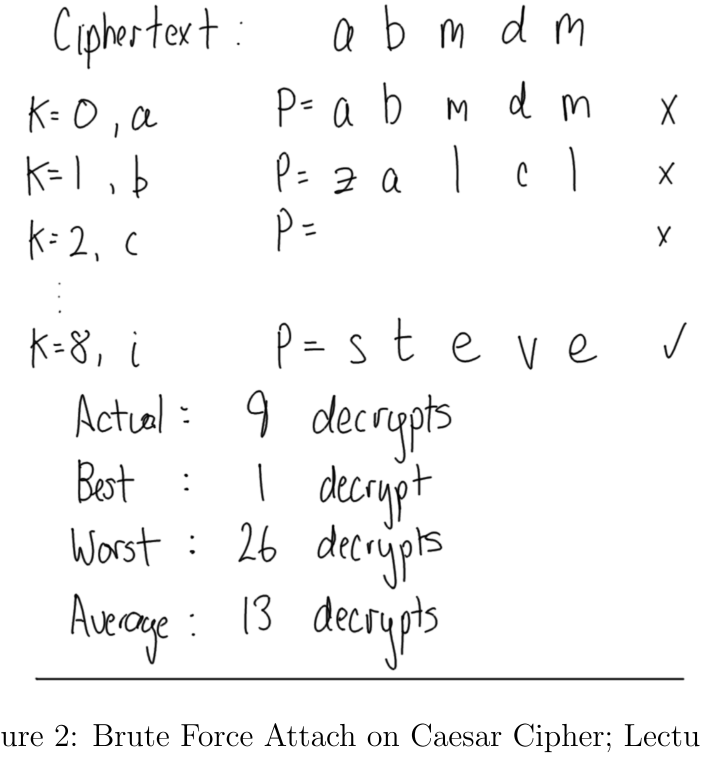


Ciphertext : p r q g d b

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 ✓

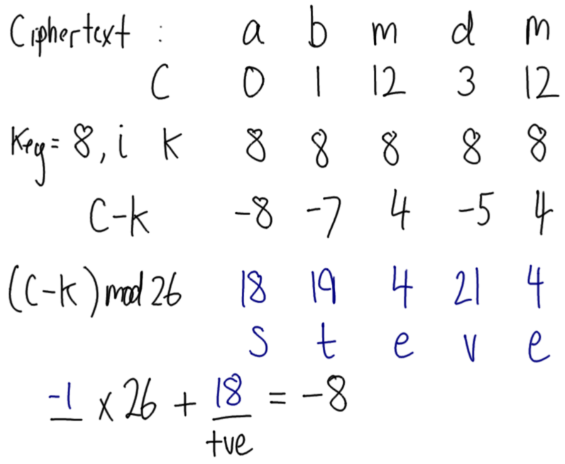
Actual : 9 decrypts

Best : 1 decrypt

Worst : 26 decrypts

Average : 13 decrypts

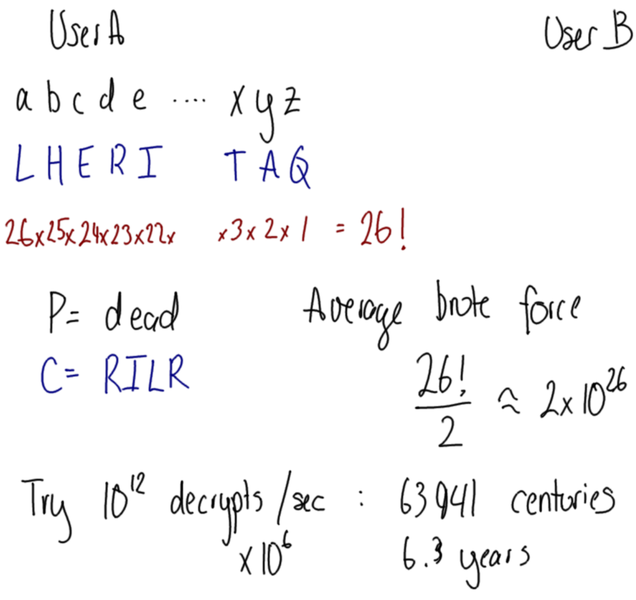
Figure 2: Brute Force Attach on Caesar Cipher; Lecture 01



Ciphertext :	a	b	m	d	m
C	0	1	12	3	12
Key = 8, i k	8	8	8	8	8
C-k	-8	-7	4	-5	4
(C-k) mod 26	18	19	4	21	4
	s	t	e	v	e

$$\underline{-1} \times 26 + \underset{+ve}{\underline{18}} = -8$$

Figure 3: Caesar Cipher with Equation; Lecture 01



User A User B

a b c d e .... x y z

L H E R I T A Q

$26\times25\times24\times23\times22\times \quad \times3\times2\times1 = 26!$

P= dead Average brute force

C= RILR $\frac{26!}{2} \approx 2\times10^{26}$

Try 10^{12} decrypts/sec : 63941 centuries

$\times10^{6}$ 6.3 years

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

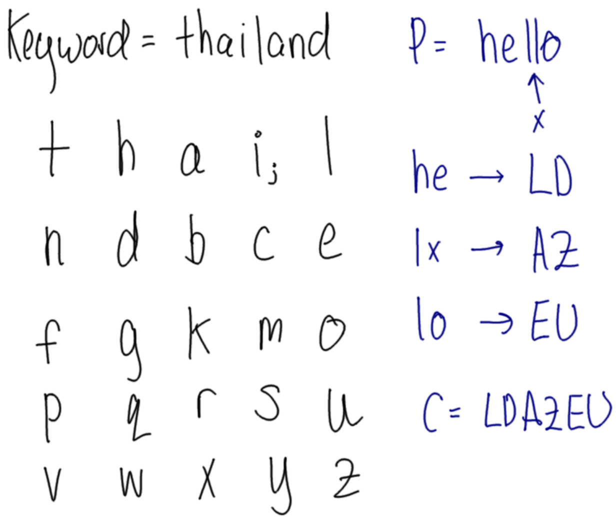


Figure 5: Playfair Cipher Example; Lecture 03

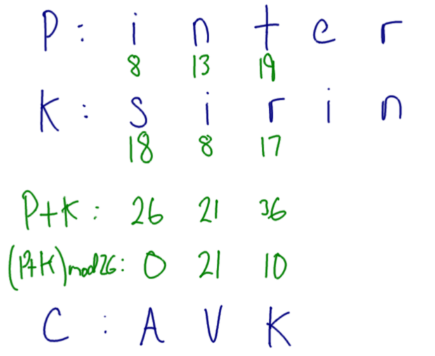


Figure 6: Vigenere Cipher Example; Lecture 03

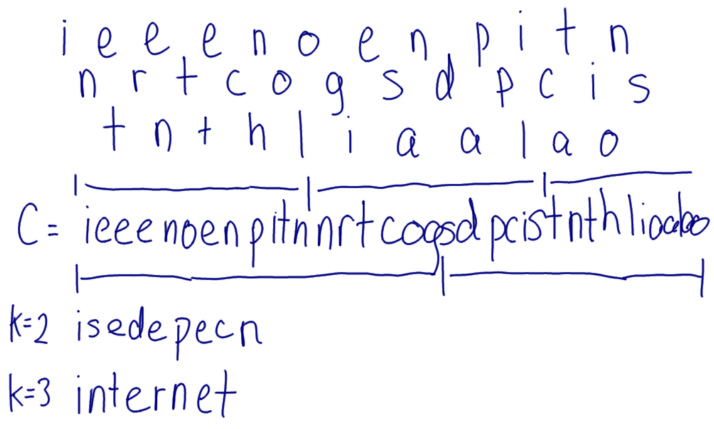
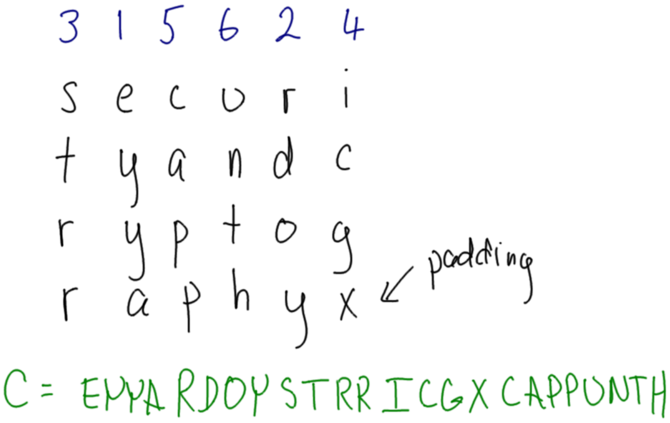


Figure 7: Rail Fence Cipher Example; Lecture 03



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

C = EYYA RDOY STRR ICGX CAPPUNTH

Figure 8: Rows Columns Cipher Example; Lecture 03