Cryptography Tutorial

Prepared by

Dr. T. Sree Sharmila

Tutorial 1 Solutions

1. `Iwxhxhpctphnidqgtpzhnhitb`

is encrypted with classical Caesar - the plaintext messages consist of small-case letters only and no other signs or blanks exist in the message. Find out the **encryption keys** used to encrypt the two messages (different keys may have been used for the two messages) and the text that can be read in those files.

Solutions:

- File 1 contains the text "thisisaneasytobreaksystem" encrypted with Caesar with encryption key 12

2. L FDPH L VDZ L FRQTXHUHG decode the message using by Julius Caesar decryption, and find out the key.

I CAME I SAW I CONGUERED

The mapping is as follows:

Plain Text: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher Text: DEFGHIJKLMNOPQRSTUVWXYZABC

3. Encrypt the following message using playfair cipher.
Plaintext: targetatnewyork
Key : simple

Key construction:

S	I/J	M	P	L
E	A	B	C	D
F	G	H	K	N
O	Q	R	T	U
V	W	X	Y	Z

Plaintext grouping:
Hint: add x as padding if it's not grouped with last letter.
ta rg et at ne wy or kx

4. Encrypt the following message using vigenere cipher.

Plaintext THISPROCESSCANALSOBEEXPRESSED
Keyword CIPHER

Plaintext	THISPROCESSCANALSOBEEXPRESSED
Keyword	CIPHERCIPHERCIPHERCIPHERCIPHE
Cipher text	VPXZTIQKTZWTCVPSWFDMTETIGAHLH

Encode the following messages.

(1) Caesar cipher with shift +3
hello tom
khoorwrp

(2) Caesar cipher with shift +12
klondike nuggets
wxazpuwqzgssqfe

Decode the following messages.

(3) Caesar cipher with shift +5
ltytufwnx
go to Paris

(4) Caesar cipher with shift +21 = −5
adiyevhznwjiy
find James Bond

(5) Caesar cipher with shift +24 = −2
ncwrmlkyllgle
Peyton Manning

(6) (a) Caesar cipher with shift +23 = −3
aliip
dolls

(b) Caesar cipher with shift +4
aliip
wheel

(7) Caesar cipher using frequency analysis. Shift is +6
kbkxeutk
everyone

(8) Caesar cipher using frequency analysis. Shift is +11
espntaspcsldmppymczvpy
the cipher has been broken

(9) Caesar cipher using frequency analysis. Shift is +6
kgyezuhxkgq
easy to break