Cryptography Tutorial

Prepared by

Dr. T. Sree Sharmila

CRYPTOGRAPHY TUTORIAL

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.

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

3. Encrypt the following message using playfair cipher.

Plaintext: targetatnewyork
Key : simple

4. Encrypt the following message using vigenere cipher.

Plaintext THISPROCESSCANALSOBEEXPRESSED
Keyword CIPHER

Encode the following messages.

(1) Caesar cipher with shift +3
hello tom

(2) Caesar cipher with shift +12
klondike nuggets

Decode the following messages.

(3) Caesar cipher with shift +5
ltytufwnx

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

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

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

(b) Caesar cipher with shift +4
aliip

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

(8) Caesar cipher using frequency analysis. Shift is espntaspcsldmppymczvpy

(9) Caesar cipher using frequency analysis. Shift is kgyezuhxkgq

(10) Caesar cipher using frequency analysis. Shift is xskixxsxlisxlivwmhi

(11) Caesar cipher using frequency analysis. Shift is ----------

espntaspcsldmppymczvpy
the cipher has been broken (e)

(12) Caesar cipher using frequency analysis. Shift is ----------

ncwrmlkyllgleylbhmckmlryly
Peyton Manning and Joe Montana (n)