

1- Write passive security attacks with possible scenarios.

+10p

2-

a) What is perfect secrecy

+15p

b) write in terms of the key, cipher and plain lengths, and write two strict conditions:+20p

c) Explain if any, realizable?

+10p

3-

a) For the given hill cipher, $K = \begin{bmatrix} 13 & 7 \\ 26 & 18 \end{bmatrix}$,

Encrypt the message given below.

+10p

And decrypt enciphered message.

+15p

Message: "floating under the waves of the gravitational forces in fractal time"

b) What is the vulnerability of hill cipher, does higher the key dimensions provide stronger key? +10

4- Does the set of residue classes modulo 3 form a group

a. with respect to addition? +8

b. with respect to multiplication? +12