

CNS M1L3

# Classical Encryption Techniques

Introduction:  
Some Simple Cryptosystems

# Outline

- [1] Introduction: Some Simple Cryptosystems
  - <1> The Shift Cipher
  - <2> The Substitution Cipher
  - <3> The Affine Cipher
  - <4> The Vigenère Cipher
  - <5> The Hill Cipher
  - <6> The Permutation Cipher
  - <7> Stream Ciphers
- [2] Cryptanalysis
  - <1> Cryptanalysis of the Affine Cipher
  - <2> Cryptanalysis of the Substitution Cipher
  - <3> Cryptanalysis of the Vigenère Cipher
  - <4> Cryptanalysis of the Hill Cipher
  - <5> Cryptanalysis of the LFSR Stream Cipher

# Introduction:

## Some Simple Cryptosystems

- <4> Vigenère Cipher ( poly alphabetic substitution cipher)
  - Cryptosystem 1.4: Vigenère Cipher
    - $m$ : a positive integer
    - $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$
    - For a key  $K = (k_1, k_2, \dots, k_m)$ 
      - $e_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$
      - $d_K(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$

# Example Vigenere Cipher

$$E_i = (P_i + k_i) \bmod 26, D_i = (E_i - K_i) \bmod 26$$

**Key:** venus;      **Plain text:** college vasai,

**Cipher Text:** XSYFWBIIOKVM

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

PlainText	C	O	L	L	E	G	E	V	A	S	A	I
P value	2	14	11	11	4	6	4	21	0	18	0	8
Key	V	E	N	U	S	V	E	N	U	S	V	E
K value	21	4	13	20	18	21	4	13	14	18	21	4
C value	23	18	24	5	22	1	8	8	14	10	21	12
Cipher	X	S	Y	F	W	B	I	I	O	K	V	M

# Vigenère Square

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

Plaintext-  
R, Key-C

# Introduction:

## Some Simple Cryptosystems

- e.g.: Suppose  $m=4$  and  $K=(2,8,15,7)$ 
  - Plaintext: student, **technology**
  - Ciphertext: UBJKGVI

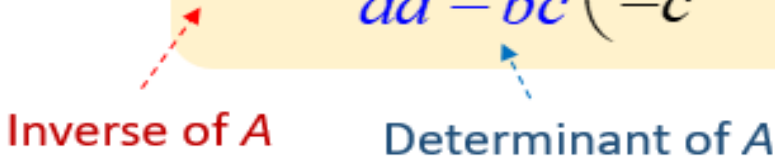
A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

plaintext	s	t	u	d	e	n	t
	18	19	20	3	4	13	19
+K	2	8	15	7	2	8	15
ciphertext	20	1	9	10	6	21	8

# Matrix operations

## Inverse of 2x2 Matrix

If  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  then  $A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$



Inverse of A      Determinant of A

$$AA^{-1} = A^{-1}A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \quad \text{Identity Matrix}$$

If  $ad - bc = 0$  then  $A^{-1}$  cannot be found and  $A$  is a **singular matrix**.

If  $ad - bc \neq 0$  then  $A^{-1}$  can be found and  $A$  is a **non-singular matrix**.



## How to multiply matrices

$$\begin{bmatrix} -2 & 1 \\ 0 & 4 \end{bmatrix} \times \begin{bmatrix} 6 & 5 \\ -7 & 1 \end{bmatrix} = \begin{bmatrix} -2 \times 6 + 1 \times -7 & -2 \times 5 + 1 \times 1 \\ 0 \times 6 + 4 \times -7 & 0 \times 5 + 4 \times 1 \end{bmatrix}$$

$$= \begin{bmatrix} -19 & -9 \\ -28 & 4 \end{bmatrix}$$

# Introduction:

## Some Simple Cryptosystems

- <5> Hill Cipher
  - Definition 1.5: Suppose  $A=(a_{i,j})$  is an  $m \times m$  matrix
    - $A_{i,j}$ : the matrix obtained from  $A$  by deleting the  $i$ th row and the  $j$ th column
    - $\det A$ : the determinant of  $A$ 
      - $m=1$ :  $\det A=a_{1,1}$      $\det A = \sum_{j=1}^m (-1)^{i+j} a_{i,j} \det A_{i,j}$
      - $m>1$ : for any fixed  $i$

# Introduction:

## Some Simple Cryptosystems

- Theorem 1.3: Suppose  $K=(k_{i,j})$  is an  $m \times m$  invertible matrix over  $\mathbb{Z}_n$

- $K^{-1}=(\det K)^{-1}K^*$

- e.g.:  $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$   $K_{1,2} = 3 \quad \therefore \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

$$K^* = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \qquad \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

- $\det K = 11 \times 7 - 8 \times 3 \pmod{26} = 1$

- $K^{-1}=(\det K)^{-1}K^*=$

# Introduction:

## Some Simple Cryptosystems

- Cryptosystem 1.5: Hill Cipher (Lester Hill 1929)
    - $M \geq 2$  is an integer
    - $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$
    - $\mathcal{K} = \{m \times m \text{ invertible matrices over } \mathbb{Z}_{26}\}$
    - For a key  $K$ 
      - $e_K(x) = xK$
      - $d_K(y) = yK^{-1}$
- where  $K^{-1}$  is the inverse of  $K$

# Introduction:

## Some Simple Cryptosystems

- e.g.:

•

$$K = \begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix}, \quad K^{-1} = \begin{pmatrix} 21 & 15 & 17 \\ 23 & 2 & 16 \\ 25 & 4 & 3 \end{pmatrix}$$

- Plaintext: GOD      (6   14   3)
- Ciphertext: WTJ      (22   19   9)

$$(6 \quad 14 \quad 3) \begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix} = (22 \quad 19 \quad 9)$$

# Hill Cipher: Polyalphabetic substitution cipher based on linear algebra, Ex.1

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

1. Multiplication of key and plain text matrix.
2. Perform Mod 26 Operation on the resultant multiplication.
3. Use table to convert back to alphabets, ciphertext.

Encrypt message “exam” using cipher with the key  $\{\{9,4\},\{5,7\}\}$

Convert plain text exam in number matrix  $\{\{4,0\},\{23,12\}\}$

Multiply key and plain text matrix  $\{\{9,4\},\{5,7\}\} \times \{\{4,0\},\{23,12\}\}$   
 $=\{\{128,48\},\{181,84\}\}$

Perform Mod Operation: mod 26

$=\{\{24,22\},\{25,6\}\}$ , convert to cipher text as per table “YWZG”

## Ex.2

- Encrypt the message "DEF" USING Hill Cipher with key  $\{2,4,5\},\{9,2,1\},\{3,8,7\}$
- Convert plain text to number matrix:
- $\{3,4,5\}$
- Multiplay  $\{2,4,5\},\{9,2,1\},\{3,8,7\} \times \{3,4,5\}$
- $=\{47,40,76\}$  perform Mod 26
- $\{21,14,22\}$  convert in alphabets
- "VOY"

## Ex.3

- Plain Text "attack" Key  $k = \{\{2,3\}, \{3,6\}\}$
- $C = \text{FKMFIO}$
- Determinant  $d = \{\{a,b\}, \{c,d\}\}$
- $d = \{ad-bc\} = 2 \times 6 - 3 \times 3 = 3$
- Find multiplicative inverse of determinant
- $D \text{ inverse} = 1 \text{ mod } 26$  (identity matrix)
- $27 \text{ mod } 26 = 1$
- $D \text{ inverse} = 9$
- Adjoint of matrix



# Playfair Cipher

- It is symmetric -key based encryption technique that uses digraph (pair of alphabets) substitution cipher.
- Significantly hard to break.
- Involves 625 combinations of alphabet pairs.

# Algorithm

- Create 5x5 matrix, occurrence is only once, I j combined to treat one position,
- Plain text, remove punctuation, special characters, numbers etc. make pair of alphabets of plain text, if one alphabet left out take x to make pair, same alphabets in pair replace by x.
- Use the pair of plaintext to substitute key square position, locate the alphabets in key square, follow substitution rules:
- A. if alphabet appears on same row of key square, replace them with the alphabets to their immediate right.
- If alphabet appear on same column of the key square, replace them with the alphabets immediately below respectively.
- If alphabets are in different row and column, replace the pair with the alphabets on the same row respectively but at the corners of rectangle

# Ex.1

- Word : thaksen; Key: parvat, th, ak, se, nz

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

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

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

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

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

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

# University QP

- Encrypt "This is final exam" with playfair cipher using key "Guidance".  
Podrdrpobngeiolido
- Encrypt the message "Surgical Strike" with key "bharat" using Playfair technique.
- Enrypt the word "greet" using the key "moon mission". hqczdu

# Introduction:

## Some Simple Cryptosystems

- <6> Permutation Cipher
  - Cryptosystem 1.6: Permutation Cipher
    - $m$  is a positive integer
    - $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$
    - $\mathcal{K}$  consist of all permutations of  $\{1, \dots, m\}$
    - For a key(a permutation)  $\pi$

$$d_{\pi}(y_1, \dots, y_m) = (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(m)})$$
$$- e_{\pi}(x_1, \dots, x_m) = (x_{\pi(1)}, \dots, x_{\pi(m)})$$

where  $\pi^{-1}$  is the inverse permutation to  $\pi$

# Introduction:

## Some Simple Cryptosystems

- e.g.: Suppose  $m=6$ 
  - Plaintext: CYBERFORMULA
  - Ciphertext: BRCFEYMLOAUR

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

plaintext	C	Y	B	E	R	F	O	R	M	U	L	A
ciphertext	B	R	C	F	E	Y	M	L	O	A	U	R

# Introduction:

## Some Simple Cryptosystems

- <7> Stream Ciphers
  - Block ciphers

Plaintext string  $x = x_1 x_2 \dots$  (each  $x_i$  is a plaintext)

Ciphertext string  $y = y_1 y_2 \dots = e_k(x_1) e_k(x_2) \dots$

- Stream ciphers
- Plaintext string  $x = x_1 x_2 \dots$

Generate a keystream (by using some  $K$ )  $z = z_1 z_2 \dots$

Ciphertext string  $y = y_1 y_2 \dots = e_{z_1}(x_1) e_{z_2}(x_2) \dots$

# Introduction:

## Some Simple Cryptosystems

- Definition 1.6: A synchronous stream cipher is a tuple  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, E, D)$  with a function  $g$ 
  - $\mathcal{P}$ : a finite set of possible plaintexts
  - $\mathcal{C}$ : a finite set of possible ciphertexts
  - $\mathcal{K}$ : a finite set of possible keys
  - $\mathcal{L}$ : a finite set called the keystream alphabet
  - $g$ : the keystream generator
    - Input:  $K$
    - $g$  generates an infinite string  $z_1 z_2 \dots$



# Introduction:

## Some Simple Cryptosystems

- Definition 1.6 (cont.)
  - For each  $z \in \mathcal{L}$ , there is an encryption rule  $e_z \in \mathcal{E}$  and a corresponding decryption rule  $d_z \in \mathcal{D}$ 
    - $e_K : \mathcal{P} \rightarrow \mathcal{C}$
    - $d_K : \mathcal{C} \rightarrow \mathcal{P}$
    - $d_z(e_z(x)) = x$  for every plaintext  $x \in \mathcal{P}$

# Introduction:

## Some Simple Cryptosystems

- Vigenère Cipher can be defined as a synchronous stream cipher

- $\mathcal{K} = (\mathbb{Z}_{26})^m$

- $\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathbb{Z}_{26}$

- $e_z(x) = (x+z) \bmod 26$

- $d_z(y) = (y-z) \bmod 26$

- Keystream  $z_1 z_2 \dots$

$$= k_1 k_2 \dots k_m k_1 k_2 \dots k_m k_1 k_2 \dots k_m \dots$$

$$z_i = \begin{cases} k_i & \text{if } 1 \leq i \leq m \\ z_{i-m} & \text{if } i \geq m+1 \end{cases}$$

# Introduction:

## Some Simple Cryptosystems

- Keystream can be produced efficiently in hardware using a LFSR (Linear Feedback Shift Register)
  - $k_1$  would be tapped as the next keystream bit
  - $k_2, \dots, k_m$  would each be shifted 1 stage to the left
  - The new value of  $k_m$  would be

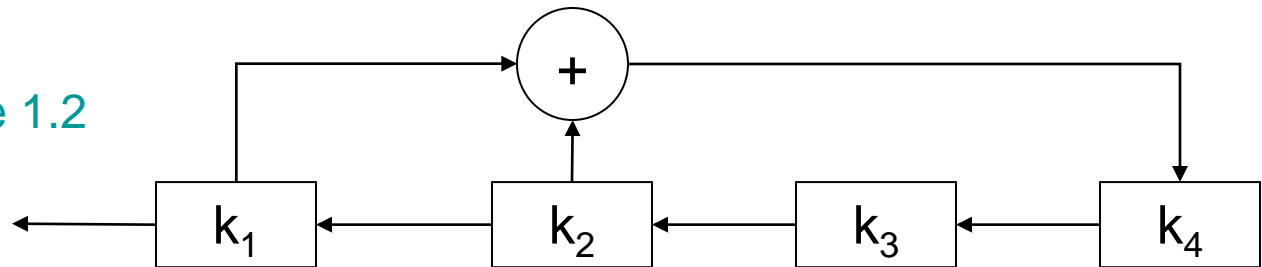
$$\sum_{j=0}^{m-1} c_j k_{j+1}$$

this is “linear feedback“ (see Figure 1.2)

- This system is modulo 2

# Introduction: Some Simple Cryptosystems

Figure 1.2



- e.g.: in Figure 1.2, suppose  $K=(1,0,0,0)$ 
  - $c_0=1, c_1=1, c_2=0, c_3=0$
  - The keystream is  
100010011010111...

# Introduction:

## Some Simple Cryptosystems

- Non-synchronous stream cipher:
  - Each keystream element  $z_i$  depends on previous plaintext or ciphertext elements
- Cryptosystem 1.7: Autokey Cipher
  - $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = \mathbb{Z}_{26}$
  - $z_1 = K, z_i = x_{i-1}$  for all  $i > 1$
  - For  $x, y, z \in \mathbb{Z}_{26}$ 
    - $e_z(x) = (x + z) \bmod 26$
    - $d_z(y) = (y - z) \bmod 26$

# Introduction:

## Some Simple Cryptosystems

- e.g.: Suppose  $K=8$ 
  - Plaintext: student
  - Ciphertext: ALNXHRG

plaintext	s	t	u	d	e	n	t
	18	19	20	3	4	13	19
keystream	8	18	19	20	3	4	13
ciphertext	0	11	13	23	7	17	6
	A	L	N	X	H	R	G

# Steganography

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.

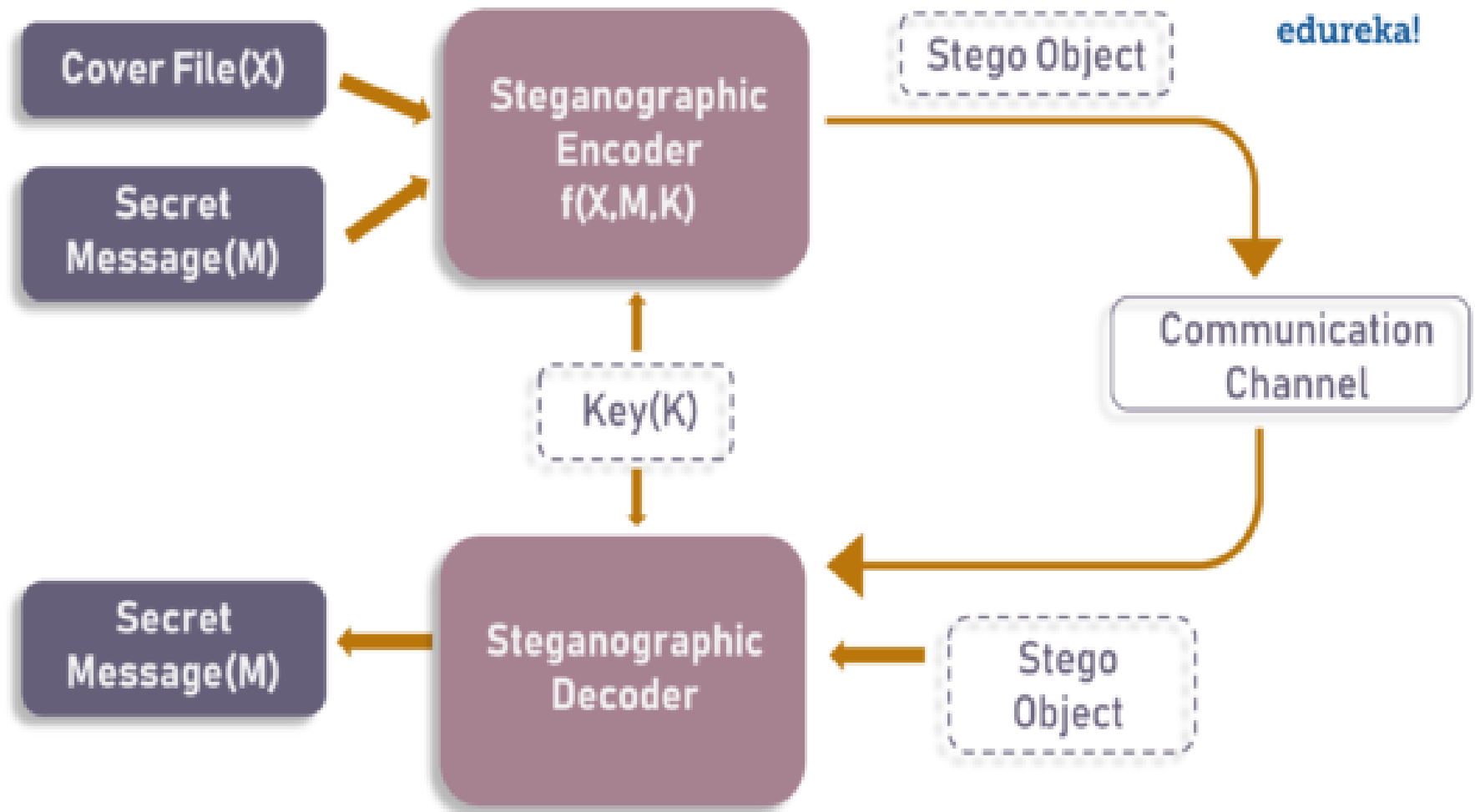
The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

# What is Steganography?

Steganography is the art and science of embedding secret messages in a cover message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message



# Basic Steganographic Model.



# Steganography Techniques

1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Network Steganography

# Steganography different from Cryptography ?

	STEGANOGRAPHY	CRYPTOGRAPHY
<b>Definition</b>	It is a technique to hide the existence of communication	It's a technique to convert data into an incomprehensible form
<b>Purpose</b>	Keep communication secure	Provide data protection
<b>Data Visibility</b>	Never	Always
<b>Data Structure</b>	Doesn't alter the overall structure of data	Alters the overall structure of data
<b>Key</b>	Optional, but offers more security if used	Necessary requirement
<b>Failure</b>	Once the presence of a secret message is discovered, anyone can use the secret data	If you possess the decryption key, then you can figure out original message from the ciphertext

# Question Bank

1. What is the OSI security architecture?
2. What is the difference between passive and active security threats?
3. List and briefly define categories of passive and active security attacks.
4. List and briefly define categories of security services.
5. List and briefly define categories of security mechanisms.
6. What are the essential ingredients of a symmetric cipher?
7. What are the two basic functions used in encryption algorithms?
8. How many keys are required for two people to communicate via a cipher?
9. What is the difference between a block cipher and a stream cipher?
10. What are the two general approaches to attacking a cipher?

11. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
12. What is the difference between an unconditionally secure cipher and a computationally secure cipher?
13. Briefly define the Caesar cipher.
14. Briefly define the monoalphabetic cipher.
15. Briefly define the Playfair cipher

