SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

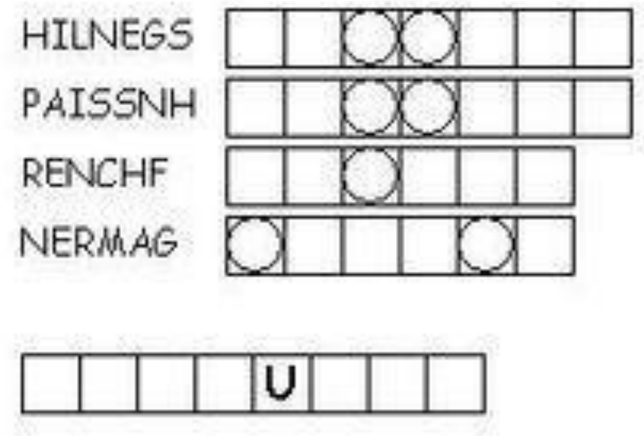
III YEAR / VI SEMESTER

Unit 2: SYMMETRIC KEY CRYPTOGRAPHY

Topic : TRANSPOSITION TECHNIQUES

TRANSPOSITION TECHNIQUES

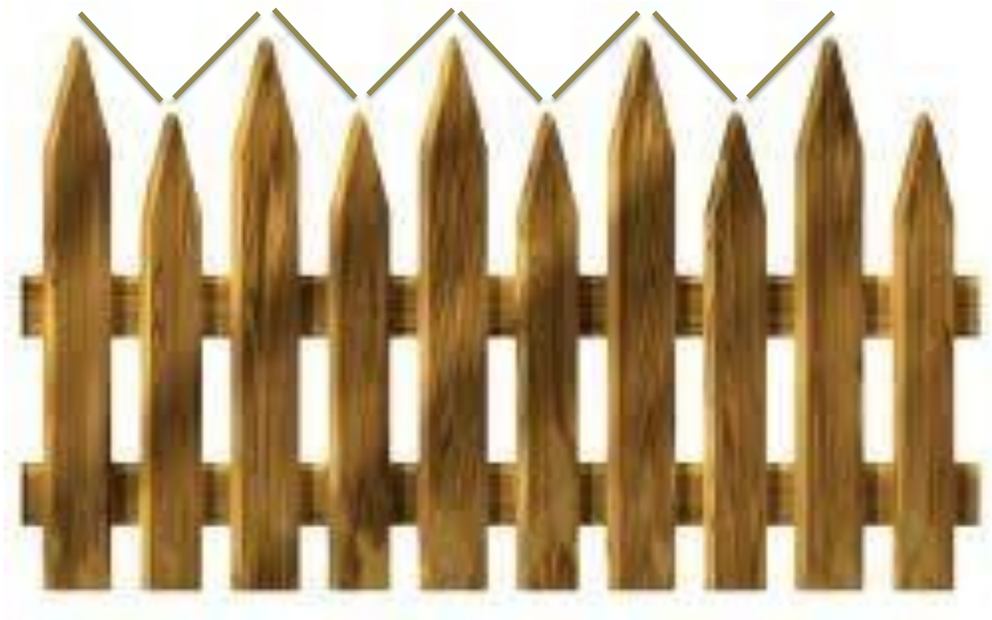
- Different kind of mapping is achieved by performing some sort of permutation on the plaintext letters
- Simplest such cipher is the rail fence technique
- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows



RAIL FENCE TECHNIQUE

- Encrypted like the rail fence
- Example: Encrypt **meet me after the toga party** with the depth of 2

M	E	M	A	T	R	H	T	G	P	R	Y
E	T	E	F	E	T	E	O	A	A	T	



Encrypted message :
MEMATRHTGPRYETEFETEOAAT

COLUMNAR TRANSPOSITION TECHNIQUES

- Message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.
- The order of the columns then becomes the key to the algorithm

Key	4	3	1	2	5	6	7
Plaintext	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Cipher text:
TTNAAPTMTSUOAODWCOIXKN
LYPETZ

DOUBLE TRANSPOSITION

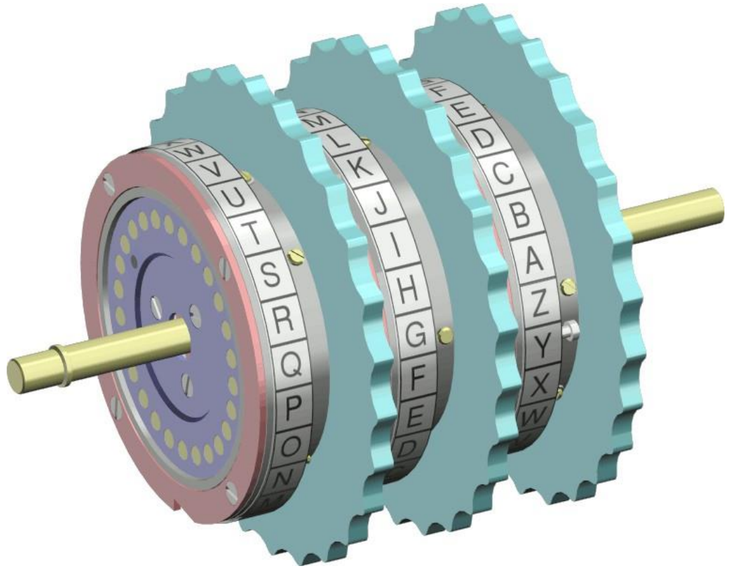
Key	4	3	1	2	5	6	7
Plaintext	**T**	**T**	**N**	**A**	**A**	**P**	**T**
	M	**T**	**S**	**U**	**O**	**A**	**O**
	D	**W**	**C**	**O**	**I**	**X**	**K**
	N	**L**	**Y**	**P**	**E**	**T**	**Z**

Cipher text:
TTNAAPTMTSUOAOD
WCOIXKNLYPETZ

Output:
NSCYAUOPTTWLTMD
NAOIEPAXTTOKZ

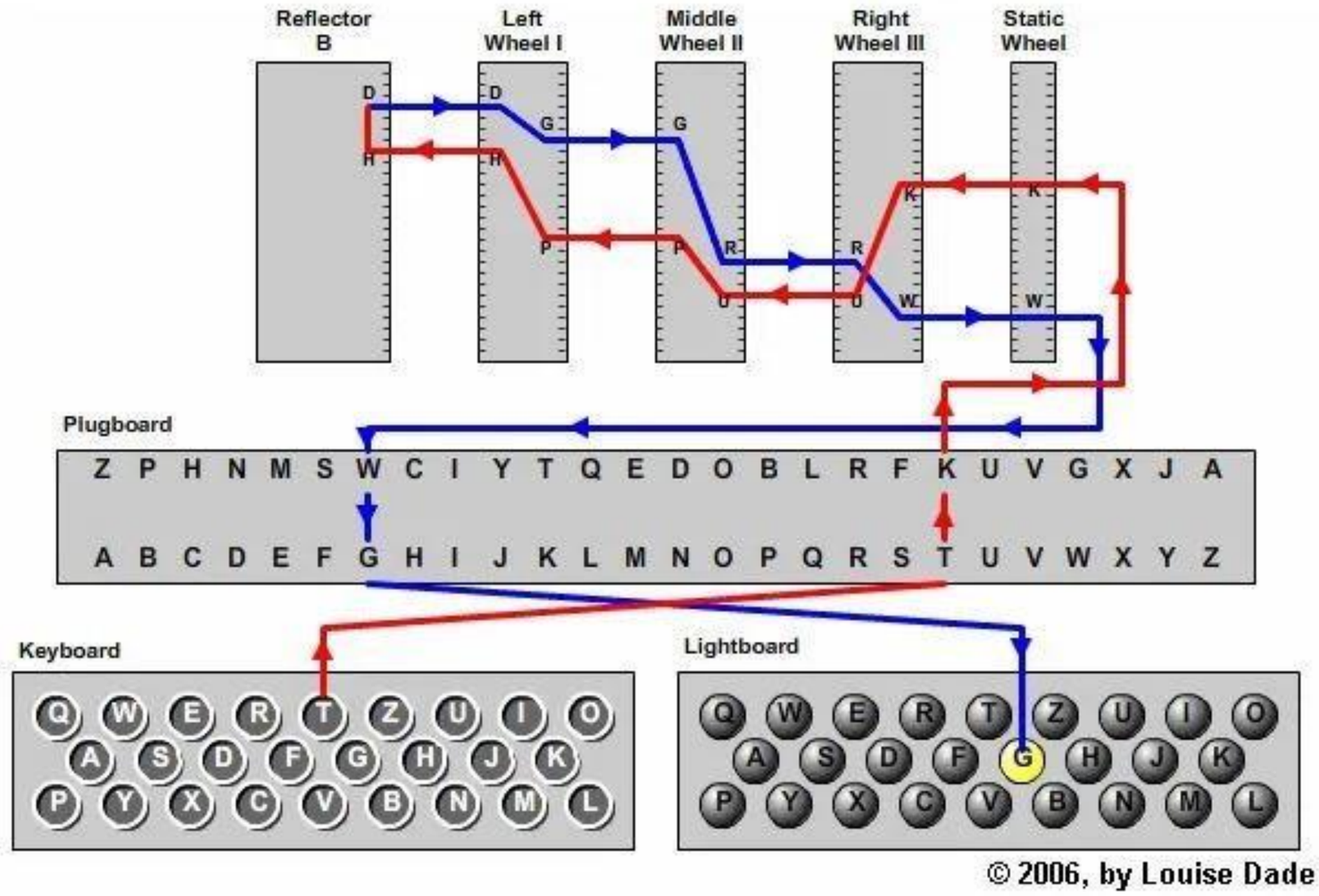
Less structured permutation and is much more difficult to cryptanalyze.

ROTOR MACHINE

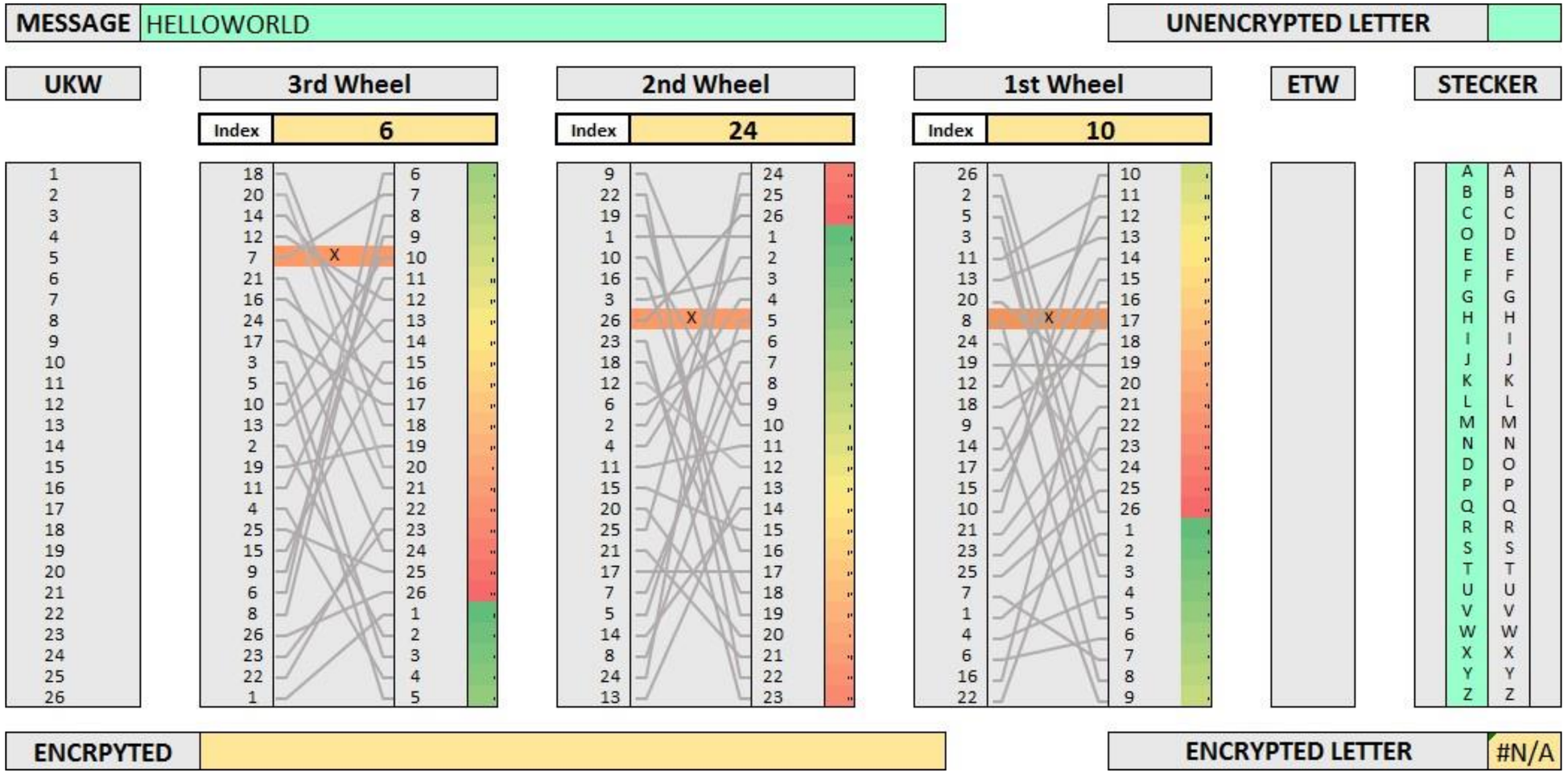


- A set of independently rotating cylinders through which electrical pulses can flow
- 26 input and output pins with internal wiring.

ENIGMA MACHINE - WORKING



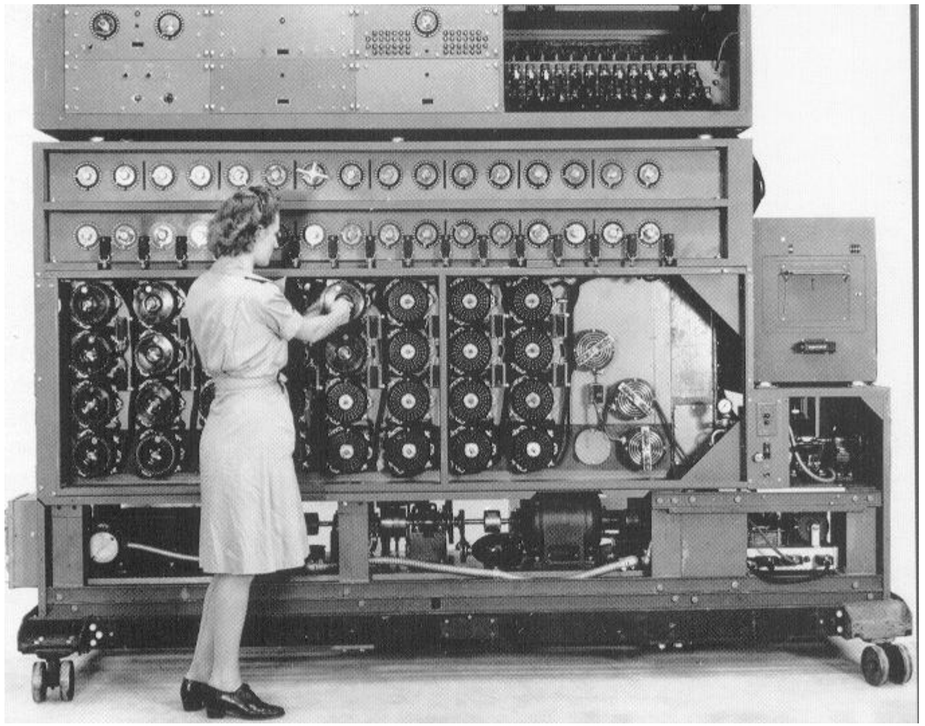
ENIGMA MACHINE - WORKING ANIMATED



ACTIVITY

Imagine how many combinations are Possible with Enigma!

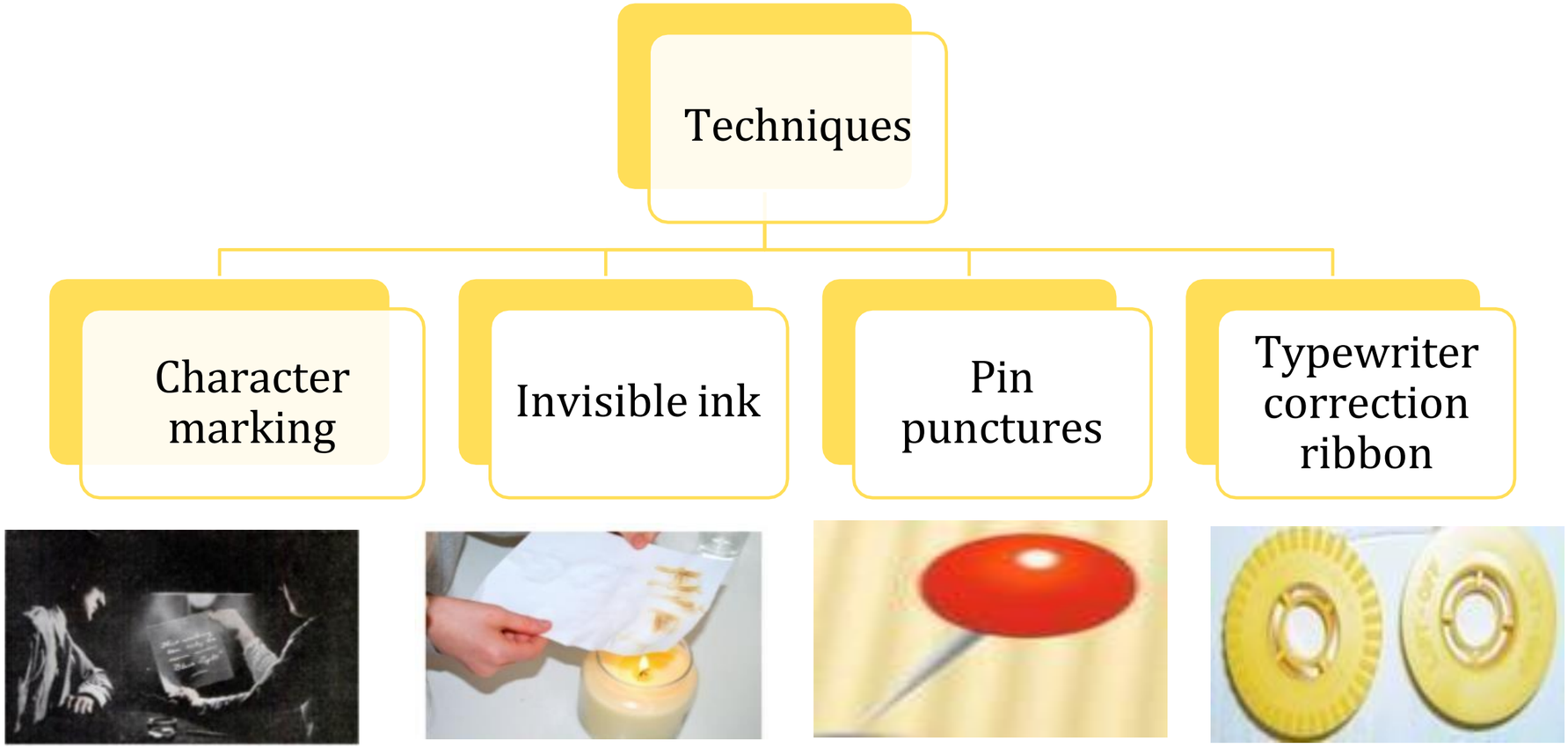
150,738,274,900,000



STEGANOGRAPHY

- Conceal the existence of the message

STEGANOGRAPHY TECHINIQUES



Overwritten in pencil
Paper at an angle at bright light

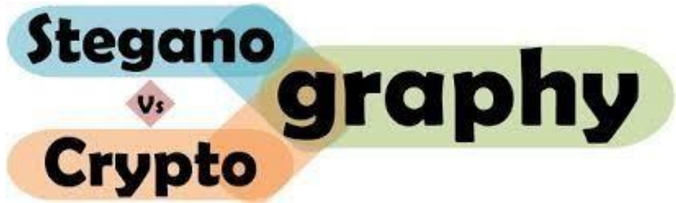
No visible trace
Heat / chemical on the paper

Pin punctures
light

Correction tape between lines typed in black ribbon
Strong light

STEGANOGRAPHY VS CRYPTOGRPHY

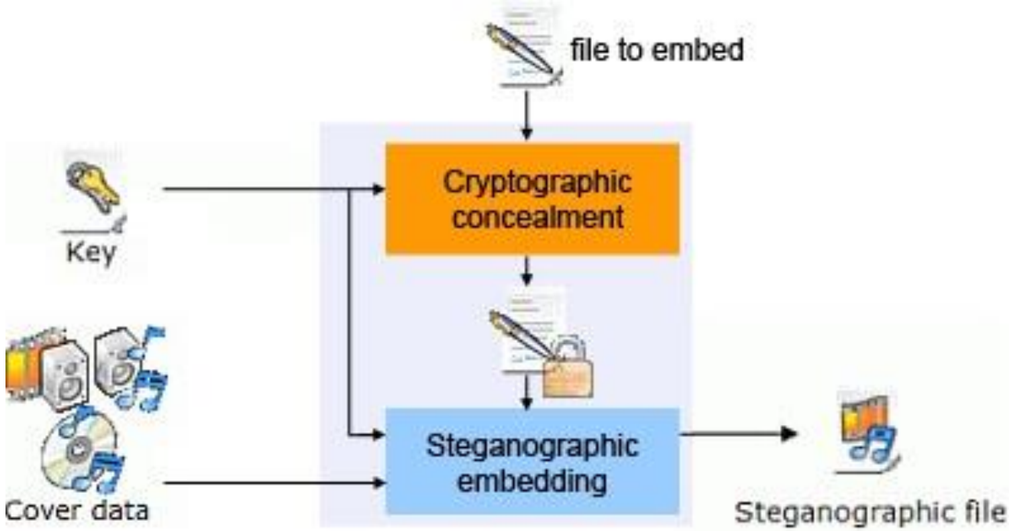
Basis for comparison	Steganography	Cryptography
Basic	It is known as cover writing.	It means secret writing.
Goal	Secret communication	Data protection
Structure of the message	Not altered	Altered only of the transmission.
Popularity	Less popular	More commonly used.
Relies on	No parameters.	Key.
Supported security principles	Confidentiality and authentication	Confidentiality, data integrity, authentication, and non-repudiation.
Techniques	Spacial domain, transform domain, model-based and ad-hoc.	Transposition, substitution, stream cipher, block ciphers.
Implemented on	Audio, video, image, text.	Only on text files.
Types of attack	Steganalysis	Cryptanalysis



DISADVANTAGES

- Requires lot of overhead to hide a relatively few bits of information.
- Virtually Worthless, once discovered.

Encryption+ Steganography



ASSESSMENT – Identify the terms?

REFERENCES

William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.

THANK YOU