

Data Security Using Cryptography & Steganography

Presented By:-

Tushar Bhatt	2129119
Rahul bagaria	2129140
Rakesh Kumar	2129144
Vishesh Raj Solanki	2129124
Avi Bhagat	2129062

CRYPTOGRAPHY

"Cryptography is an art of Secret writing"

Or

"Cryptography –from the Greek for "secret writing" (Kryptos means 'Hidden, graphein means 'writing') –is the mathematical

"scrambling" of data into unreadable form to preserve confidentiality. "

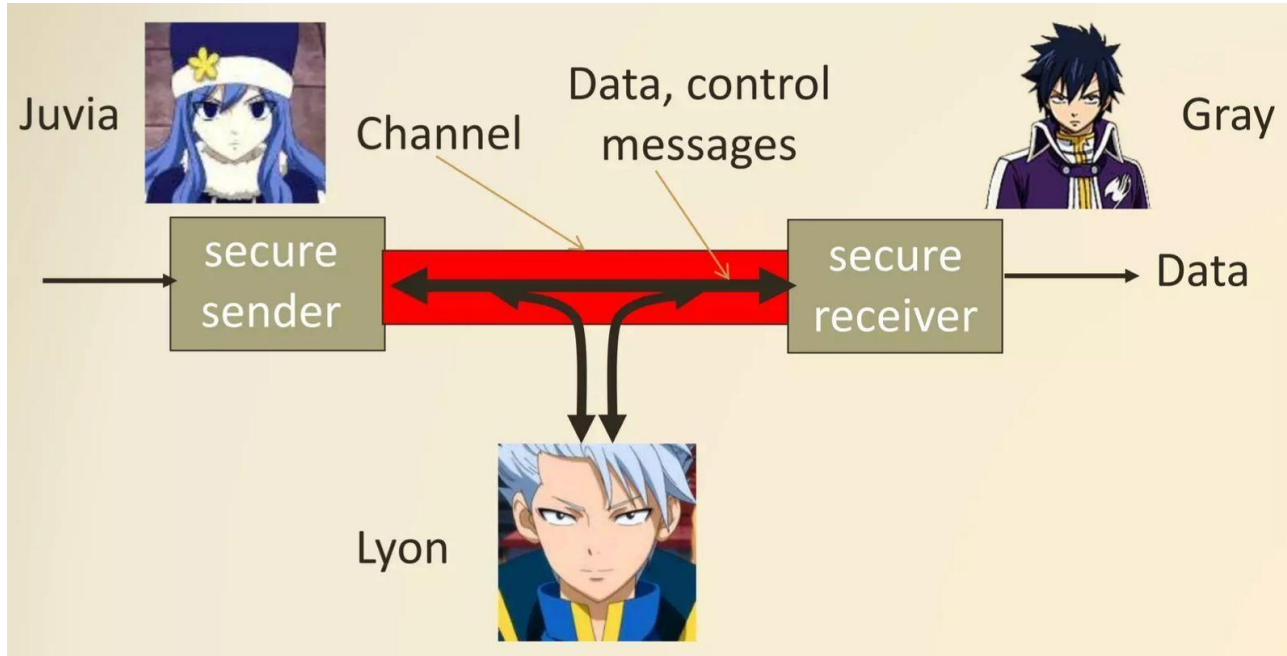
Or

"Cryptography is the process of converting plaintext into ciphertext"



Friends & Foes: Juvia, Gray, Lyon

- Juvia and Gray wants to communicate securely.
- Lyon (Intruder) may intercept and tamper the communication.



Need for Cryptography

- Establishing a Secure communication.
- Fulfil the security goals.
- Preservation of Authentic information.
- Secure Transaction.
- Privacy.



Category of Cryptography

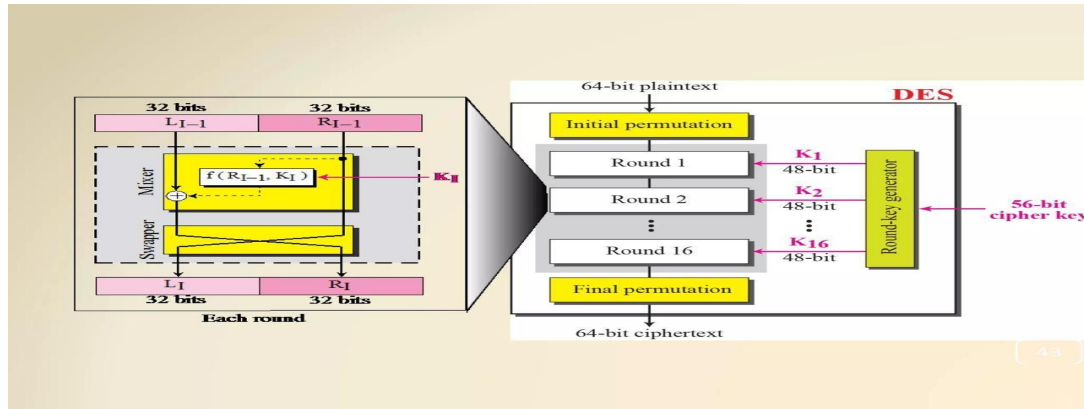
Design Principles of

DES

To achieve high degree of diffusion and confusion.

Diffusion: making each plaintext bit affect as many ciphertext bits as possible.

Confusion: making the relationship between the encryption key and the ciphertext as complex as possible.



TRIPLE DES

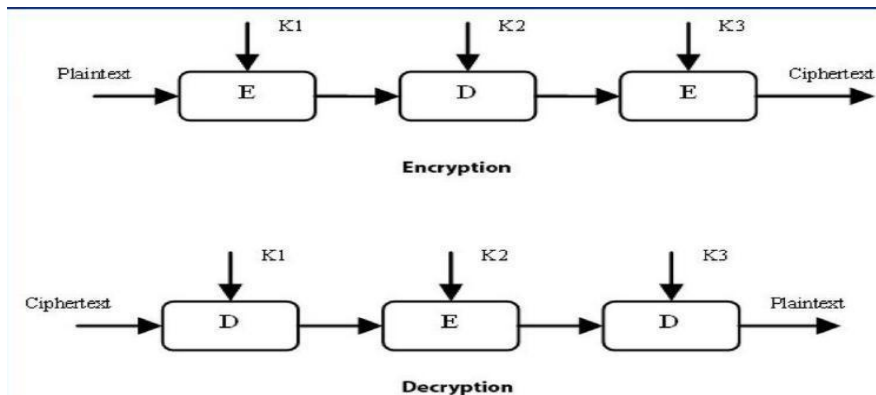
Algorithm

Uses a block of size 64 bits.

- Triple DES comprises of three DES keys, K1, K2 and K3, each of 56 bits. The encryption algorithm follows a EDE sequence:

$$C = E(K3, D(K2, E(K1, P)))$$

- i.e., DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.



STEGANOGRAPHY


Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.

STEGONOGRA PHY EXAMPLE	RANDOM TEXT	Since everyone can read, encoding text in neutral sentences is doubtfully effective
	SOME HIDDEN PATTERN	Since Everyone Can Read, Encoding Text In Neutral Sentences Is Doubtfully Effective
	ORIGINAL MESSAGE	SECRET INSIDE

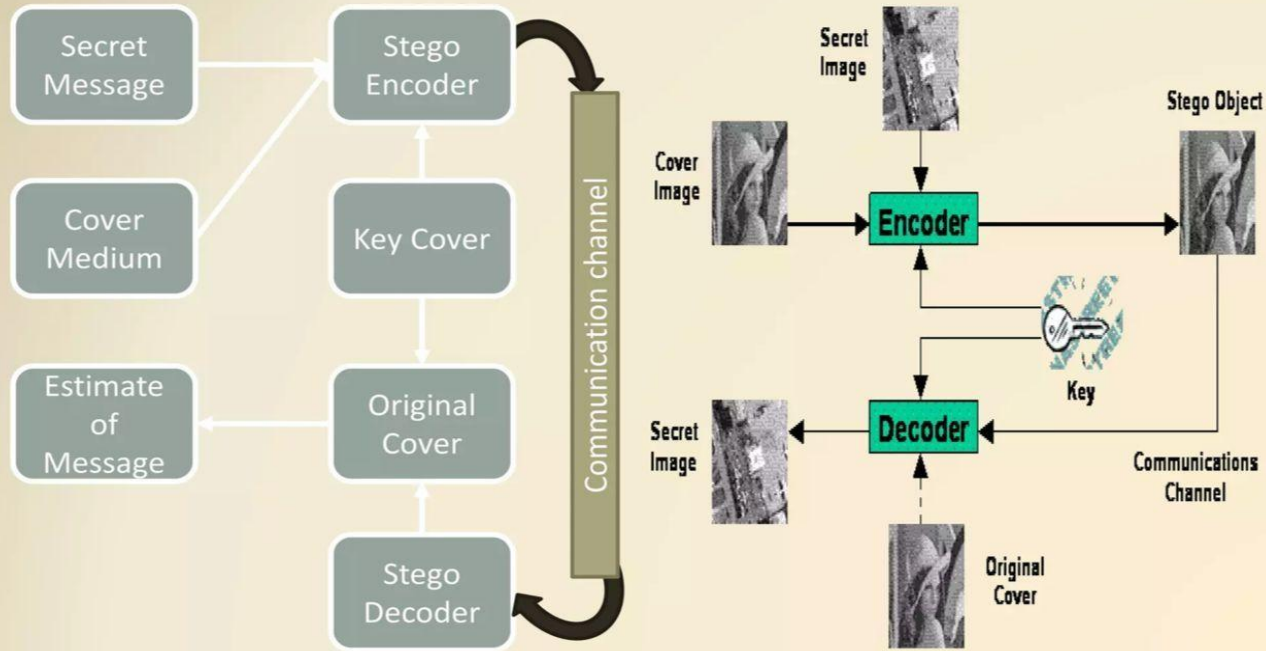
TECHNIQUES

- Hidden messages on paper written in secret inks under other messages or on the blank parts of other messages.
- Hidden messages within wax tablets.
- Messages written on envelopes in the area covered by postage stamps.

DIGITAL TECHNIQUES:

- Concealing data within encrypted data or within random data (an unbreakable cipher like the one-time pad generates cipher texts that look perfectly random if one does not have the private key).
 - Concealed messages in tampered executable files, exploiting redundancy in the targeted instruction set.
 - Pictures embedded in video material (optionally played at slower or faster speed).
- 

Basic Steganography Model

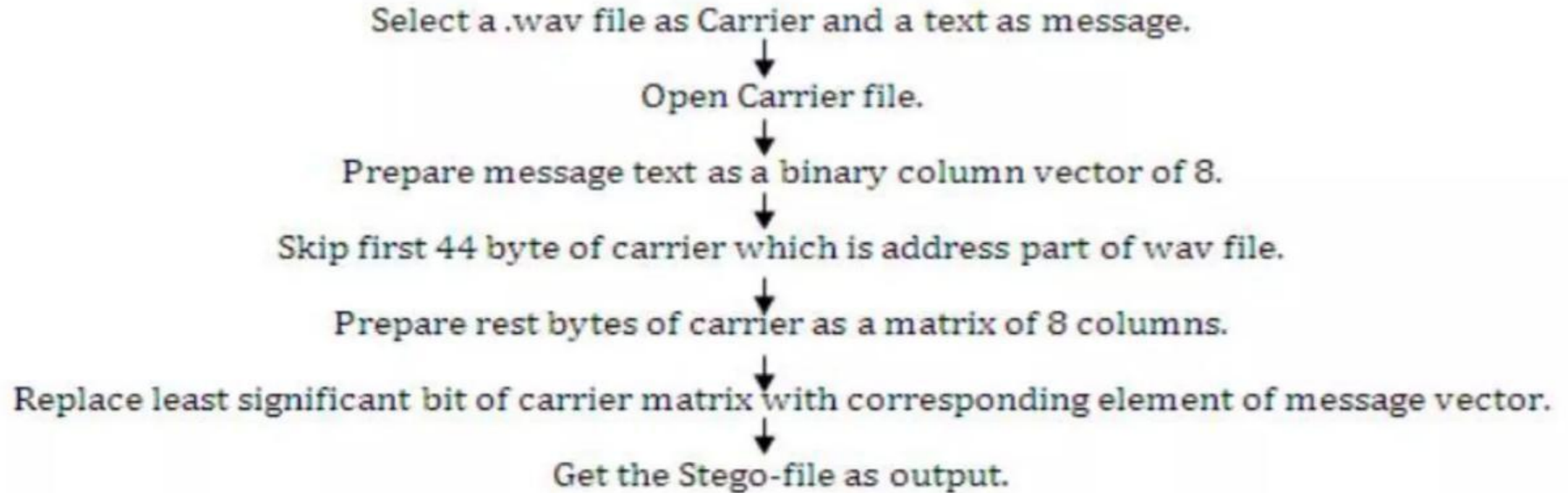


Audio Steganography

- Embedding secret messages into digital sound is known as audio Steganography.
- Audio Steganography methods can embed messages in WAV, AU, and even MP3 sound files.
- The properties of the human auditory system (HAS) are exploited in the process of audio Steganography
- To embed data secretly onto digital audio file there are few techniques introduced :
 - LSB Coding
 - Phase Coding
 - Parity Coding
 - Spread Spectrum



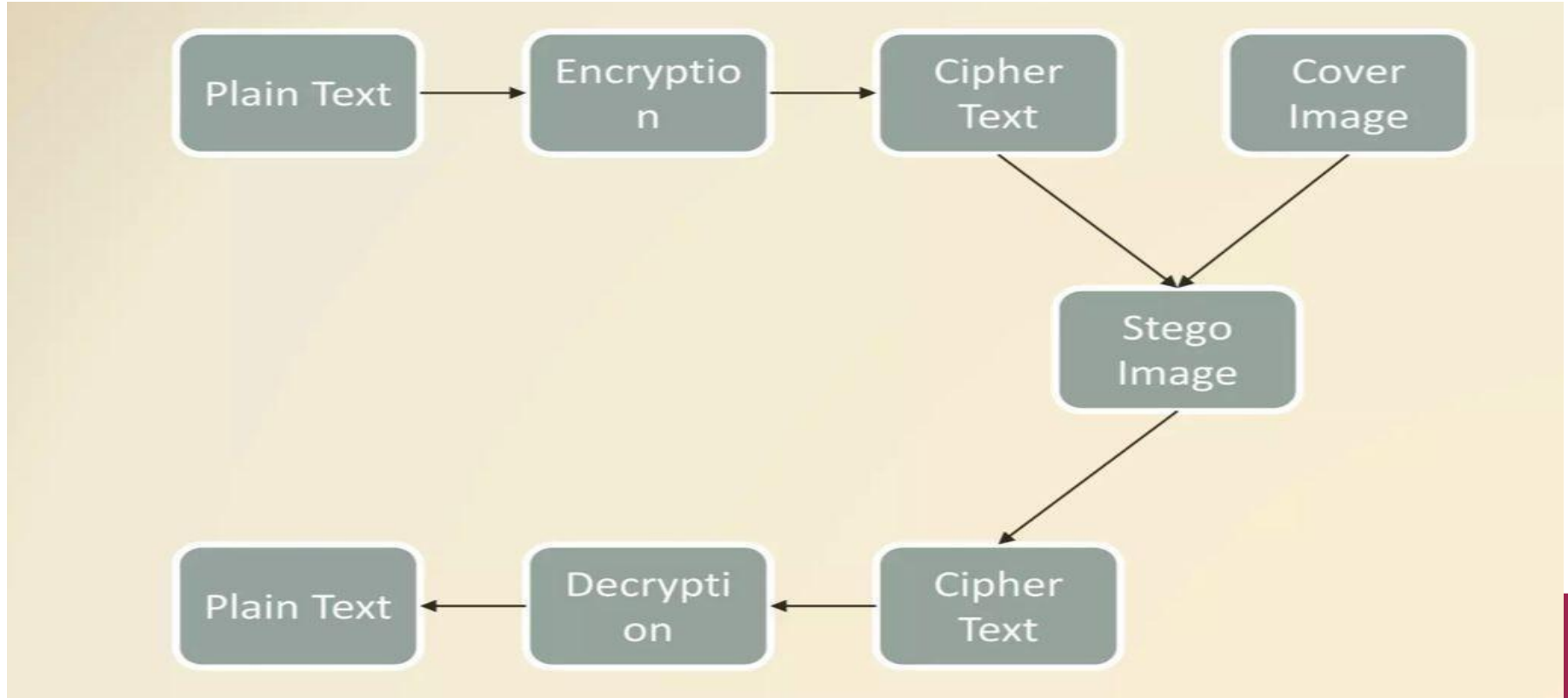
FLOW CHART OF STEGANOGRAPHY



Comparison of Secret communication techniques

Communication Technique	Confidentiality	Integrity	Availability
Cryptography	✓	✗	✓
Digital Signatures	✗	✓	✗
Steganography	✓	✓	✓

Combined Crypto - Steganography



APPLICATIONS

Confidential communication and secret data storing

Steganography provides us with:

- Potential capability to hide the existence of confidential data
- Hardness of detecting the hidden (i.e., embedded) data

Strengthening of the secrecy of the encrypted data

- Protection of data alteration
- Access control system for digital content distribution
- Media Database systems
- Usage in modern printers
- Alleged use by intelligence services



FUTURE SCOPE

Steganography, though is still a fairly new idea.

There are constant advancements in the computer field, suggesting advancements in the field of steganography as well.

It is likely that there will soon be more efficient and more advanced techniques for Steganalysis.

What is scary is that such a small file of only one or two sentences may be all that is needed to commence a terrorist attack. In the future, it is hoped that the technique of Steganalysis will advance such that it will become much easier to detect even small messages within an image.



CONCLUSION

With the smooth integration of audio steganography and TDES encryption, the project effectively met its overall goal of enhancing data security. A more secure and robust network environment is created by the methods used, which guarantees that data is secured throughout transmission. The protection of sensitive data in an increasingly linked world may be facilitated by future developments in data security technology brought about by ongoing research and development in this field.



THANK YOU

