Cyber Security and Cyber Forensics (Chapter - 4 : DISSA Course) **Part 2**

Arijit Chakraborty

June 20 , 2021

Today's session

- Mobile Hacking
- Cyber-forensic Software
- Encryption Technology
- Defending from cyber-threat
- Cryptography & Steganography
- LSB Algorithms
- Digital Signature
- IS Audit – Industry requirements

Mobile hacking

- **Key Features**
- Track location and sim card activity
- Check messages & calls
- View media files
- Hidden details - passwords , usernames, browser history,
- ● Control remotely
- 1. **Ultimate Phone Spy**
- Features - , sent & received messages, social media activities, browsing history, etc.
- inbuilt GPS tracker implanted - even track location of targeted device

Ultimate Phone Spy

- **Key Features of Ultimate Phone Spy to Hack phone number**
- Stealth monitoring
- Social apps coverage
- View calls and messages
- Access the gallery
- Track location and sim card activity
- Browser history and in-built keylogger

Hacking - Wireless Hacking

- **DDoS :**
- attack on network & computer - prohibits, prevents, or reduces system from retrieving accessibility to legitimate users.
- Intruder - **deprive authorized users of access :** sites, networks, computers.
- Attacker primarily aims at bandwidth of victim for attack.
- When DoS attack executed using **different compromised devices** for attacking specific system, **distributed nature of attack** -DDoS
- **Indication of the Denial of Service Attacks**

✓ Hanging a system

✓ Slower performance of the network

✓ Shutting down or Rebooting the specific system

✓ Idle responses from system

✓ Incapable of accessing any websites / targeted website

✓ Radical increase in Spam emails

✓ Deleting & Damaging hardware or network resource

Pen Testing

- Agreement parameters
- The time of Penetration test
- The place where IP Source of attack shall be conducted
- Detailing penetration fields that are found on system
- Penetration testing = executed by professional Ethical hackers - use automated tools, manual checks.

Data Monitoring

Employee Internet Activity

SPECTOR 360

captures employee web activity including :

- Which employees are spending the most time surfing web sites?
- Which employees chat the most?
- Who is sending the most emails with attachments?
- Who is arriving to work late and leaving early?
- What are my employees searching for on the Internet?
- Keystrokes Typed
- Chat/Instant Messages
- User Activity/Inactivity
- File Transfers, Applications/Programs Used
- Document Tracking
- Online Searches, Network Activity

CODING AND DECODING- cryptography/ secret message

- Before transmitting, **data encoded** & at receiver side encode **data is decoded** in order to obtain original data **by determining common key** in encoded data.
- The Coding and Decoding is classified into:
- **Type 1: Letter Coding**
- **Type 2: Number Coding**
- **Type 1: Letter Coding**
- Real alphabets in a word **replaced by certain other alphabets** according to a specific rule (Algorithm) to form its code.

- **Case1: To form code for another word**
- **Example :** If in a certain language MYSTIFY is coded as NZTUJGZ, how is MENESIS coded in that language?
- **Explanation:** Each letter in MYSTIFY is moved 1 step forward to obtain the corresponding letter of the code.
- M Y S T I F Y
- +1
- N Z T U J G Z
- So, in MENESIS, N will be coded as O, E as F, M as N
- So - code becomes NFOFTJT.

- **Example 2:** If TAP is coded as SZO, then how is FRIEND coded?
- **Explanation:** Each letter in TAP is moved **1 step backward** to obtain corresponding letter of code.
- S Z O
- -1
- T A P
- Thus, in FRIEND, F = coded as E, R as Q , I as G, E as D, N as M and D as C.
- So, code = EQGDMC.

Type 2: Number Coding

- Either numerical code values are assigned to word or alphabetical code letters are assigned to the numbers.
- **Case 1: When a numerical code values are assigned to words.**
- **Example 1:** If in a certain language A is coded as 1, B is coded as 2, and so on, how is AICCI is coded in that code?
- So in AICCI, A is coded as 1, I as 9,and C as 3.
- Thus, AICCI = 19339.

Number coding

- **Example 2:** If PAINT is coded as 74128 and EXCEL is coded as 93596, then how would you encode ANCIENT ?
- So, in ANCIENT, A is coded as 4, N is coded as 2, C as 5, I is coded as 3, E as 9, and T as 8.
- Hence, code = 4251928

P	A	I	N	T	E	X	C	L
7	4	1	2	8	9	3	5	6

Basic Cryptography – Coding

- **Example 3**: If DELHI is coded as CCIDD, how to encode BOMBAY?
- Algorithm : (**order : -1, -2,-3, -4, -5)**
- AMJXVS
- **Example 4 :** If PALAM could be given the code number 43, what code can be given to SANTACRUZ?
- (A=1, B=2, …Z= 26)
- Answer = **123**

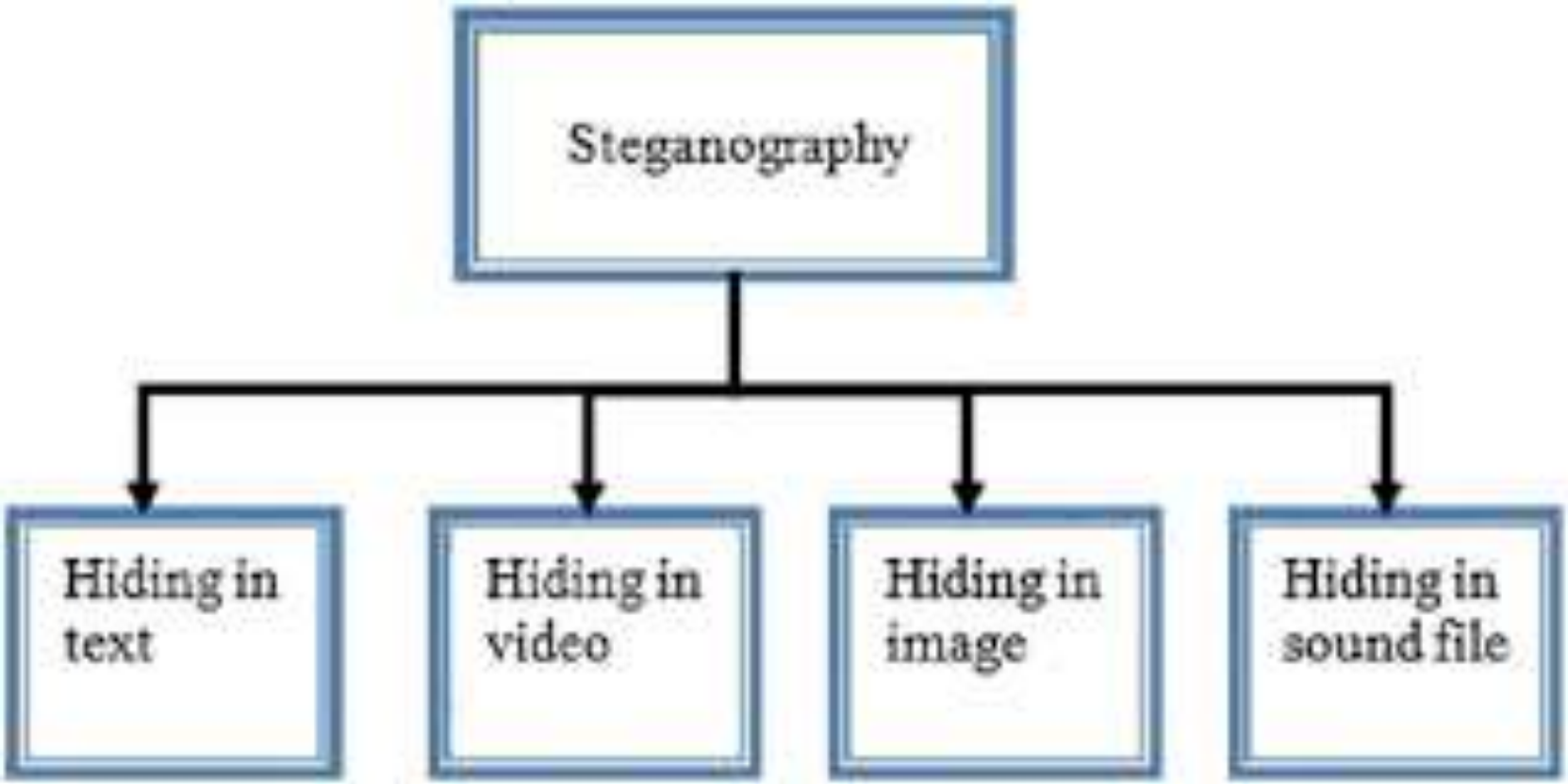
Cryptography & Steganography

- **Steganography** = technique of hiding secret data within ordinary, non-secret, file or message in order to avoid detection;
- Secret data is then **extracted at destination.**
- **Steganography** = combined with encryption for hiding or protecting data.
- Attackers = **embedding actual scripts** within Excel & Word documents.
- Once victim opens Excel or Word doc, **they activate embedded**, secret script.
- Attacks = DDoS, Ransomware etc

Comparison

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

Types


Steganography
Hiding in text
Hiding in video
Hiding in image
Hiding in sound file

Technology

- **Steganography techniques**
- Digital steganography, - data encrypted or obfuscated
- inserted using special algorithm, into data - part of particular file format such as a JPEG image, audio or video file.
- Secret message = embedded into ordinary data files.
- Passing messages **written with invisible ink**, then read by intended recipient by applying **certain chemical techniques**

Common technique

- Hide data in bits that represent **same color pixels** repeated in a row in an image file.
- By applying **the encrypted data to this redundant data** in some **inconspicuous way**,
- **Result =** image file that appears identical to original image

Steganography
Algorithms

- Converting decimal to binary
- ***Conversion steps:***
- Divide number by 2.
- Get integer quotient for next iteration.
- Get remainder for binary digit.
- Repeat steps until quotient is equal to 0.

Convert 13_{10} to binary:

Division by 2	Quotient	Remainder
13/2	6	1
6/2	3	0
3/2	1	1
1/2	0	1

So $13_{10} = 1101_2$

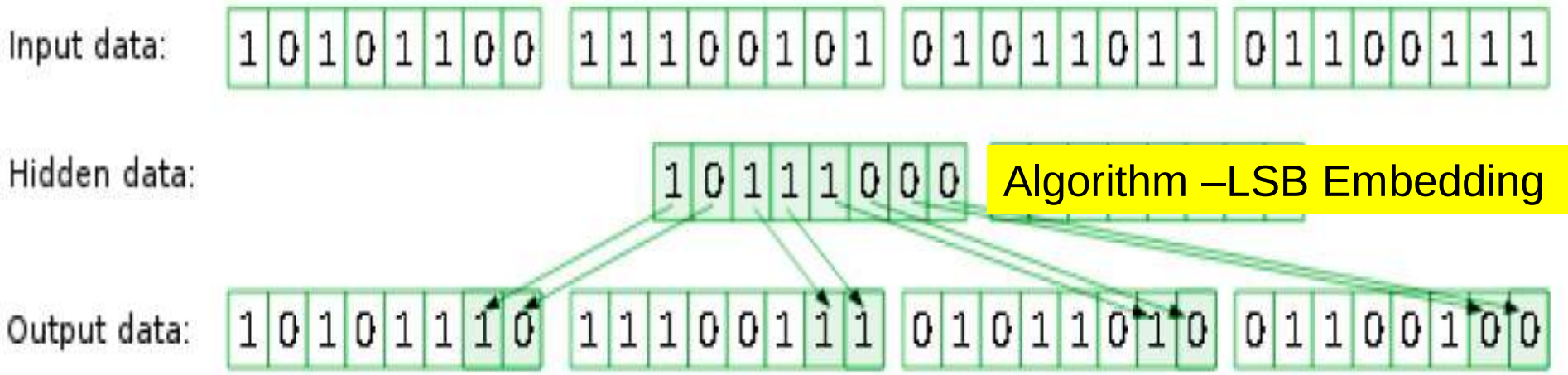
Algorithm

- hides files within image files on a computer.
- Hidden file encoded in **the least significant bits** of values encoding **the color of each pixel of the image.**
- Changing **the least significant bits** changes the appearance of the image **very slightly, & is not perceptible to naked eye**.
- If change is detectable at all, **colors will just look a little off as if the image was taken from a low quality camera on in poor light**.
- Similar process : to conceal data in sound files since human ear is limited in its ability **to differentiate different, similar frequencies (and in the range of frequencies it can detect).**

RGB Colour system- LSB Technique

- ***RGB color model*** = *additive color model = red, green & blue light added together in various ways to reproduce broad array of colors.*
- *RGB color model : sensing, representation & display of images in electronic systems – TV / Displays /photography*
- Each pixel has 3 values (RGB), each RGB value is 8-bit (can store 8 binary values) & **rightmost bits** are less significant.
- range is 0–255
- So, if we change rightmost bits = have a **small visual impact** on final image.
- Steganography key to hide an image inside another.
- ***Replace least significant bit of base image by one bit of the data to be hidden***

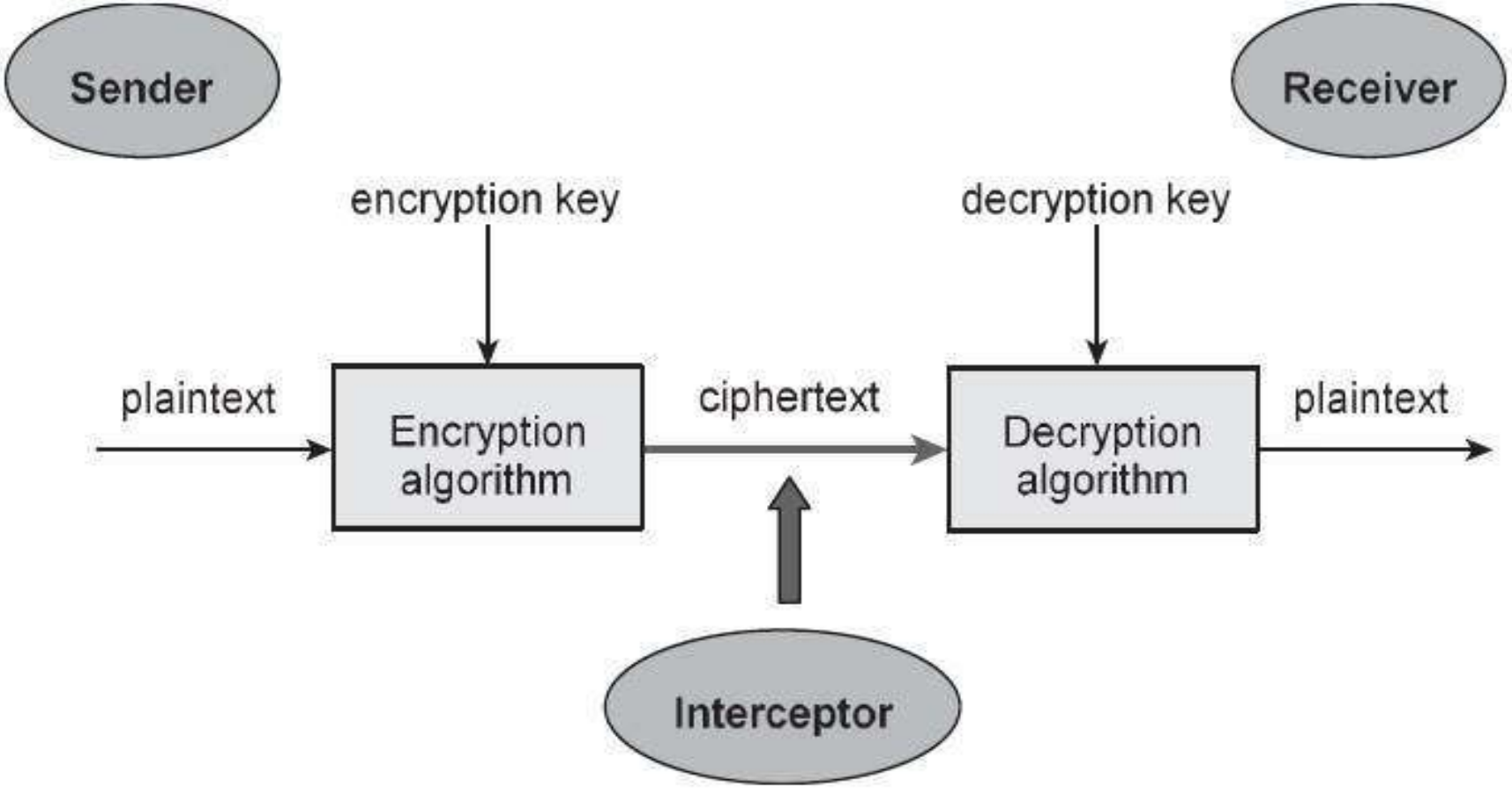
Illustration – Stega Algorithm



Stega – video file

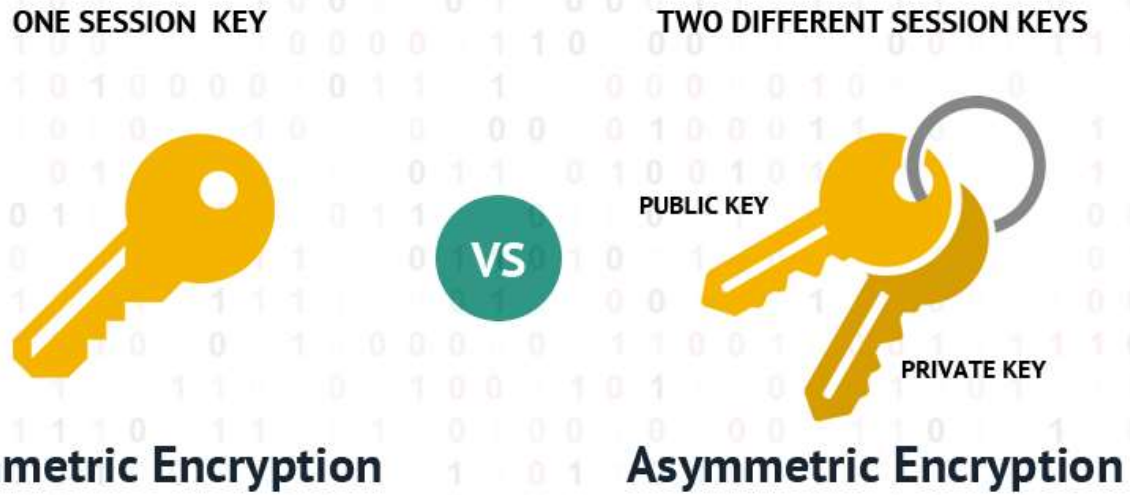
- Concealing pictures within video file.
- Human eye & brain **capable of seeing up to 1000 frames per second.**
- If video running **at 3000 frames per second**
- **Every 3rd frame =** a hidden image,

Cryptography = Encryption



Comparison


Symmetric Encryption
One key
Session
Asymmetric Encryption
Two keys
Public
Private


ONE SESSION KEY
TWO DIFFERENT SESSION KEYS
VS
PUBLIC KEY
PRIVATE KEY
Symmetric Encryption
Asymmetric Encryption

Digital Signature Certificate (DSC)

- IT Act, 2000 : provisions for use of DS on documents submitted in electronic form to ensure security & authenticity of documents filed electronically.
- All filings done by companies/LLPs under MCA21 e-Governance programme required to be filed using DS by person authorised to sign documents.
- Under GST , a company can get registered only by verifying GST application through digital signature.
- Signer electronically signs document, signature created using signer's private key, **always securely kept by signer.**
- Mathematical algorithm = cipher, creating data matching signed document, called **hash**, encrypting the data.
- Resulting encrypted data = digital signature.
- Signature also marked **with the time** that document was signed.
- If document **changes after signing**, digital signature is invalidated.
- Both entity sending the document & recipient signing it **must agree to use a given CA.**

Regulations

- **Legal Warning:**
- Use only valid Digital Signatures issued to signor.
- Illegal to use Digital Signatures of anybody else
- **Certification Agencies: (CA)**
- Certification Agencies appointed by office of **Controller of Certification Agencies** (CCA) under IT Act, 2000.
- The DSCs issued with 1 year validity and 2 year validity & renewable
- **Class 2:** identity of a person is verified against a trusted, pre-verified database.
- **Class 3:** highest level where the person needs to **present himself or herself in front of a Registration Authority (RA**) & prove his/ her identity.
- Generally CAs issue DSC within a day.

Classes of DSC

- **Class 1 Certificates:**
- issued **to individual/private subscribers** to confirm that user's name & email details from clearly defined subject lie within database of the CA
- **Class 2 Certificates:**
- issued to **director/signatory authorities of the companies** for e-filing with ROC.
- **Class 2 certificate is mandatory** for individuals who have to sign manual documents while filing returns with ROC.
- However, from 01.01.2021, CCA has instructed to discontinue Class 2 Certificates -- **Class 3 Certificates will be issued** in place of Class 2
- **Class 3 Certificates:**
- used in **online participation/bidding in e-auctions & online tenders** anywhere in India. Vendors who wish to participate in online tenders must have a Class 3 digital signature certificate.

Cyber risk and internal audit

- Threat from cyberattacks significant & evolving.
- Audit committees & BOD set expectation for internal audit to understand & assess organization's capabilities in risk management.
- **1st step for internal audit** : conduct cyber risk assessment & distil findings = summary for audit committee
- BOD will drive risk-based, multiyear cybersecurity internal audit plan.

Thank you