Cyber Forensics, Cryptography, Steganography (Module - 4 : DISSA Course)

Arijit Chakraborty

March 05, 2022

CYBER FORENSIC

- **Digital Forensic**
- *"Process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law)."*
- **Digital Evidence** =
- any information, data of probative value stored in binary form, transmitted , received by an electronic devices.

High –risk Cyber & forensic cases

- ✓ Criminal conspiracy ,
- ✓ Terrorist financing
- ✓ Corporate frauds
- ✓ Money laundering
- ✓ Tracking proceeds of organised crime
- ✓ National security
- ✓ Travel & field-work in high-risk countries with minimum occupational security or war zones

Safety Checklist of Forensic Auditor

- Cyber & Forensic auditor - develop Safeguards in professional engagement comprising:
- firm-wide safeguards &
- engagement-specific safeguards.
- Include appropriate Safety Checklist .
- Significance of personal **risk / threat to be evaluated**, monitored & safeguards applied when necessary.

Insurance Coverage

- Forensic audit firm =
- securing adequate insurance cover &
- Professional indemnity Insurance

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.

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**

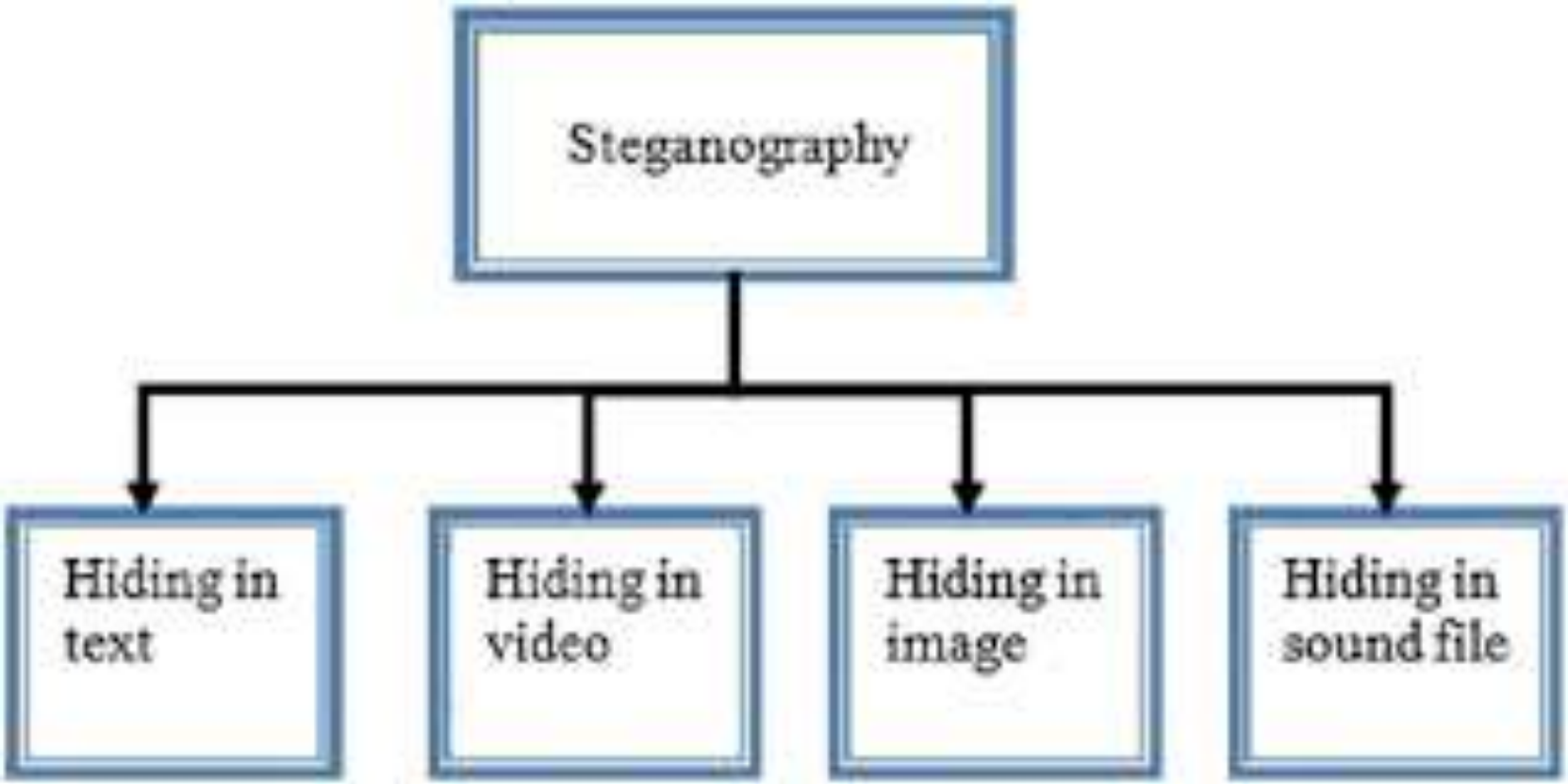
Cryptography & Steganography

- **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

AES

- AES (Advanced Encryption Standard) = most widely used symmetric encryption algorithm.
- AES used in applications -encryption of data at rest, & secure file transfer protocols like HTTPS.
- AES = successor to DES.
- **AES** = fast and secure form of encryption that keeps prying eyes away from our data.
- We see it in messaging apps like **WhatsApp** & **Signal**, programs like **VeraCrypt** , **WinZip**, in range of hardware & variety of tech
- Data Encryption Standard (DES) = symmetric encryption algorithm that was developed at IBM, DES only has a **56-bit key**
- When user to encrypt something, user taking the unencrypted data, called plaintext, and performing an algorithmic function on it to create a piece of encrypted ciphertext.
- Algorithm used is called the key.

256-Bit Encryption

- 256-bit encryption = data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files.
- One of the most secure encryption methods after 128- and 192-bit encryption,
- Used in most modern encryption algorithms, protocols and technologies including AES and SSL.
- A hacker or cracker will require 2^{256} different combinations to break a 256-bit encrypted message, =virtually impossible to be broken by even fastest computers.

Asymmetric encryption

- **Defence service**
- Devise mechanism for Defence agents to report securely.
- need regular detailed reports coming in
- **Asymmetric encryption** = allow to create public keys for agents to encrypt their information & private key at Defence HQ to decrypt it
- provides impenetrable form of 1-way communication.

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.**

DISSA - Exam related MCQ

- **1. MCAfee is an example of**
- A. Photo Editing Software
- B. Quick Heal
- C. Virus
- D. Antivirus
- **2. Which of the following is known as Malicious software?**
- A. illegalware
- B. badware
- C. malware
- D. maliciousware

- **3. To protect a computer from virus, user should install -------- in his computer.**
- A. backup wizard
- B. disk cleanup
- C. antivirus
- D. disk defragmenter
- **4. VIRUS stands for**
- A. Very Intelligent Result Until Source
- B. Very Interchanged Resource Under Search
- C. Vital Information Resource Under Siege
- D. Viral Important Record User Searched

- **5. Which of the following is/are threats for electronic payment systems?**
- A. Computer worms
- B. Computer virus
- C. Trojan horse
- D. All of the above
- **6. Key logger is a**
- A. Firmware
- B. Antivirus
- C. Spyware
- D. All of the above

- **7. A -------- is a computer program that can replicate itself and spread from one computer to another.**
- A. Antivurs
- B. PenDrive
- C. Mouse
- D. Computer Virus
- **8. Authentication is**
- A. modification
- B. insertion
- C. assure identity of user on a remote system
- D. none of the above

- **9. A ------- is a computer program that can invade Laptop & perform variety of functions from annoying(e.g. popping up messages) to dangerous (e.g. deleting files or destroying hard disk).**
- A. Ms Word
- B. Ms Access
- C. Antivirus
- D. Computer Virus
- **10. Which are the reasons for committing cyber crime :**
- A. Identity of attacker is unknown
- B. attack may be done remotely
- C. Fraud may not be discovered quickly
- D. It is considered ‘’ work of art’’ by some hackers
- Options
- 1. A & B
- 2. B&C
- 3. A,B,C
- 4. A,B,C,D