Chapter-5

Security

Chapter - 5

5. Basics of Information Security :

Introduction to security, Security threats: detection and prevention, Indian Cyber laws.

Gtech Poly

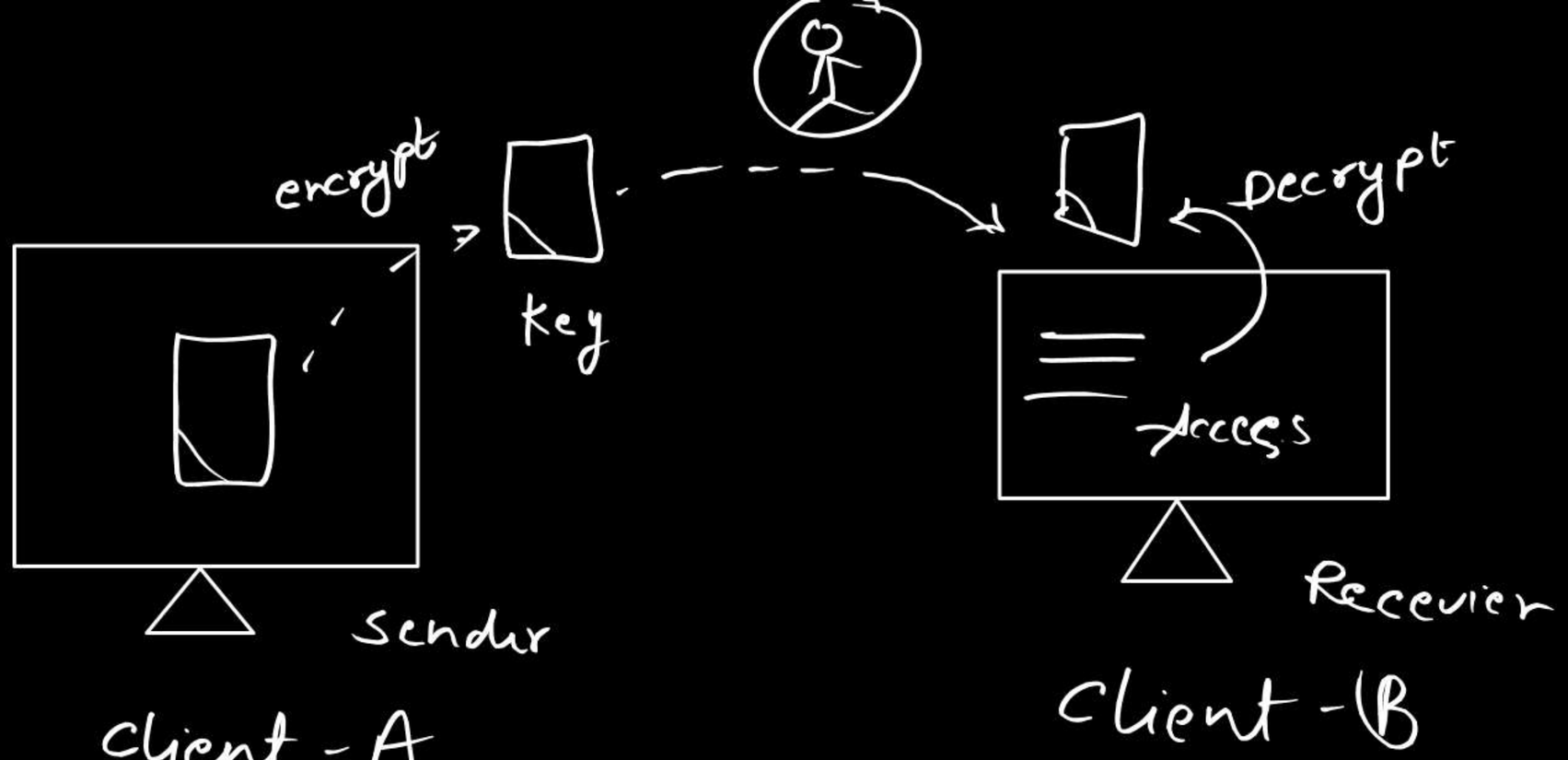
- **Basics of Information Security**

1. Introduction to Security:

Information Security (Infosec) का उद्देश्य डेटा और सूचना को अनधिकृत एक्सेस, उपयोग, प्रकटीकरण, संशोधन, या नष्ट होने से सुरक्षित रखना है।

मुख्य उद्देश्य:

- **Confidentiality (गोपनीयता):** डेटा को केवल अधिकृत उपयोगकर्ताओं तक सीमित रखना।
- **Integrity (अखंडता):** डेटा को सटीक और अप्रभावित बनाए रखना।
- **Availability (उपलब्धता):** डेटा और सिस्टम अधिकृत उपयोगकर्ताओं के लिए हमेशा उपलब्ध रहना।


encrypt
key
decrypt
Access
Sender
Receiver
Client - A
Client - B

English Notes:

- **Basics of Information Security**

1. Introduction to Security:

The purpose of Information Security (Infosec) is to protect data and information from unauthorized access, use, disclosure, modification, or destruction.

Main objectives:
Confidentiality: Restricting data to authorized users only.
Integrity: Keeping data accurate and unaltered.
Availability: Data and systems are always available to authorized users.

2. Security Threats: Detection and Prevention:

Security Threats (सुरक्षा खतरे) वे कारक होते हैं जो सूचना प्रणाली की सुरक्षा को प्रभावित कर सकते हैं।

Security Threats are factors that can affect the security of an information system.

Major types(प्रमुख प्रकार):

A. Malware (मैलवेयर):

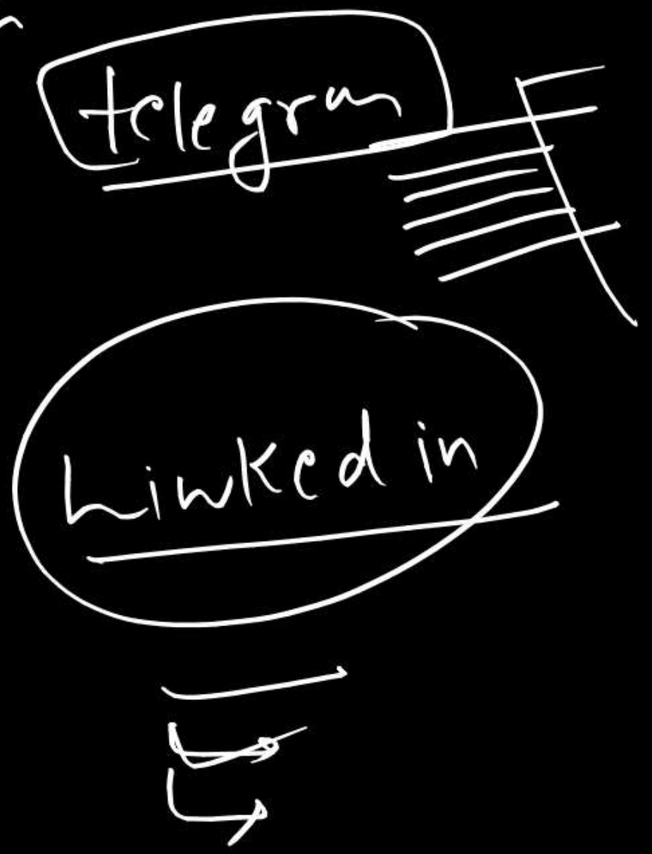
- Virus (वायरस): यह एक हानिकारक प्रोग्राम होता है जो खुद को अन्य फाइलों में जोड़ता है और सिस्टम को नुकसान पहुँचाता है।
- Worms (वर्म्स): यह वायरस की तरह ही होते हैं लेकिन स्वयं को नेटवर्क में फैलाने में सक्षम होते हैं।
- Trojan Horse (ट्रोजन हॉर्स): यह वैध सॉफ़्टवेयर की तरह दिखता है लेकिन वास्तव में हानिकारक कोड छुपाए रहता है।
- Ransomware (रैनसमवेयर): यह डेटा को एन्क्रिप्ट कर देता है और फिर फिरौती (ransom) मांगता है।
- Spyware (स्पाइवेयर): यह गुप्त रूप से उपयोगकर्ता की गतिविधियों को ट्रैक करता है।

A. Malware:

Virus: It is a harmful program that attaches itself to other files and damages the system.
Worms: These are similar to viruses but are capable of spreading themselves over networks.
Trojan Horse: It looks like legitimate software but actually hides harmful code.
Ransomware: It encrypts data and then demands ransom.
Spyware: It secretly tracks user activities.

Detection & Prevention:

- Antivirus & Anti-malware सॉफ़्टवेयर का उपयोग करें।
- संदिग्ध लिंक और अटैचमेंट को न खोलें।
- अपना सॉफ़्टवेयर और ऑपरेटिंग सिस्टम अपडेट रखें।



Detection & Prevention:

- Use antivirus & anti-malware software.
- Do not open suspicious links and attachments.
- Keep your software and operating system updated.

B. Phishing Attacks (फिशिंग हमले):

http://www.youtube.com
https://

- यह एक प्रकार का साइबर हमला है जिसमें धोखेबाज नकली ईमेल या वेबसाइट बनाकर उपयोगकर्ताओं से संवेदनशील जानकारी (जैसे पासवर्ड, बैंक विवरण) प्राप्त करने की कोशिश करता है।
- (It is a type of cyber attack in which fraudsters try to obtain sensitive information (such as passwords, bank details) from users by creating fake emails or websites.)

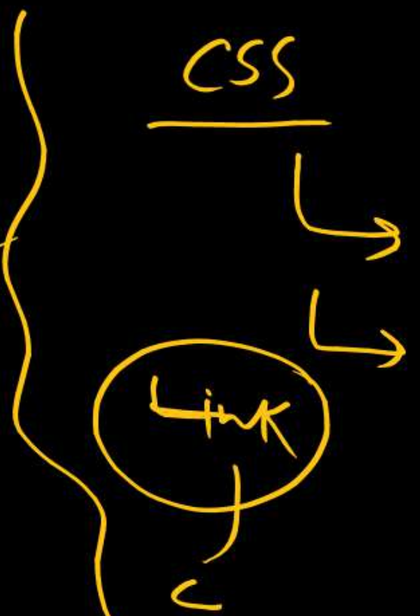
two fa

-Detection & Prevention:

- असली और नकली ईमेल की पहचान करना सीखें।
- HTTPS-enabled वेबसाइट्स का उपयोग करें।
- Two-Factor Authentication (2FA) चालू करें।

C. Denial of Service (DoS) और Distributed Denial of Service (DDoS) हमले:

- DoS: किसी सर्वर या नेटवर्क को अधिक ट्रैफिक भेजकर ठप कर देना।
- DDoS: यह DoS का ही उन्नत रूप होता है, जिसमें कई कंप्यूटर मिलकर हमला करते हैं।



Detection & Prevention:

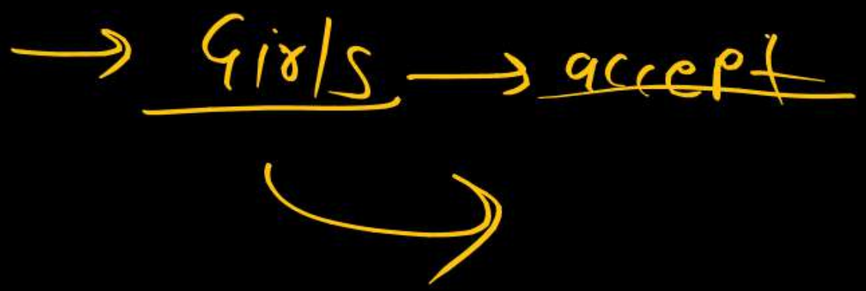
- Intrusion Detection Systems (IDS) और Firewalls का उपयोग करें।
- Content Delivery Networks (CDN) का उपयोग करें।

D. Social Engineering (सामाजिक अभियंत्रण):

- यह एक प्रकार की साइबर अपराध तकनीक है जिसमें लोगों को मनोवैज्ञानिक रूप से धोखा देकर संवेदनशील जानकारी प्राप्त की जाती है।

Detection & Prevention:

- अज्ञात कॉल, ईमेल, या संदेशों का उत्तर न दें।
- संदिग्ध अनुरोधों की पुष्टि करें।



3. Indian Cyber Laws (भारतीय साइबर कानून):

भारत में साइबर अपराधों को रोकने और सूचना सुरक्षा को बनाए रखने के लिए Information Technology Act, 2000 (IT Act, 2000) लागू किया गया।

The Information Technology Act, 2000 (IT Act, 2000) was enacted to prevent cyber crimes and maintain information security in India.

महत्वपूर्ण प्रावधान:

- **Section 43:** अनधिकृत एक्सेस, डेटा चोरी, वायरस हमले के लिए जुर्माना और दंड।
- **Section 66:** साइबर अपराधों के लिए सजा (हैकिंग, धोखाधड़ी, पहचान की चोरी)।
- **Section 66C:** पहचान की चोरी और इलेक्ट्रॉनिक दस्तावेजों की जालसाजी।
- **Section 66D:** फ़िशिंग और साइबर धोखाधड़ी के लिए दंड।
- **Section 67:** अश्लील सामग्री का प्रसार करने पर दंड।
- **Section 69:** सरकारी एजेंसियों को राष्ट्रीय सुरक्षा के लिए संचार निगरानी करने का अधिकार।

- **Important provisions:**

Section 43: Penalties and penalties for unauthorised access, data theft, virus attack.
Section 66: Punishment for cyber crimes (hacking, fraud, identity theft).
Section 66C: Identity theft and forgery of electronic documents.
Section 66D: Penalties for phishing and cyber fraud.
Section 67: Penalty for disseminating obscene material.
Section 69: Power of government agencies to conduct communications surveillance for national security.