Cryptography: Introduction

Prof. Ashok K Bhateja, IIT Delhi

Definitions

- Cryptology: Making & Breaking Codes & Ciphers
- Cryptography: Science of *creating* codes or ciphers
- Cryptanalysis: Science of *breaking* codes and ciphers
- Code: Substitution of words or phrases by others
- Cipher: Algorithm for encrypting and decrypting data
  - Algorithmic scrambling/unscrambling
  - Example: Caesar cipher

    Replace each letter with the letter 3 positions after it in the alphabet (a $\Rightarrow$ d, b $\Rightarrow$ e, etc.)

Cryptography vs. Steganography

- In Greek
  - Cryptography: secret writing
  - Steganography: covered writing
- Steganography: is the hiding of a secret message within an ordinary message or image
- Steganography and Cryptography make great partners. It is common practice to use cryptography with steganography.

Cybersecurity

- Cyber security is the practice of protecting information and data from cyberspace i.e., outside sources, on the Internet.
- Cybersecurity professionals ensures that only authorized people have access to the information.
- Modern industries and research organizations are heavily dependent on the computers that store and transmit sensitive information like
  - intellectual property
  - financial data
  - personal information

  for whose exposure may have negative consequences.
- Attackers attempt to access these sensitive informations with the aim to disable, disrupt, destroy or steal the data.

Elements of Cyber Security

- Network security
- Application security
- Information security
- Operational security
- Cloud Security
- Internet of Things (IoT) security

Network Security

- It is process/activity to protect the computer networks from intruders, may be targeted attackers or opportunistic malware.
- Network security combines the defences of the network layers by implementing security policies and controls so that only authorized user may get access in the network, but unauthorized users are blocked to get access in the network.
- Network security professionals make the network more secure by providing technical expertise including help with intrusion detection systems, encryption, firewalls, and digital certificates.

Types of Network Security

- Firewalls
- Anti-malware program
- Email security
- Network Segmentation
- Data Loss Prevention
- Intrusion Prevention System

Application security

- Cyber criminals try to find the vulnerability in the application of the organization to steal sensitive data and intellectual property.
- Application security includes various security features like authentication, encryption, application security testing to reduce the vulnerability.

Information security

- Information is data (or raw data) converted into useful form for human being. It includes records, personal data and intellectual property of an organization.
- Protecting the information is very important as it is the heart of the organization.
- Cryptography techniques are used to protect the information from cyber threats and unauthorized access.

Operational security

- Operational security also known as procedural security or administrative security.
- It encloses the creation and enforcement of policies, procedures, and guideline documents.
- Its goal is to control information and observable actions about an organization's capabilities, limitations, and intentions to prevent or control exploitation of available information by an adversary.

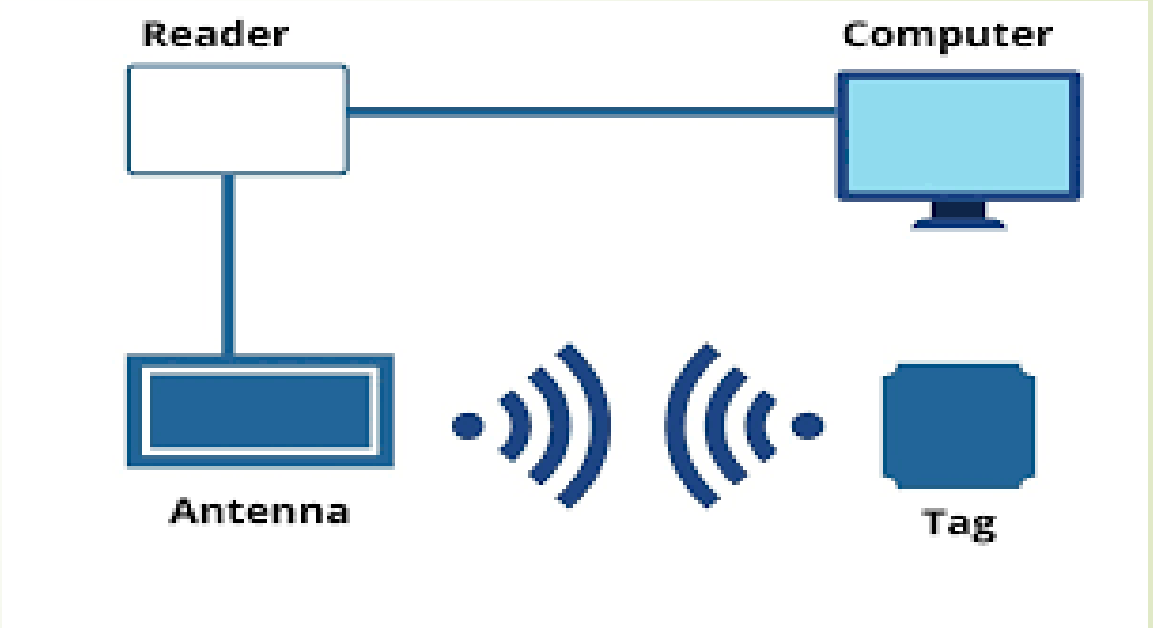
Cloud Security

- Cloud security refers to the technologies, policies, control and services to protect data, applications and infrastructure stored in cloud platforms.
- The privacy and safety of these systems depends on the security efforts of cloud provider and clients that use the cloud.
- Major threats to the cloud security are data breaches and data leaks, data loss, insecure application user interfaces (APIs) stored in the cloud include data loss, misconfigured cloud storage, account hijacking, service traffic hijacking.
- The wide range of raw data and processed data in the cloud attracts the hackers to extract the important informations.
- Encryption of the data is an excellent precaution against any kind of threat. It ensures that no one have the access of the private information stored in the cloud.

Internet of Things (IoT) security

- The IoT is a global network connecting things consists of any real-world object like home appliances, clothes, etc. or living things (plants, animals, and people) through numerous technologies such as RFID (Radio Frequency Identification) and barcodes.

- RFID is gaining strong support from the business community due to its maturity, low cost, and low power.
- RFID comprised of two components: tags and readers.
- Sensors and actuators are also important to IoT.



Cryptography in Cyber Security

- Cryptography lies at the heart of all cyber security technologies
- Cryptography plays very important role to protect enterprise information and communication from cyber threats using mathematical encryption functions.
- These cryptographic techniques allow only the authorized sender and recipient to see the content of a message.
- Cryptography helps to achieve the goals of cyber security by ensuring confidentiality, integrity and Authentication.

Main Components of Security

Information security model made up of the three main components (CIA triad)

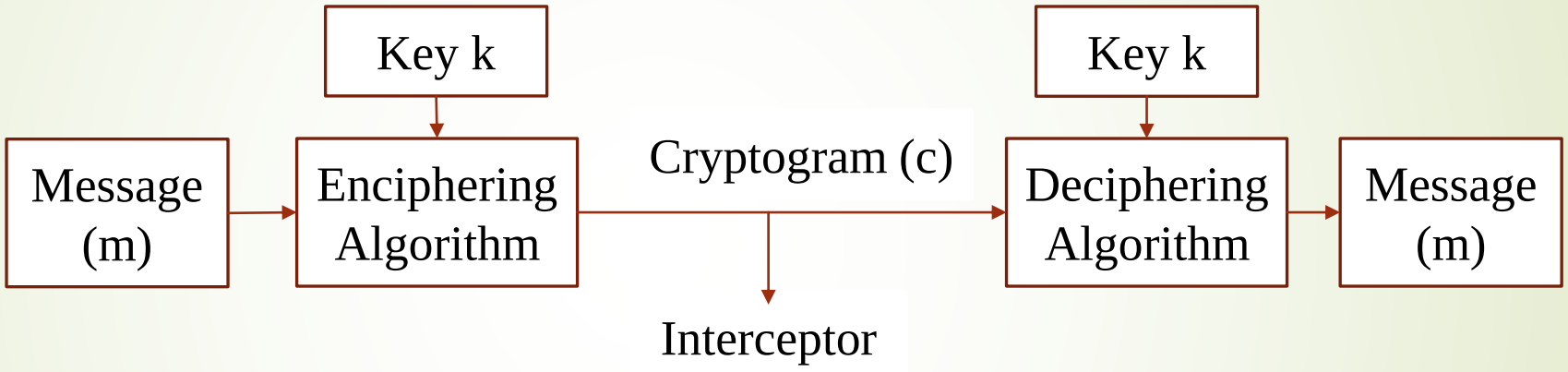
- Confidentiality: Ensuring that no one can read the message except the intended receiver.
  - Encryption.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
  - to protect data integrity hashing the data is used.
- Authentication: The process of proving one's identity.
  - Message Authentication Code (MAC).

Authenticity and Non-repudiation

- Authenticity is about one party (say, Alice) interacting with another (Bob) to convince Bob that some data really comes from Alice.
- Non-repudiation is about Alice showing to Bob a proof that some data really comes from Alice, such that not only Bob is convinced, but Bob also gets the assurance that he could show the same proof to Charlie, and Charlie would be convinced, too, even if Charlie does not trust Bob.
- Therefore, a protocol which provides non-repudiation necessarily provides authenticity as a byproduct; in a way, authenticity is a sub-concept of non-repudiation.
- The recipient of data is provided with proof of the origin of data. This will protect against any attempt by the sender to falsely deny sending the data or its contents

Cipher System

- Also called secrecy system



- Message space *M*: set of all possible messages, m $\in$ *M*
- Cryptogram Space C: set of all cryptograms, c $\in$ *C*
- Key space *K*: set of all keys, k $\in$ *K*
- c = *f* (m, k); f is enciphering algorithm

Properties of a secure cipher (Confusion and Diffusion)

Shannon's definitions

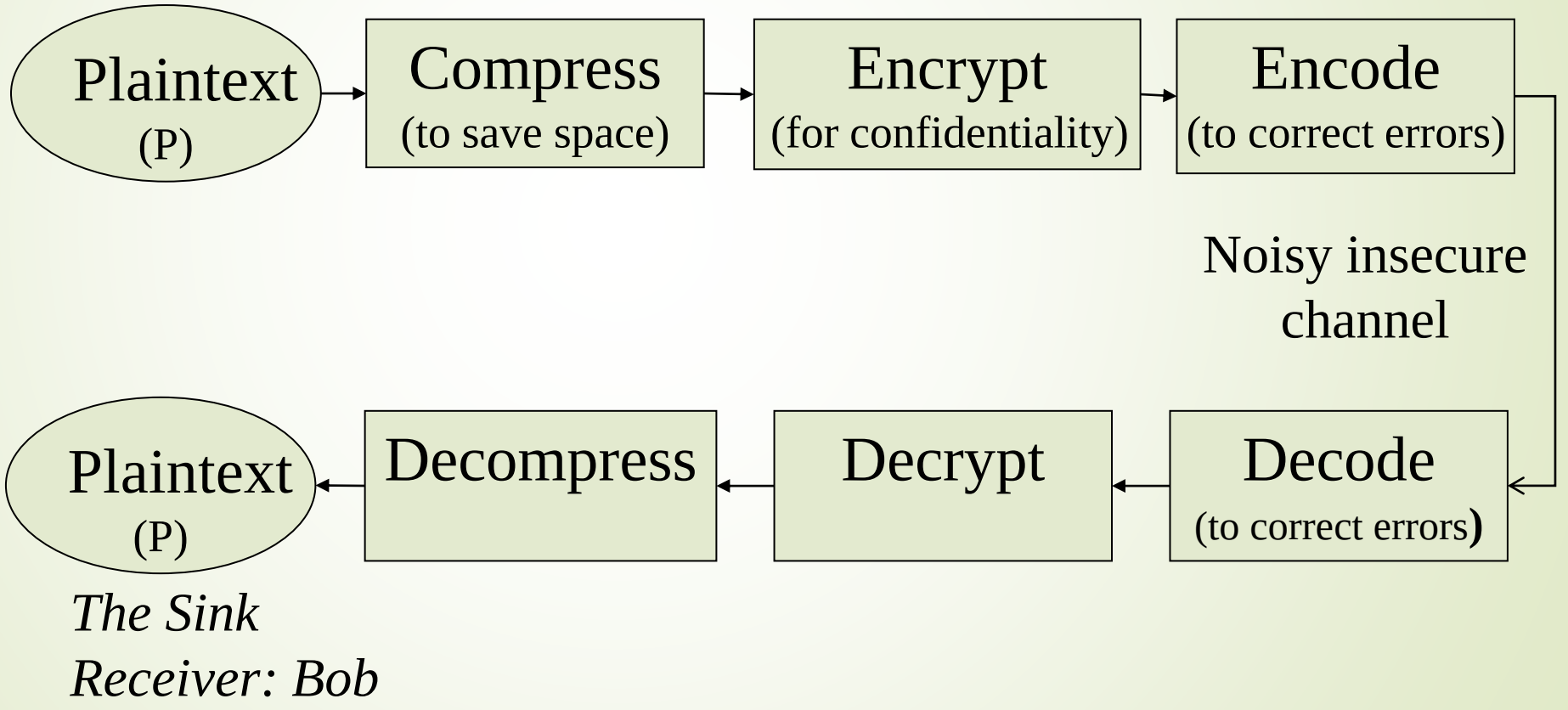
- Confusion refers to making the relationship between the ciphertext and the symmetric key as complex and involved as possible.

  Confusion makes it difficult to find the key from the ciphertext.

- Diffusion refers to dissipating the statistical structure of plaintext over the bulk of ciphertext.

Secure Communication

The Source
Sender: Alice



The Sink
Receiver: Bob

Kerckhoffs's principle

- A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.
- Kerckhoffs gave six design principles for military ciphers:
  - The system must be practically, if not mathematically, indecipherable.
  - It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
  - Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents.
  - It must be applicable to telegraphic correspondence.
  - Apparatus and documents must be portable, and its usage and function must not require the concourse of several people.
  - Lastly, given the circumstances in which it is to be used, the system should be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Cryptanalytic Attacks

- Ciphertext Only
  - The ciphertext c = *f* (m, k) is known to the opponent; m and k are unknown.
- Corresponding Plain and Ciphertext
  - The plaintext m and ciphertext c = *f* (m, k) are both known to the opponent; k is unknown.
- Chosen Plaintext and corresponding Ciphertext.
  - The plaintext m and ciphertext c = *f* (m, k) are both known for some set of chosen plaintext.
- Chosen Ciphertext and corresponding Plaintext
  - The ciphertext c = *f* (m, k) and plaintext m are both known for some set of chosen ciphertext.