Cryptographic Systems

CST 332-2

M.RAMASHINI

DEPARTMENT OF COMPUTER SCIENCE AND TECHNOLOGY

Recommended Texts:

- Katz,J and Lindell,Y, 2007, Introduction to Modern Cryptography
- Stallings ,W, 2013 Cryptography and Network Security: Principles and Practice , 6th Edition

History and overview of cryptography

Cryptography and Modern Cryptography

- Cryptography as the art of writing or solving codes.(Oxford Dictionary)
- This definition may be historically accurate, but it does not capture the essence of modern cryptography.
- In the late 20th century, this picture of cryptography radically changed.
- A rich theory emerged, enabling the rigorous study of cryptography as a science.

- Now it deals with the problems of message authentication, digital signatures, protocols for exchanging secret keys, authentication protocols, electronic auctions and elections, digital cash and more…….

- In fact, modern cryptography can be said to be concerned with problems that may arise in any distributed computation that may come under internal or external attack

MODERN CRYPTOGRAPHY

Scientific study of techniques for securing digital information,

transactions, and

distributed computations.

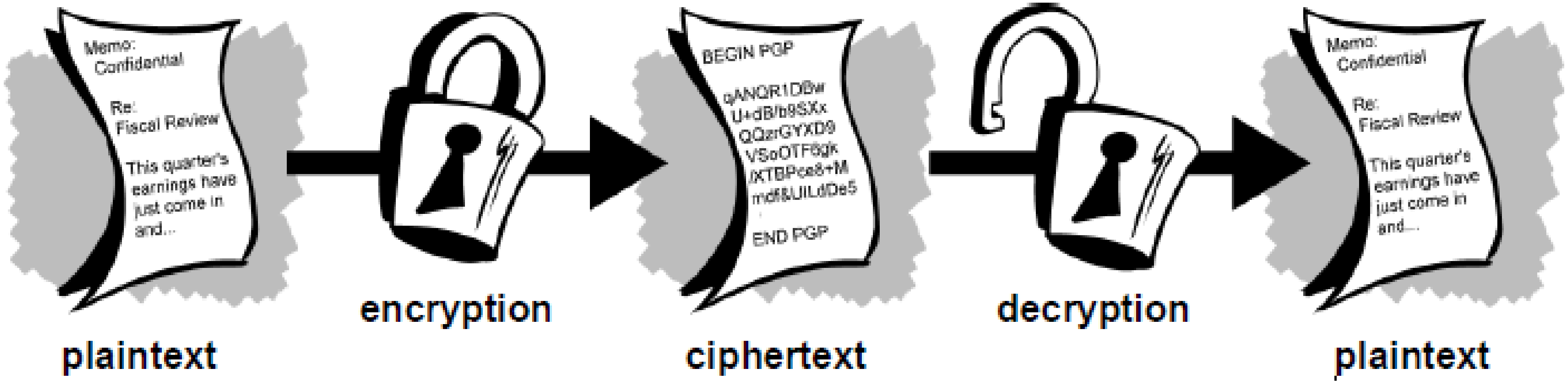
- Historically, the major consumers of cryptography were military and intelligence organizations

But Today…………….

- Security mechanisms that rely on cryptography are an integral part of almost any computer system.
- Users (often unknowingly) rely on cryptography every time they access a secured website.
- Cryptographic methods are used to enforce access control in multi-user operating systems, and to prevent thieves from extracting trade secrets from stolen laptops.
- Software protection methods employ encryption, authentication, and other tools to prevent copying.

- Cryptography has gone from an art form that deal with secret communication for the military to a science that helps to secure systems for ordinary people all across the globe.
- This also means that cryptography is becoming a more and more central topic within computer science.

Encryption and decryption



- Data that can be read and understood without any special measures is called *plaintext* or *cleartext*
- The method of disguising plaintext in such a way as to hide its substance is called *encryption*
- Encrypting plaintext results in unreadable gibberish called *ciphertext*.
- You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data.

How does cryptography work?

- A *cryptographic algorithm*, or *cipher*, is a mathematical function used in the encryption and decryption process.
- A cryptographic algorithm works in combination with a *key* (a word, number, or phrase) to encrypt the plaintext.
- The same plaintext encrypts to different ciphertext with different keys.
- The security of encrypted data is entirely dependent on two things:

  The strength of the cryptographic algorithm

  The secrecy of the key
- A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a *cryptosystem*.

Computer Security:

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity, availability**, and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

- This definition introduces three key objectives that are at the heart of computer security

Confidentiality

This term covers two related concepts:

- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

- **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity:

This term covers two related concepts:

- **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.

- **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability:

- Assures that systems work promptly and service is not denied to authorized users.

- These three concepts form what is often referred to as the **CIA triad**. The three concepts embody the fundamental security objectives for both data and for information and computing services

NIST standard FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*)

Characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and afteraction recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Thank you