Cryptography

LECTURE 4

Cryptography: Early Applications and Examples

Cryptography deals with protection and preservation of information in all its forms. This science has evolved dramatically over time, but its underlying goal has never changed, even though the tools have.

In cryptography field, encryption gets by far the most attention for manipulating and protecting information.

cryptanalysis, which deals with unlocking or uncovering the secrets that others try so hard to hide or obscure

History of Cryptography

- The intricate patterns and glyphs used in Egyptian hieroglyphics
- The ancient Egyptians were probably using the system not so much to withhold secrets but because they wanted a special writing system to commune with their gods and eternity.
- It is believed that only members of the royal family and the religious orders could fully understand how to read and write the system and comprehend it fully.
- the writing system became more complex; eventually the public and those who could write the language either passed away or turned their interests to other endeavors, and the ability to decipher the symbols was lost for a time.

The Rosetta stone

The Rosetta stone was the key that allowed modern civilization to understand a language that was nearly lost,

though it took over 20 years of concerted effort to reveal the language to the world once again.

Tracing the Evolution

One of the most widely used applications of cryptography is in the safeguarding of communications between two parties wanting to share information.

In today's world, not only must information be kept secret, but provisions to detect unwelcome or unwanted modifications are just as important.

Is the body of knowledge relating to cryptography concerned only with protecting information?

Well, in the first few generations of its existence, the answer was yes, but that has changed

Goals cryptography nowadays seek to achieve

Confidentiality: is the primary goal that encryption seeks to achieve. Encryption is done to keep secret information from disclosure, away from prying eyes.

Integrity: Cryptography can detect changes in information and thus prove its integrity or original unmodified state.

Authentication: Cryptography allows a person, object, or party to be identified with a high degree of confidence. Authentication is an essential component of a secure system because it allows software and other things to be positively identified. (Two-key authentication)

Nonrepudiation: The ability to provide positive identification of the source or originator of an event is an important part of security. (a person engaged in an agreement can not claim later on he is not the issuer of this agreement)

Key Distribution: One of the most valuable components of a cryptosystem is the key, which is the specific secret combination or code used in a cryptographic function.

How Does It Work?

Plain Text/Clear Text: lain text is the original message. It has not been altered; it is the usable information.

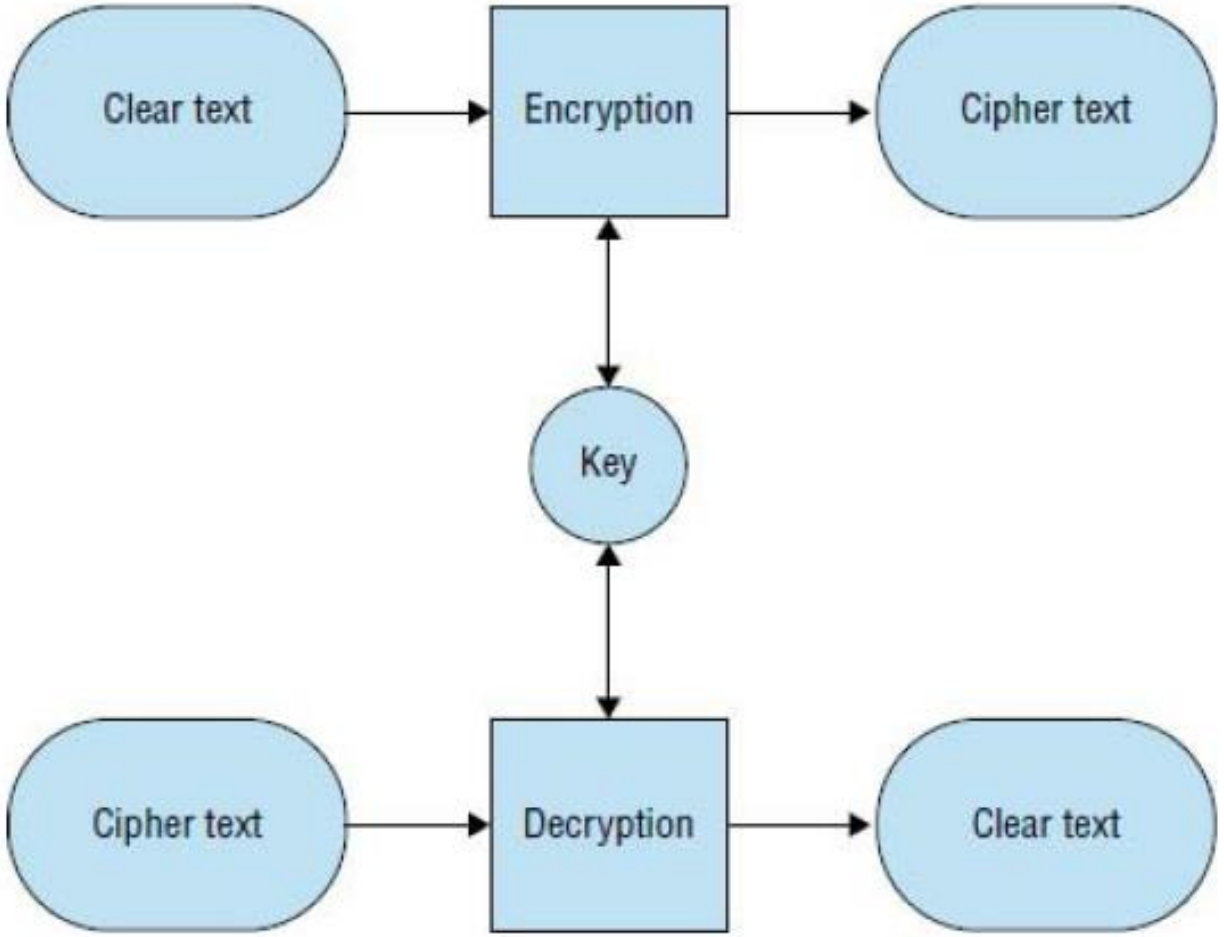
Cipher Text Cipher text is the opposite of plain text; it is a message or other data that has been transformed into a different format using a mechanism known as an algorithm. It is also something that can be reversed using an algorithm and a key

Algorithms transform clear text into cipher text. a formula that includes discrete steps that describe how the encryption and decryption process is to be performed in a given instance.

Keys: A key is a discrete piece of information, usually random in nature, that determines the result or output of a given cryptographic operation. It can be thought of in the same way a key in the physical world is, as a special item used to open or unlock something—in this case, a piece of information.

types of cryptography

- symmetric
- asymmetric (aka public-key cryptography).



Symmetric Cryptography

The Same key is used for both encryption and decryption and must be kept secret

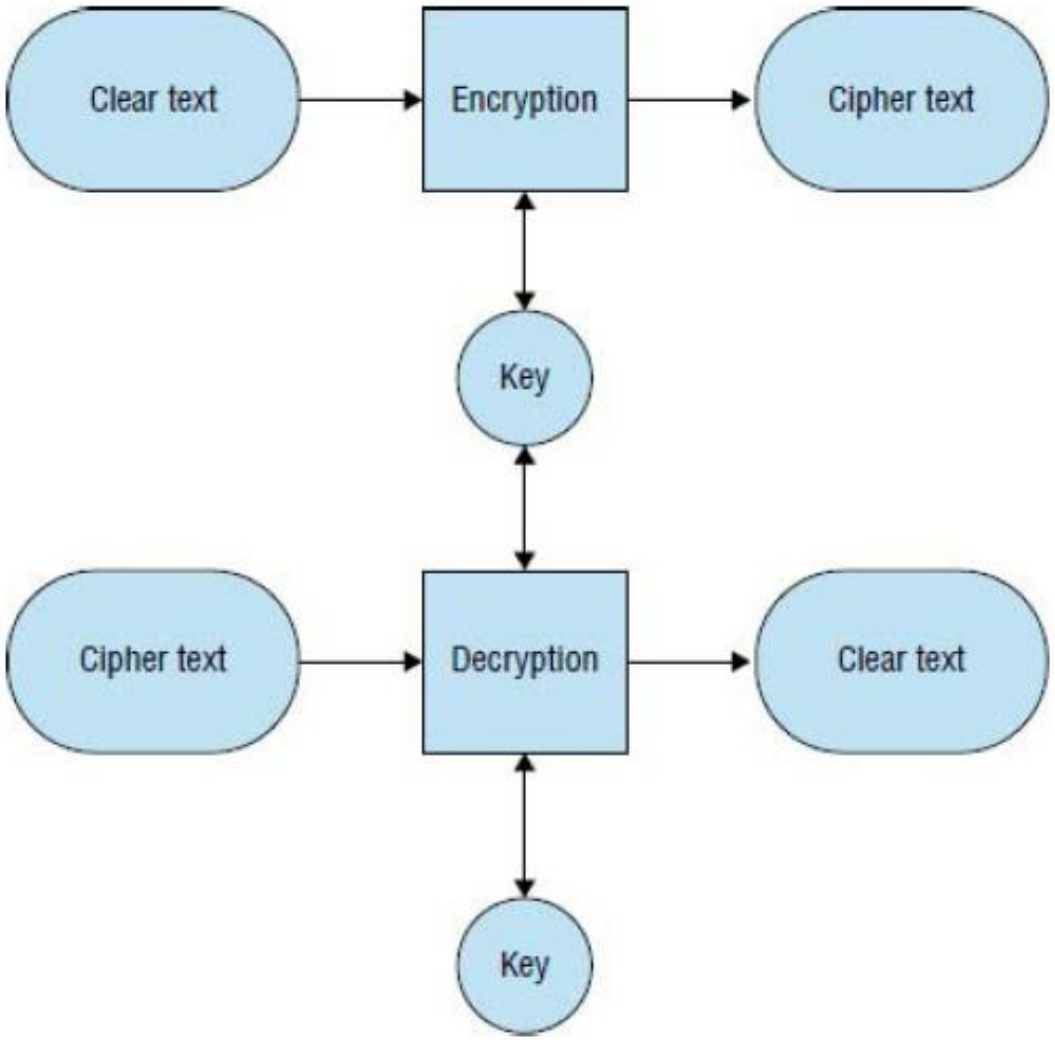
Symmetric Cryptography

symmetric algorithms are great at all of the following:

- Preserving confidentiality
- Increased speed over many non-symmetric systems
- Ensuring simplicity (relatively speaking, of course)
- Providing authenticity

Symmetric algorithms have drawbacks in these areas:

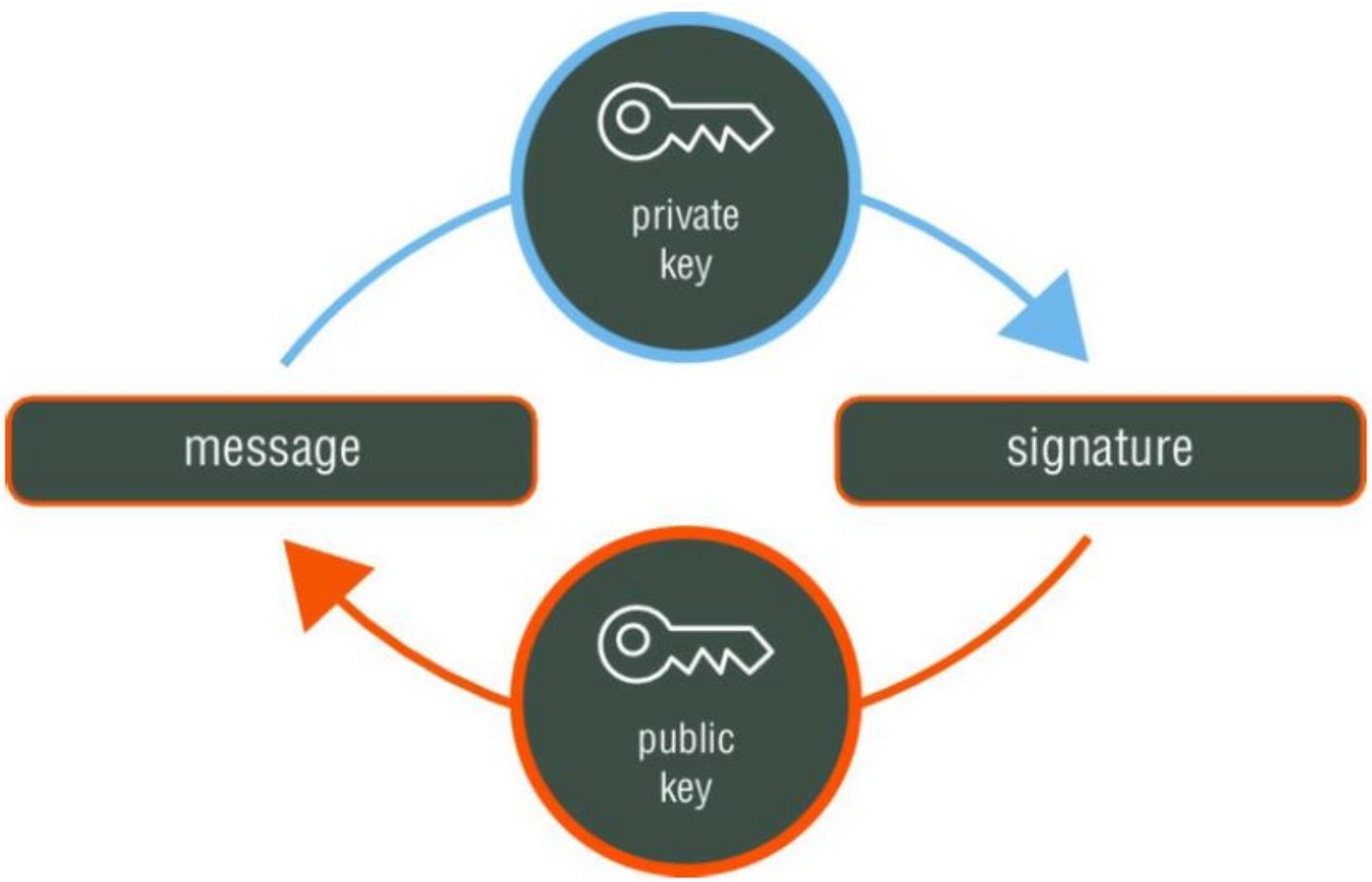
- Key management issues
- Lack of nonrepudiation features



Asymmetric, or Public Key, Cryptography

How it works

- The concept of public key cryptography was intended to overcome the key management problems inherent in previous systems.
- In this system, each user who is enrolled receives a pair of keys called the public key and the private key. Each person's public key is published, whereas the private key is kept secret.
- By creating the keys this way, the need for a shared symmetric key is eliminated. This option also secures the communication against eavesdropping or betrayal.
- In addition, this system of generating keys provides a means of nonrepudiation that is not possible with symmetric systems.



Digital Signature

Since anything encrypted with the private **key can be reversed only with the corresponding public** key and only one person holds the private key, then the identity of the encrypting party can be assured.

Understanding Hashing

hashing can be considered a type of one-way encryption. More accurately, it is a process that creates a scrambled output that cannot be reversed. The process outputs what is known as a *hash*, *hash value*, or *message digest*. (Passwords storage)

Designed to be a one-way process, hashing is commonly used to validate the integrity of information.

A hash function generates a fixed-length value that is always the same length no matter how large or small the data entering the process or algorithm is.

The fixed-length value is unique for every different input that enters the process. It is because of this unique property and its behavior that hashes are used to detect the changes that can happen in data of any type.

Issues with Cryptography

Cryptographic systems are all vulnerable to what is known as a brute-force attack. In such an attack, every possible combination of characters is tried in an attempt to uncover a valid key.

Budget	40-bit Key	56-bit Key
Regular user	1 week	40 years
Small business	12 minutes	556 days
Corporation	24 seconds	19 days
Large multinational	0.005 seconds	6 minutes
Government	0.0002 seconds	12 seconds