

CYB650

Introduction to Cryptography

Foundations and principles of Cryptography



Prepared by Dr. Esraa Saleh Alomari
Lecture #1



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

The modules during this course are as follows:

- *Module 1: Foundations and principles of Cryptography*
- *Module 2: Cryptography protocols*
- *Module 3: Cryptography techniques*
- *Module 4: Cryptography Algorithms*
- *Module 5: Public key Algorithms*



The module covers the basics of Foundations and principles of Cryptography are as follows:

- *Story of Cryptography*
- *Definitions*
- *Encryption & Decryption*
- *Strong Cryptography*
- *How does Cryptography work?*
- *Classical encryption techniques*
- *Symmetric Cipher Model*



When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the “shift by 3” rule could decipher his messages.

From Here We Begin



Definitions (Stallings W.)

- ◆ ***Plaintext***: an original message
- ◆ ***Ciphertext*** : the coded message
- ◆ ***Enciphering or Encryption*** : the process of converting from plaintext to ciphertext

Definitions (Stallings W.)

- ◆ ***Deciphering OR Decryption:*** restoring the plaintext from the ciphertext
- ◆ ***Cryptography:*** the many schemes used for encryption constitute the area of study such a scheme is known as a ***cryptographic system*** or a ***cipher***
- ◆ ***Cryptanalysis :*** Techniques used for deciphering a message without any knowledge of the enciphering, cryptanalysis is what the layperson calls ***“breaking the code.”***

The areas of cryptography and cryptanalysis together are called

cryptology

◆ **Cryptography** is the science of keeping secrets secret. Assume a sender referred to here and in what follows as Alice (as is commonly used) wants to send a message m to a receiver referred to as Bob. She uses an insecure communication channel.

◆ For example, the channel could be a computer network or a telephone line. There is a problem if the message contains confidential information. The message could be intercepted and read by an eavesdropper. Or, even worse, the adversary, as usual referred to here as Eve, might be able to modify the message during transmission in such a way that the legitimate recipient Bob does not detect the manipulation.

One objective of cryptography is to provide methods for preventing such attacks

◆ *Cryptography* is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

◆ *Cryptanalysis* is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

◆ **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 make sure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of converting ciphertext to its original plaintext is called *decryption*.

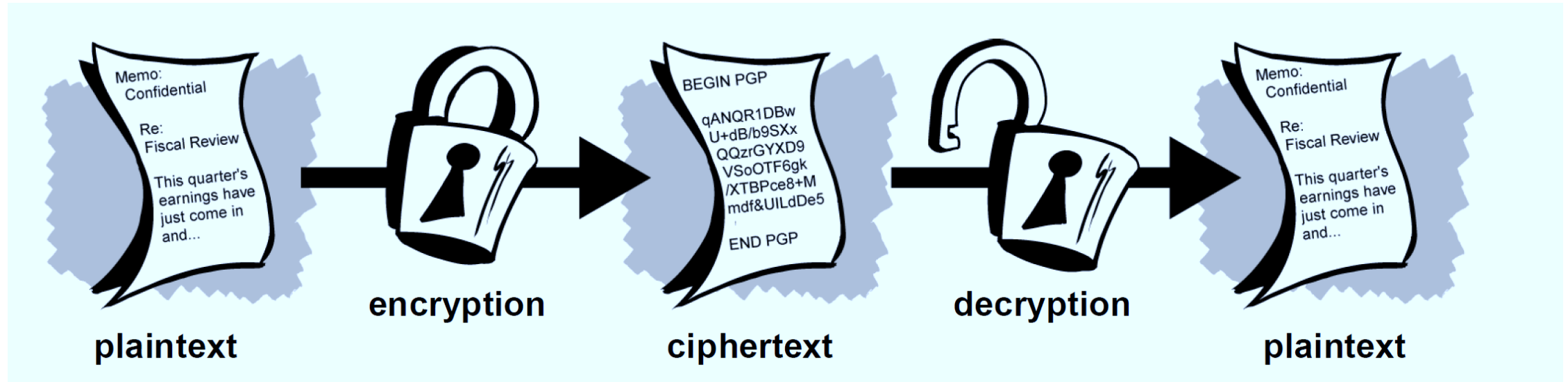


Figure 1 : Encryption & Decryption Process

“There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files”

❑ **Cryptography** can be *strong* or *weak*, as explained above.

Cryptographic strength is measured in the time and resources it would require to recover the plaintext. The result of *strong cryptography* is ciphertext that is very difficult to decipher without possession of the appropriate decoding tool.

How does Cryptography Work?

- ❑ **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.
- ❑ **A cryptographic algorithm**, plus all possible keys and all the protocols that make it work, comprise a *cryptosystem*. **PGP is a cryptosystem.**

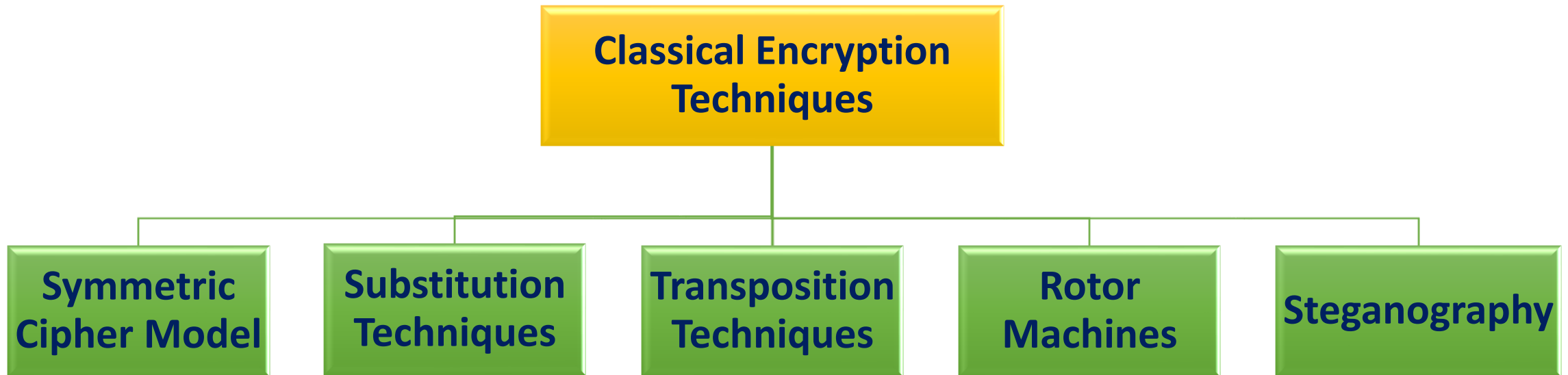


Figure 2 : Classical Encryption Techniques

- ❑ Is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic data. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys - one public and one private - is used to encrypt and decrypt messages.

❑ *A symmetric encryption scheme has five ingredients:*

- ✓ **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input
- ✓ **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext

- ✓ **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key

- ✓ **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- ✓ **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Symmetric Cipher Model

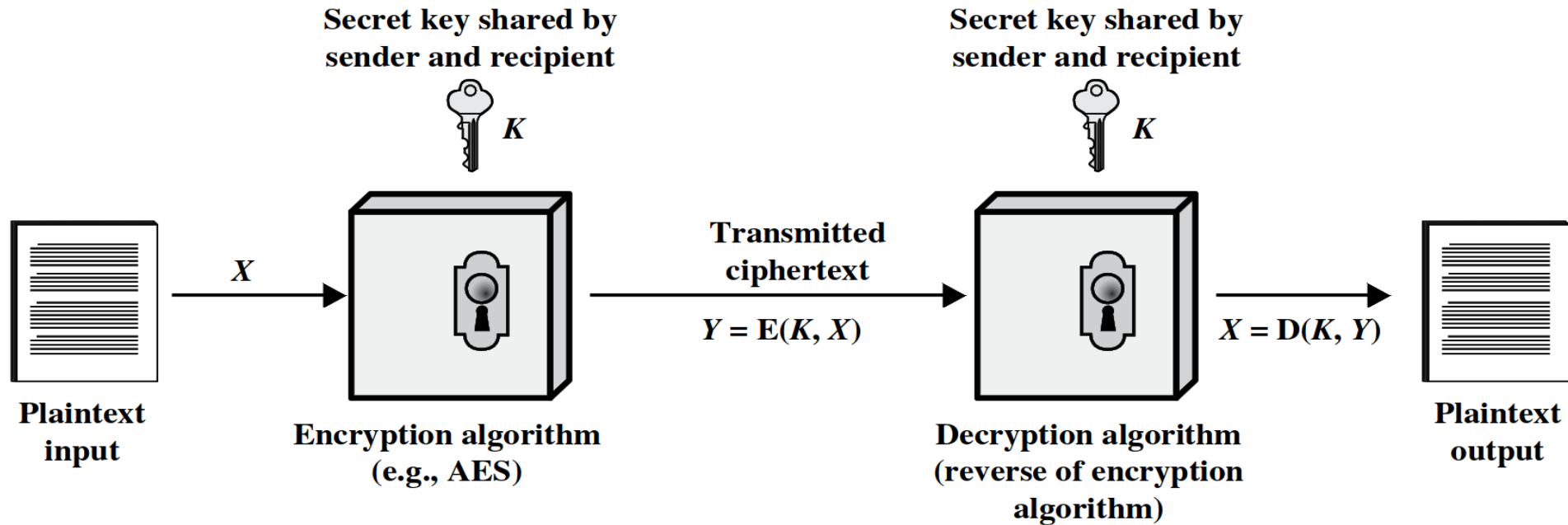


Figure 3 : Simplified Model of Symmetric Encryption

❑ *There are two requirements for secure use of conventional encryption:*

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plain-text that produced each ciphertext

❑ *There are two requirements for secure use of conventional encryption:*

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

❑ *Hints....*

- ✓ *We do not need to keep the algorithm secret; we need to keep only the key secret. This feature of symmetric encryption is what makes it feasible for widespread use.*

- ✓ The fact that the algorithm need not be kept secret means that manufacturers can and have developed low-cost chip implementations of data encryption algorithms. These chips are widely available and incorporated into a number of products. With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key

Symmetric Cipher Model

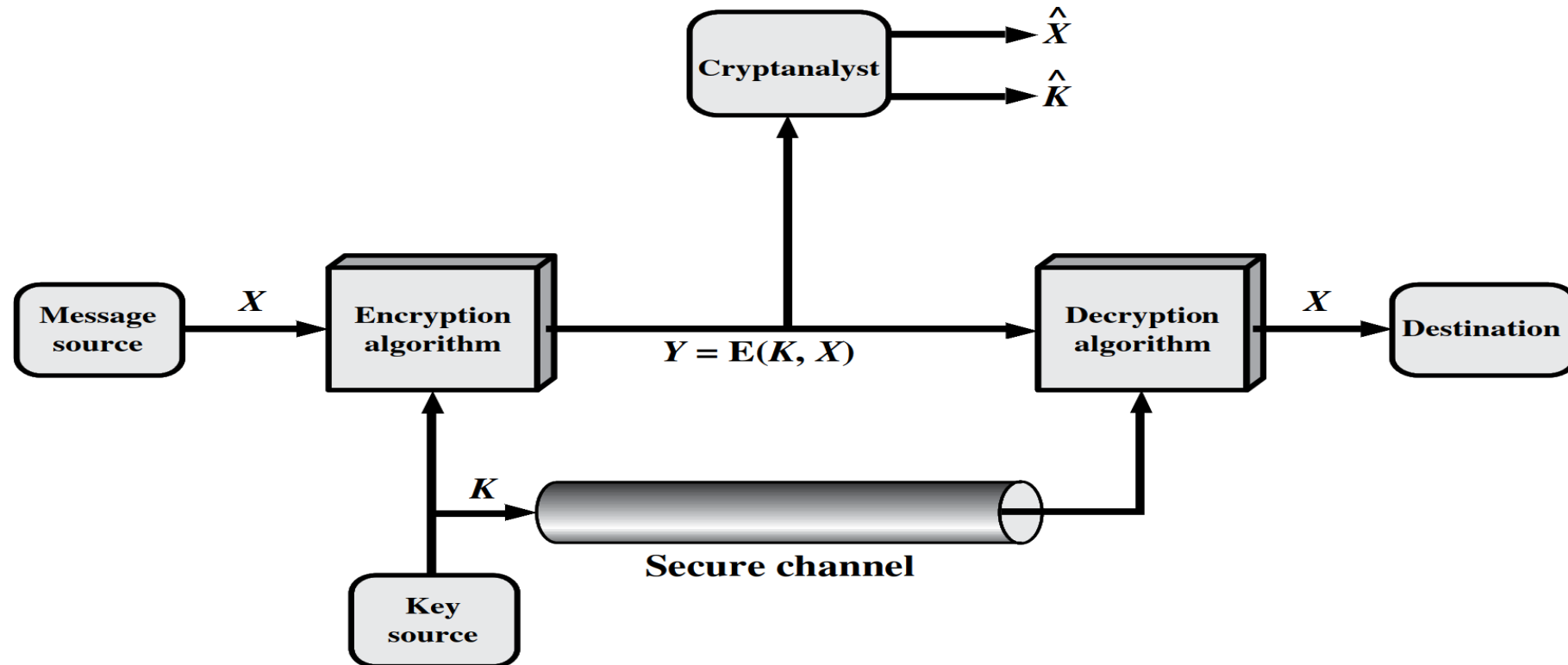


Figure 4 : Model of Symmetric Cryptosystem

- Let us take a closer look at the essential elements of a symmetric encryption scheme
- A source produces a message in plaintext, $X = [X_1, X_2, c, X_M]$
- The M elements of X are letters in some finite alphabet

Symmetric Cipher Model (An Example)

- Traditionally, the alphabet usually consisted of the 26 capital letters. Nowadays, the binary alphabet $\{0, 1\}$ is typically used. For encryption, a key of the form $K = [K_1, K_2, c, K_J]$ is generated
- If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination

Symmetric Cipher Model (An Example)

- With the message X and the encryption key K s input, the encryption algorithm forms the ciphertext $Y = [Y_1, Y_2, c, Y_N]$ We can write this as

$$Y = E(K, X)$$

- This notation indicates that Y is produced by using encryption algorithm E as a function of the plaintext X with the specific function determined by the value of the Key K

- The intended receiver, in possession of the key, is able to invert the transformation:

$$X = D(K, Y)$$

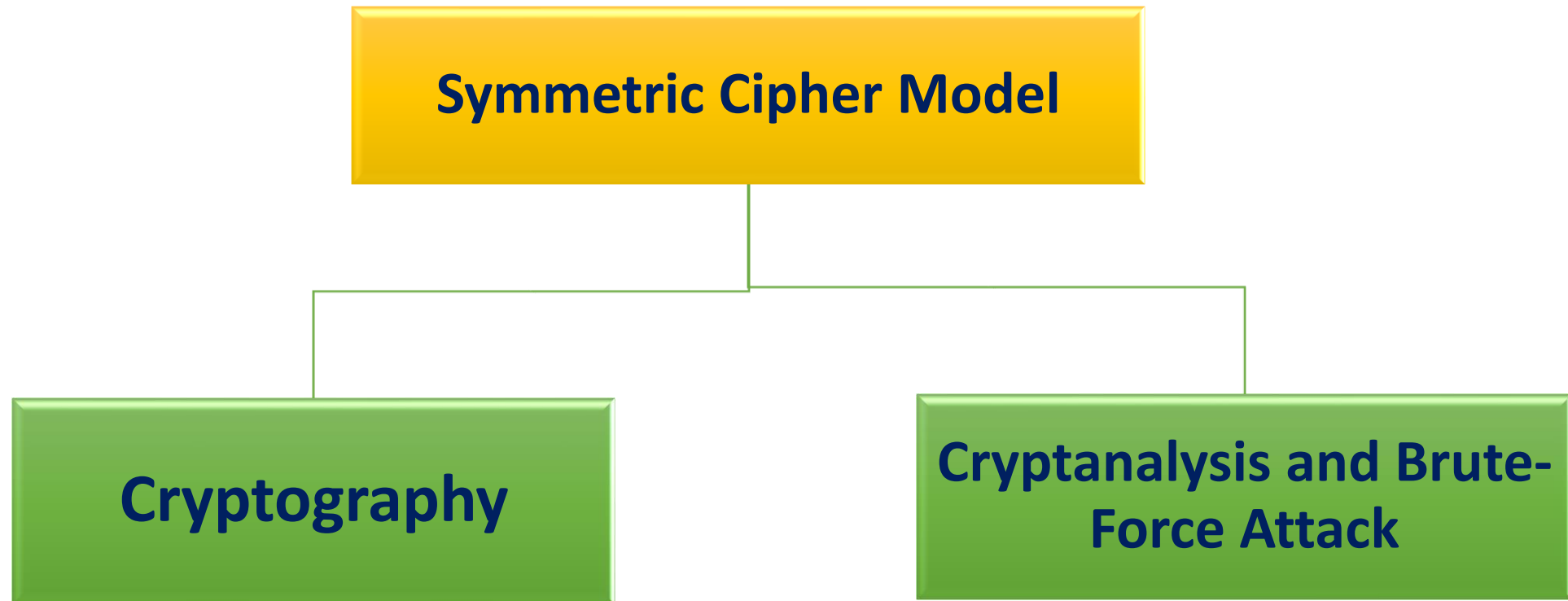


- The intended receiver, in possession of the key, is able to invert the transformation:

$$X = D(K, Y)$$

- An opponent, observing Y but not having access to **K or X** may attempt to recover **X or K or both X and K** It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms

- If the opponent is interested in only this particular message, then the focus of the effort is to recover X by generating a plaintext estimate $\hat{X}$. Often, however, the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating an estimate $\hat{K}$.



❑ *Cryptographic systems are characterized along three independent dimensions:*

1. The type of operations used for transforming plaintext to ciphertext.

All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged.

The fundamental requirement is that no information be lost (i.e., that all operations are reversible). Most systems, referred to as *product systems*, involve multiple stages of substitutions and transpositions.

2.The number of keys used.

If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

3. The way in which the plaintext is processed.

A **block cipher** processes the input one block of elements at a time, producing an output block for each input block. A **stream cipher** processes the input elements continuously, producing output one element at a time, as it goes along.

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. *There are two general approaches to attacking a conventional encryption scheme:*

- *Cryptanalysis*
- *Brute-force attack*

- ✓ **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

- ✓ **Brute-force attack:** The attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Types of Attacks on Encrypted Message

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Cryptanalysis and Brute-Force Attack

- ✓ The ciphertext-only attack is the easiest to defend against because the opponent has the least amount of information to work with
- ✓ In many cases, the analyst has more information.
- ✓ The analyst may be able to capture one or more plaintext messages as well as their encryptions.
- ✓ The analyst may know that certain plaintext patterns will appear in a message

- ✓ For example, a file that is encoded in the Postscript format always begins with the same pattern, or there may be a standardized header or banner to an electronic funds transfer message, and so on. All these are examples of *known plaintext*
- ✓ With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed.

- ✓ Closely related to the known-plaintext attack is what might be referred to as a probable-word attack. If the opponent is working with the encryption of some general prose message, he or she may have little knowledge of what is in the message.

Thank You

ANY
QUESTIONS?

