Information security

Computer Science Department

4th stage / 1st sem.

Lecturer Wafaa Mustafa Hameed

2023-2024

categories of Attacks

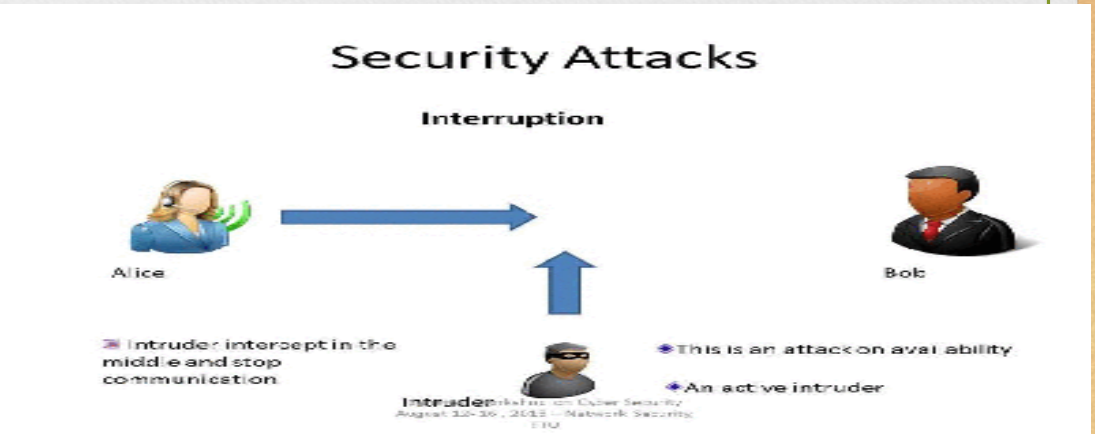
- In an Information Security context there are 4 broad based categories of attacks:
- Fabrication
- Interception
- Interruption
- Modification

INTERRUPTION

- An asset of the system is destroyed or becomes unavailable or unusable. It is an attack on availability.

Examples:

- Destruction of some hardware
- Jamming wireless signals
- Disabling file management systems



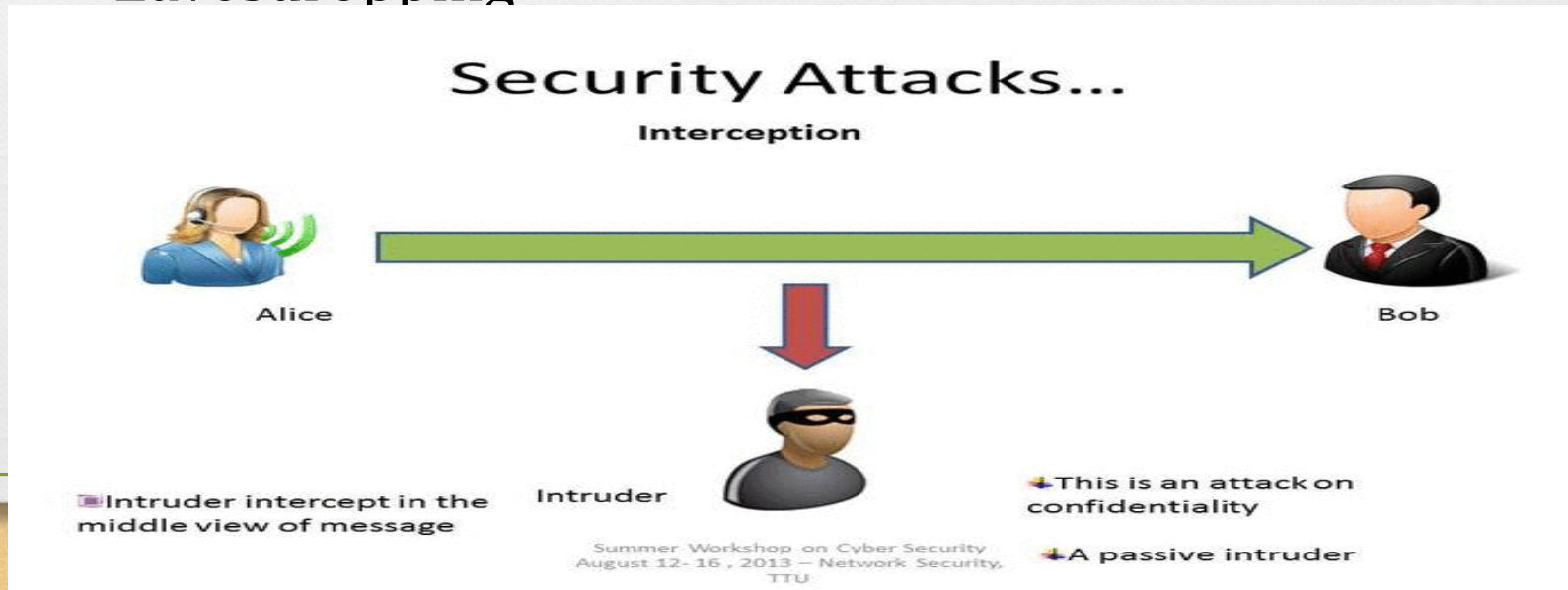
INTERCEPTION

- An unauthorized party gains access to an asset.

Attack on confidentiality.

Examples:

- Wire tapping to capture data in a network.
- Illicitly copying data or programs
- Eavesdropping



MODIFICATION

- When an unauthorized party gains access and tampers an asset. Attack is on Integrity.

Examples:

- Changing data file
- Altering a program and the contents of a message

FABRICATION

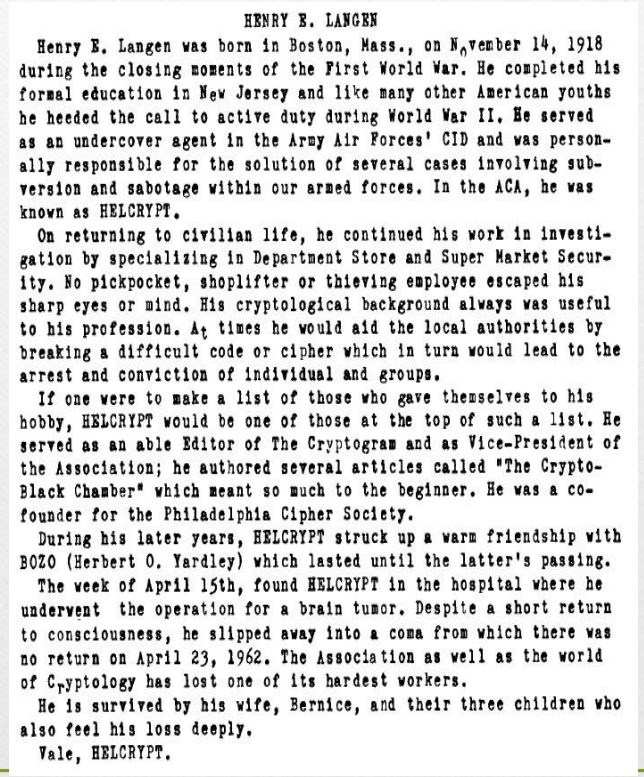
- An unauthorized party inserts a counterfeit object into the system. Attack on Authenticity. Also called impersonation

Examples:

- Hackers gaining access to a personal email and sending message
- Insertion of records in data files
- Insertion of spurious messages in a network

Cryptography

- **Cryptography(Cryptosystem)** word comes from two Greek words meaning “Secret Writing”, it is an art and science of concealing meaning.



HENRY E. LANGEN

Henry E. Langen was born in Boston, Mass., on November 14, 1918 during the closing moments of the First World War. He completed his formal education in New Jersey and like many other American youths he heeded the call to active duty during World War II. He served as an undercover agent in the Army Air Forces' CID and was personally responsible for the solution of several cases involving subversion and sabotage within our armed forces. In the ACA, he was known as HELCRYPT.

On returning to civilian life, he continued his work in investigation by specializing in Department Store and Super Market Security. No pickpocket, shoplifter or thieving employee escaped his sharp eyes or mind. His cryptological background always was useful to his profession. At times he would aid the local authorities by breaking a difficult code or cipher which in turn would lead to the arrest and conviction of individual and groups.

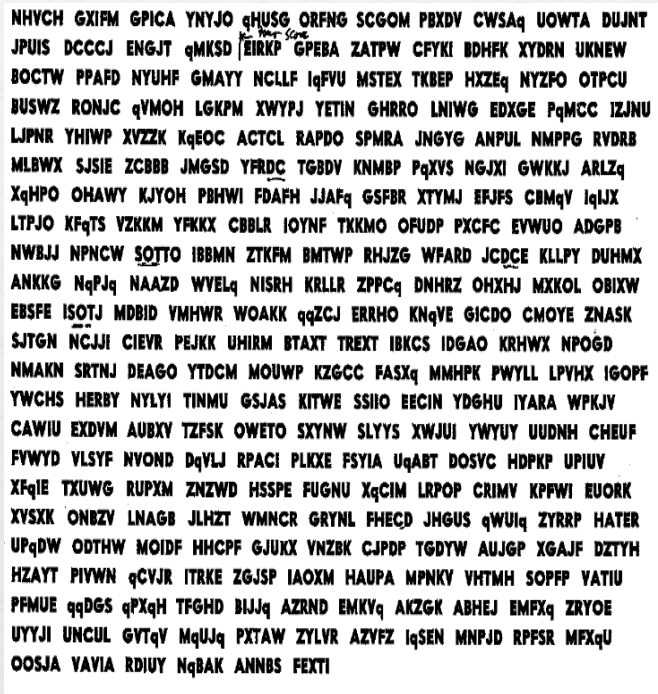
If one were to make a list of those who gave themselves to his hobby, HELCRYPT would be one of those at the top of such a list. He served as an able Editor of The Cryptogram and as Vice-President of the Association; he authored several articles called "The Crypto-Black Chamber" which meant so much to the beginner. He was a co-founder for the Philadelphia Cipher Society.

During his later years, HELCRYPT struck up a warm friendship with BOZO (Herbert O. Yardley) which lasted until the latter's passing.

The week of April 15th, found HELCRYPT in the hospital where he underwent the operation for a brain tumor. Despite a short return to consciousness, he slipped away into a coma from which there was no return on April 23, 1962. The Association as well as the world of Cryptology has lost one of its hardest workers.

He is survived by his wife, Bernice, and their three children who also feel his loss deeply.

Vale, HELCRYPT.



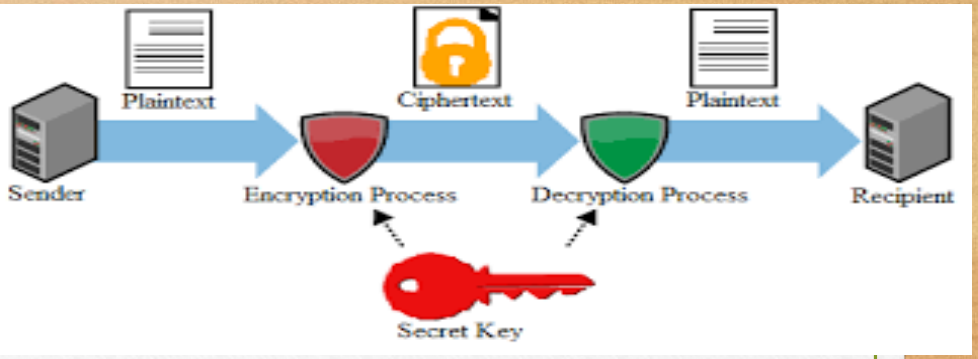
NHVCH GXIFM GPICA YNYJO qHUSG ORFNG SCGOM PBXDV CWSAq UOWTA DUJNT
JPUIS DCCCJ ENGJT qMKSD EIRKP GPEBA ZATPW CFYKI BDHFK XYDRN UKNEW
BOCTW PPAFD NYUHF GMAYY NCLLF IqFVU MSTEX TKBEP HXZEq NYZFO OTPCU
BUSWZ RONJC qVMOH LGKPM XWYPJ YETIN GHRRO LNIWG EDXGE PqMCC IZJNU
LJPNR YHIWP XVZZK KqEOC ACTCL RAPDO SPMRA JNGYG ANPUL NMPPG RVDRB
MLBWX SJSIE ZCBBB JMGSD YFRDC TGBDV KNMBP PqXVS NGJXI GWKKJ ARLZq
XqHPO OHAWY KJYOH PBHWI FDAFH JJAFq GSFBR XTYMJ EFJFS CBMqV IqIJX
LTPJO KFqTS VZKKM YFKKX CBBLR IOYNF TKKMO OFUDP PXCFC EVWUO ADGPB
NWBJJ NPNCW SOTTO IBBMN ZTKFM BMTWP RHJZG WFARD JCDCE KLLPY DUHMX
ANKKG NqPJq NAAZD WVELq NISRH KRLLR ZPPCq DNHRZ OHXHJ MXKOL OBIXW
EBSFE ISOTJ MDBID VMHWR WOAKK qqZCJ ERRHO KNqVE GICDO CMOYE ZNASK
SJTGN NCJJI CIEVR PEJKK UHIRM BTAXT TREXT IBKCS IDGAO KRHWX NPOGD
NMAKN SRTNJ DEAGO YTDCM MOUWP KZGCC FASXq MMHPK PWYLL LPVHX IGOPF
YWCHS HERBY NYLYI TINMU GSJAS KITWE SSIIO EECIN YDGHU IYARA WPKJV
CAWIU EXDVM AUBXV TZFSK OWETO SXYNW SLYYS XWJUI YWYUY UUDNH CHEUF
FVWYD VLSYF NVOND DqVLJ RPACI PLKXE FSYIA UqABT DOSVC HDPKP UPIUV
XFqIE TXUWG RUPXM ZNZWD HSSPE FUGNU XqCIM LRPOP CRIMV KPFWI EUORK
XYSXK ONBZV LNAGB JLHZT WMNCR GRYNL FHECD JHGUS qWUIq ZYRRP HATER
UPqDW ODTHW MOIDF HHCPF GJUKX VNZBK CJPDP TGDYW AUJGP XGAJF DZTYH
HZAYT PIVWN qCVJR ITRKE ZGJSP IAOXM HAUPA MPNKV VHTMH SOPFP YATIU
PFMUE qqDGS qPXqH TFGHD BIJJq AZRND EMKVq AKZGK ABHEJ EMFXq ZRYOE
UYYJI UNCUL GVTqV MqUJq PXTAW ZYLVR AZVFZ IqSEN MNPJD RPFSR MFXqU
OOSJA VAVIA RDIUY NqBAK ANNBS FEXTI

Interceptor (Intruder):

- The interceptor (intruder) try to do one or more of the following:

1. Block the message, by preventing its reaching recipient, thereby affecting the availability of the message.
2. Intercept the message, by reading or listening to the message, thereby affecting the confidentiality of the message.
3. Modify the message, by seizing the message and changing it in some way, affecting the message‘s integrity.
4. Fabricate an authentic-looking message, arranging for it to be delivered as if it came from the sender, thereby also affecting the integrity of the message.

What is a Cipher?



- A ***cipher*** is simply a method for encrypting and decrypting messages.
- The original data is known as ***plaintext,*** and the result of encryption is ***ciphertext.***
- The encryption and decryption *rules*, called ***algorithms***.
- A system for encryption and decryption is called a ***cryptosystem***
- A ***key*** is used to configure a cryptosystem for encryption and decryption.
- In ***symmetric cipher*** (secret key) the same key is used to encrypt and to decrypt. because the only key is copy or share by another party to decrypt the cipher text. It is faster than the public key cryptography.

What is a cipher? Cont.

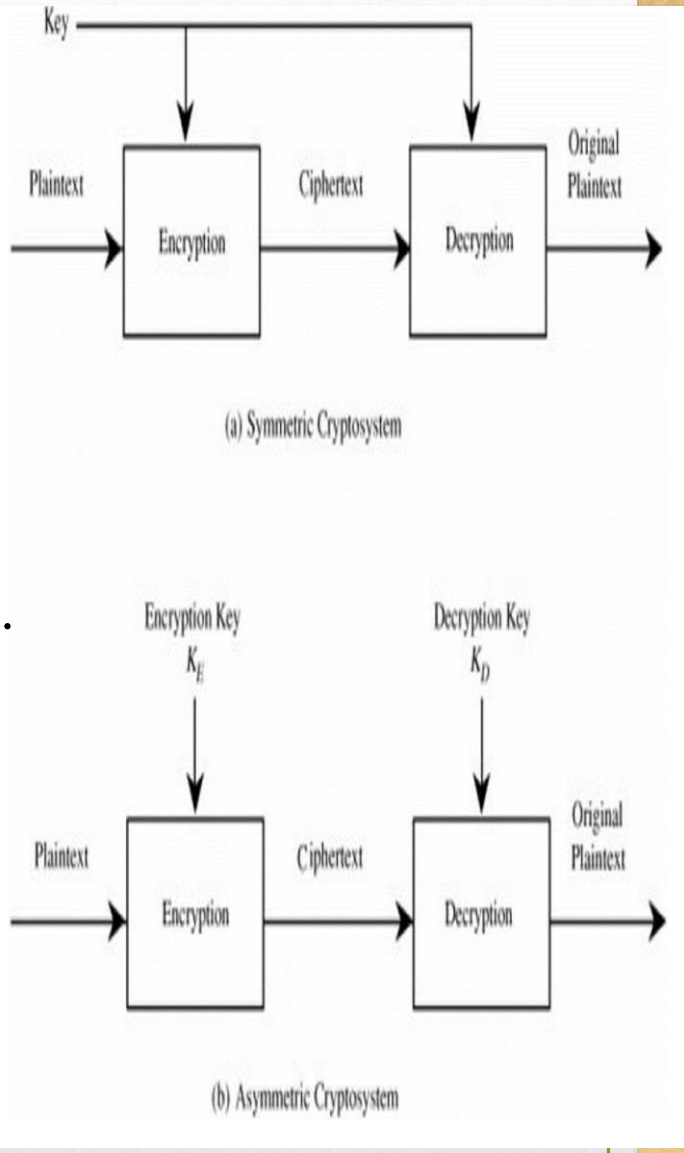
- There is also a concept of ***public key*** cryptography where the encryption and decryption keys are different.
- Since different keys are used, it's possible to make the encryption key public. In public key crypto, the encryption key is appropriately known as the ***public key***, whereas the decryption key, which must remain secret, is the ***private key*** (secret key). the key is known as ***Asymmetric*** key.

C ciphertext(massage)
P plaintext
E [K, P] encryption of P using key K
D [K,C] decryption of C using key K

Confusion: it is a technique for ensuring that ciphertext has no clue about the original message.

Diffusion: it increases the redundancy of the plaintext by spreading it across rows and columns.

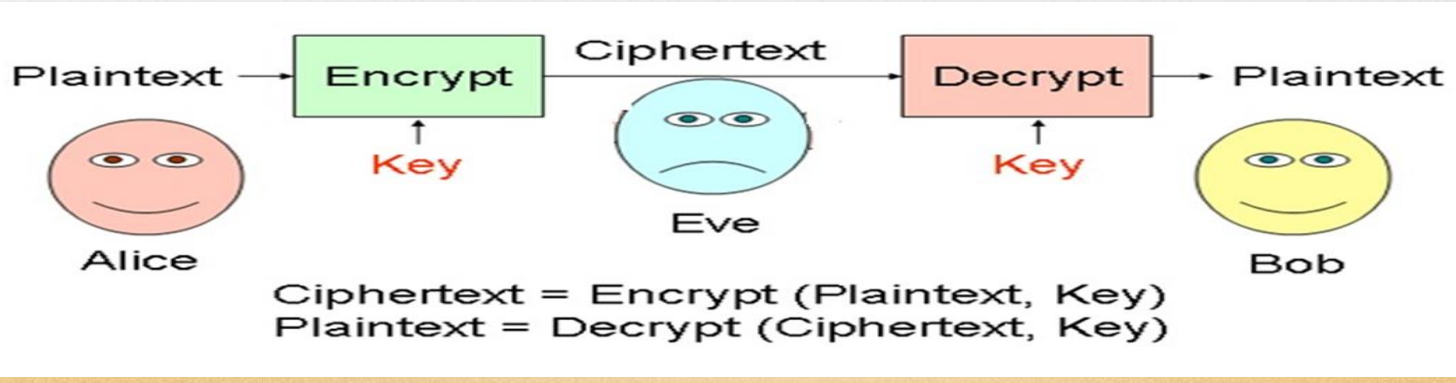
The Vernam Cipher is based on the principle that each plaintext character from a message is 'mixed' with one character from a key stream. If a truly random key stream is used, the result will be a truly 'random' ciphertext which bears no relation to the original plaintext



Cryptography

Procedures of the basic Cryptography

- 1-Alice and Bob agree on a pair of keys (K).
- 2- Alice encrypts (E) a message (M) and sends it to Bob.
- 3-An adversary Eve will try to get the ciphertext (C) and crack it to open.
- 4-Bob will decrypt (D) the ciphertext (C) received from Alice by the agreed (k).



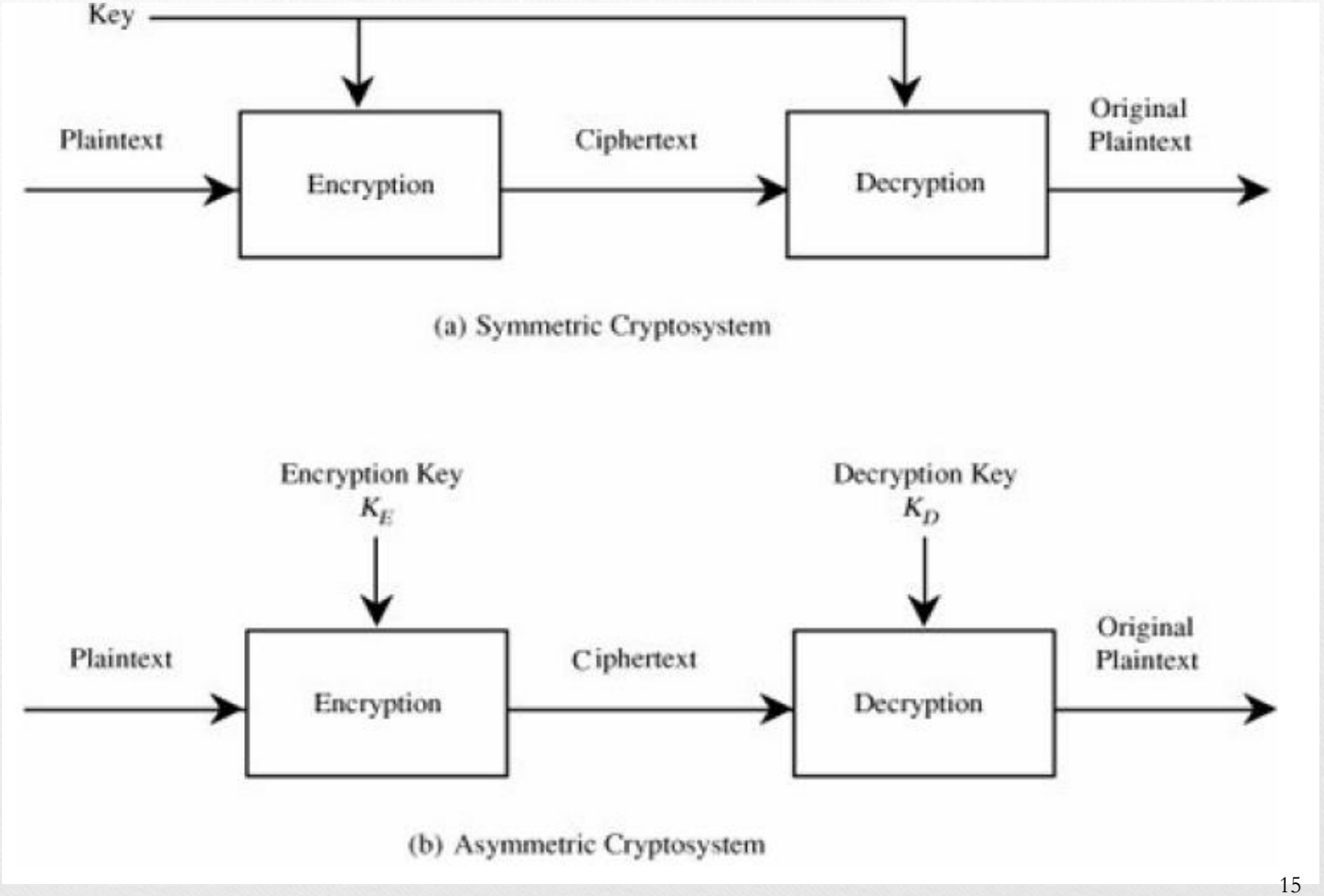
Encryption Algorithms

- The cryptosystem involves a set of rules for how to encrypt the message (plaintext) and how to decrypt the ciphertext. The encryption and decryption rules, called **algorithms**
- These algorithms often use a device called a key (K).
- The ciphertext depends on the original message, the algorithm, and the key value.
- Some encryption algorithms are keyless but that keyed encryptions are more difficult to break.

Encryption Algorithms cont.

- If encryption and decryption keys are the same, this form is called **symmetric** encryption because encryption and decryption are mirror-image processes.
- If encryption and decryption keys come in pairs. Then, a decryption key, inverts the encryption key. Encryption algorithms of this form are called **asymmetric**.
  - because converting ciphertext back to the original message involves a series of steps and a key that are different from the steps converting original message to ciphertext.

Encryption Algorithms cont.




THANK
YOU