Introduction to Cryptography & Steganography

Lecture-13

Department of CSE, IUT

Attack, Mechanism And Service

- Security attacks: any action that compromises the security of information
- Security Mechanism: a **mechanism** that is designed to detect, prevent or recover from a security attack
- Security Service: a service that enhances the security of data processing systems and information transfers.

A security service makes use of one or more security mechanisms.

Security Services

- Data Confidentiality
- Data Integrity
  - Anti-change
  - Anti-replay
- Authentication
  - Peer entity
  - Data origin
- Non-repudiation
  - Proof of origin
  - Proof of delivery
- Access control

Security Mechanisms

- Encipherment (Encryption)
- Integrity protection
- Digital signature
- Notarization
- Authentication Exchange
- Access control
- Traffic padding
- Routing control
- Etc.

Security Services And Mechanisms

Table 1.4. Relationship between Security Services and Mechanisms

	Mechanism							
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**	**Traffic Padding**	**Routing Control**	**Notarization**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Cryptography Overview: Basic Terminologies

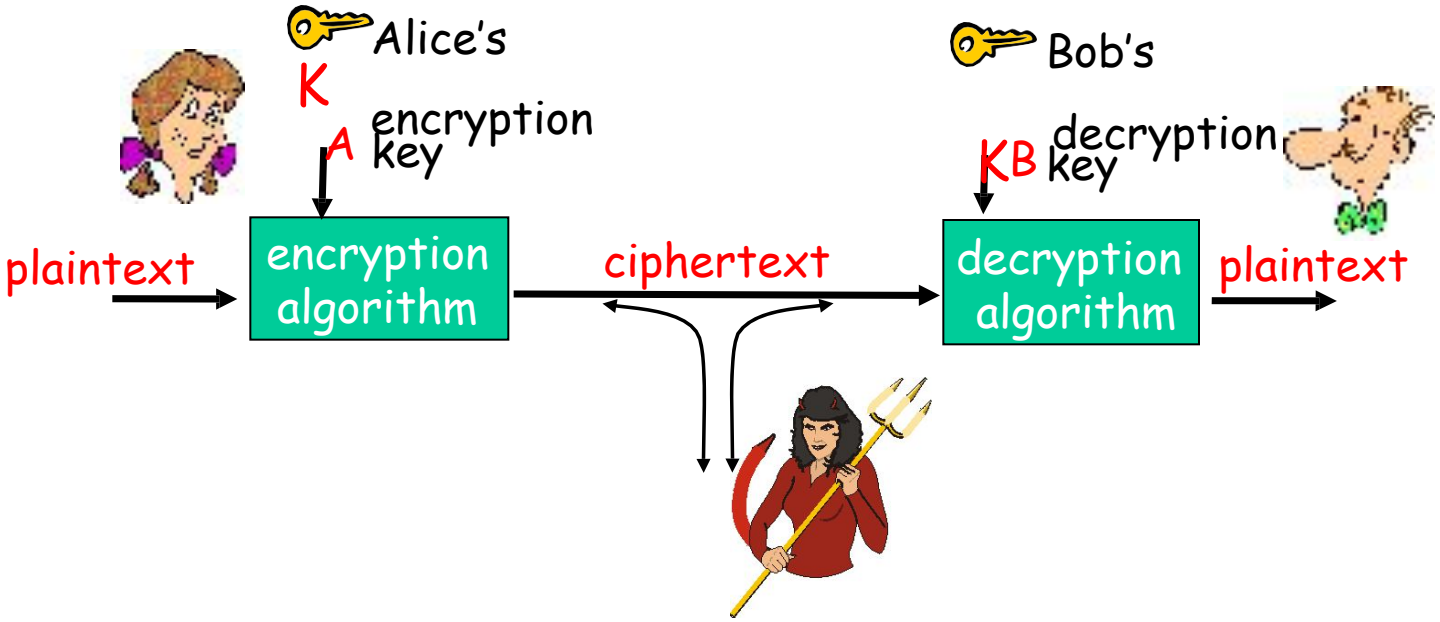
Cryptography is a strong tool against many kinds of security threats.

- Cryptography: **science of secret writing** with *ciphers*
- Cryptanalysis: **science of breaking ciphers**
- Cryptology: cryptography + cryptanalysis
- Cryptosystem (or cryptographic system)
  - Provides information security services
  - Through a combination of cryptographic primitives, protocols, operational procédures, documentation, user training, etc…
  - Encompasses systems of various sizes
    - One algorithm (e.g. RSA cryptosystem)
    - Or widely: protocols, hardware, customer training, etc.

Cryptographic primitives

- What is a cryptographic primitive?
  - A mathematical entity which meets defined (security) requirements
- Common division
  1. **Unkeyed**
  2. **Secretkey (symmetric) – "man made"**
  3. **Publickey (asymmetric) – "math made"**
- Kerckhoffs' principle – public algorithm, secret key
- Examples
  - (Symmetric) encryption – DES, 3DES, AES, Blowfish, RC4
  - (Asymmetric) encryption – RSA, DSA
  - (Unkeyed) hashing – MD5, SHA1, SHA{256,384,512}
  - (Symmetric) message authentication – HMAC{MD5,SHA1}
  - (Asymmetric) digital signatures – RSA, DSA
  - (Asymmetric) key exchange – DiffieHellman (DH)

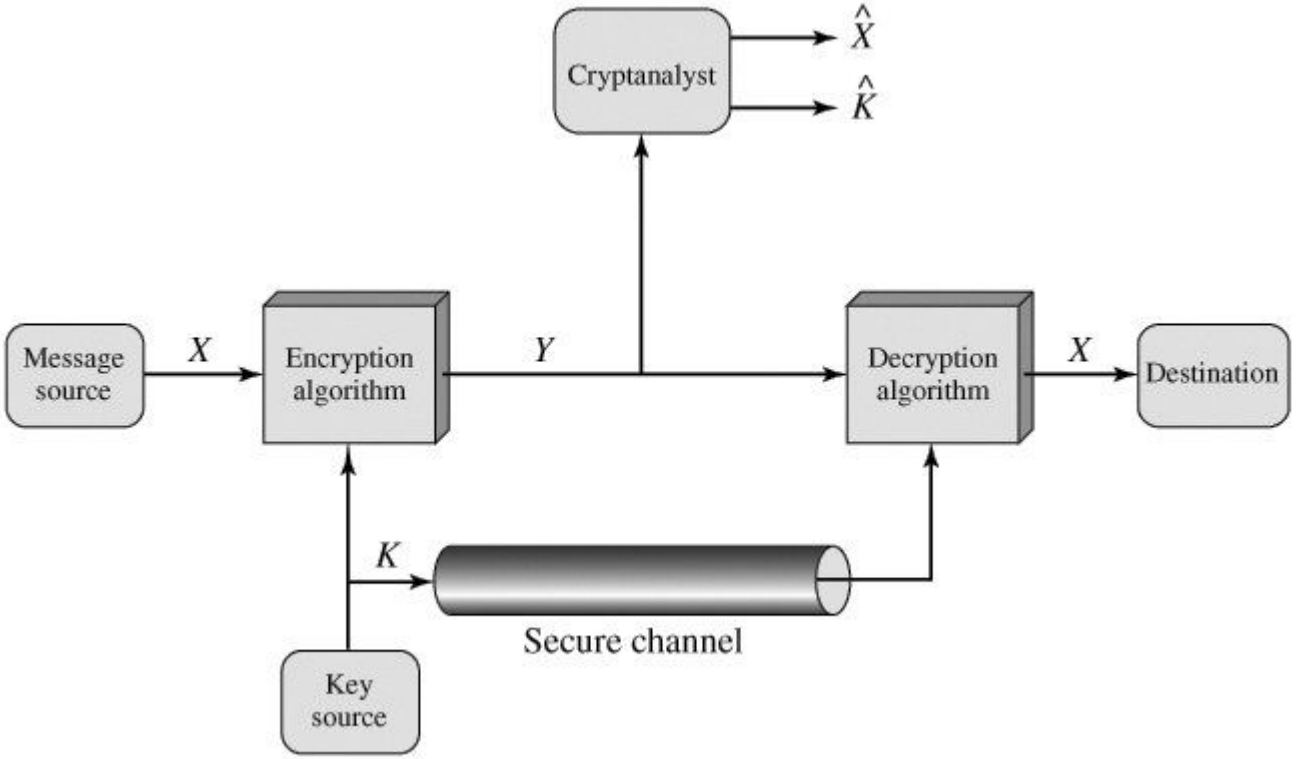
The Language Of Cryptography



symmetric key crypto: encryption and decryption **keys *identical***

public-key crypto: **encryption key *public***, **decryption key *secret*** **(private)**

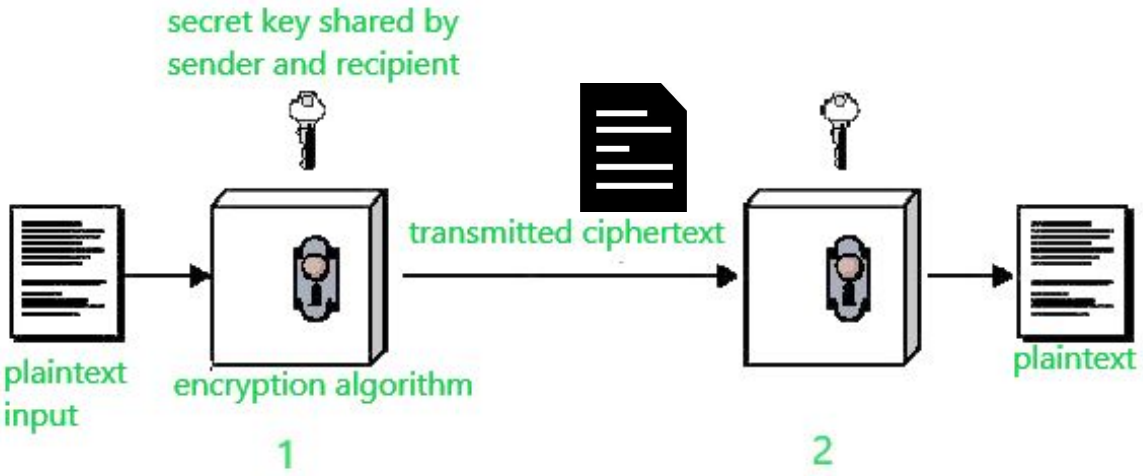
Model of Conventional Cryptosystem



Secret (Symmetric) Key Cryptography

- Also called **symmetric or conventional cryptography**
- **Five components**
  - **Plaintext:** the original message
  - **Encryption algorithm:** runs on the plaintext and the encryption key to yield the ciphertext
  - **Secret key:** an input to the encryption algorithm, value independent of the plaintext; different keys will yield different outputs
  - **Ciphertext:** the scrambled text produced as an output by the encryption algorithm
  - **Decryption algorithm:** runs on the ciphertext and the key to produce the plaintext
- Requirements for secure conventional encryption
  - Strong encryption algorithm
    - **An opponent who knows one or more ciphertexts would not be able to find the plaintexts or the key**
    - **Ideally, even if he knows one or more pairs plaintext-ciphertext, he would not be able to find the key**
  - **Encryption algorithm is not a secret**
  - **Sender and receiver must share the same key.**

Model of Conventional Cryptosystem



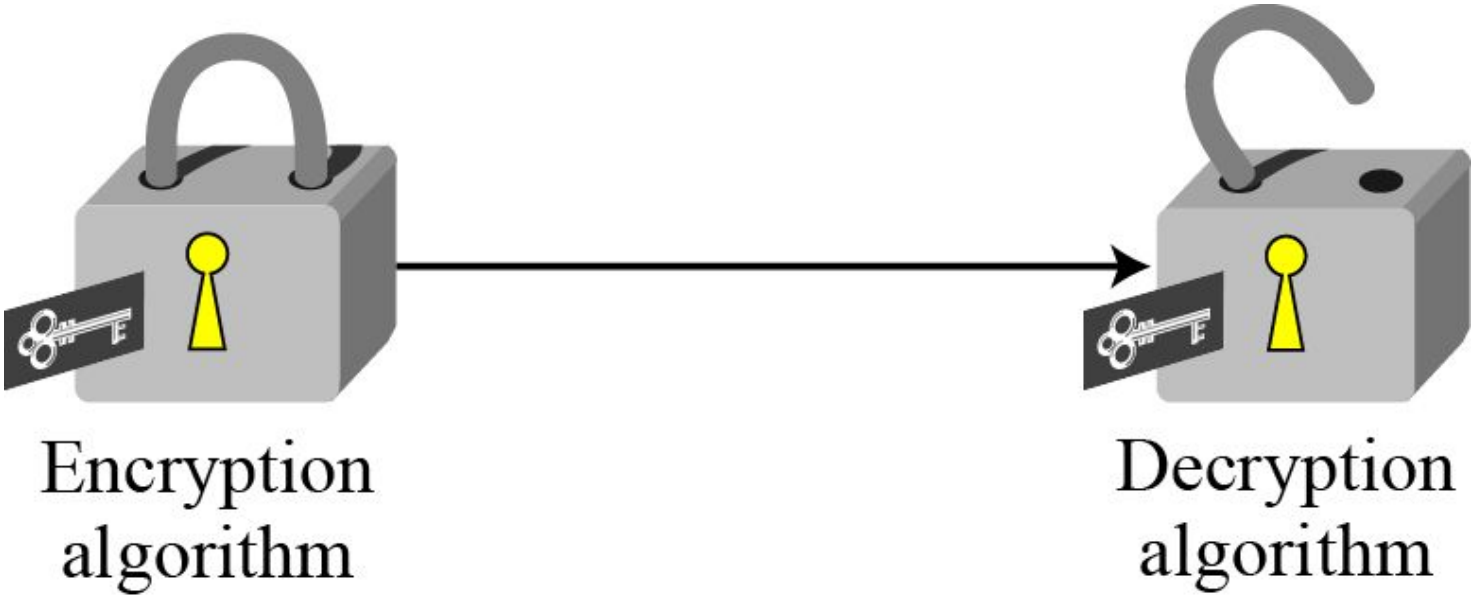
Kerckhoff's Principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

- **One should always assume that the adversary, Eve, knows the encryption/decryption algorithm.**
- **The resistance of the cipher to attack must be based only on the secrecy of the key.**

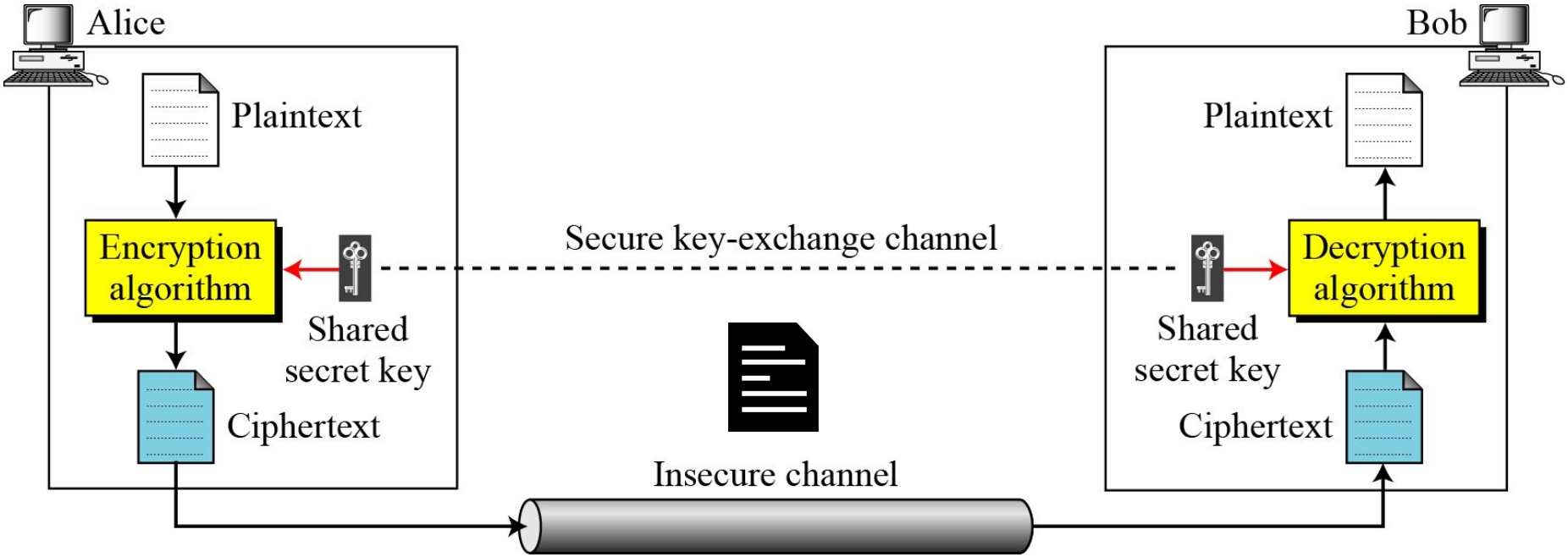
Secret (Symmetric) Key Cryptography

Figure 3.2 *Locking and unlocking with the same key*



Secret (Symmetric) Key Cryptography

Figure 3.1 *General idea of symmetric-key cipher*



Model for Symmetric Key Encryption

- Suppose Alice wants to send a message to Bob. She wishes the message not to be understood by others.
- "secret codes"
  - **substitute** a letter for each letter in the original message.
  - The codes must be agreed by Bob

Bob

Alice

Original	m	e	e	t		m	e		a	f	t	e	r		t	h	e		p	a	r	t	y
Translated	P	H	H	W		P	H		D	I	W	H	U		W	K	H		S	D	U	W	B

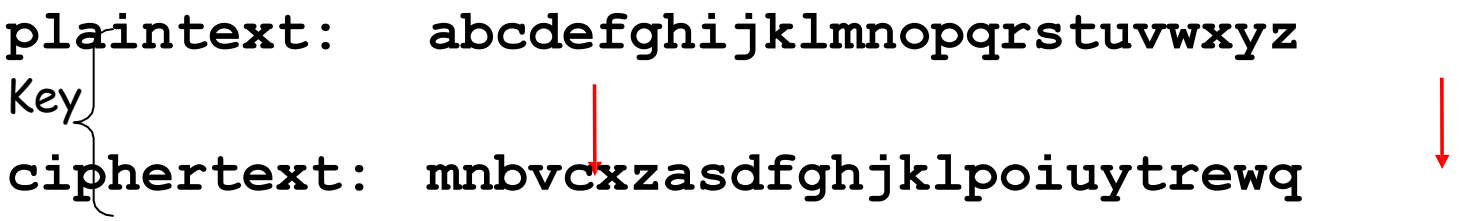
TABLE II

MESSAGE ENCRYPTED BY CAESAR CIPHER

Symmetric Key Cryptography

substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

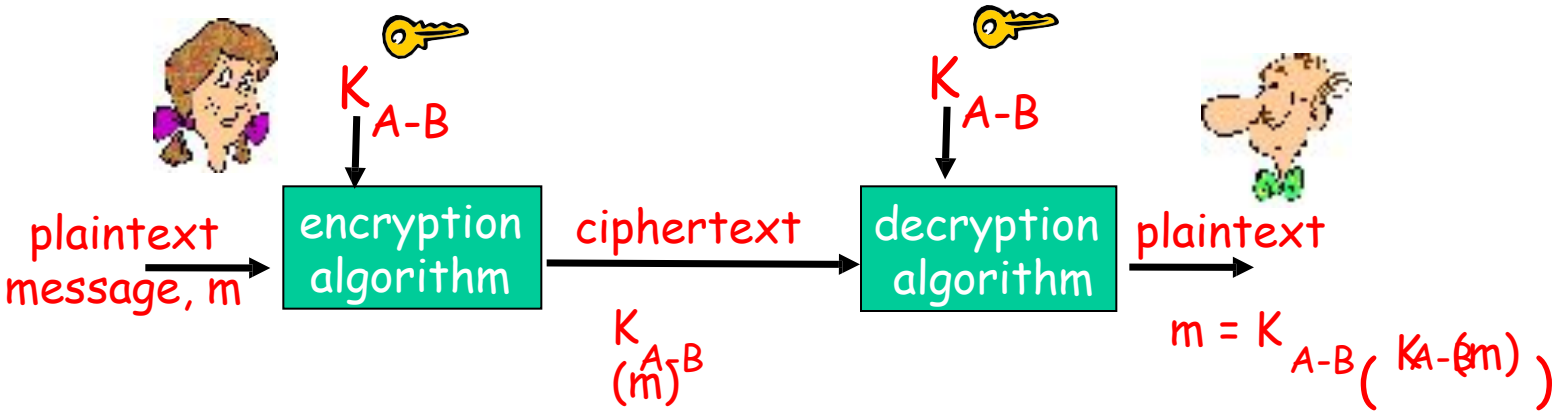


Plaintext:	bob. i love you. alice
Ciphertext:	nkn. s gktc wky. mgsbc

How hard to break this simple cipher?

- brute force (how hard?)
- other?

Symmetric Key Cryptography



symmetric key crypto: Bob and Alice share know same (symmetric) key: K_{A-B}

- For example, key is substitution pattern in monoalphabetic substitution cipher

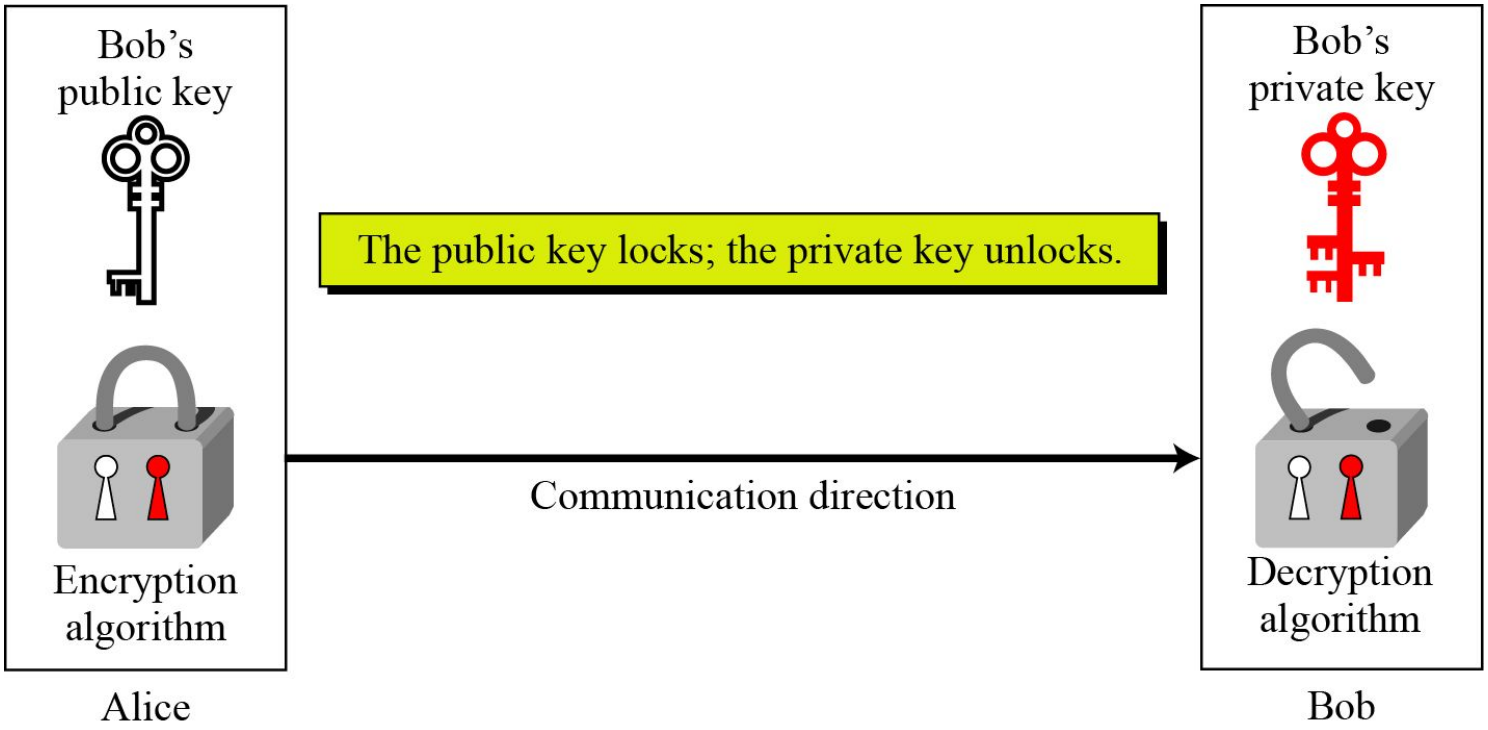
- How do Bob and Alice agree on a key?

- **DES, AES, IDEA, Blowfish, …**

Asymmetric key cryptography or Public Key Cryptography

Asymmetric key cryptography uses two separate keys: one private and one public.

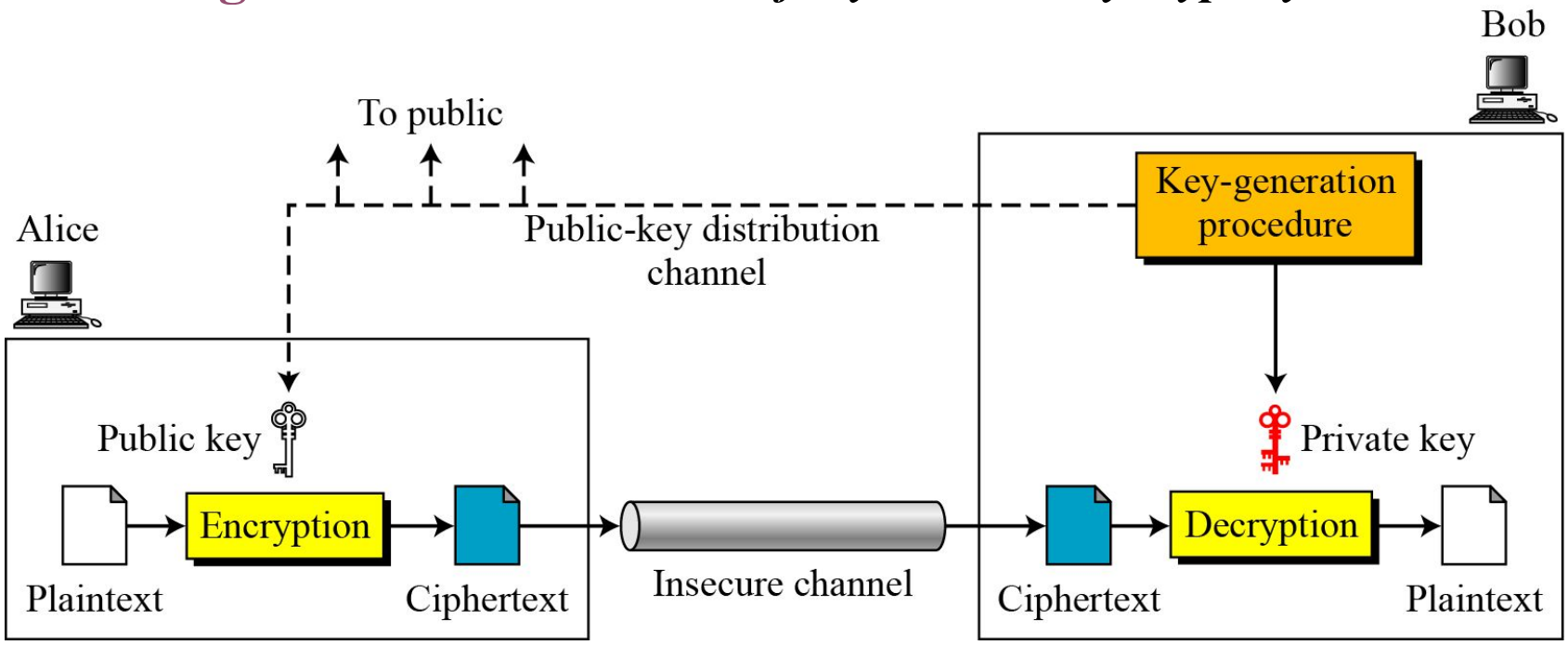
Figure 10.1 *Locking and unlocking in asymmetric-key cryptosystem*



Public Key Cryptography

General Idea

Figure 10.2 ***General idea of asymmetric-key cryptosystem***



Public Key Cryptography

General Idea

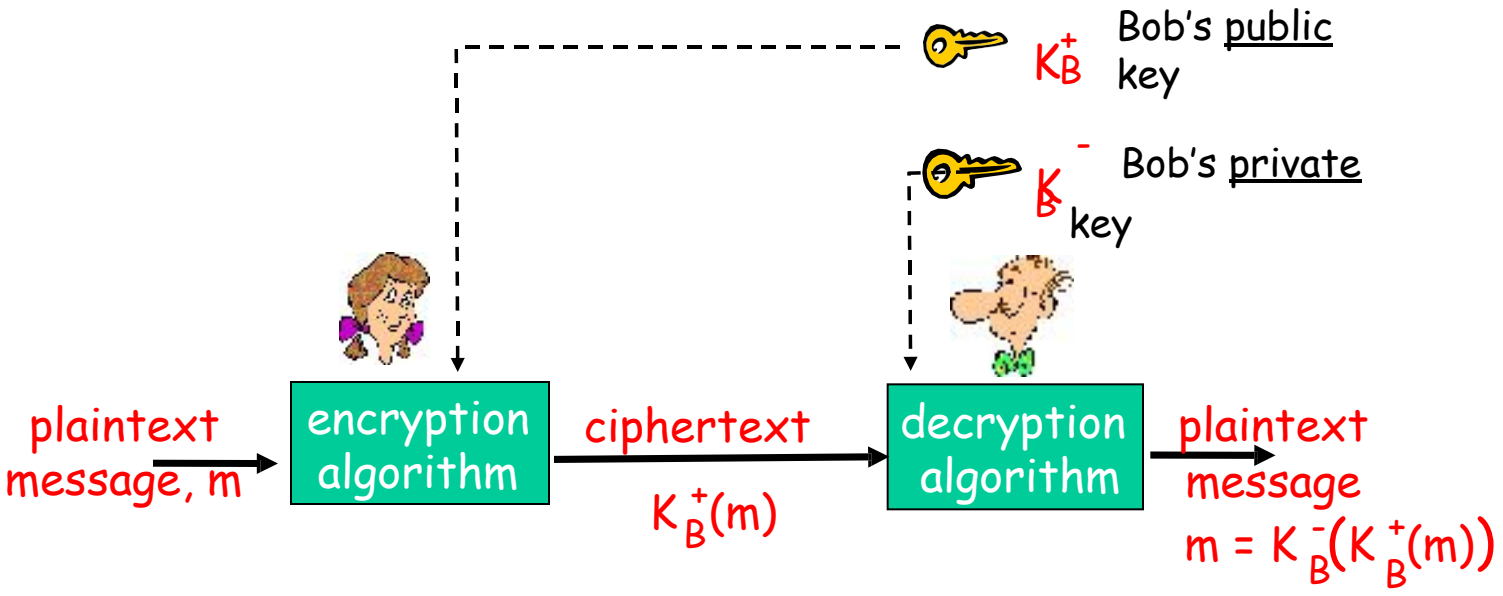
Plaintext/Ciphertext

Unlike in symmetric-key cryptography, plaintext and ciphertext are treated as integers in asymmetric-key cryptography.

Encryption/Decryption

$$C = f(K_{public}, P) \qquad P = g(K_{private}, C)$$

Public Key Cryptography



Public Key Encryption Algorithms

Requirements:

1. need $K_B^+(\ )$ and $K_B^-(\ )$ such that

$$K_B^-(K_B^+(m)) = m$$

2. given public key K_B^+, it should be impos_sible to compute private key K_B^-

RSA: Rivest, Shamir, Adelson algorithm

Need for Both

There is a very important fact that is sometimes misunderstood: The advent of asymmetric-key cryptography does not eliminate the need for symmetric-key cryptography.

Public key encryption

- Each person has two keys: one public key and one private key.
- Privacy
  - The sender uses the public key of the receiver to encrypt a message, only the receiver can decrypt it. WARNING!!!!
- Integrity
  - The sender uses its own private key to encrypt a message (or message digest) and any one can verify that no one has tampered with it.

Public key encryption

- Authentication
  - Pick a number and encrypt it using the public key of the other part, if she can decrypt it she has been authenticated.
- Digital signature
  - Sign a letter by encrypting the letter (or a message digest) using your private key. Any one can verify you signature and .... you can not repudiate it!

Digital Signatures

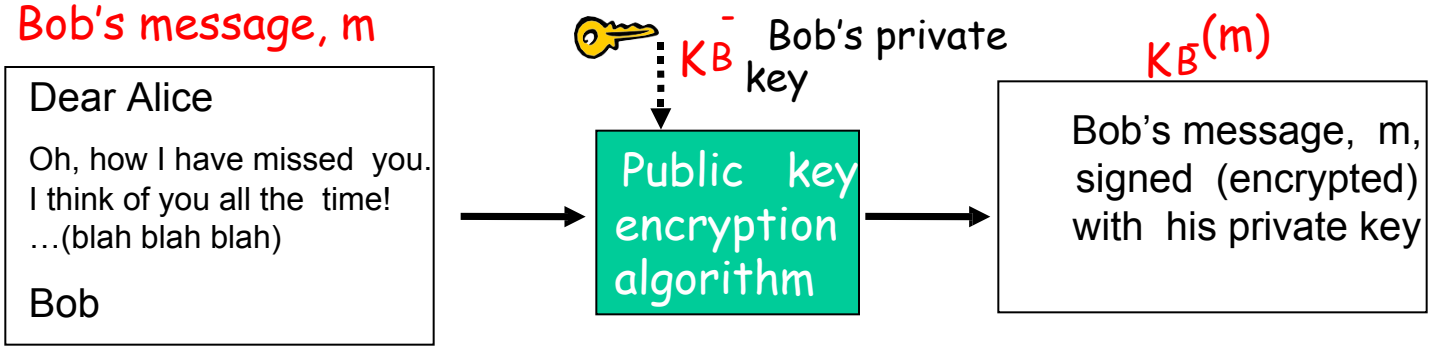
Cryptographic technique analogous to hand-written signatures.

- sender (Bob) digitally signs document,establishing he is document owner/creator.
- verifiable, nonforgeable: Alice knows that Bob, and no one else, must have signed document
- Integracy: no other document could have that signature, so it must be the original document

Digital Signatures

Simple digital signature for message m:

- Bob signs m by encrypting with his private key K_B^-, cr_eating "signed" message, $K_B^-(m)$



Symmetric Key Cryptography

symmetric key cryptography

- requires sender, receiver know shared secret key

- **Question: how to agree on key in first place (particularly if never "met")?**

Symmetric Key Cryptography

***symmetric* key cryptography**

- requires sender, receiver know shared secret key

asymmetric key cryptography

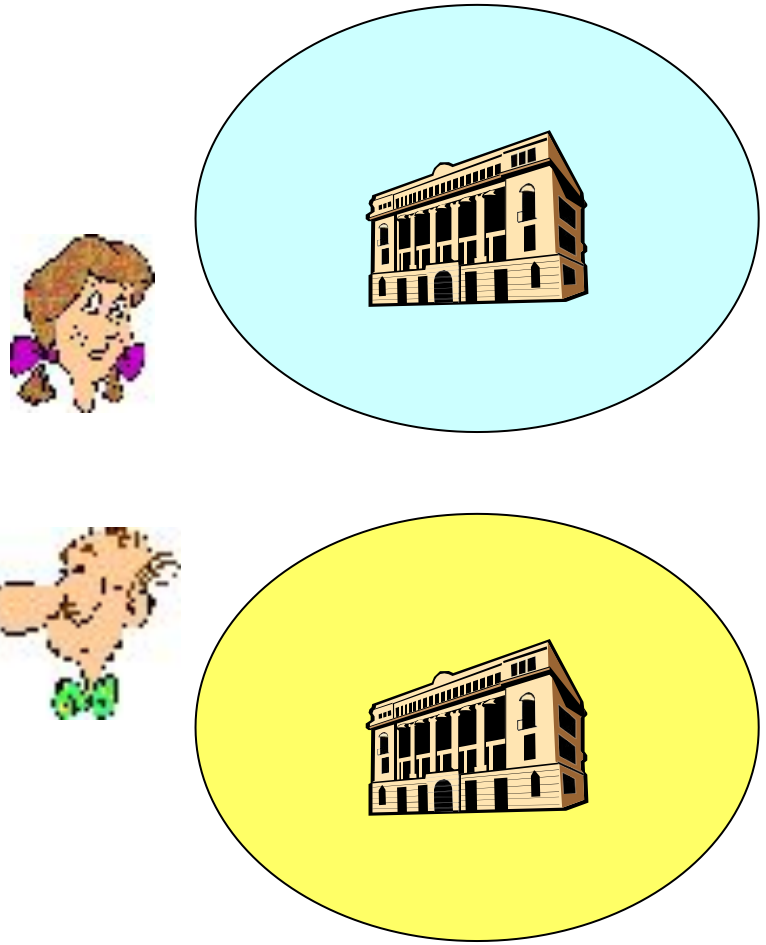
- radically different approach [Diffie-Hellman76, RSA78]
- sender, receiver **do *not* share secret key**
- *public* encryption key **known to *all***
- *private* decryption key known **only to receiver**

- **Question: how to agree on key in first place (particularly if never "met")?**

- **Question: how to trust that a public key is genuine?**

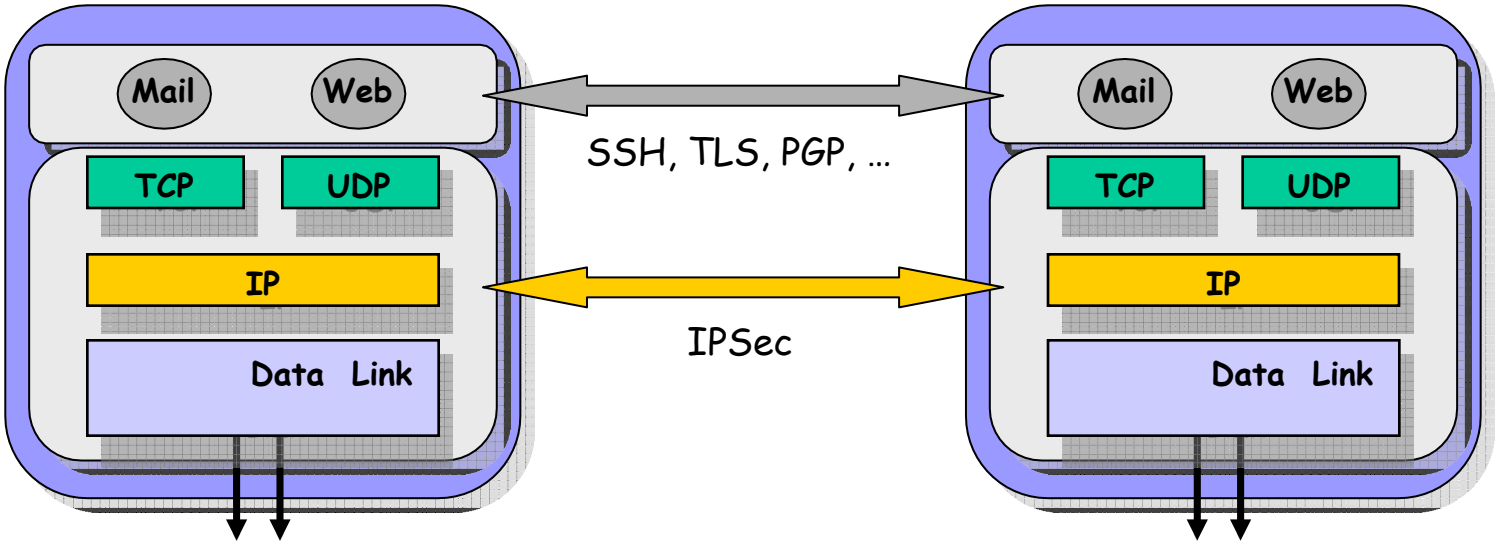
Key Management

- How can Alice and Bob get the keys they need?
- How can they be confident that the keys are genuine?
- Use a trusted third party
  - Key Distribution Center
    - Shared keys
  - Certification Authority
    - Public keys



Secure Communication

- Security in network or application?



Attacking Encryption Scheme

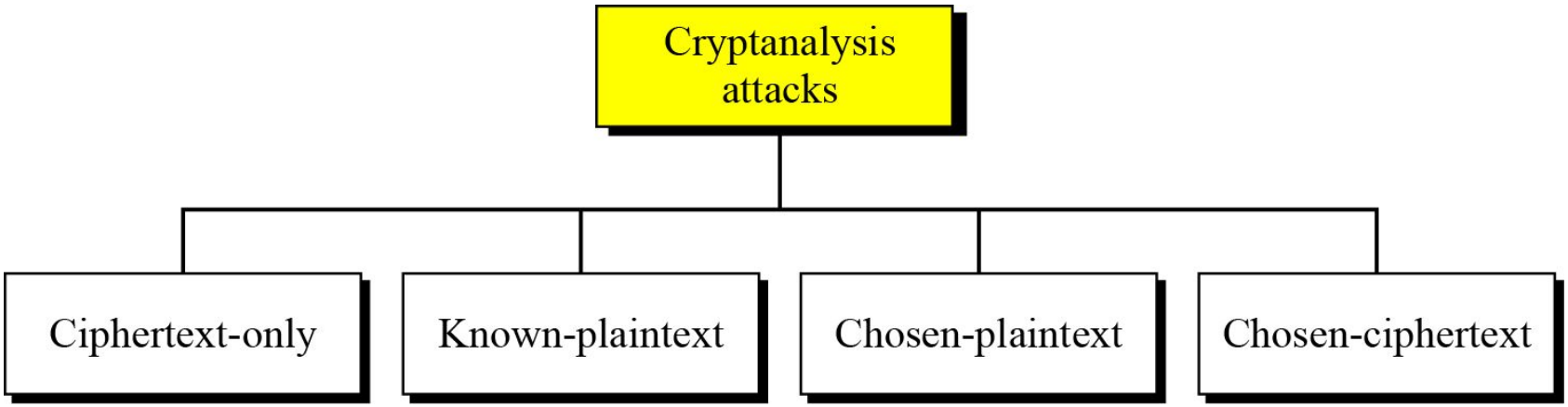
- Brute-force attack: tires every possible key on a piece of cihphertext until an intelligible translation into plaintext is obtained.

- Cryptanalysis: exploits the characteristics of the algorithm and the traces of structure or pattern in the plaintext that survive encryption
  - break a single message
  - deduce the key in order to break the subsequent messages.
  - How ? -- Use statistical tools and properties of languages.

Cryptanalysis

As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes.

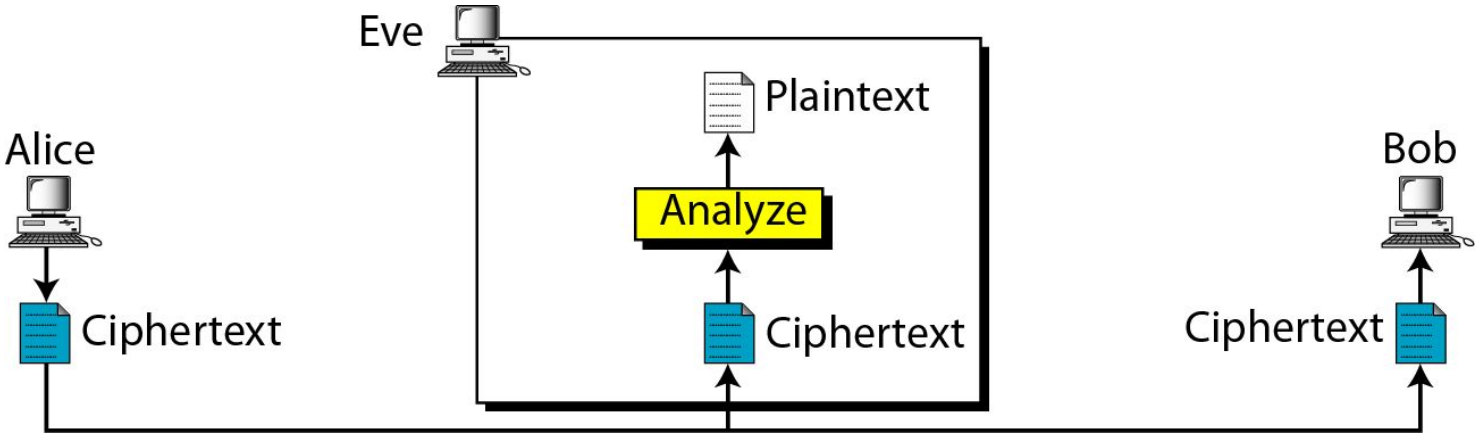
Figure 3.3 *Cryptanalysis attacks*



Cryptanalysis

Ciphertext-Only Attack

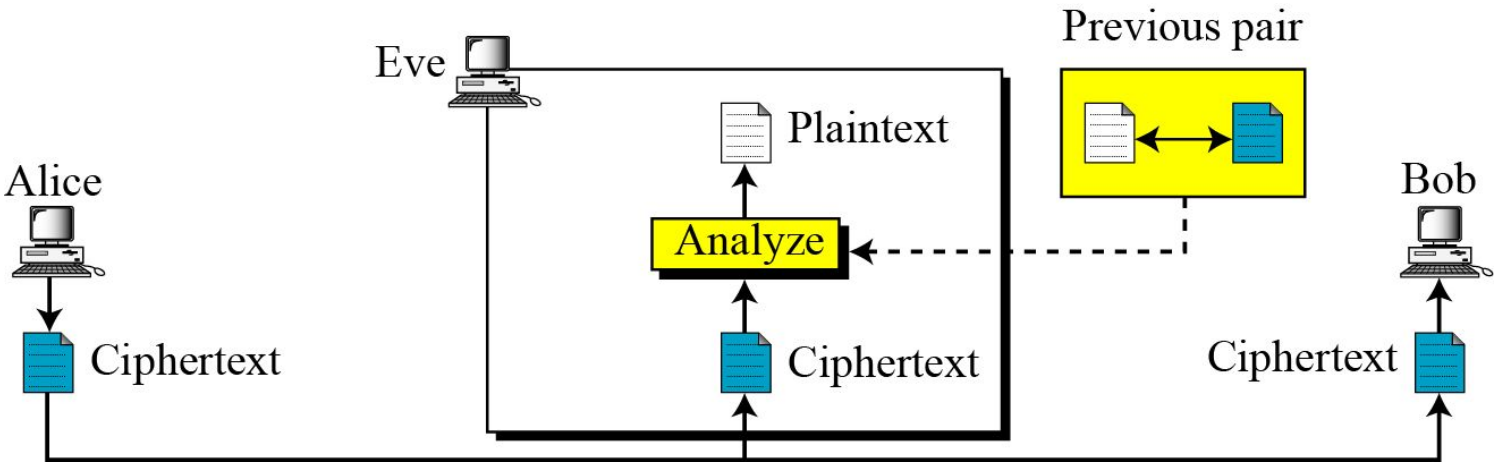
Figure 3.4 *Ciphertext-only attack*



Cryptanalysis

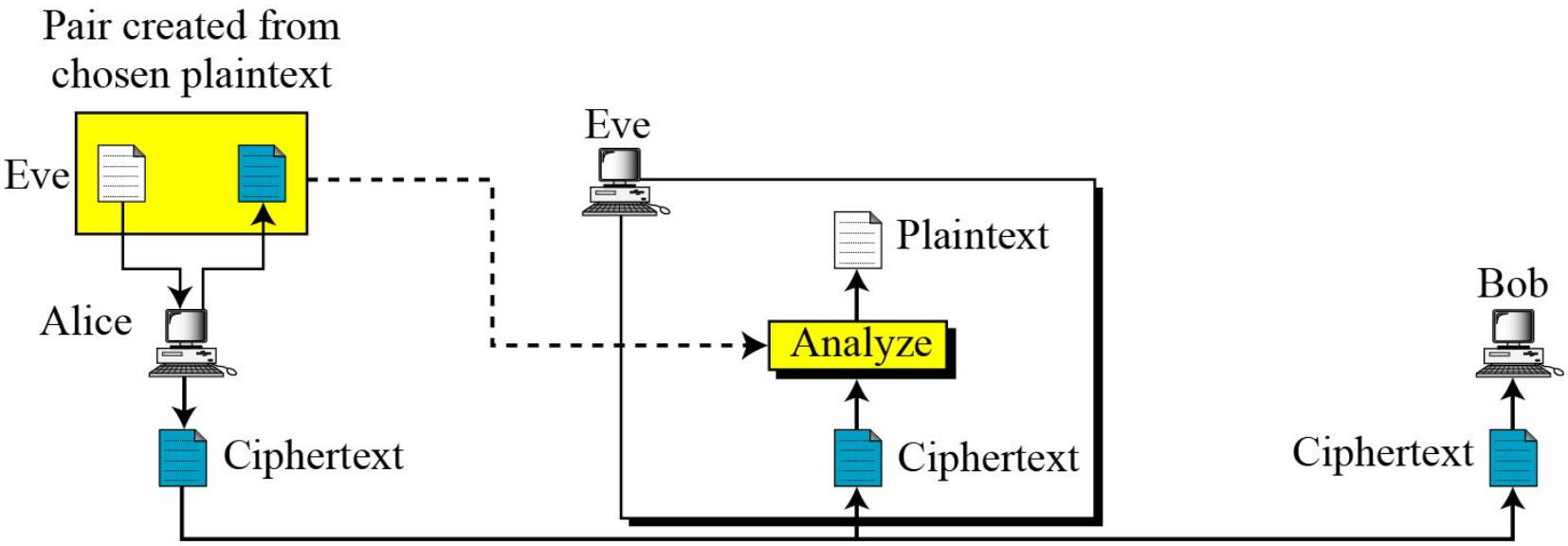
Known-Plaintext Attack

Figure 3.5 ***Known-plaintext attack***



Chosen-Plaintext Attack

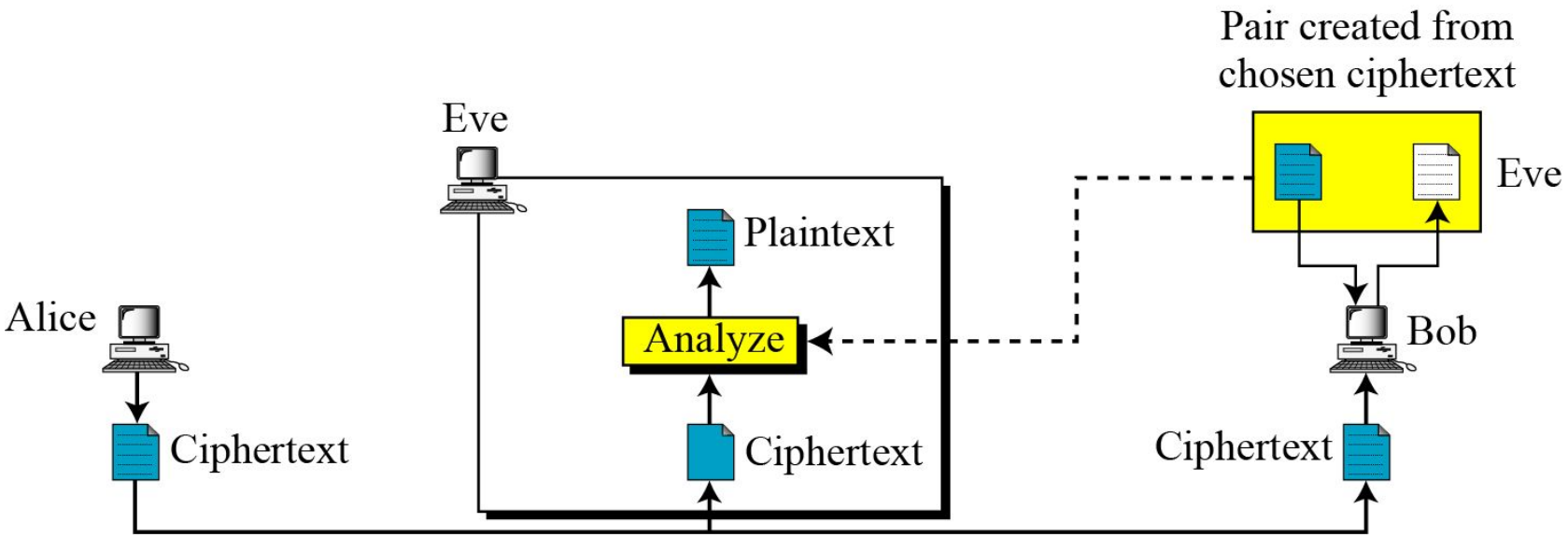
Figure 3.6 *Chosen-plaintext attack*



Cryptanalysis

Chosen-Ciphertext Attack

Figure 3.7 *Chosen-ciphertext attack*



Encryption Algorithm Security

- **Unconditionally secure**
  - If it is impossible to determine the plaintext from the generated ciphertext given enough time and resources.

- **Computationally secure**
  - The cost of breaking the cipher exceeds the value of the encrypted information
  - The time required to break the cipher exceeds the useful lifetime of the information

Steganography

Steganography:

- Steganography is the art and **science of writing hidden message**
- Such that, no one, apart from the sender and intended recipient, suspects the existence of the message.

- Steganography works by replacing bits of useless or unused data in regular computer files
- (such as graphics, sound, text, html or even floppy disks) with bits of different, invisible information.

Steganography:

- This hidden information can be plain text, cipher text or even images.

Since everyone can read, encoding text in neutral sentences is doubtfully effective

***S**ince **E**veryone **C**an **R**ead, **E**ncoding **T**ext*
***I**n **N**eutral **S**entences **I**s **D**oubtfully **E**ffective*

'Secret inside'

Steganography process

- Steganography process :
  - **Cover-media + Hidden data + Stego-key = Stego-medium**
- **Cover media:**
  - It is the file in which we will hide the hidden data
  - Cover-media can be image or audio file.
- **stego-key:**
  - Cover-media can be encrypted using stego-key:
- **stego-medium.**
  - The resultant file is of above process called stego medium.

Types Of Steganography

1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. & many more

Historical Use of Steganography

- Runners were memorizing messages
  - Sometimes killed after delivering the message
- Demaratus tells Athens of Persia's attack plans
  - Writes the secret message on a tablet, and covers it with wax
- Greek Histaiaeus encouraged Aristagoras of Miletus to revolt against the Persian King.
  - Writes message on the shaved head of the messenger, and sends him after his hair grew
- Chinese silk balls
  - Message is written on silk, turned into wax-covered ball that was swallowed by the messenger…
- Invisible ink-jet technology
  - Ink that is too small for human eye (Univ of Buffalo, 2000)

Examples of Text Steganography

- Physical Techniques
  - Hidden messages within wax tablets
  - Hidden messages on messenger's body
  - Hidden messages on paper written in secret inks
  - Messages written in Morse code on knitting yarn and then knitted into a piece of clothing worn by a courier
  - Messages written on envelopes in the area covered by postage stamps.

Examples of Text Steganography

Since everyone can read, encoding text
in neutral sentences is doubtfully effective

S*ince* ***E****veryone* ***C****an* ***R****ead,* ***E****ncoding* ***T****ext*
I*n* ***N****eutral* ***S****entences* ***I****s* ***D****oubtfully* ***E****ffective*

'Secret inside'

Examples of Text Steganography

Since everyone can read, encoding text
in neutral sentences is doubtfully effective

S*ince* ***E****veryone* ***C****an* ***R****ead,* ***E****ncoding* ***T****ext*
I*n* ***N****eutral* ***S****entences* ***I****s* ***D****oubtfully* ***E****ffective*

'Secret inside'

Example Image Steganography

Least Significant Bit (LSB) Method

- Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image
- The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message
- When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data
- In its simplest form, LSB makes use of BMP images, since they use lossless compression

Least Significant Bit (LSB) Method

- A grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

- When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Least Significant Bit (LSB) Method

Original Image

Stego Image

Original Image

Stego Image

Audio Steganography

- It is a technique used to transmit hidden information by modifying an **audio** signal in an imperceptible manner.
- It is the science of hiding some secret text or **audio** information in a host message.
- The host message before **steganography** and stego message after **steganography** have the same characteristics.

Pros and Cons of Steganography

- **Advantages:**
  - No one suspects existence of message
  - Highly secure

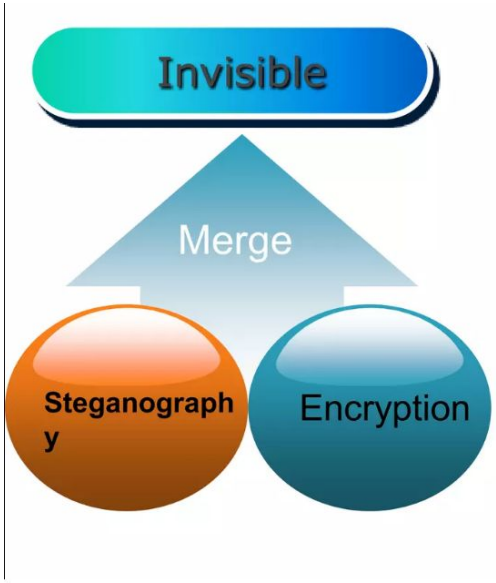
- **Disadvantages:**
  - It requires a lot of overhead to hide a relatively few bits of information

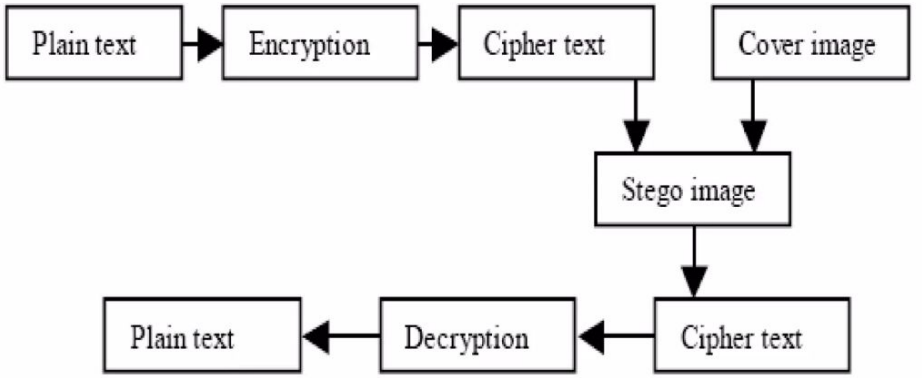
Steganography V/s Cryptography

Steganography	Cryptography
Unknown message passing	Known message passing
Steganography prevents discovery of the very existence of communication	Encryption prevents an unauthorized party from discovering the contents of a communication
Little known technology	Common technology
Technology still being develop for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithm are resistant to attacks ,larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message

Modern Steganography:

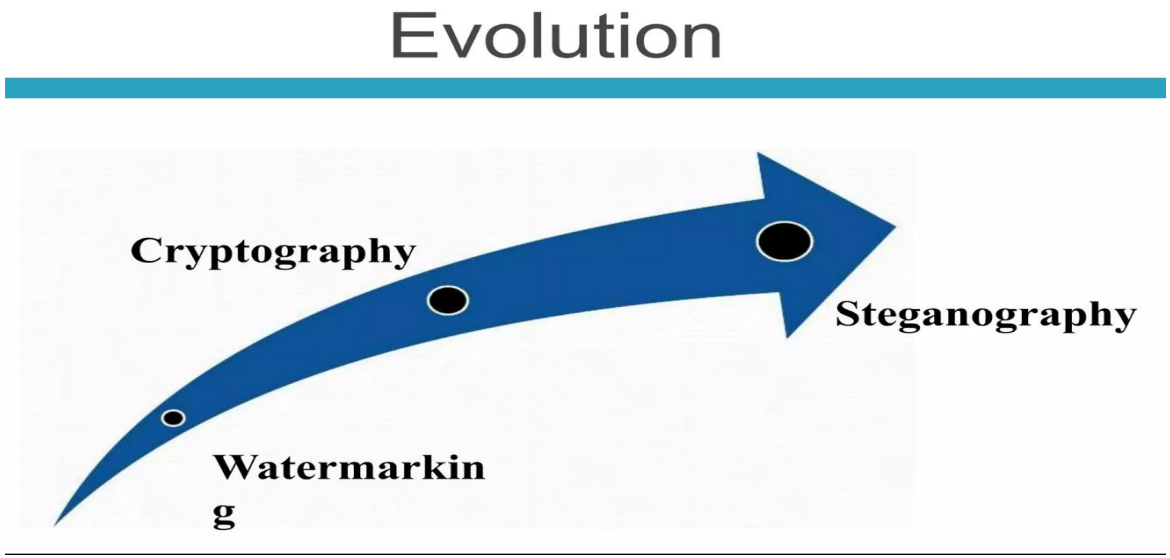
- In modern steganography, data is first **encrypted** by the usual means and then inserted, using a special algorithm, into redundant data that is part of a particular file format such as a JPEG image, Bitmap image.





Modern Steganography:

- In modern steganography, data is first **encrypted** by the usual means and then inserted, using a special algorithm, into redundant data that is part of a particular file format such as a JPEG image, Bitmap image.



References

- Chapter-1 : Cryptography and Network Security: Forouzan