Developed and Presented By Dr. Mehrdad Sepehri Sharbaf
CSUDH
Computer Science Department

http://csc.csudh.edu/

The some of the materials are excerpted from Firouz Forouzan's Book, and Jorge Ramió Aguirre's Book

CRYPTOGRAPHY

CRYPTOGRAPHY

Initial branch of Mathematics and currently of Computer Science and Telematics, which makes use of methods and technics with the main purpose of encrypting and/or protecting a message or file through an algorithm, using one or more keys. This gives rise to different types of cipher systems, denominated cryptosystems, that let us to assure any of these four aspects of information security: confidentiality or secret, integrity, availability and non repudiation of sender and receiver.

CRYPTOGRAPHY

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

Cryptanalysis: the art and science of decrypting messages.

Cryptology: cryptography + cryptanalysis

CRYPTOGRAPHIC STRENGTH

1. Secrecy of key
2. Difficulty of guessing the key (longer is harder)
3. Difficulty of reversing algorithm without key (breaking code)
4. Lack of back doors (decrypt without key)
5. Difficulty of using partial plaintext to find rest
6. Vulnerability of code to repeated texts

Generally, cannot prove encryption program strong, only prove weak.

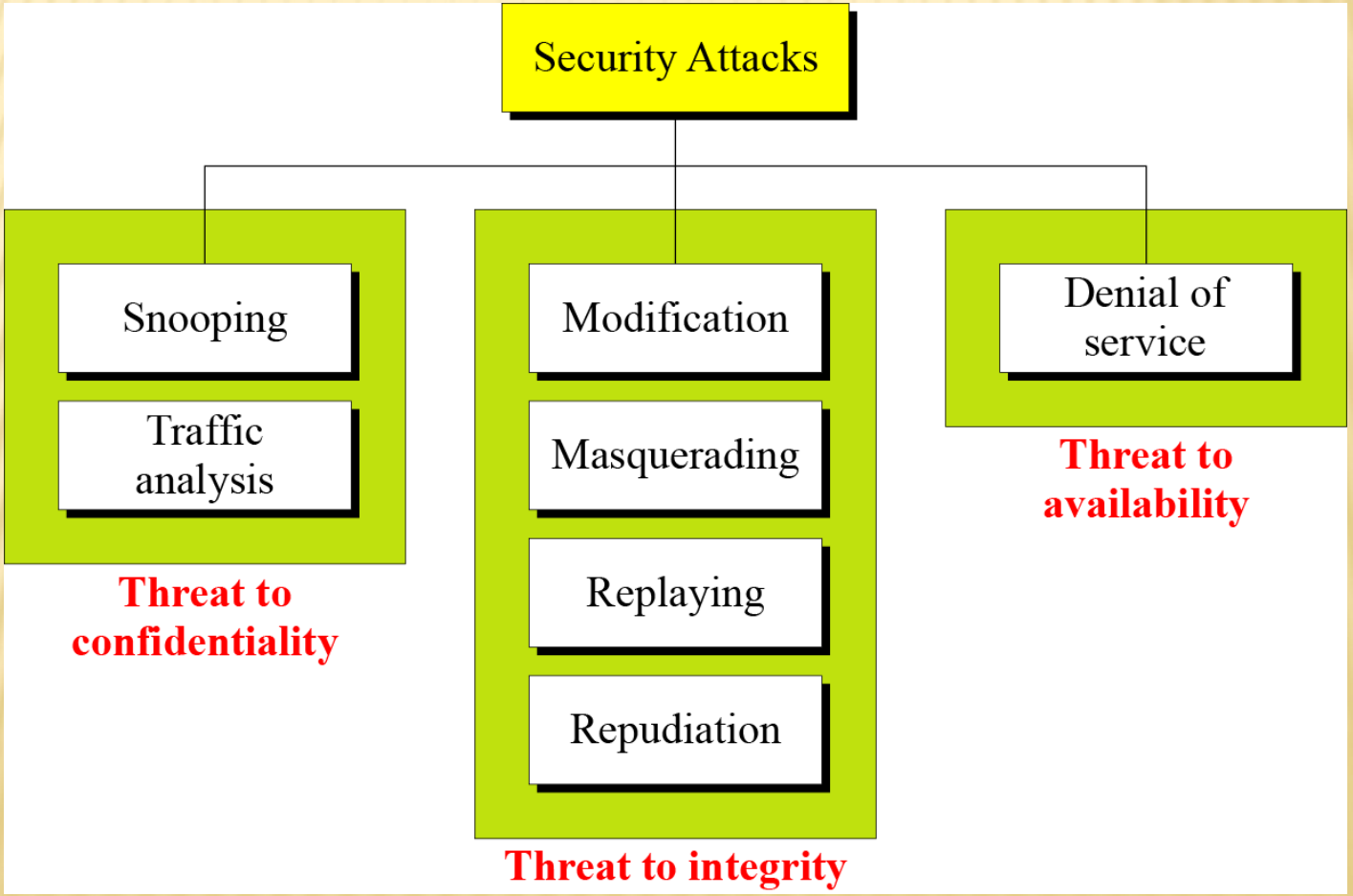
DEFINITIONS

- Plaintext: easy to understand form (original message)
- Ciphertext: difficult to understand form
- Encryption: encoding (plaintext -> ciphertext)
- Decryption: decoding (ciphertext -> plaintext)
- Cryptology: study of encryption
- Cryptography: use of encryption
- Cryptanalysis: breaking encryption

ATTACKS

The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.

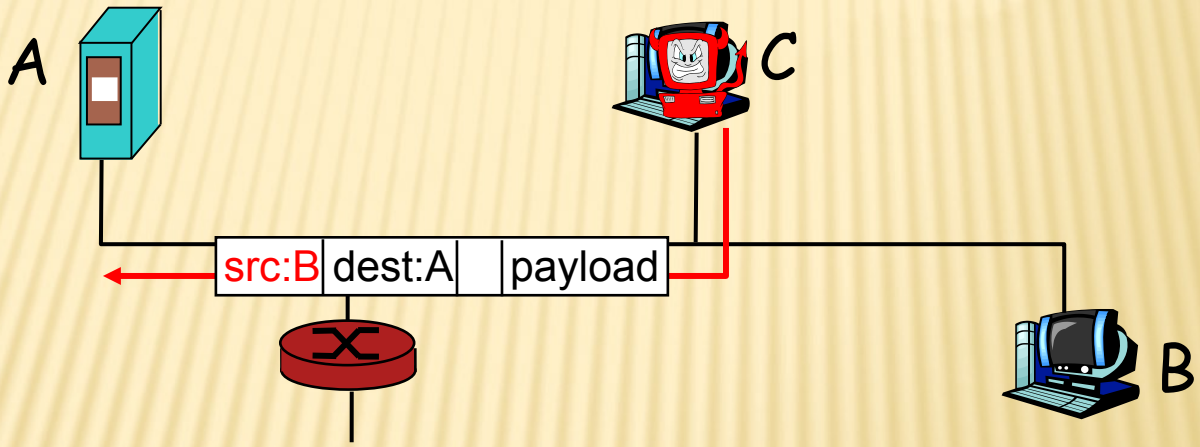
Taxonomy of attacks with relation to security goals



ATTACKS THREATENING CONFIDENTIALITY

Snooping refers to unauthorized access to or interception of data.

e.g. IP spoofing: send packet with false source address

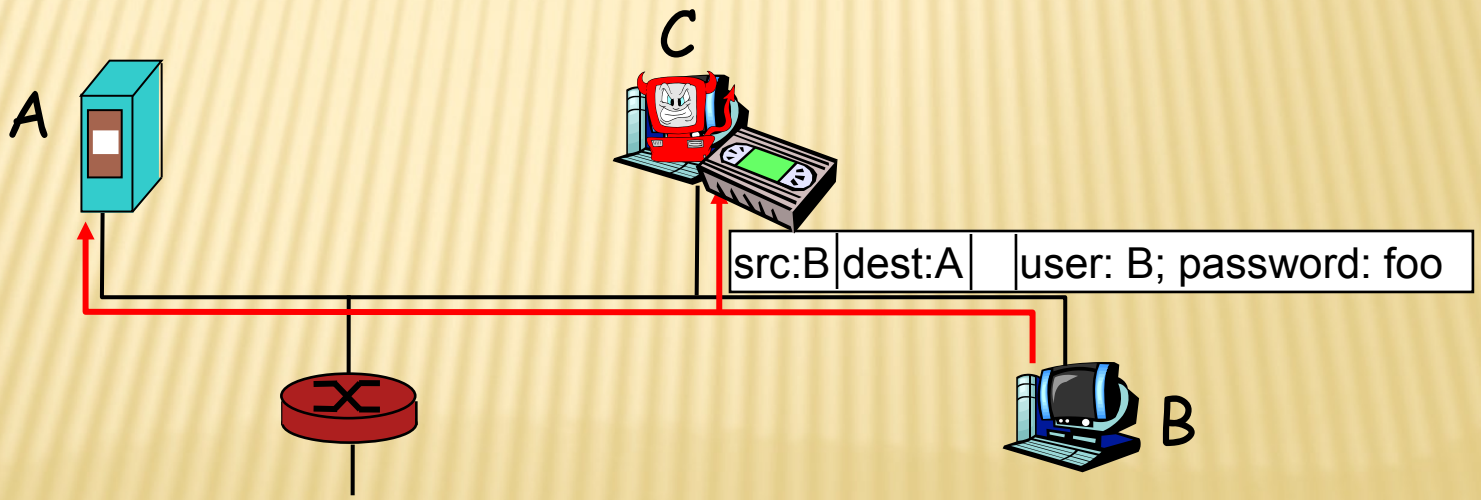


Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

ATTACKS THREATENING INTEGRITY

Masquerading or spoofing happens when the attacker impersonates somebody else.

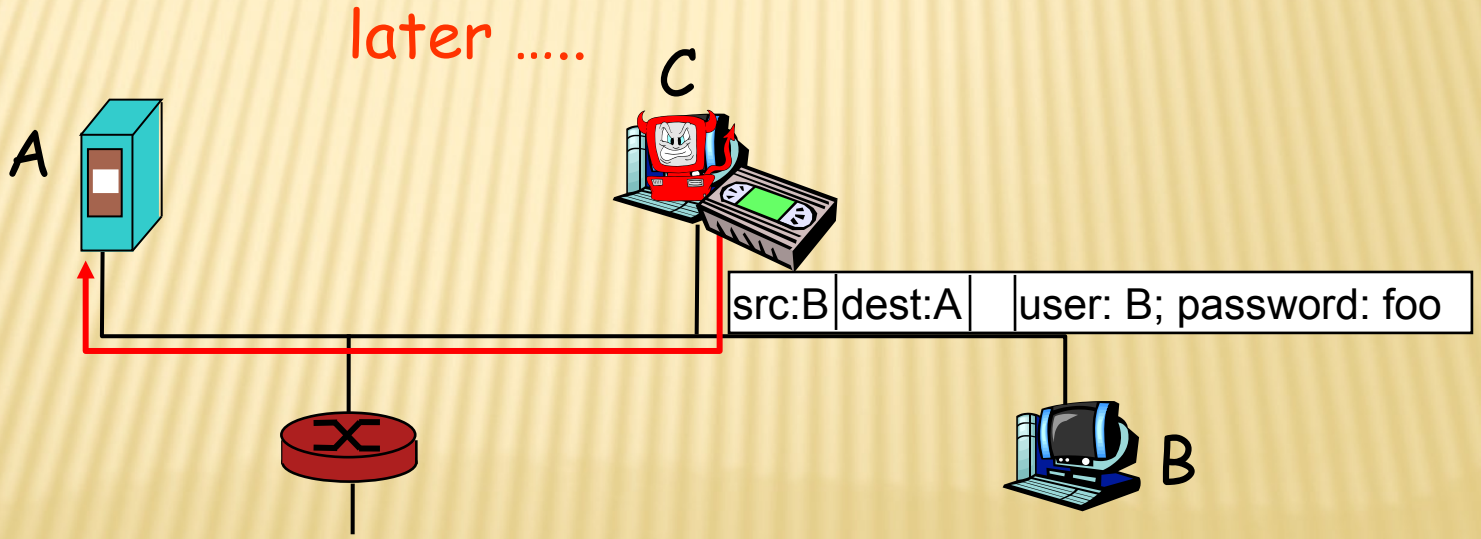
Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.



ATTACKS THREATENING INTEGRITY

Masquerading or spoofing happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.



ATTACKS THREATENING INTEGRITY

Modification means that the attacker intercepts the message and changes it.

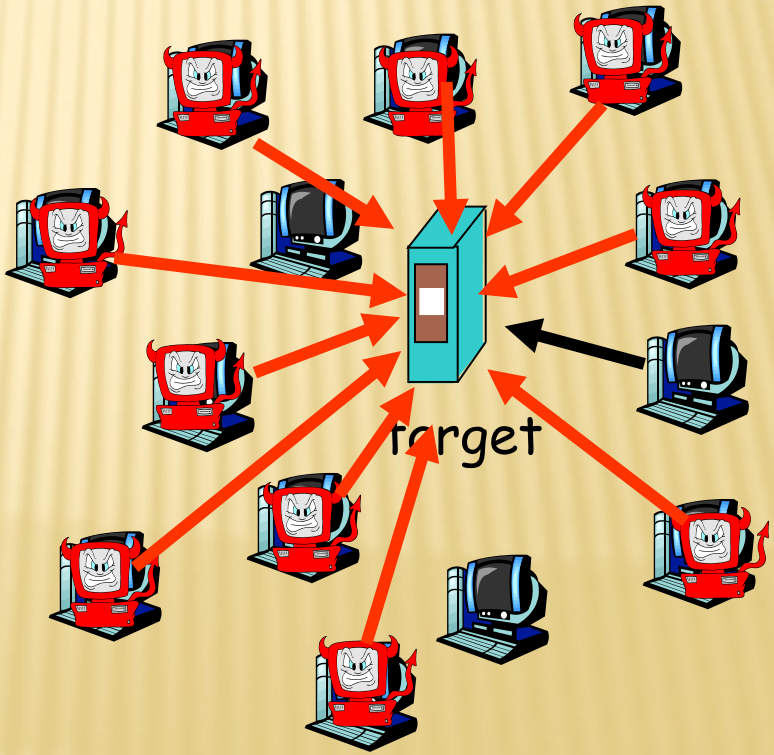
Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

ATTACKS THREATENING AVAILABILITY

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

- attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

1. select target
2. break into hosts around the network
3. send packets toward target from compromised hosts



PASSIVE VERSUS ACTIVE ATTACKS

Categorization of passive and active attacks

Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

In a passive attack, the attacker's goal is just to obtain information. The attack does not modify data or harm the system, and the system continues with its normal operation.

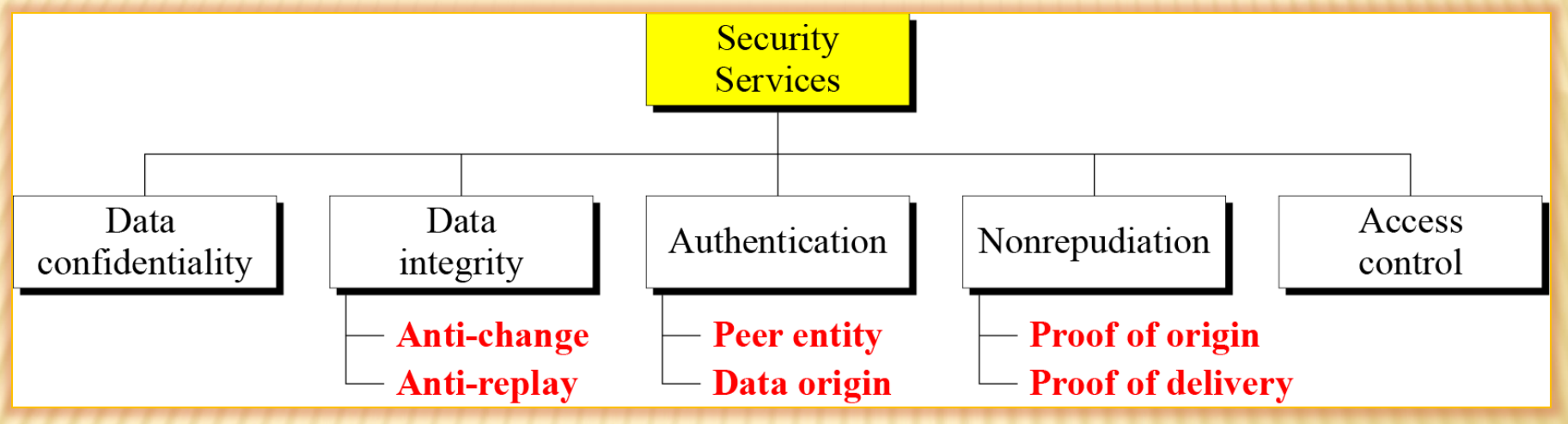
An active attack may change the data or harm the system.

SERVICES AND MECHANISMS

- The International Telecommunication Union-Telecommunication Standardization Section (ITU-T) provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.

- Security Services
  Security Mechanism
  Relation between Services and Mechanisms

SECURITY SERVICES



Data confidentiality protects data from disclosure attack.

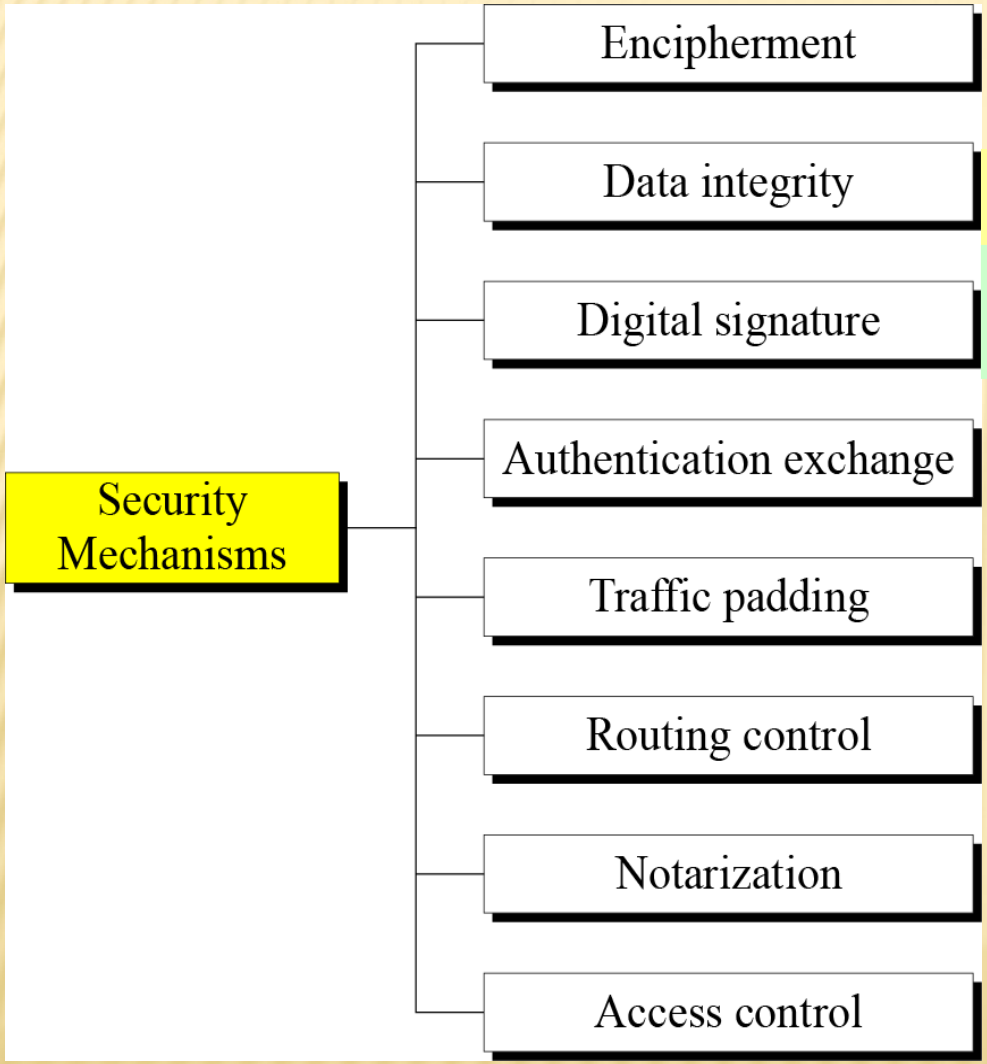
Data integrity protect data from modification, insertion, deletion, and replaying attacks.

Authentication provides proof of sender, or receiver, or source of the data.

Nonrepudiation protects against repudiation by either the sender to the reveiver.

Access control provides protection again unauthorized access to data

SECURITY MECHANISM



Hiding or covering data

Appends to data a short check value

Sender signs data, receiver verifies data

Two entities exchange msg to prove their identity to each

Insert bogus data into the data traffic to thwart traffic analysis

Continuously change routes b/w sender and receiver to prevent eavesddropping

A third trusted party controls communication

Prove and verify that a user has access right to resources

Security mechanisms

Relation between Services and Mechanisms

Relation between security services and mechanisms

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

TECHNIQUES

Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today: cryptography and steganography.

Cryptography
Steganography

STEGANOGRAPHY

- Steganography is the art and science of hiding information into covert channels so as to conceal the information and prevent the detection of the hidden message.
- Today, steganography refers to hiding information in digital picture files and audio files.

STEGANOGRAPHY

- Hide a message by using the least significant bits of frames on a CD
- Kodak photo CD format's maximum resolution is 2048 by 3072 pixels, with each pixel containing 24 bits of RGB color information.
- The least significant bit of each 240bit pixel can be changed without greatly affecting the quality of the image.
- Drawbacks:
  - Overhead
  - Worthless once discovered (encryption)

STEGANOGRAPHY

- Steganography conceals the existence of the
- Steganography conceals the existence of the message
- Cryptography render the message unintelligible to outsides by various transformations of the text.
- Examples:
  - Hide a msg in an image: https://www.petitcolas.net/steganography/image_downgrading/

The image in which we want to hide another image

The image we wish to hide: ‘F15’

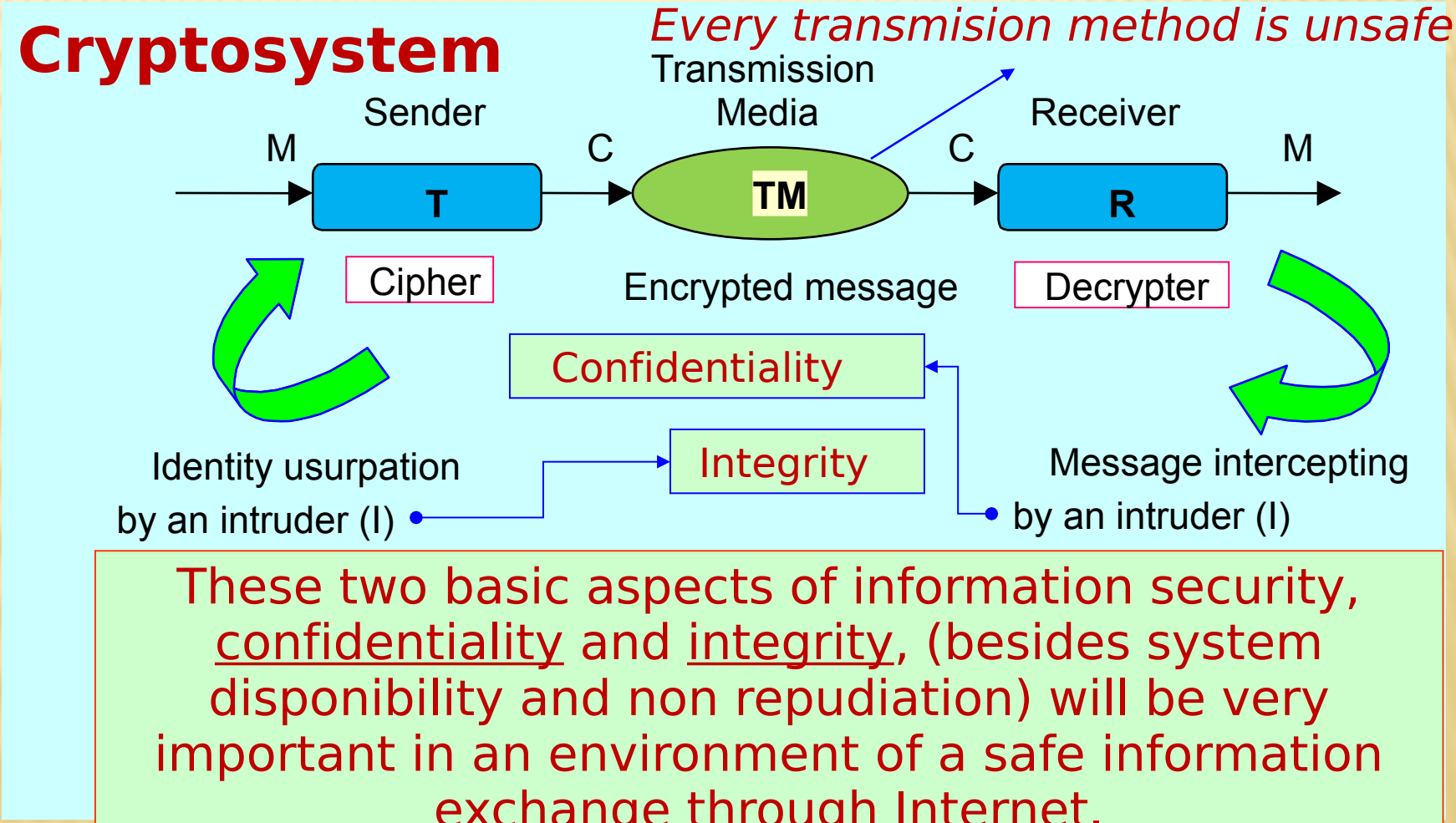
The stego-image (i.e., after the hiding process)

The image extracted from the stego-image

STEGANOGRAPHY

- Steganography is defined as "hiding information within a noise; a way to supplement (not replace) encryption, to prevent the existence of encrypted data from being detected".
- Steganography and Cryptography are cousins in the data hiding techniques.
- Cryptography is the practice of scrambling a message to an obscured form to prevent others from understanding it.
- Steganography is the study of obscuring the message so that it cannot be seen.
- More tools:
- DMOZ - Computers: Security: Products and Tools: Cryptography: Steganography (dmoz-odp.org)

CONFIDENTIALITY AND INTEGRITY



These two basic aspects of information security, confidentiality and integrity, (besides system disponibility and non repudiation) will be very important in an environment of a safe information exchange through Internet.

TYPE OF CRYPTOSYSTEMS

Classification of Cryptosystems

According to the treatment of the message they are:

Block cipher (IDEA, AES, RSA* ...) 64-128 bits

Stream cipher (A5, RC4, SEAL ...) encryption bit by bit

According the type of keys they can be:

Symmetric Systems

Asymmetric Systems

Secret key cipher

Public key cipher

(*) As we'll see in another chapter, actually systems like RSA do not encrypt by blocks: they encrypt a single number.

SYMMETRIC & ASYMMETRIC CRYPTOSYSTEMS

Symmetric Cryptosystems :

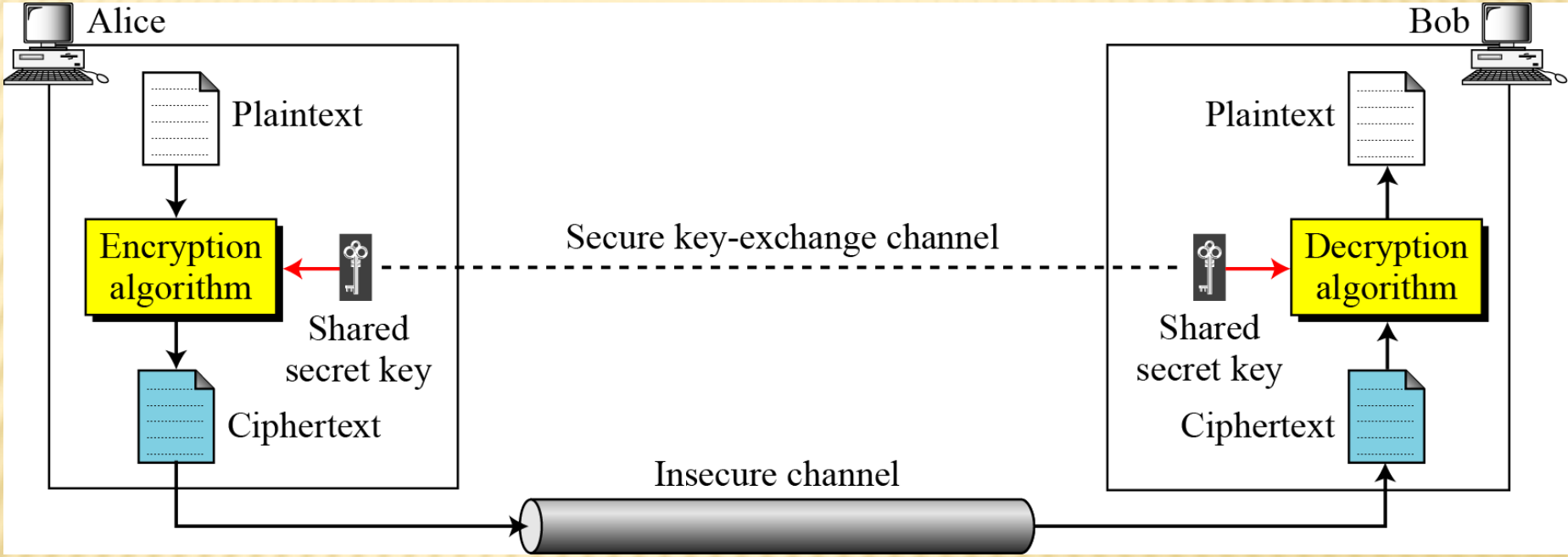
There will be a unique key (secret) that sender and receiver must share. Same key is used to encrypt and decrypt so the security just resides in maintaining the secret of the key.

Asymmetric Cryptosystems :

Every user creates a pair of keys, one private and other public, inverses of a finite field. What is encrypted in transmission with a key, is decrypted when receiving with the inverse key. The system security resides in the computing difficulty of discovering the private key through the public. For that, they use mathematical one-way functions.

Symmetric Key

General idea of symmetric-key cipher



The original message from Alice to Bob is called plaintext; the message that is sent through the channel is called the ciphertext. To create the ciphertext from the plaintext, Alice uses an encryption algorithm and a shared secret key. To create the plaintext from ciphertext, Bob uses a decryption algorithm and the same secret key.

Encryption Algorithm

If P is the plaintext, C is the ciphertext, and K is the key,

Encryption: $C = E_k(P)$ Decryption: $P = D_k(C)$

In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

We assume that Bob creates P_1; we prove that $P_1 = P$:

Alice: $C = E_k(P)$

Bob: $P_1 = D_k(C) = D_k(E_k(P)) = P$

Encryption Algorithm

Locking and unlocking with the same key

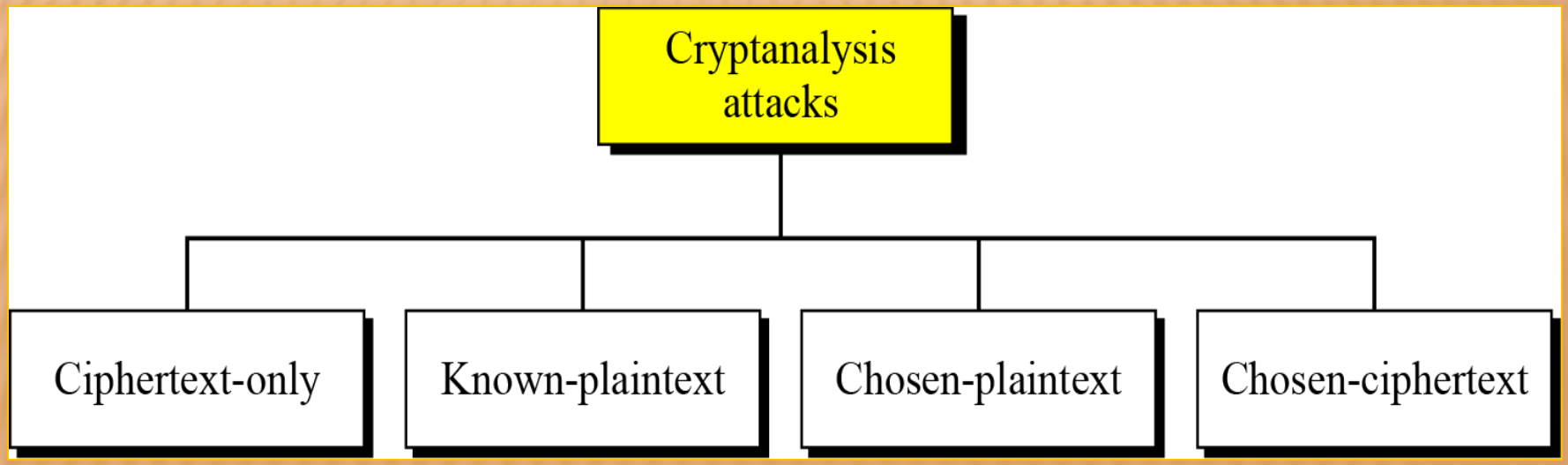
KERCKHOFF'S PRINCIPLE

- Based on Kerckhoff's principle, 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.

CRYPTANALYSIS

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

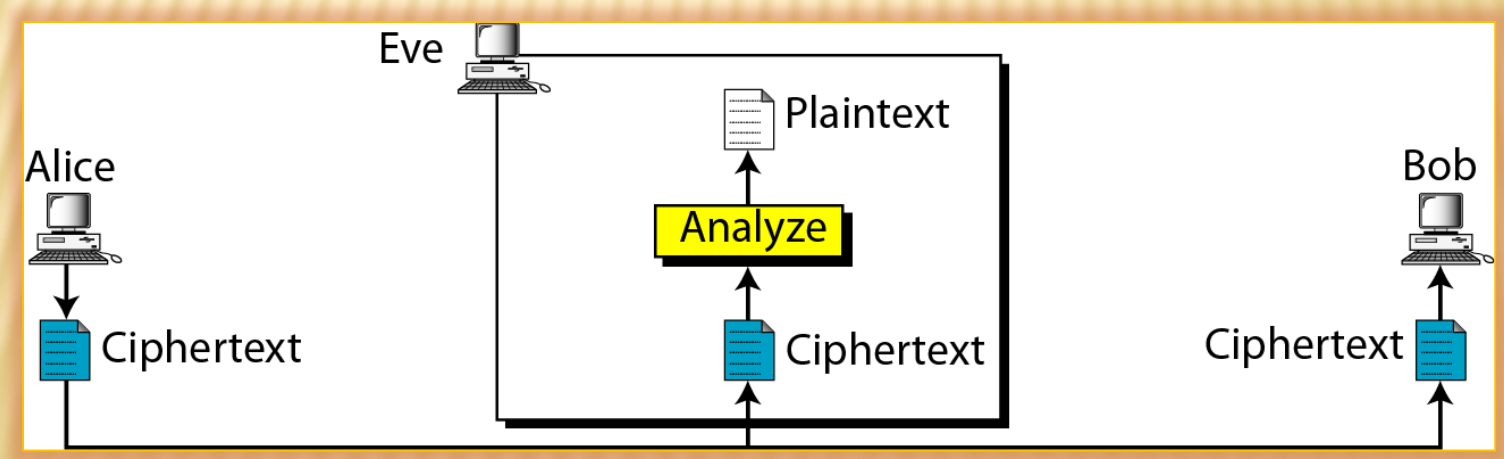
Cryptanalysis attacks



CIPHERTEXT-ONLY ATTACK

Ciphertext + algorithm ☾ key and the plaintext

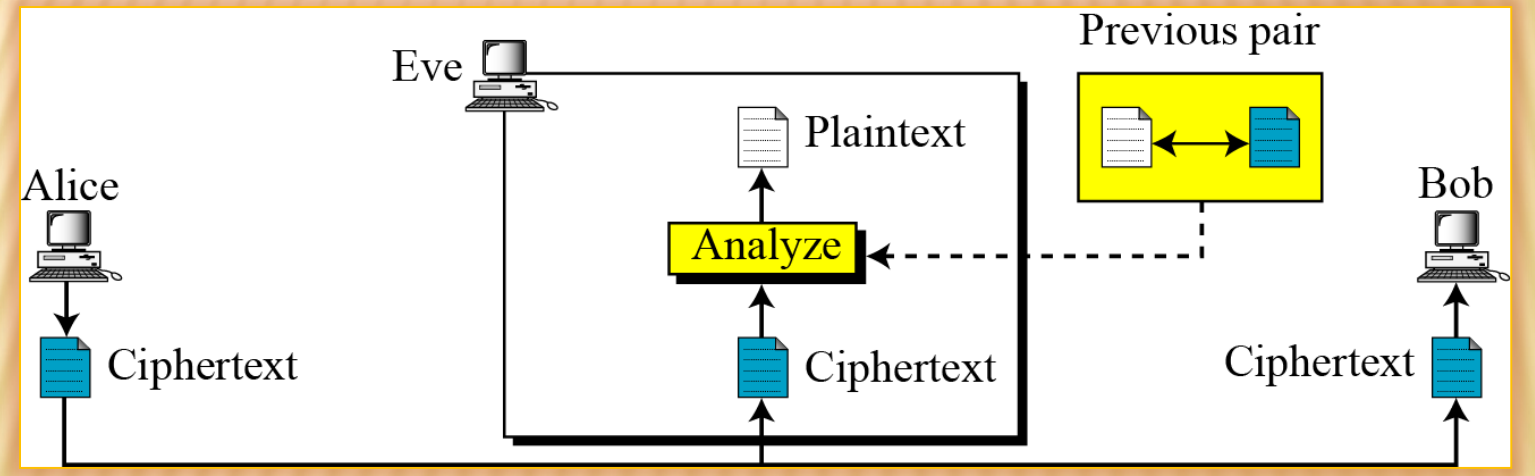
- Brute-Force attack: exhaustive key search attack
- Statistical attack: benefit from inherent characteristics of the plaintext language. E.g. E is the most frequently used letter.
- Pattern attack: discover pattern in ciphertext.



KNOWN-PLAINTEXT ATTACK

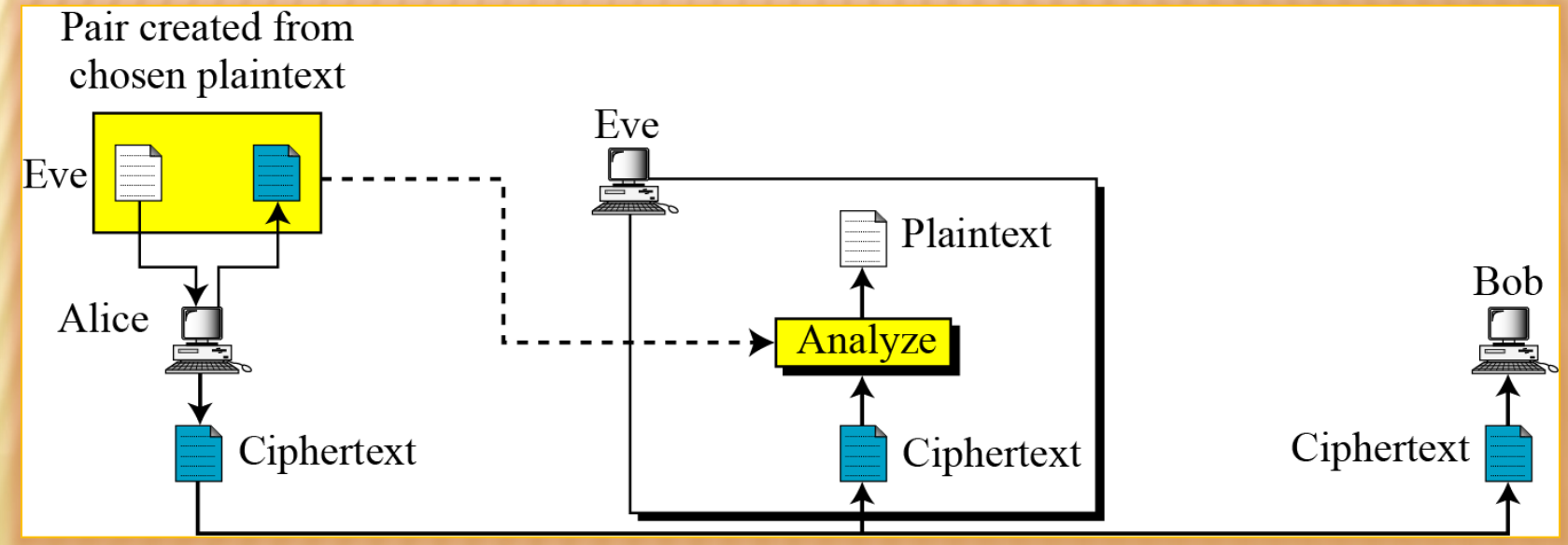
Eve has access to some plaintext/ciphertext pairs in addition to the intercepted ciphertext.

Eve uses the relationship b/w the previous pair to analyze the current ciphertext.



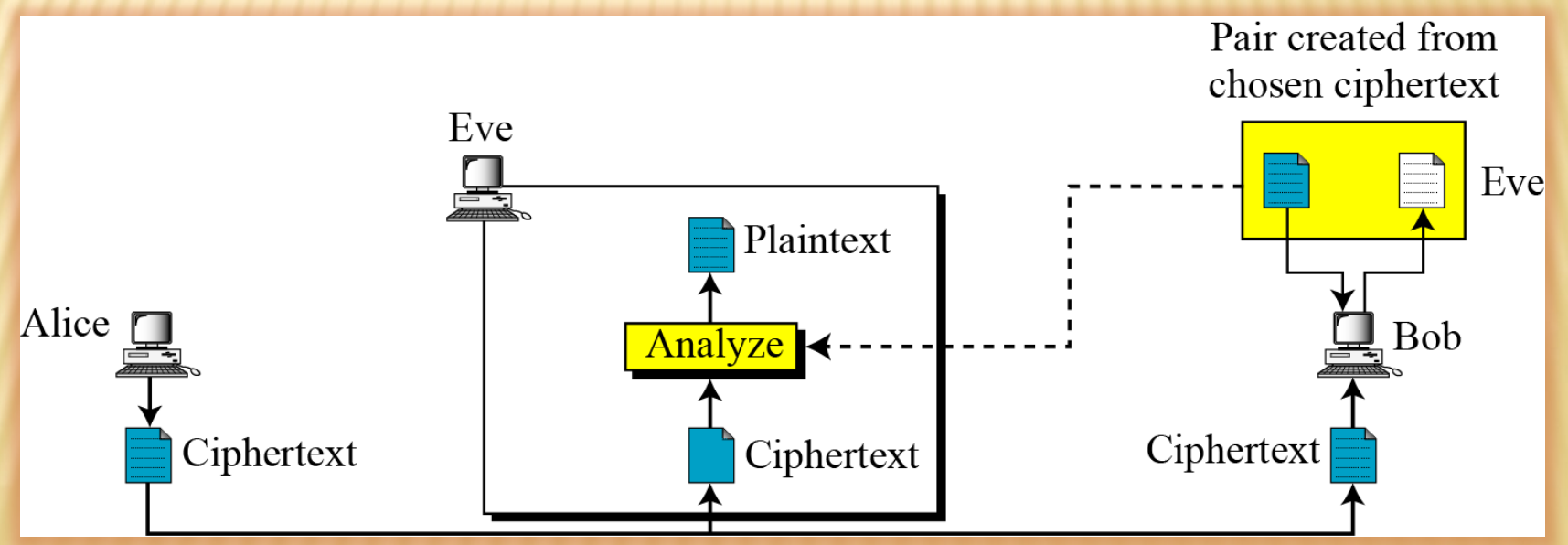
CHOSEN-PLAINTEXT ATTACK

The plaintext/ciphertext pairs have been chosen by the attacker herself.

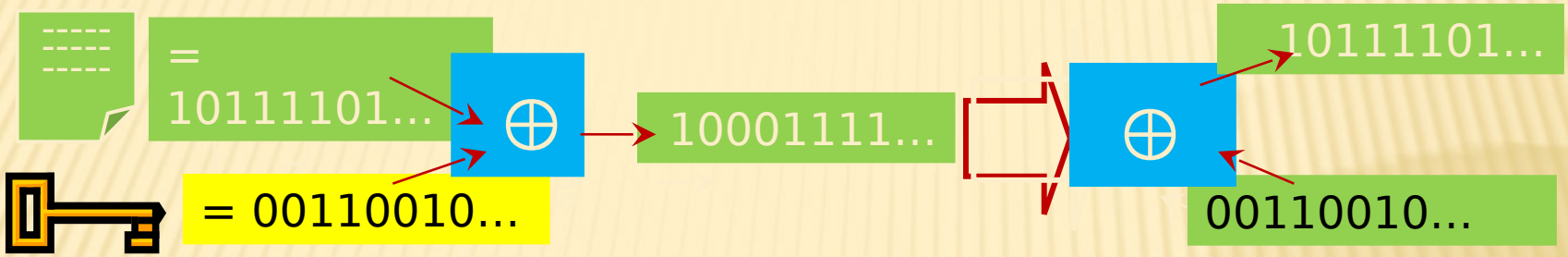


CHOSEN-CIPHERTEXT ATTACK

Eve chooses some ciphertext and decrypts to form a ciphertext/plaintext pair. This can happen if Eve has access to Bob's computer.



SIMPLE IDEA: ONE-TIME PAD



Key is a never-repeating bit sequence as long as plaintext

Encrypt by bitwise XOR of plaintext and key:
ciphertext = plaintext ⊕ key

Decrypt by bitwise XOR of ciphertext and key:
ciphertext ⊕ key = (plaintext ⊕ key) ⊕ key = plaintext ⊕ (key ⊕ key) = plaintext

Cipher achieves perfect secrecy if and only if there are as many possible keys as possible plaintexts, and every key is equally likely (Claude Shannon's result)

ADVANTAGES OF ONE-TIME PAD

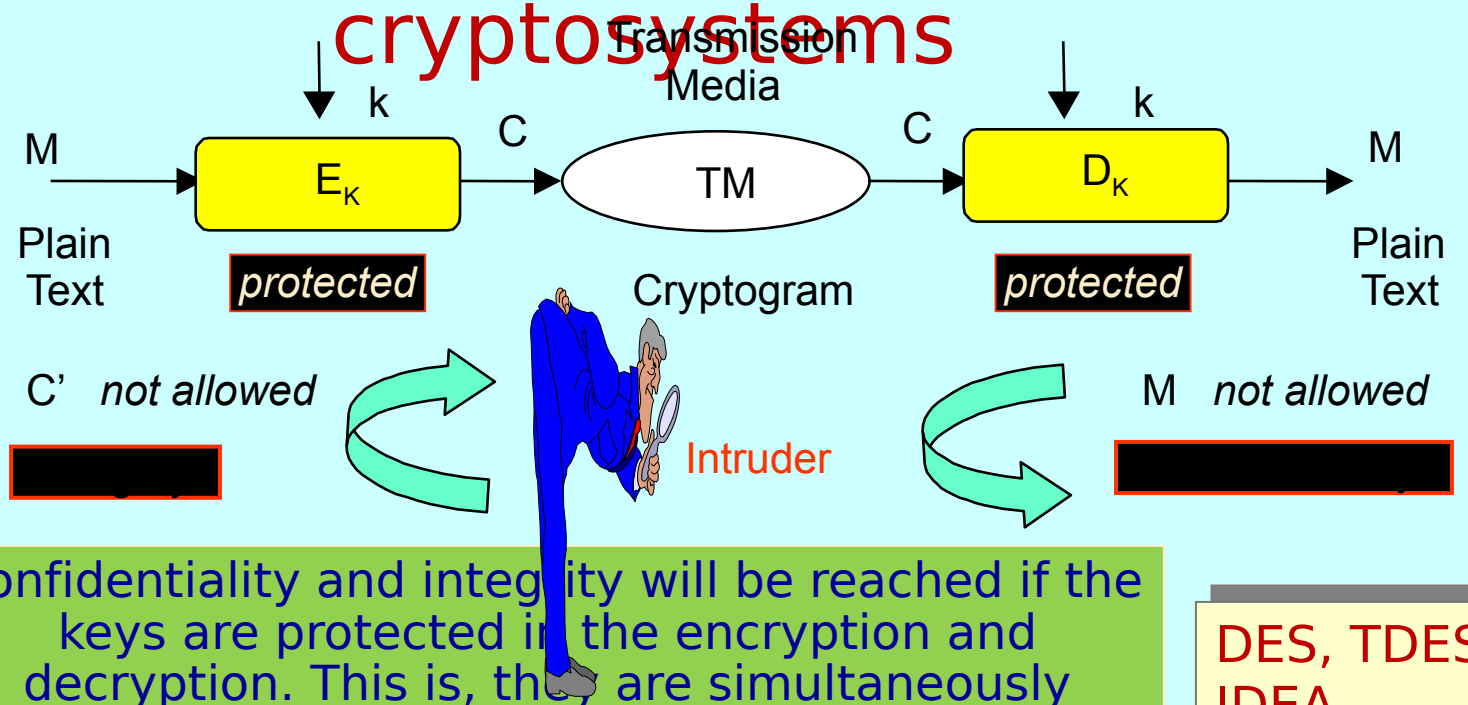
- Easy to compute
  - Encryption and decryption are the same operation
  - Bitwise XOR is very cheap to compute
- As secure as possible
  - Given a ciphertext, all plaintexts are equally likely, regardless of attacker's computational resources
  - ...as long as the key sequence is truly random
    - True randomness is expensive to obtain in large quantities
  - ...as long as each key is same length as plaintext
    - But how does the sender communicate the key to receiver?

PROBLEMS WITH ONE-TIME PAD

- Key must be as long as plaintext
  - Impractical in most realistic scenarios
  - Still used for diplomatic and intelligence traffic
- Does not guarantee integrity
  - One-time pad only guarantees confidentiality
  - Attacker cannot recover plaintext, but can easily change it to something else
- Insecure if keys are reused
  - Attacker can obtain XOR of plaintexts

SYMMETRIC CRYPTOSYSTEMS

Encryption with secret key cryptosystems



Confidentiality and integrity will be reached if the keys are protected in the encryption and decryption. This is, they are simultaneously obtained if the secret key is protected.

DES, TDES, IDEA, CAST, AES...

STREAM AND BLOCK CIPHERS

The literature divides the symmetric ciphers into two broad categories: stream ciphers and block ciphers. Although the definitions are normally applied to modern ciphers, this categorization also applies to traditional ciphers.

Stream Ciphers
Block Ciphers
Combination

SYMMETRIC KEY CRYPTOSYSTEMS

- **Stream ciphers**
  - Operate on the plaintext a single bit (or sometimes byte) at a time
  - Simple substitution
  - Poly-alphabetic substitution
  - **ORYX** is the algorithm used to encrypt data sent over digital cellular phones. t is a stream cipher based on three 32-bit Galois Linear Feedback Shift Register (LFSR)s. The cryptographic tag-team from Counterpane Systems (David Wagner, John Kelsey, and Bruce Schneier) have developed an attack on ORYX that requires approximately 24 bytes of known plaintext and about 2^{16} initial guesses.

SYMMETRIC KEY CRYPTOSYSTEMS

- **Stream ciphers**
  - **SEAL**, designed by Don Coppersmith of IBM Corp, is probably the fastest secure encryption algorithm available. The key setup process of SEAL requires several kilobytes of space and rather intensive computation involving SHA1, but only five operations per byte are required to generate the keystream. SEAL is particularly appropriate for disk encryption and similar applications where data must be read from the middle of a ciphertext stream. SEAL is patented, and can be licensed from IBM.
  - RC4 algorithm is a stream cipher from RSA Data Security, Inc. There are no known attacks against RC4. RC4 is not patented by RSA Data Security, Inc; it is just protected as a trade secret. The 40-bit exportable version of RC4 has been broken by brute force! (used by WLAN IEEE 802.11 in WEP)

SYMMETRIC KEY CRYPTOSYSTEMS

- **Block ciphers**
  - Operate on the plaintext in groups of bits. The groups of bits are called **blocks**.
  - Typical block size is 64 bits or multiple of it, e.g. 128 bits, 256 bits.
  - DES, AES
  - IDEA, developed in Zurich is generally regarded to be one of the best and most secure block algorithm available to the public today. It utilizes a 128-bit key and is designed to be resistant to differential cryptanalysis. Some attacks have been made against reduced round IDEA.

SYMMETRIC KEY CRYPTOSYSTEMS

- **Block ciphers**
  - Blowfish is a block cipher designed by Bruce Schneier, and is perhaps one of the most secure algorithms available.
  - RC5 is a group of algorithms designed by RSA that can take on a variable block size, key size, and number of rounds. RC5 generally has a 64-bit block size. David Wagner, John Kelsey, and Bruce Schneier have found weak keys in RC5, with the probability of selecting a weak key to be 2^{-10r}, where r is the number of rounds. For sufficiently large r values (greater than 10), this is not a problem as long as you are not trying to build a hash function based on RC5. Kundsen has also found a differential attack on RC5.
  - Different modes of operation

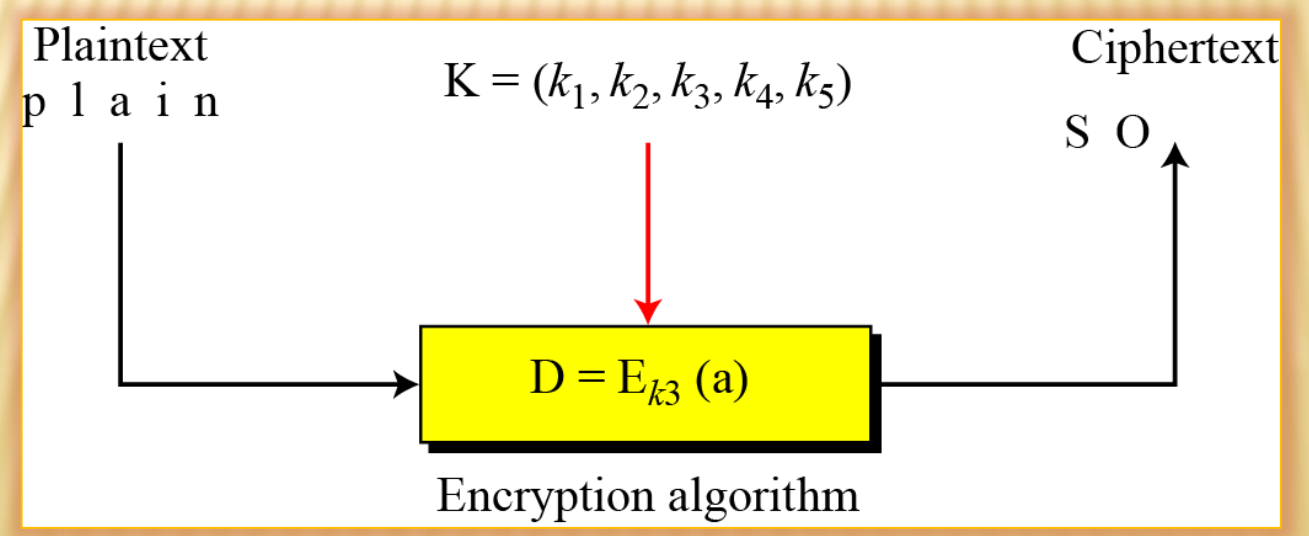
STREAM CIPHERS

Call the plaintext stream P, the ciphertext stream C, and the key stream K.

$$P = P_1P_2P_3, \ldots \qquad C = C_1C_2C_3, \ldots \qquad K = (k_1, k_2, k_3, \ldots)$$

$$C_1 = E_{k1}(P_1) \qquad C_2 = E_{k2}(P_2) \qquad C_3 = E_{k3}(P_3) \ldots$$

Stream cipher



STREAM CIPHERS

Example

Additive ciphers can be categorized as stream ciphers in which the key stream is the repeated value of the key. In other words, the key stream is considered as a predetermined stream of keys or $K = (k, k, \ldots, k)$. In this cipher, however, each character in the ciphertext depends only on the corresponding character in the plaintext, because the key stream is generated independently.

Example

The monoalphabetic substitution ciphers discussed in this chapter are also stream ciphers. However, each value of the key stream in this case is the mapping of the current plaintext character to the corresponding ciphertext character in the mapping table.

STREAM CIPHERS

Example

Vigenere ciphers are also stream ciphers according to the definition. In this case, the key stream is a repetition of m values, where m is the size of the keyword. In other words,

$$K = (k_1, k_2, \ldots k_m, k_1, k_2, \ldots k_m, \ldots)$$

Example

We can establish a criterion to divide stream ciphers based on their key streams. We can say that a stream cipher is a monoalphabetic cipher if the value of k_i does not depend on the position of the plaintext character in the plaintext stream; otherwise, the cipher is polyalphabetic.

STREAM CIPHERS

Example

- Additive ciphers are definitely monoalphabetic because k_i in the key stream is fixed; it does not depend on the position of the character in the plaintext.

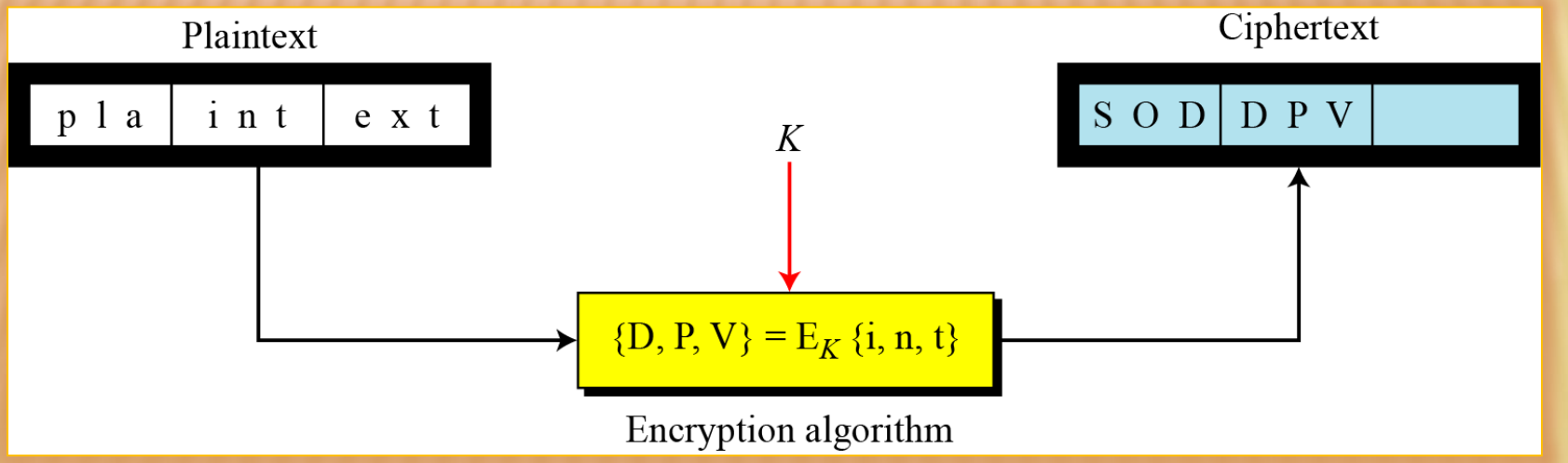
- Monoalphabetic substitution ciphers are monoalphabetic because k_i does not depend on the position of the corresponding character in the plaintext stream; it depends only on the value of the plaintext character.

- Vigenere ciphers are polyalphabetic ciphers because k_i definitely depends on the position of the plaintext character. However, the dependency is cyclic. The key is the same for two characters m positions apart.

BLOCK CIPHERS

In a block cipher, a group of plaintext symbols of size m (m > 1) are encrypted together creating a group of ciphertext of the same size. A single key is used to encrypt the whole block even if the key is made of multiple values. Figure 3.27 shows the concept of a block cipher.

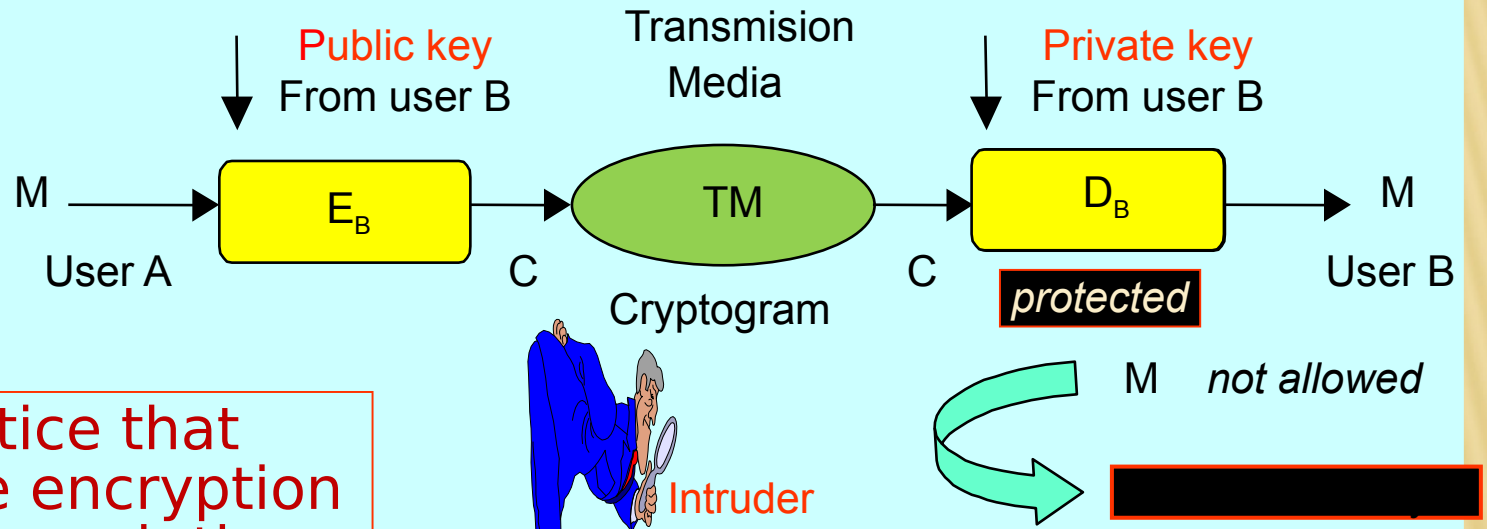
Block cipher



ASYMMETRIC CRYPTOSYSTEMS

Receiver Public Key Cipher

RSA Keys exchange



Notice that the encryption is trough the public key of receiver.

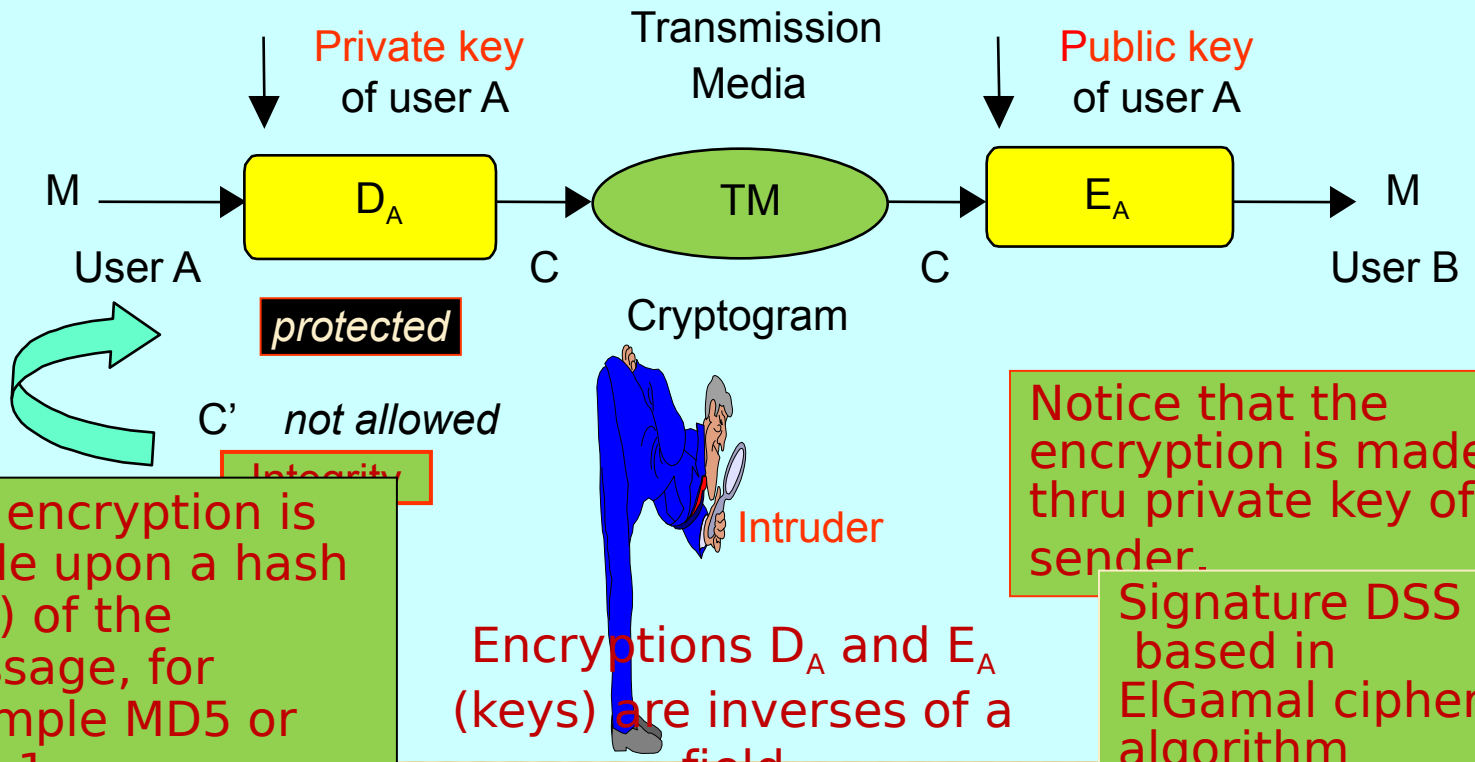
Encryptions E_B and D_B (keys) are inverses of a field

A similar system is Diffie & Hellman (DH) key agreement

ASYMMETRIC CRYPTOSYSTEMS

Encryption with private key of sender
Digital signature RSA

Signatures: RSA and DSS



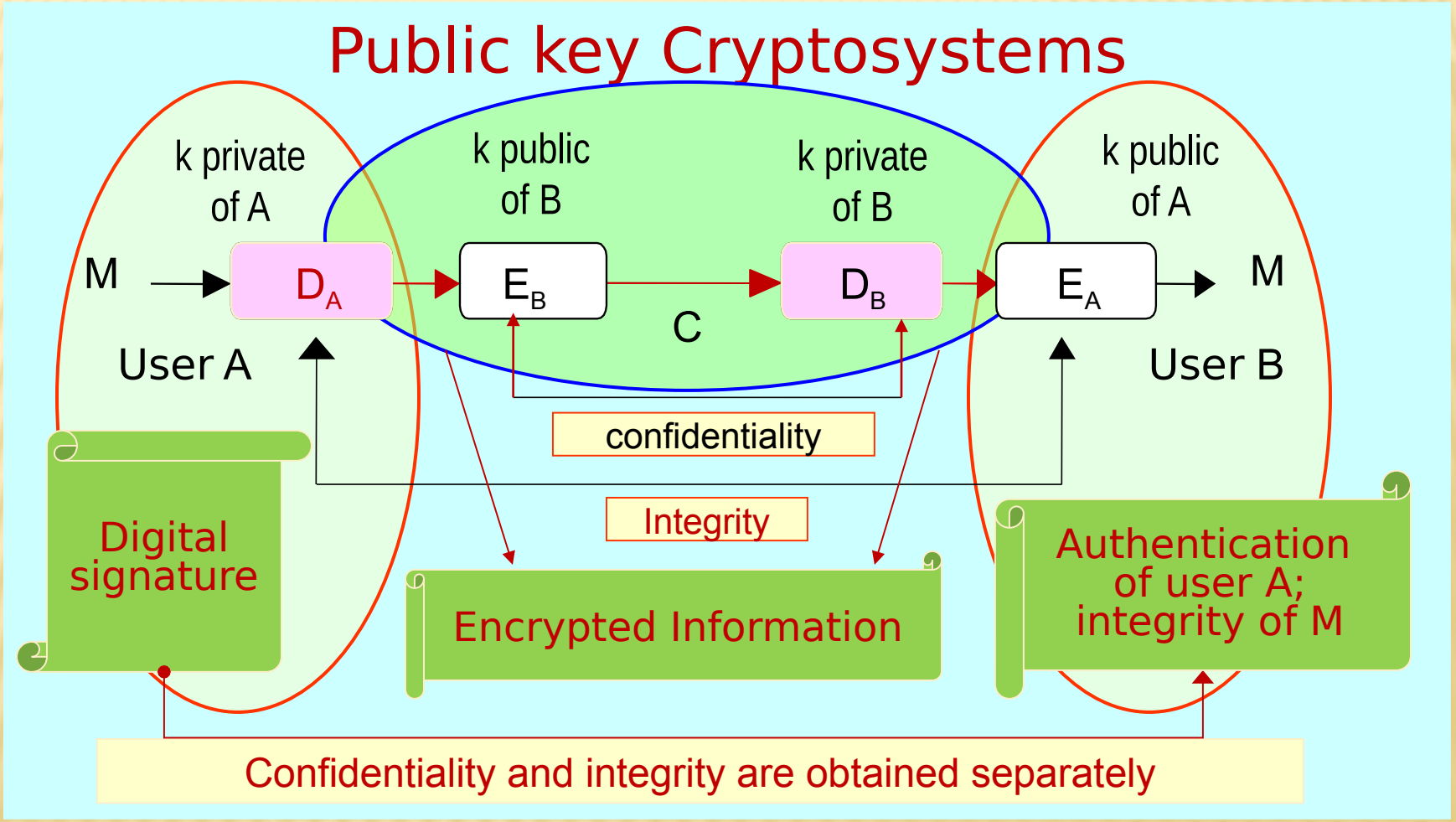
The encryption is made upon a hash H(M) of the message, for example MD5 or SHA-1

Encryptions D_A and E_A (keys) are inverses of a field

Notice that the encryption is made thru private key of sender.

Signature DSS is based in ElGamal cipher algorithm

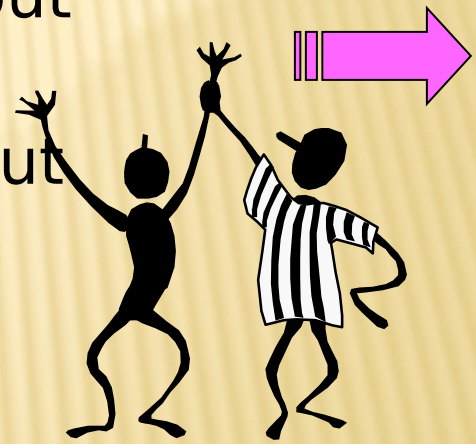
TYPES OF CIPHER WITH ASYMMETRIC SYSTEMS



SYMMETRIC OR ASYMMETRIC CIPHER?

Public key systems are very slow but they have digital signature.

Secret key systems are very fast but they do not have digital signature.

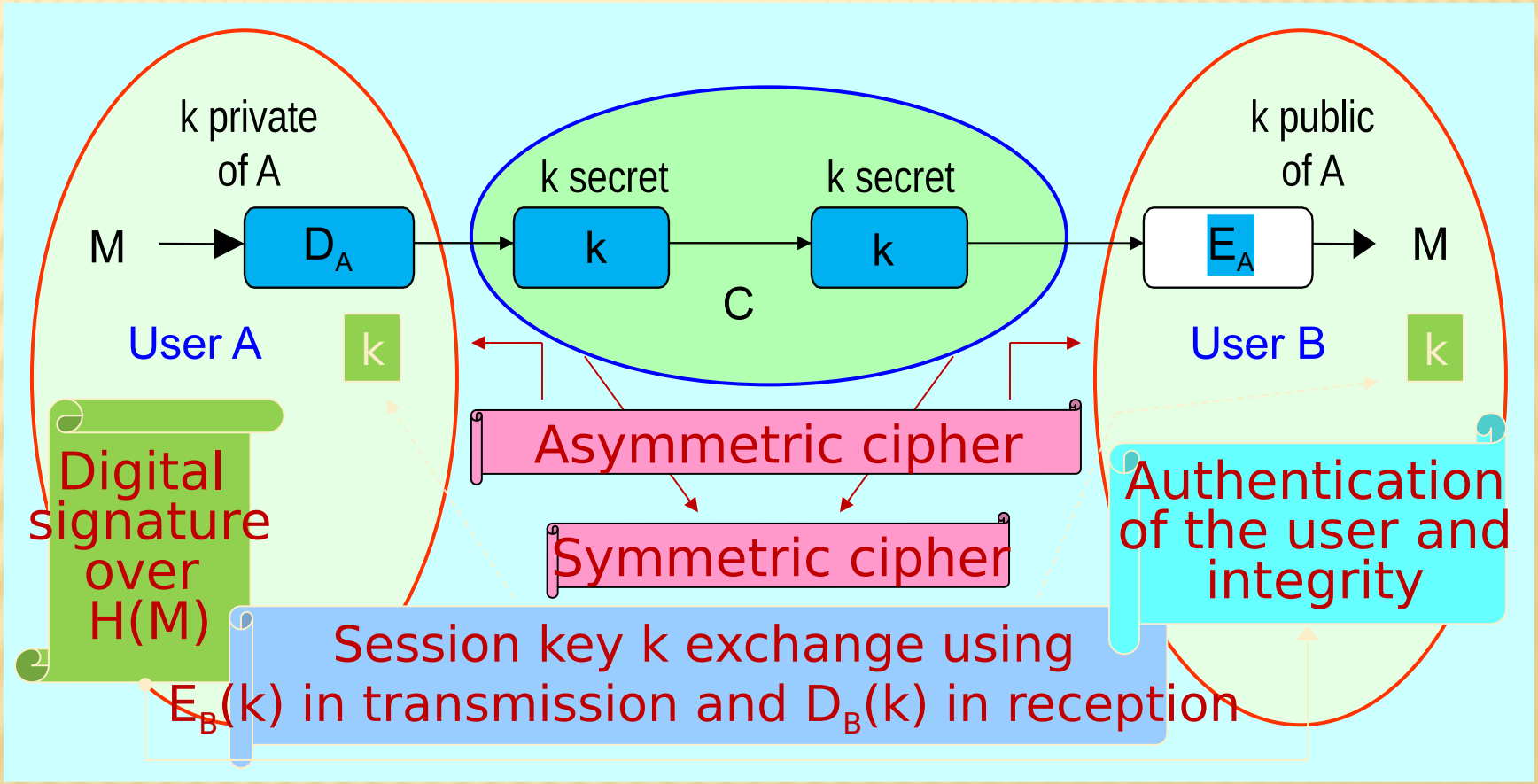


What should we do?

Information encryption:
- We´ll use secret key systems

Signature and session key exchange:
- We´ll use public key systems

HYBRID SYSTEM OF CIPHER AND SIGNATURE



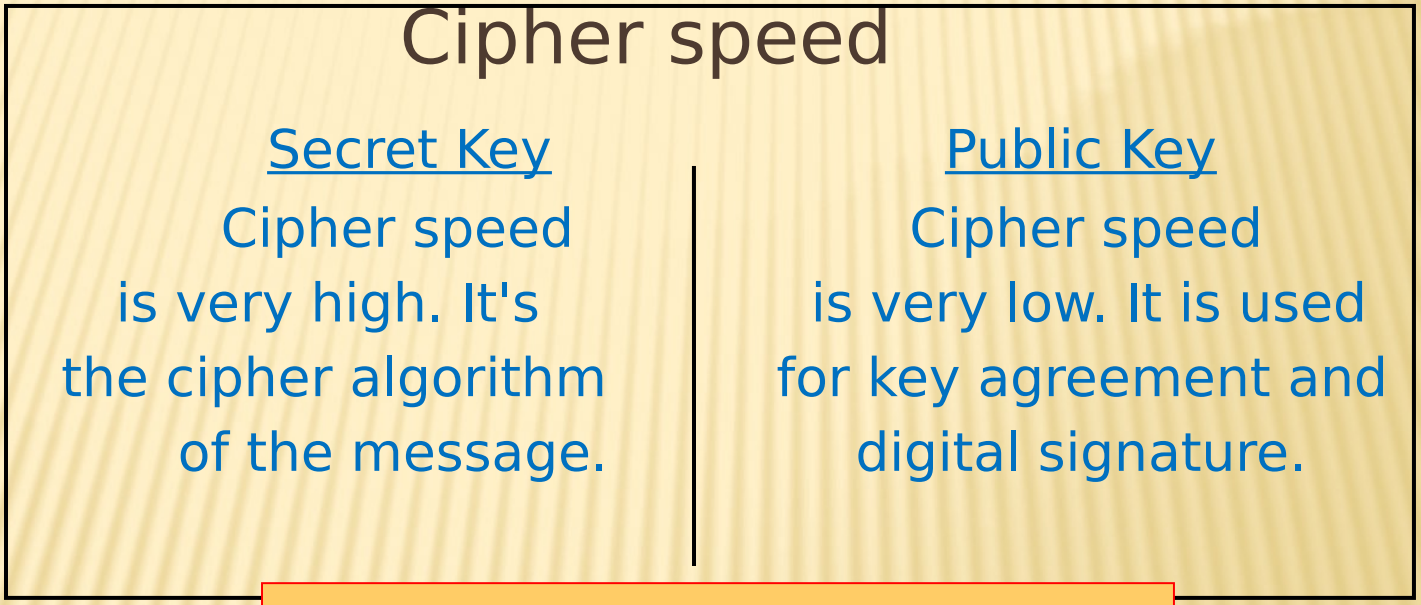
COMPARATIVE: SENDER'S AUTHENTICATION

Authentication

Secret Key	Public Key
The messsage can be authenticated but not the sender in an easy and efficient way.	Having a public key and another private, both the message and the sender can be authenticated.

Regarding authentication, symmetric systems have a heavier authentication and with only a third part of trust. Asymmetric ones allow a real digital signature, efficient and simple, where the third part of trust is just presential.

COMPARATIVE: CIPHER SPEED



Hundreds of M Bytes/seg in HW

Regarding cipher speed, symmetric systems are from 100 to 1.000 times faster than asymmetrics. In SW cipher speed is lower.

Hundreds of K Bytes/seg in HW

ummary symmetric cipher v/s asymmet

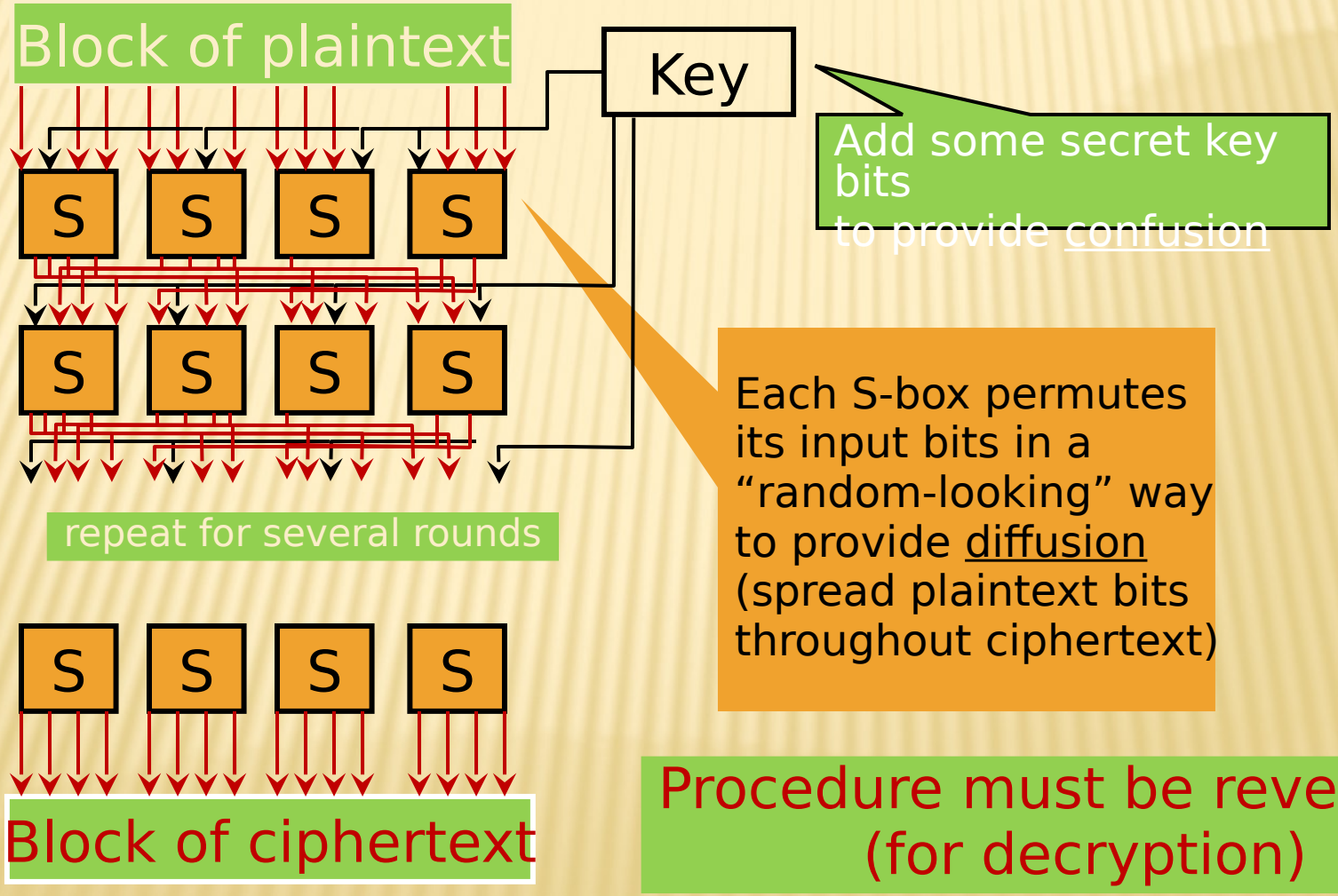
Symmetric Cipher

- Confidentiality
- Partial authentication
- No digital signature
- Keys:
  - Small lenght
  - Short lifetime (session)
  - Elevated number
- High speed

Asymmetric Cipher

- Confidentiality
- Total authentication
- With digital signature
- Keys:
  - Big lenght
  - Long lifetime
  - Number reduced
- Slow speed

BLOCK CIPHER OPERATION (SIMPLIFIED)



Procedure must be reversible (for decryption)

DESIGN PRINCIPLES

- **block size**
  - increasing size improves security, but slows cipher
- **key size**
  - increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- **number of rounds**
  - increasing number improves security, but slows cipher
- **subkey generation**
  - greater complexity can make analysis harder, but slows cipher
- **round function**
  - greater complexity can make analysis harder, but slows cipher
- **fast software en/decryption & ease of**

DATA ENCRYPTION STANDARDS

- 1972 – NBS issues call for proposals
- 1974 – IBM responds with “lucifer” (DEA)
- 1976 – DES adopted
- 1986 – DES re-certification denied
- 1997 – NIST issues call for AES proposals
- 1999 – 5 submissions selected as finalists
- 2001 – Rijndahl algorithm selected

DES OVERVIEW

- Combination cipher
- 16 rounds of combined substitution and transposition
- Plaintext encrypted in 64-bit blocks
- Keys are 56 bits long (plus 8 error bits)
- Uses only arithmetic and logical operations on 64-bit numbers

AES STRUCTURE

- Apply round *n* times, where *n* depends on key size: 9 for 128, 11 for 192, 13 for 256
- Longer key sizes can be accommodated by increasing *n*.
- Each operation is very fast (add is actually an xor/shift) so algorithm is very efficient

DIGITAL SIGNATURES

How do you know that I sent that message?

- Knowing its me -- asymmetric key encryption
- Knowing its my message -- message digest (checksum)

Digital signatures can be legally equivalent to physical signatures

MESSAGE DIGESTS

Calculate function based on message content

- Irreversible (can’t go from value to message)
- Fixed size output (relatively small)
- Known method (to produce and check)
- Low collision (few texts with same value)

Common functions:

- MD2 – slow but strong
- MD4 – fast but weak
- MD5 – stronger than MD4, widely used
- SNEFRU – reportedly broken
- SHA – Similar to MD4/MD5

PICKING A CODE

- How important is the data?
- What cost for interception?
- What cost for modification?
- What cost for loss?
- Privacy of holding or privacy of sharing?
- How much delay is acceptable?
- US or Non-US?

PGP

- Freely distributed hybrid-key cryptosystem for non-commercial purposes
- 1991 version - violated RSA patent, exported without clearance
- Operation - uses Diffie/Hellman encryption for exchange of IDEA keys; digital signature MD5
- Commercial version - Network Associates (recently discontinued)
- Open-source workalike (Gnu Privacy Guard) http://www.gnupg.org/
- Available for wide variety of operating systems

WEB OF TRUST

- How do you know which is right public key?
  - Key signatures
  - Trusted introducer signature
  - Out of band verification
  - Expiring key
- Key servers

PUBLIC KEY INFRASTRUCTURE

- Organized means of handling public keys
- Key authorities
  - Trusted parties
  - Central source of distribution and cancellation
  - Division of trust
- What if authorities disagree?
- Which is most trusted?
- How do you handle lost keys?
- How do you protect against disclosure?