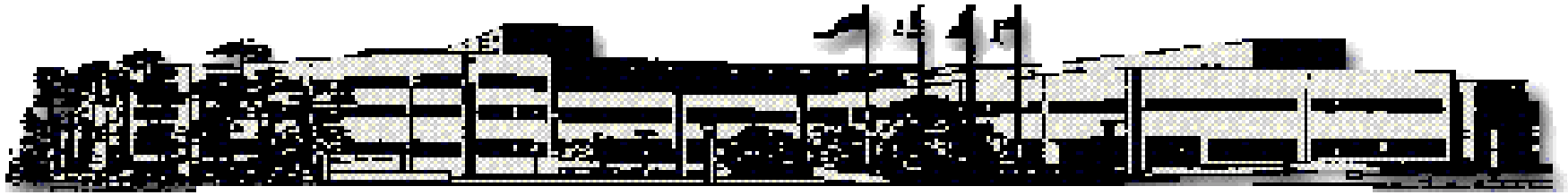
PUBLIC KEY INFRASTRUCTURE

FOR

AIR TRAFFIC MANAGEMENT SYSTEMS



Federal Aviation Administration (FAA) William J. Hughes Technical Center (WJHTC)

Vic Patel

vidyut.patel@tc.faa.gov

609-485-5046

Basic Cryptography Definitions

***CRYTOGRAPHY*: It allows two parties to exchange sensitive information in a secure manner via mathematical techniques**

***CONFIDENTIALITY*: Assures the information owner that his/her information is protected**

***AUTHENTICATION*: Assures the information owner that he/she knows with whom the he/she is doing business with**

***INTEGRITY*: Assures the information owner that the information is not being modified or substituted,**

***NON-REPUDIATION*: Assures the information owner that the originator cannot deny originating a message or business transaction**

BASIC CRYPTOGRAPHIC TECHNIQUE

Symmetric Cryptography:

- It relies on a symmetric encipherment algorithm
- It is also called secret key cryptography
- Single secret key to encipher and decipher
- Used for Encryption or Authentication

Asymmetric Cryptography:

- It is also called public key cryptography
- Keys comes in pairs – public and private
- Public key is available to anyone – like phone number in the phone book
- Private key is kept secret by the owner

HASH function:

- A mapping from an arbitrarily long input message to short (fixed-length) output
- Not feasible to guess an input message that results in a given output
- Used for Data Integrity

ADDITIONAL DESCRIPTIONS

***Certificate*: A digitally signed data structure defined in the X.509 standard that binds the identity of a certificate holder (or subject) to a public key.**

***Certificate Authority (CA):* A trusted entity that issues certificates to end entities and other CAs. CA issues CRLs periodically, and post certificate and CRLs to a repository**

Certificate Revocation List (CRL): A list of revoked but unexpired certificates by a CA.

Registration Authority: A set of technical and administrative functions (e.g., enrollment) performed by a component of a CA.

CRYPTOGRAPHIC TECHNIQUE AS APPLIED TO ATN

Encryption Scheme:

A cryptographic scheme for confidentiality
It has an encryption and decryption operation
May use ***Asymmetric Encipherment (under public key)***
Or alternatively may use ***Symmetric Encipherment***

Digital Signature Scheme:

It is used for data origin authentication and data integrity
It has a signing and verification operations
A receiver must be able to validate the sender's signature
The sender of a signed message must not be able to repudiate it latter
Asymmetric Encipherment (under private key)
Hash Function

CRYPTOGRAPHIC TECHNIQUE AS APPLIED TO ATN

(cont'd)

Key Agreement Scheme:

- Used for key establishment between two entities
- It creates a shared key for two entities
- ***Asymmetric Encipherment (under private key)***

Message Authentication Code (MAC) Scheme:

- A key-dependent one-way ***hash function*** is called a MAC
- MAC is useful to protect authenticity without providing secrecy
- Use of hash also provides integrity
- Only someone with the identical key can verify the hash

SECURITY SERVICE AND MECHANISM

SECURITY SERVICES

CONFIDENTIALITY	AUTHENTICATION, INTEGRITY, NON-REPUDIATION	KEY ESTABLISHMENT	AUTHENTICATION, INTEGRITY

SECURITY MECHANISMS

Cryptographic Schemes

- Encryption Scheme
- Digital Signature Scheme
- Key Agreement Scheme
- Message Authentication Code Scheme

Cryptographic Building Blocks

- Asymmetric Encipherment (under public key)
- Asymmetric Encipherment (under private key)
- Asymmetric Encipherment (under private key)
- (Keyed) Hash Function

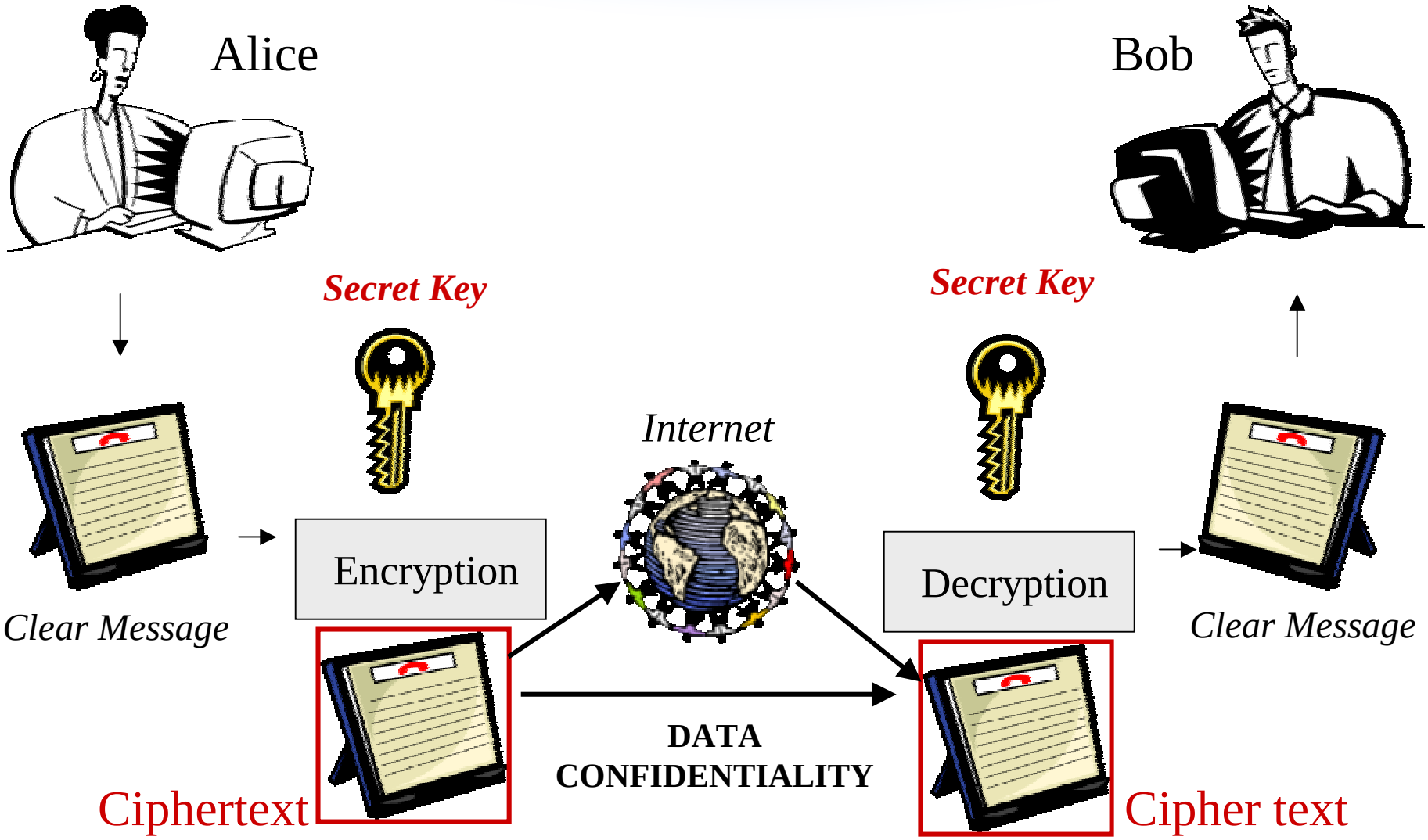
OR

- Symmetric Encipherment

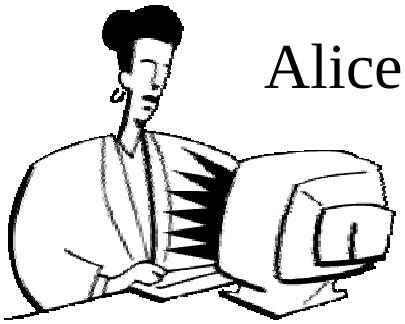
AND

- Hash Function

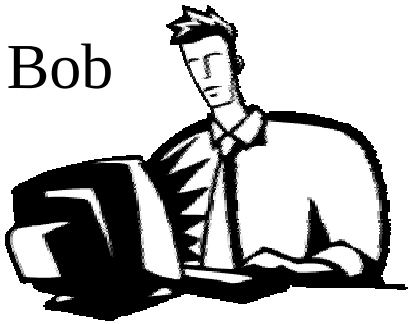
Symmetric Cryptography



Symmetric Cryptography

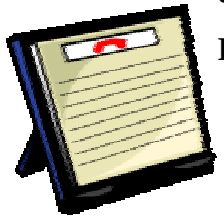


Alice



Bob

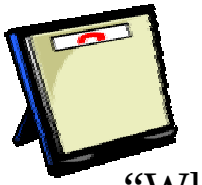
"This is a secret message"



Confidential Message

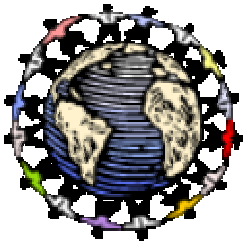
Encryption

Encrypted Message

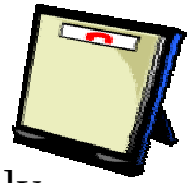


"Wklv lv d vhfuw phvvdjh"

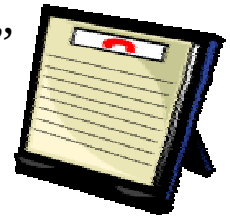
Internet



Encrypted Message



"Wklv lv d vhfuw phvvdjh"



"This is a secret message"

Confidential Message

Decryption

A = D	E = H	I = L	M = P	Q = T	U = X	E = H
B = E	F = I	J = M	N = Q	R = U	V = Y	F = I
C = F	G = J	K = N	O = R	S = V	W = Z	G = J
D = G	H = K	L = O	P = S	T = W	X = A	H = K

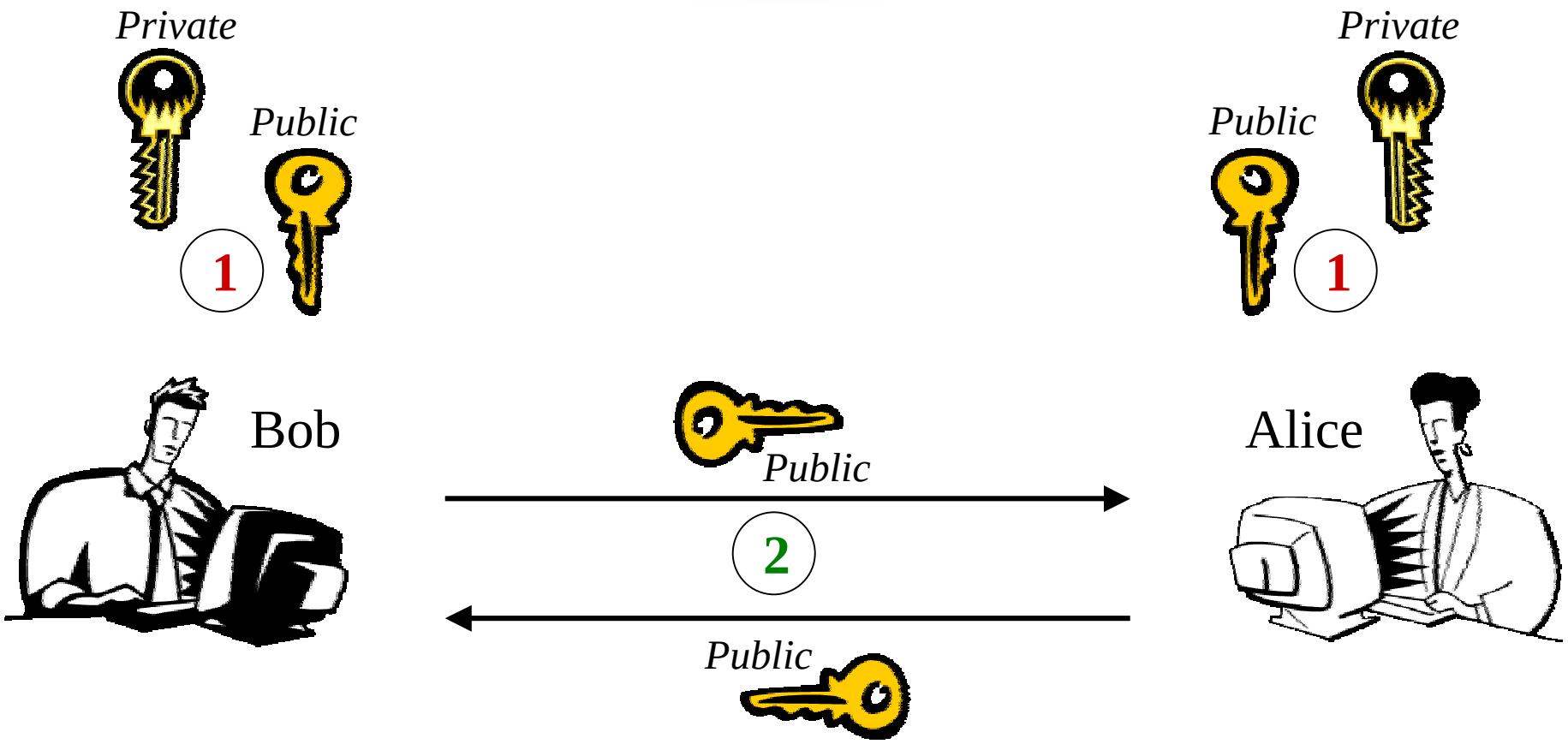
SYMMETRIC CRYPTOGRAPHY

- Shared Symmetric key or PRIVATE KEY used
- Provides data confidentiality (or authentication)
- Fast, easy to implement in hardware, widely used
- Works well for a small group of authorized parties, where keys may be pre-distributed and challenge for a large scale environment secure distribution
- E.g., DES, AES, 3DES, IDEA

SYMMETRIC CYPTOGRAPHY

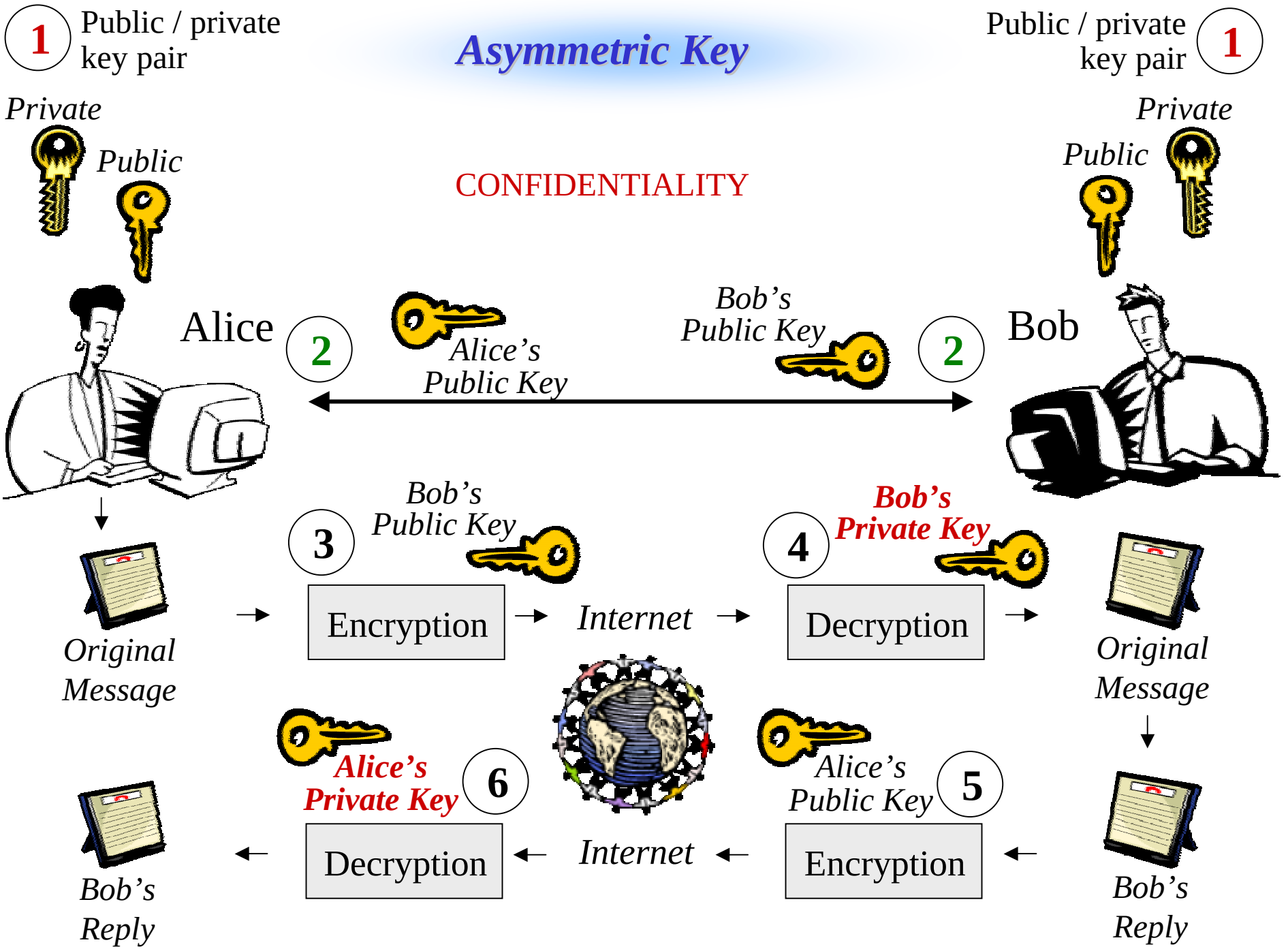
- Pro:
  - Fast, easy to implement in hardware, Widely used
- Cons:
  - Key management very difficult
  - Key must be exchanged via a trusted channel
  - Fixed length
  - Can be stolen
  - Difficult to administer

Asymmetric Cryptography

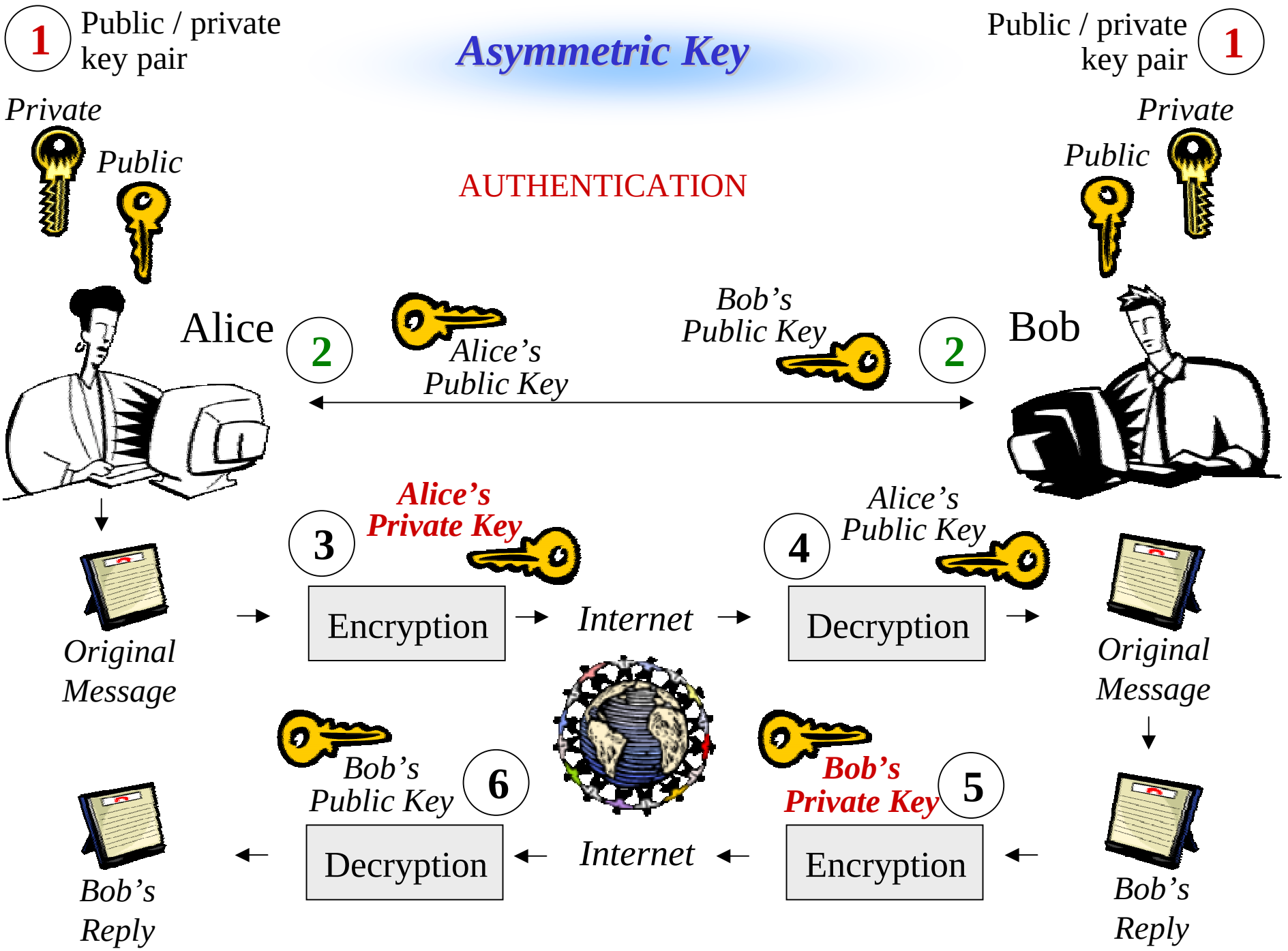


1 Create public / private key pairs

2 Exchange only public keys


1
Public / private key pair
Asymmetric Key
Public / private key pair
1
Private
Public
CONFIDENTIALITY
Private
Public
Alice
2
Alice's Public Key
Bob's Public Key
2
Bob
Bob's Public Key
3
Bob's Private Key
4
Original Message
Encryption
Internet
Decryption
Original Message
Alice's Private Key
6
Alice's Public Key
5
Bob's Reply
Decryption
Internet
Encryption
Bob's Reply

Asymmetric Key



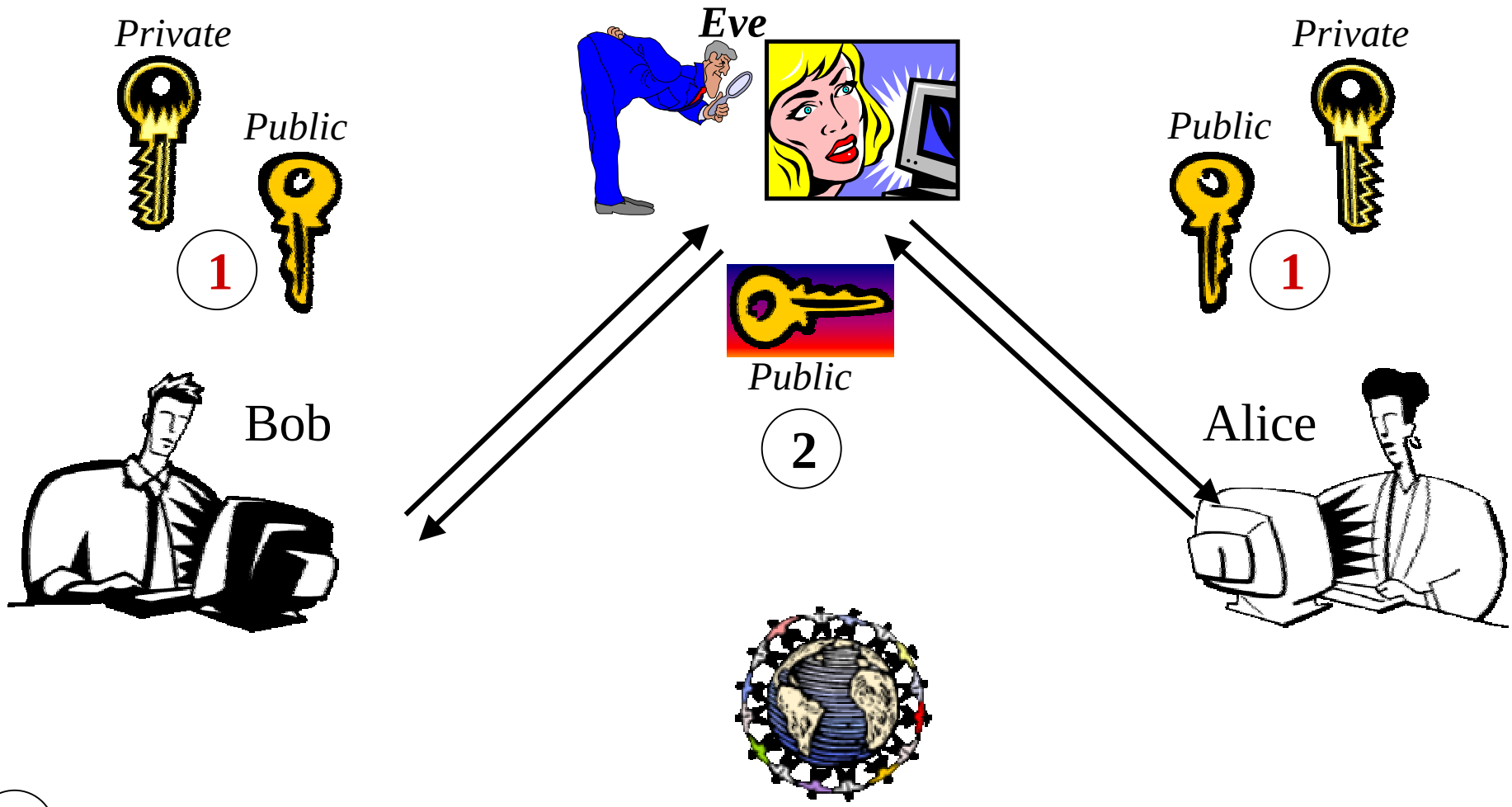
ASYMMETRIC CRYPTOGRAPHY

- Use of two distinct but related keys
- Provides data confidentiality and authentication
- Works well for a small group of authorized parties, where keys may be pre-distributed and challenge for a large scale environment secure distribution
- For example RSA

ASYMMETRIC CRYPTOGRAPHY

- Pros:
  - Scales easily and easy key management is possible
  - Provides authentication of sender
  - Variable key sizes
  - Can be used for both encryption and digital signature
- Cons:
  - Relatively slow
  - Inefficient for encrypting lots of data
  - Authentication of public keys

Asymmetric Cryptography

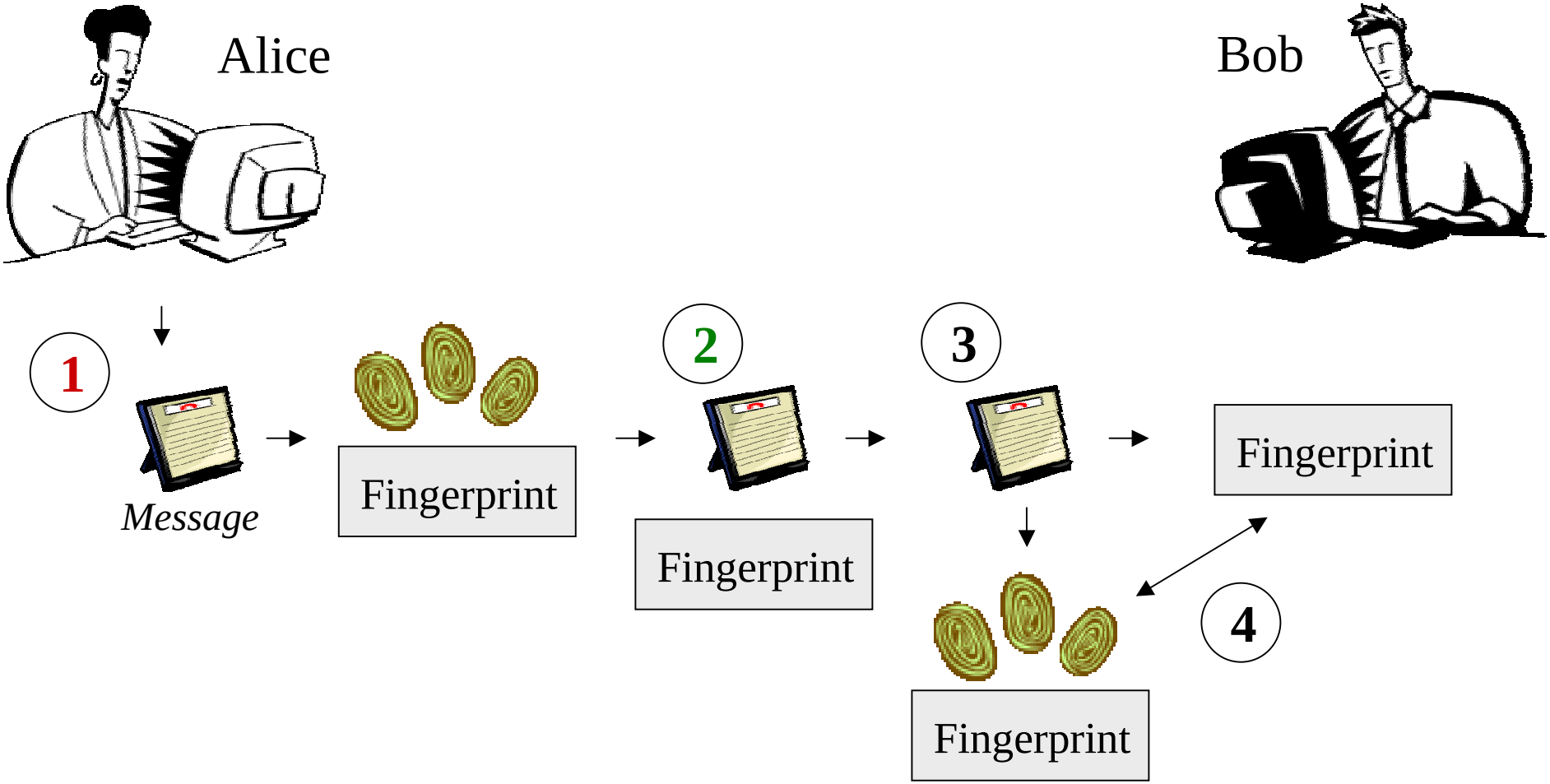


1 Create public / private key pairs

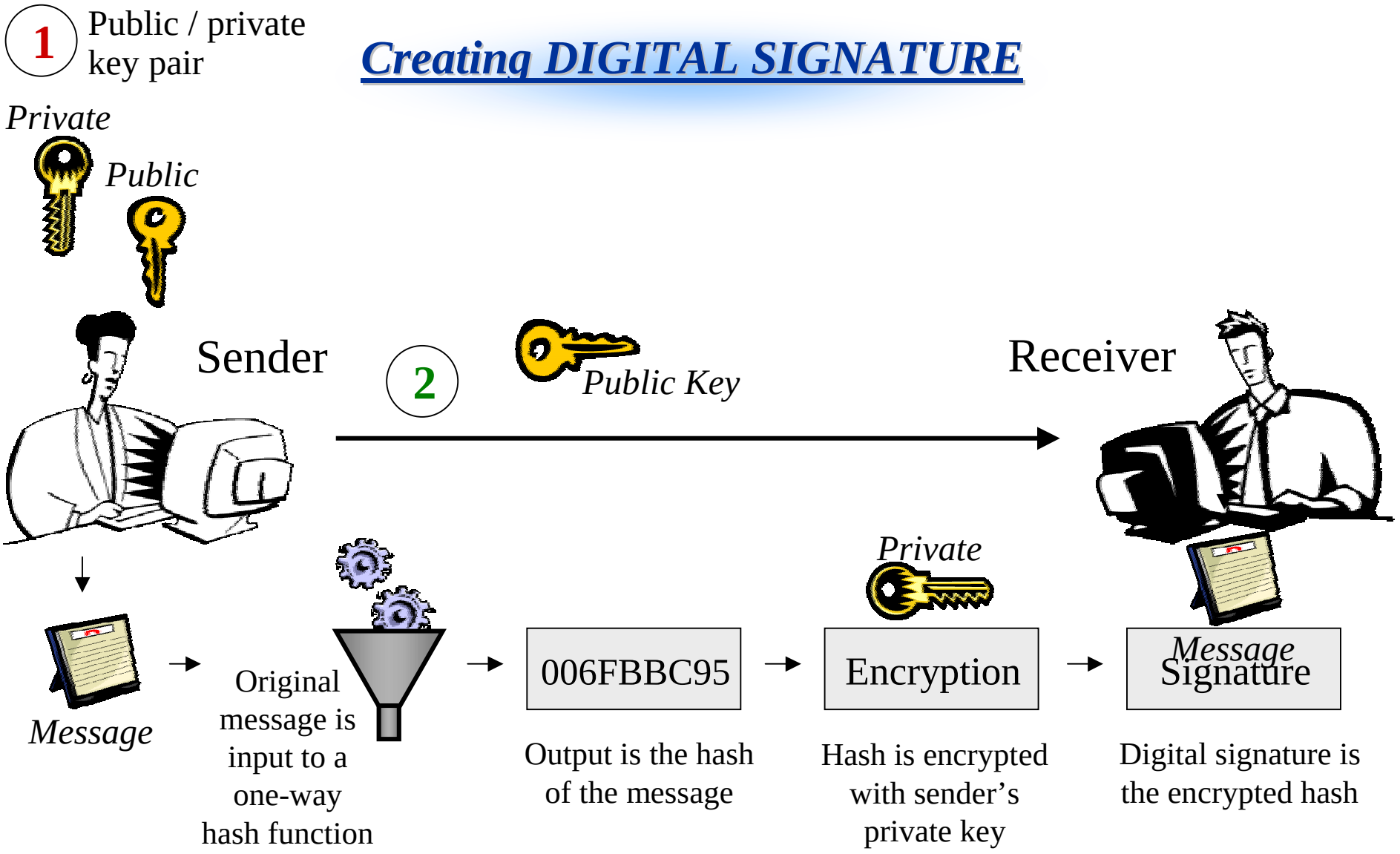
2 Exchange only public keys Eve intercepted and substituted Bob's Public Key

One-Way HASH Function

DATA INTEGRITY



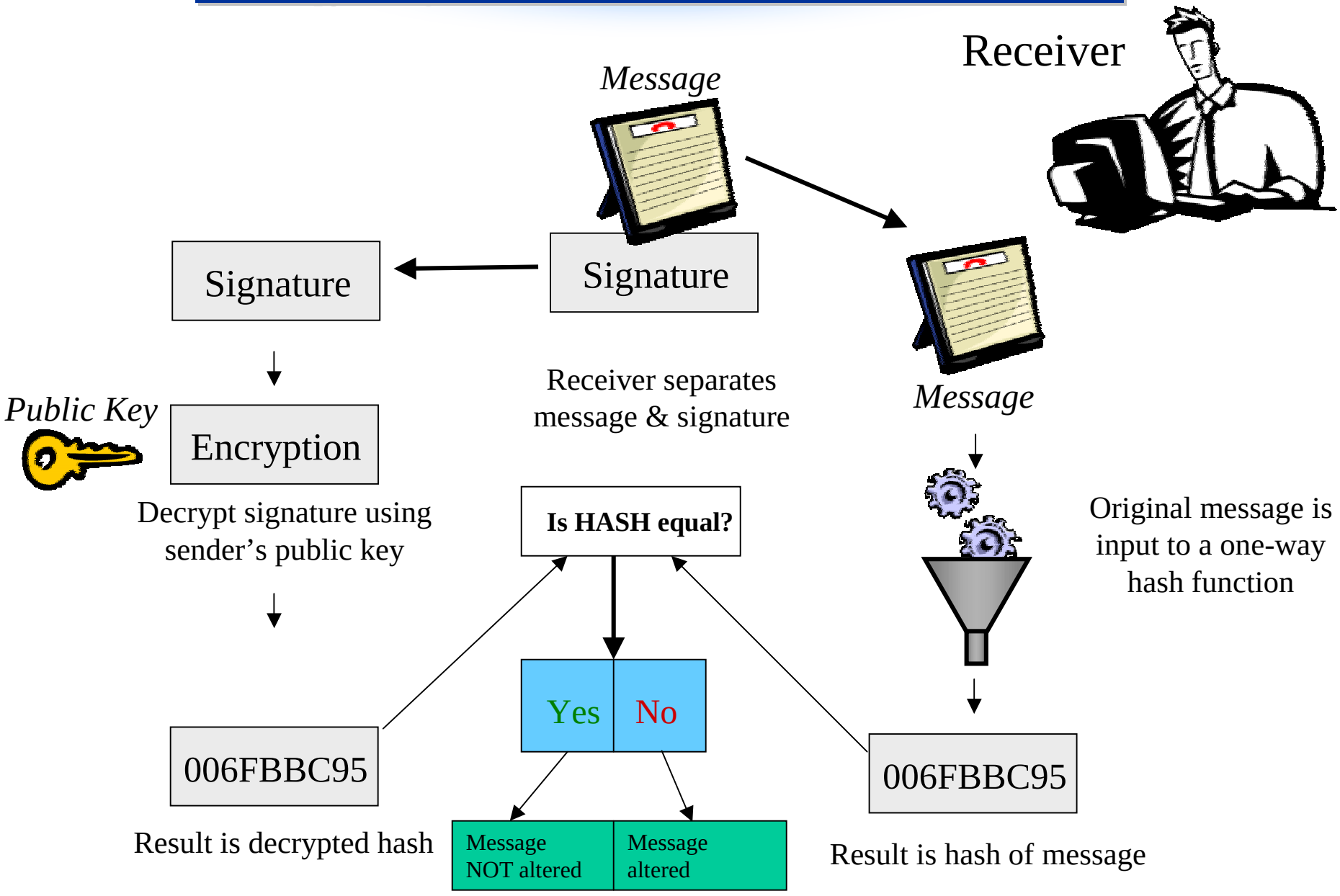
Creating DIGITAL SIGNATURE



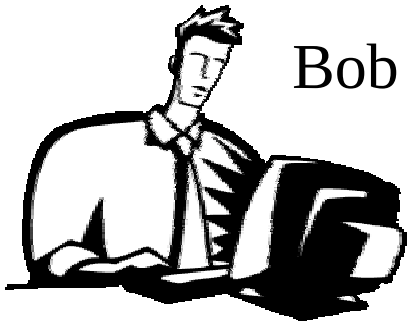
1 Create public / private key pair

2 Sender sends its public key to receiver

Verifying DIGITAL SIGNATURE



Digital Certificate Through a Certificate Authority



Bob

1 Request Alice's Certificate

Certificate Authority

Alice's Certificate

Bob's Certificate

2 Alice's Certificate

CA Signature

3 *Verify Signature*

CA Fingerprint

Decryption

CA Public Key

CA Fingerprint

CA Fingerprint

4 Alice's Certificate

Alice's Public Key