

## Lecture 11

# Information Systems Security

By Dr. Mahmoud Youssef

Based on notes by  
Professor Vijay Atluri

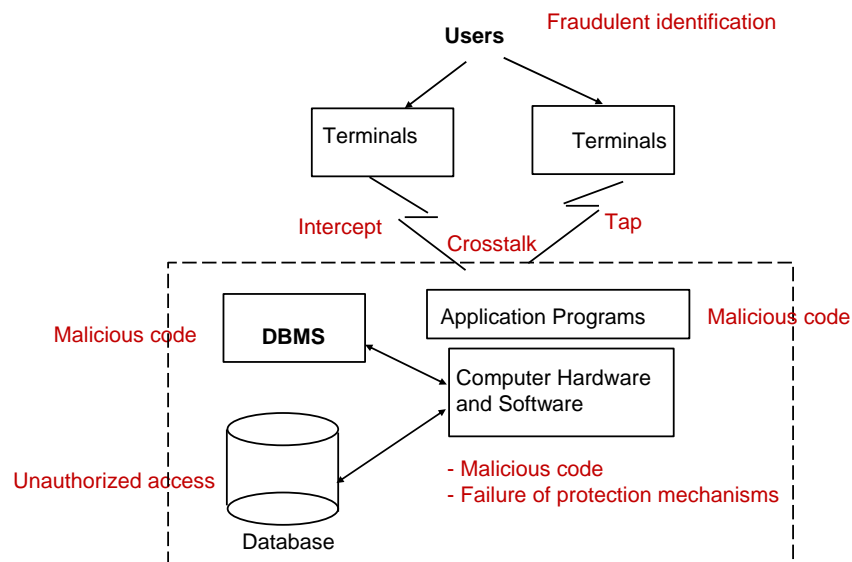
## What is there to worry about?

- **Before 1960s:** Entire system was dedicated to a single user
  - protection simply means users picking up their tapes and cards, clearing up the memory after the job is finished
- **During 1960s:** growing demand for better efficiency
  - led to multiplexing, multiprogramming, resource-sharing operating systems, time-sharing
  - security means isolation of independent and simultaneously executing processes (programs) from each other
    - primarily to prevent accidents and errors
- **During 1970s:** users demands for computing power closer to their work areas (End User Computing)
  - led to networking enabling neighbor computers and applications to communicate
  - realized the need for communication security

## What is there to worry about? (continued)

- **Beyond 1980:** Increased demand for connectivity (LANs and WANs) compounded the security problems
  - due to more sophisticated users who need to exchange data, send/receive messages via e-mail, access common databases, share programs and applications to speed up and reduce application development efforts, share expensive storage and output devices ...
  - computers have become more sophisticated and more powerful
    - What is the implications?

## Information Systems Security



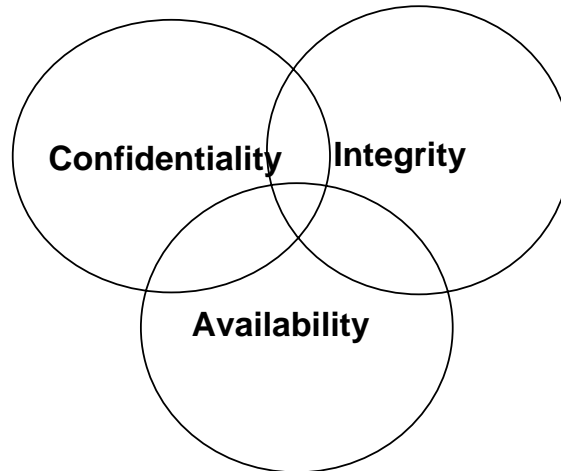
## **Major Threats to Security**

- Computer Misuse
- Human Error
- User abuse of authority
- Direct probing
- Probing with malicious software
  - Viruses, logic bombs
  - Trojan Horses
  - Covert Channels
- Subversion of security mechanism

## **The 3 Steps to Security**

- Policy
  - defines the requirements need to be implemented
  - lays out broad goals without specifying how to achieve them
- Mechanism
  - implements the requirements of the policy
  - one has to make sure that the mechanism performs intended functions (by verification, testing, and certification)
- Assurance
  - provides a measure of how well the mechanism meets the requirements of the policy

## Components of Security



**Confidentiality:** Prevention of Unauthorized disclosure of information

**Integrity:** Prevention of Unauthorized modification of information

**Availability:** Prevention of Improper denial of access to information

## Protection Requirements

- Database protection requirements
  - protection from unauthorized access
  - protection from inference
  - protection from failures
  - protect operational integrity of data
  - protect semantic integrity of data
  - Accountability
  - Multilevel protection
- Network Security Requirements
  - authentication
  - protecting the confidentiality of data during communication
  - protecting the integrity of data during communication
  - non-repudiation

## **Access Control in Commercial Systems**

- Identification and Authentication
- Grant and Revoke
- Security through Views
- Query Modification

## **Identification and Authentication**

- This is distinct from that provided by OS
- Example: CONNECT <user> IDENTIFIED BY <password>
- Not sufficient to read data from or write to the database

## Grant and Revoke

- GRANT <privilege> ON <relation>
- Privileges on tables:
  - SELECT
  - INSERT
  - UPDATE
  - DELETE
  - ALTER
  - INDEX

## Security through Views

### Example

```
CREATE VIEW AVSAL(Average_salary)
AS SELECT AVG(Salary)
FROM EMPLOYEE
```

- Privileges can then be granted or revoked on views as in case of base relations

## Query Modification

GRANT SELECT ON SALARY TO Smith WHERE Salary < 15000

Smith's Query: SELECT \*  
FROM EMPLOYEE

DBMS: SELECT \*  
FROM EMPLOYEE  
WHERE Salary < 15000

## Trojan Horse Attack

Order Processing  
Application

~~~~~  
~~~~~  
~~~~~

Read Future Products  
Write Personal Items

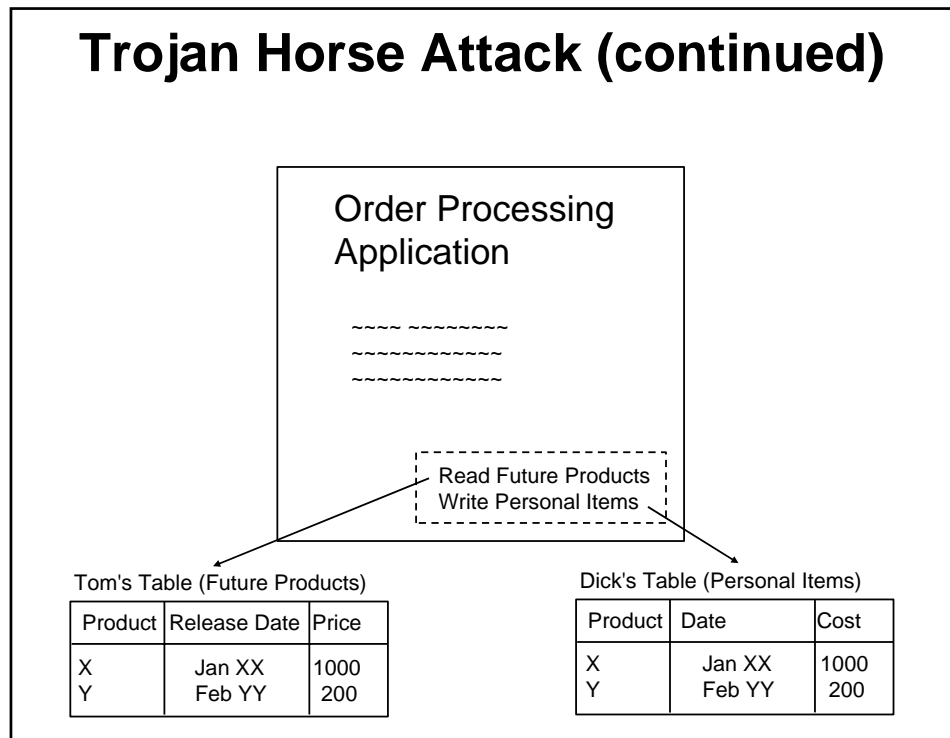
Tom's Table (Future Products)

| Product | Release Date | Price |
|---------|--------------|-------|
| X       | Jan XX       | 1000  |
| Y       | Feb YY       | 200   |

Dick's Table (Personal Items)

| Product | Date | Cost |
|---------|------|------|
|         |      |      |

## Trojan Horse Attack (continued)



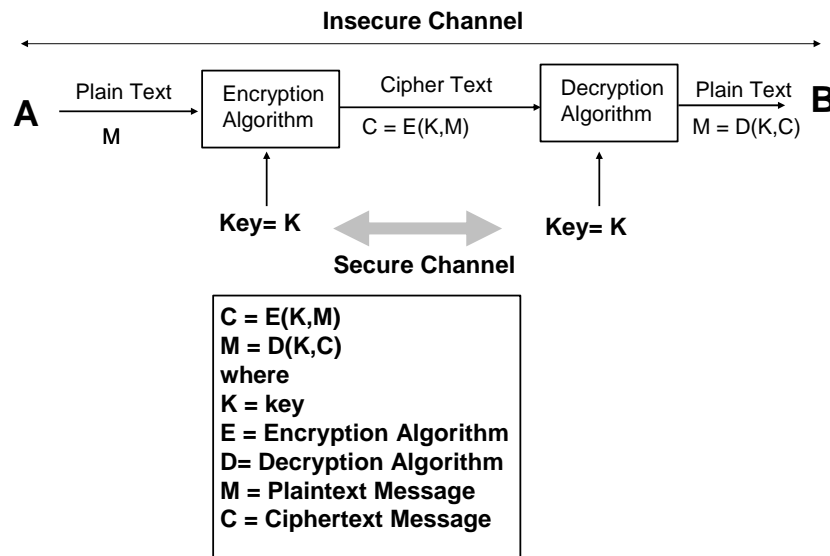
## Network Security

- Ahmed wants to send a private message to Basma over a public network
  - What if someone intercepts and reads this message? **(Confidentiality)**
  - What if someone intercepts and alters this message? **(Integrity)**
  - What if someone pretending to be Ahmed forges a message and sends it to Basma? **( Authentication)**
  - What if Ahmed denies sending of the message? **(Non-repudiation of origin, Digital Signature) page 52 of the text gives a distinction between the two**
  - What if Basma denies the receipt of the message? **(Non-repudiation of the destination)**

# Cryptography

- A tool for confidentiality, integrity, authentication, non-repudiation, and digital signatures
- Cryptology
  - cryptography: the science of encryption (the good guys)
  - cryptanalysis: analysis of cryptographic algorithms (the bad guys)
- Cryptosystems
  - Secret Key (also known as single key, symmetric key)
    - existing for more than 1000 years
  - Public Key (also known as two key, asymmetric key)
    - since 1974
    - both secret key and public key systems are in use and competing with each other

## Secret Key Cryptosystem



## Features of Secret Key Encryption

- Uses:
  - Solves confidentiality and integrity problems
  - Can be used for Authentication
  - Can be used to securely store information on insecure media
- Disadvantages:
  - Key Distribution Problem: How to get the key to Ahmed and Basma? and to others?
  - If everyone knows the Key, it is no longer a secret

## Cryptanalysis

- Objective of the cryptanalyst is to discover K (the real objective is to discover M)
- Cryptanalyst is assumed to know E and D
- Cryptanalyst must know when he/she discovers M
- Four Scenarios
  - Ciphertext only: Cryptanalyst knows only ciphertext
  - Known Plaintext:: Cryptanalyst knows some plaintext-ciphertext pairs
  - Chosen Plaintext:: Cryptanalyst knows some plaintext-ciphertext pairs for plaintext of the cryptanalyst's choice
  - Chosen Ciphertext:: Cryptanalyst knows some plaintext-ciphertext pairs for ciphertext of the cryptanalyst's choice

## Basic Encryption Techniques

- Substitution

- Simple Alphabetic Substitution

- Huge key space:  $26!$  (approximately  $10^{26}$ )
    - Trivially broken for known plaintext attack
    - Easily broken for ciphertext only attack (for natural language plaintext)
    - Multiple encipherment does not help

|                  |
|------------------|
| ABCDEFGHIJKL.... |
| FPAQFZYTLLWXM..  |

- Permutation

- Example: Caesar ciphers
  - Key space:  $N!$  for a block size of  $N$
  - Trivially broken for known plaintext attack
  - Easily broken for ciphertext only attack (for natural language plaintext)
  - Multiple encipherment does not help

|   |   |   |   |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 3 | 1 | 4 | 2 |

- Combinations and iterations of substitution and permutation

## Product Cipher

- Substitution followed by permutation followed by substitution followed by permutation ....
- Best known examples:
  - DES (Data Encryption Standard)
  - SKIPJACK
- Mathematics to design a strong product cipher is classified
- Breakable by exhaustive search of key space for known plaintext, chosen plaintext, chosen ciphertext
- Thus, security is based on computational complexity of computing the key

## Data Encryption Standard (DES)

- DES is a product cipher with 56 bit key and 64 bit block size for plaintext and ciphertext
- Developed by IBM and adopted by NIST (1977) with NSA approval for unclassified information
- efficient to implement in hardware, but relatively slow if implemented in software
- E and D are public, but the design principles are classified
- Algorithm:
  - initial permutation
  - the 56 bit key is used to generate sixteen 48-bit keys
  - 16 rounds of substitution and permutation are performed
  - swap left and right halves
  - Final permutation
- the size of the key (56-bits) is one of the most controversial aspects of DES

## How Secure is DES?

- has stood up remarkably well against 20 years of public cryptanalysis
  - 1977: approved as a Federal standard with 5 year cycle of re-certification
  - 1987: reluctantly reapproved for 5 years
  - 1992: reaffirmed by NIST
- DES known plaintext attack
  - 56-bit key can be broken in  $2^{55} = 3.6 \cdot 10^6$  trials

|               | 56 bits       | 76 bits<br>( $3.8 \cdot 10^{22}$ trials) | 46 bits<br>( $3.5 \cdot 10^{13}$ trials) |
|---------------|---------------|------------------------------------------|------------------------------------------|
| trials/second | Time required | Time required                            | Time required                            |
| 1             | $10^9$ years  | $10^{15}$ years                          | $10^6$ years                             |
| $10^3$        | $10^6$ years  | $10^{12}$ years                          | $10^3$ years                             |
| $10^6$        | $10^3$ years  | $10^9$ years                             | 1 year                                   |
| $10^9$        | 1 year        | $10^6$ years                             | 10 hours                                 |
| $10^{12}$     | 10 hours      | $10^3$ years                             | 40 seconds                               |

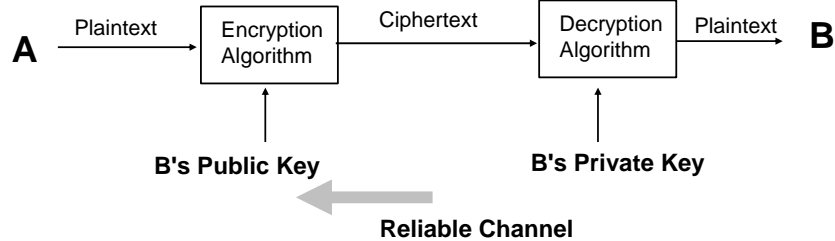
## **Advanced Encryption Standard (AES)**

- Responding to a challenge from RSA Data Security Inc., DES was recently broken in 22 + .. Hours
- Jan, 1997, NIST initiated the development of AES
  - features
    - unclassified, royalty-free algorithms
    - support 128-bit block sizes and 128-, 192-, and 256- bit key sizes
- Apr 1999, selected five candidate algorithms
- May 2000, AES was proposed
- Summer 2001, the standard was completed

## **Remarks on Secret Key System**

- Distribution of the Key is a Problem
- Trillions of keys may be required because we need at least  $n(n-1)$  different keys if we have  $n$  customers
- Public Key Cryptosystem
  - solves the problem of key distribution provided a reliable channel for communication of public keys can be implemented

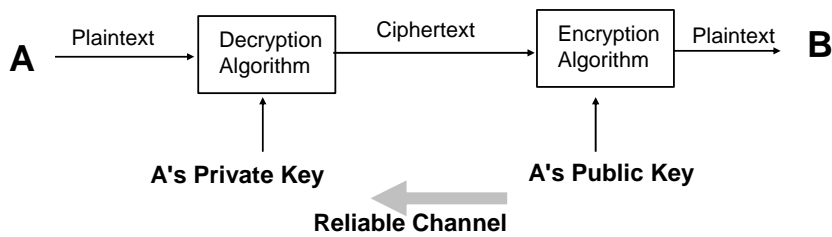
# Public Key Cryptosystem



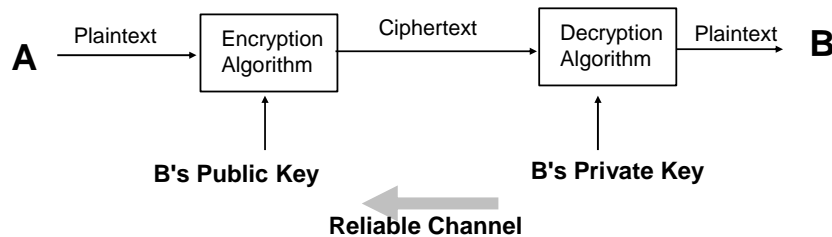
- security is based on infeasibility of computing B's private key, given the knowledge of
  - B's public key
  - chosen plaintext
  - chosen ciphertext

$C = E(KE-B, M)$   
 $M = D(KD-B, C)$   
 where  
 KE-B = Public (encryption) key of B, known to all  
 KD-B = Private (decryption) key of B, known only to B  
 E = Encryption Algorithm  
 D = Decryption Algorithm  
 M = Plaintext Message  
 C = Ciphertext Message

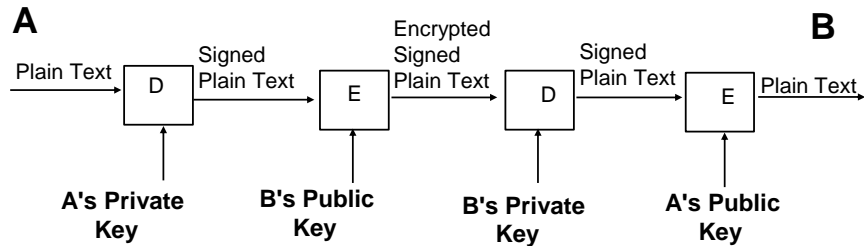
# Digital Signatures in RSA



-----  
 Compare with Encryption in RSA



## Signatures and Encryption



- we could do the encryption first followed by the signature. Signature first has the advantage that the signature can be verified by parties other than B
- We could use DES for encryption

## Firewalls

- Separate a private network from an open network
- address based
  - filters the packets originating from or delivered to an address
- application based
  - e.g., may allow email, but may not allow ftp, telnet