/ / التاريخ _____ اليوم _____ موضوع الدرس _____

Lec 1 : Computer security.

→ NIST : National institute of standards and Technology.

→ IR : Interagency Report.

→ NISTIR defines Com. Security as :

measures & controls that ensure ① confidentiality ② integrity ③ and availability, of information System, assets including hardware, Software firmware, and information being processed stored, and communicated.

→ in addition : ④ Authenticity ⑤ Accountability

→ assets include human Resources.

→ CIA triad ⇒ [confidentiality, integrity availability].

/ / التاريخ _____ اليوم _____

موضوع الدرس _____

* Confidentiality :-

preserving authorized restrictions on info
① access ② and disclosure

* Example for protected info :
① personal info ② proprietary info

* Integrity : ① حماية المعلومات من إنها تتغير أو تلتغى أو تدمر

② تأمين الـ authenticity : التأكد من ان المعلومات صدرت من الشخص المعني وأن المعلومات صحيحة ولم تتغير في الطريق .

— nonrepudiation : security concept that forbids a sender From denying that he had sent this information

non repu → sender : ما يقدر ينكر انه هو أرسل المعلومة

→ receiver : ما يقدر ينكر انه استلم المعلومة

موضوع الدرس _____ اليوم _____ التاريخ / /

*Availability: ensure that all assets and resources are available to the legal users when they want it.

→ I need to guarantee that these users can access any piece of service, any piece of information, any piece of the assets of the system. timely when they want it. and reliable access

→ Always there are certain weak points based system [Vulnerabilities] used to launch an attack.

→ increase effect of that attack on behavio of the System may move from Low to modera

→ Note: attack on Sys A is categorized as moderate.

Same attack on Sys B can be categ as low. For High

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

Levels of impact :

→ low : low effect of attack,
* some functionalities may fail, but main functionalities are fine

→ moderate : loss serious adverse effect
* it denies some of the good Functions of the sys, but sys still up and running with very Limited functionalities.

→ High : sys became not usable anymore or he deleted the information.

→ security challenges

① not simple as it might first appear to the novice

* have 100% secure system is almost impossible

② to design certain mechanism so that it will counter attack, All potential attack

③ human logic may conflict with embedded log in mechanism

- counter intuitive : not working mechanis

- may using non logical algorithms, but then you decide that they are the only way of protecting these assets.

- When you design a security for a sys one of moments that you have to consider is where to place these algorithms.

② to design certain mechanism so that it will counter attack, All potential attacks

③ human logic may conflict with embedded logic in mechanism

- counter intuitive : not working mechanism

- may using non logical algorithms, but then you decide that they are the only way of protecting these assets.

- When you design a security for a sys one of moments that you have to consider is where to place these algorithms.

5- in most of the cases, any protection mechanism will involve exterminate algorithm to protect that assets.

plus you have hundreds of users, so at certain point you need piece of secret information for them, certain PIN codes must be as well protected.

- you have to take measures & policies to protect this secret information

→ you have to design policies how to change this secret information, and policies in destroying this secret information,

* practical applications :-

① pass must be strong

② advices how to protect your pass

③ chang pass every 2-3 months

④ any one wants to leave they delete his file from System

6- designer must protect all weak points bcz, attacker only need single weakness to attack system.

7- any security prosedure [mechanism] may create certain security vulnerability.

"after system is ready we decide to put mech's to potect System.

8- Security requries ① regular ② Constant monitoring

9- after security failure occurs, managers decided to buy firewalls to potect their company sites, and systems

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

- Rfc : Request For Comments.
  ↓
- work to collect feedback from different organizations and users.

→ Rfc 2828 : main terminology used in security.

* adversary [thread agent]
جهات وفيات لها معلقة بإلحاق الضرر بـ
السيستم الخاص فيي.

* Attack : activity hurts my System

* Counter measure : any technique or device that I put to protect my system against all types of attacks

→ espionage : التجسس

*Risk : seems Like impact.
include what is probability of that attack to happen.

Risk → level of the impact.
→ probability of the attack.

*security policy : administrative rules and measures that will enhance the protection of the system.

*System Resource ((Asset)) : Every thing related to system including people [human]
[Hardware, Software, firmware, network] Facilities

*threat : Situation or the circumstance that will allow an adversary to launch an attack

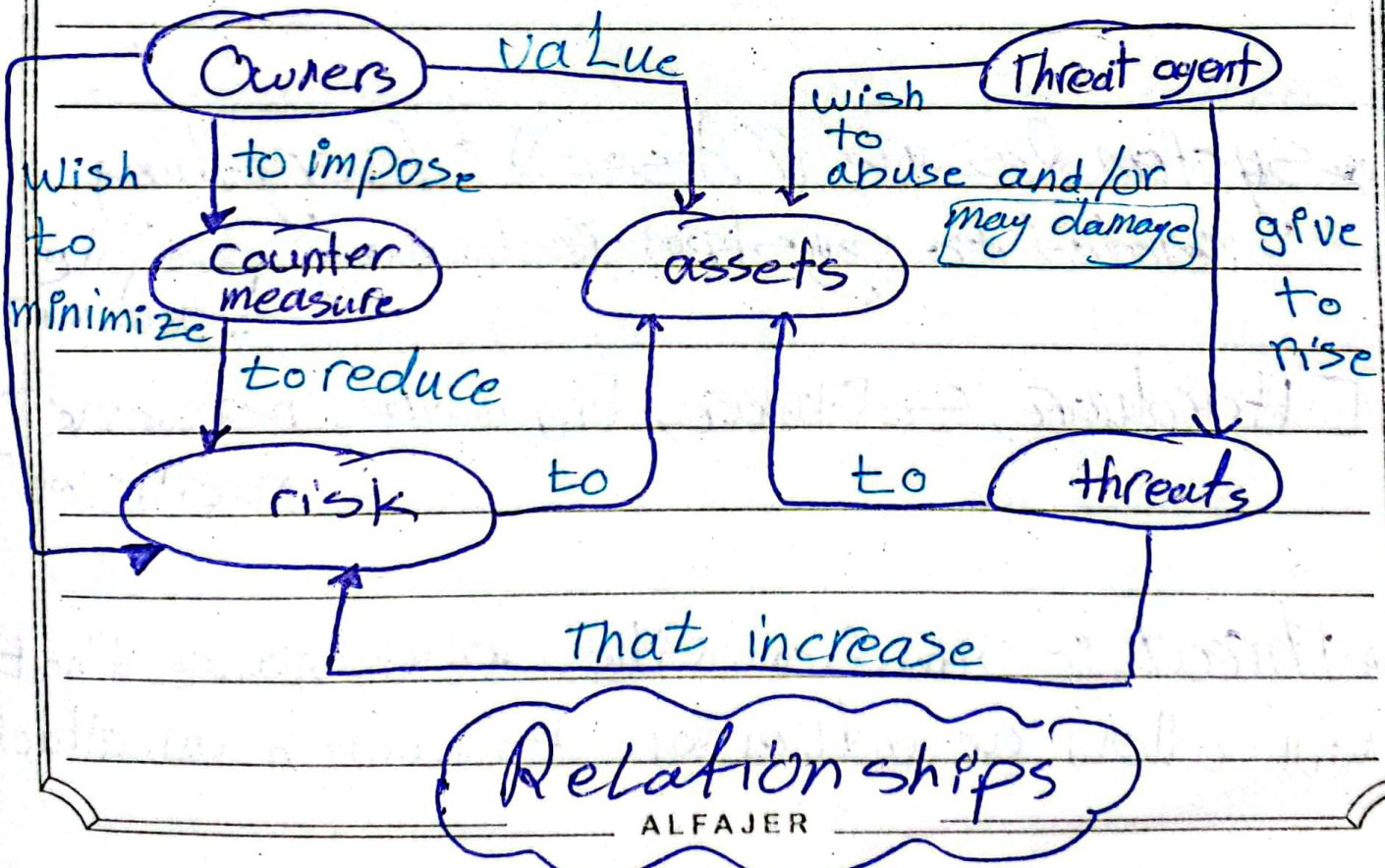
/ / التاريخ _____ اليوم _____ موضوع الدرس _____

*Vulnerability : weak point in the system.

Note :

① Countermeasure usually include technical part of the protection.

② Policies usually include adminstrative part of the protection.



/ / التاريخ اليوم موضوع الدرس

Lec 2

categories of vulnerabilities.

① Loss of integrity

② Loss of confidentiality [status or condition where some confidential information is leaked]

③ Loss of availability: if there is weak point make sys unavailable at all or can degrade performance of the system that will be affecting availability.

⇒ Threats

- have circumstance, a certain condition where I either can exploit certain vulnerabilities manually
- or I can do certain harm to the assets

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

* Attacks

- passive : will get information Without harming the system. [very difficult to detect]

- active : attack will affect the resources [easier to detect]

- Insider : means the system is attacked from within the perimeter of the system
  - usually comes from legal user.

- outsider : attack comes from out of the perimeter of the system.

Note : may the attack is [passive or active] also it can be outsider or insider at the same time

- How to deal with security attack?
  * prevent
  * if we fail to prevent that attak, then we have to put measure to detect it
  * if I could not prevent & could not detect then I should take measure to recover from that attack

- recover: What actions I have to take in Order to either minimize the effect or remove the effect of the attack.

- While you are doing certain measures to remove certain vulnerability, you may be required to add some hardware or add some software by itself can create a weak point or can create additional vulnerability.

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

- Threats Actions

Consequence : Unauthoriz Disclosure

* EXposure : illegal user take informations

* Interception : Taking information from data Lines of the network

* InFerence : you can get confidential information out of Non-confidential information.

* Intrusion : illegal user attack system physically

- Conseq uence : Deception : خداع

illegal user receiving data but this's data is not correct.

* masquerade : get username & pass of user and you are using that legal user account to do certain attacks or to get certain information

* falsification: provide the authorized entity with incorrect data [false data]

* Repudiation: action to deceive your manager. When you do illegal action And want to deny that action

- Consequence: Disruption

* أغلب لها علاقة بتعطيل الـ sys وتؤثر مباشرة على الـ availability

* Incapacitation: interrupt the behavior of the system or prevent system from doing All or part of its functionalities.

* corruption: change the sys, so from outside it looks like the system is working, but the functionality of sys is not correct.

* abstruction : any act that changes functionality of the system So that it's not delivering the properly it's required services

[تعطيل الـ component أو إضافة عليه]

- consequence : Usurpation.

← السيطرة على السيستم كاملاً .

* Missappropriation : if you deceive certain measure to login as authorized and have a full control of the System mainly, here we talk about hardware hijacking [physically hack]

* Misuse : Can I go & affect or change the performance of a certain Component of the System or cannot ?

Figure 1.3 : scope of computer Security

* Access data : Counter measure should Control who can access, this data inside network & outsider

* Access to the Computer : take measures to control the access to my computer facility, physically externally.

* Data must be Security transmitted : must do something to protect data in data transmitters, if someone try to reach that data, then he must fail.

* sensitive data must be secure : if I have files include passwords, then I have to protect these files [must be highly protected].

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

• All our Security mainly is concerned with access control.

• passive & active attacks.

* passive :- تحصل على المعلومة ولكن ما تغيرها

- Eavesdropping on transmission Lines:
means put clampon Line & read bits so that he can monitor transmission. then he can guess what type of encryption is on the Line

- can affect actually all parameters, but mainly it affect the confidentiality.

* Active attack : very easily detected

- Categories:

① Replay: actually does not change the resource, but it utilizes a certain technique to get again in.

② masquerade : get my pass, and attacker log in with my informations.

- replay & masque : access without change anything

③ modification : change certain data in order to gain access to certain resources

④ Denial : He will make System so busy So that Legal users are either cannot enter to the System, or they will enter, but the Sys becomes with very slow response
[actually does not make change to resources]

- FIPS 200
Federal Information Processing Standards
certain rules & commence & information to improve certain aspect of any thing.

موضوع الدرس _____ اليوم _____ التاريخ / /

- FIPS : standards & guidlines in information systems that Developed by the NIST

- NIST : makes dev for systems either computer sys, or information sys.

- FISMA : organization put certain rules by this rules NIST do it's developments & FIPS put standards & guidLines for the security of the system that are developed by the NIST in accordance to FISMA regulations.

- certification, accreditation : guidline to organization that have compute systems tell them what to do in order to improve security requirements.

- Contingency planning : there should be certain plan How to protect & deal with any attack.

- Incident response : what should I do in the org sys to deal with this attack

- whatever happens, you have to record it
  Why?
  bcz When the Audit comes, I want to check how you dealt with these emergencies & how you minimize risk of these attacks

- Maintenance : maintenance of security measures [to be able to improve & develop your countermeasures]

- Identification, authentication :
  [username] [pass]

- media protection : standards how to deal with your media & your drives

if your data must be removed, you must not keep data available

- physical & you must put certain measures, how physically to access your sys
  [should be highly protected physically]

- disaster recovery : if harm happened, how to restore the functionality as soon as possible

Note : backup happens for whole computer center

- personnel security : provide counter measures to prevent the personnel harm process.

- risk assessment : ① What are the attacks would happen?
  ② what is the consequence of these attacks

org: organization

*risk assess must updated continuously

- Sys & serv acquisition : you must be assured that the people there & org is trustworthly. [third part involving in the development & securing your System.]

- {Sys & comm} protection : the countermeasures of data that is transmitted on the Lines, should be in place

- Sys integrity : make sure that there are no violation on the integrity, either on System or on data placed in ~~transmission~~ Lines in your System.

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

* Fundamental Security design :

- ~~Economy of mechanism : how the sys is built & operated~~

- majority of the content of these principles deals with the administrative measure

- mechanism that you use, should be as simple as possible

simple : mean the less that can go wrong

- Eco of mech : we must do these measures in the simplest form possible.

"minimize vulnerable points in that measure"

" // effort "

- fail-safe defaults : minimize possibility of the failure

"Everything is forbidden, Except ...."

Those users with their permissions

- Complete mediation : I will not permit any subject to access any object except after authorization check.

- separation of privilege : ① I have to segment user privileges in groups of users & their accounts

And it includes the compartmentalization of privilegs across various applications

- Functionality of application needs different levels of privileges.

- Least privilege : give each subject the minimum that he requries to do his Job.

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

- Modularity : separated the system into subsystems, edch subsystem called as modul

-the more simpler the modul must be easier to secure it

- Layering : segmenting your system into parts

the the approach is to decrease the effort and the countermeasures dealing with specific layer than dealing with group of layers altogether.

- Attack Surfaces : What are the places or the domains or the regions where certain Vulnerabilit are in the System and can be Exploited

* open port s .
* services available on the firewall .
* An employee with access to sensitive info .
"an Employee may be a weak poin in the Sys"

- Attack Surface categories :

(A) Network attack Surface :
* All communication protocols , They have certain weak points

(B) Human attack :
* Social engineering : information needed to access the System
* may happen bc of human error, trusted insiders

(C) software attack

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

* figure 1.4

* attack surface = small → mean num of Vulnerabilit is small.

* Small attack surface → Deep layering = Low Risk security
→ Shallow Layering = Medium Risk

* ideal case : layering very deep and try to minimize num of Vulnerabilites on this surface. [all types surfaces]

موضوع الدرس _____ اليوم _____ التاريخ / /

Computer Security strategy.

* Security policy : Rules usually imposed by the higher administration, but by the recommendation of security officer

* Security implementation : Four actions
  - prevent — Technical part
  - Deteet — Techiral part
  - response — administrative measure
  - recovery — set by administration, but usually is implemented by technical measures.

* Assurance : How much should I as user or adminstrator or owner, have to trust in my information System.

* Evaluation : ① by paper
  ② by real-cases [usually used]
  - ethical hackers are part of evaluation process

- standards
  - NIST : put technology to develop certain information [Technical]
  - ISOC : Technical standard
  - (ITU-T) : Technical stand
  - (ISO) : usually this is a administrative standard

Computer Security: Principles and Practice

Fourth Edition, Global Edition

By: William Stallings and Lawrie Brown

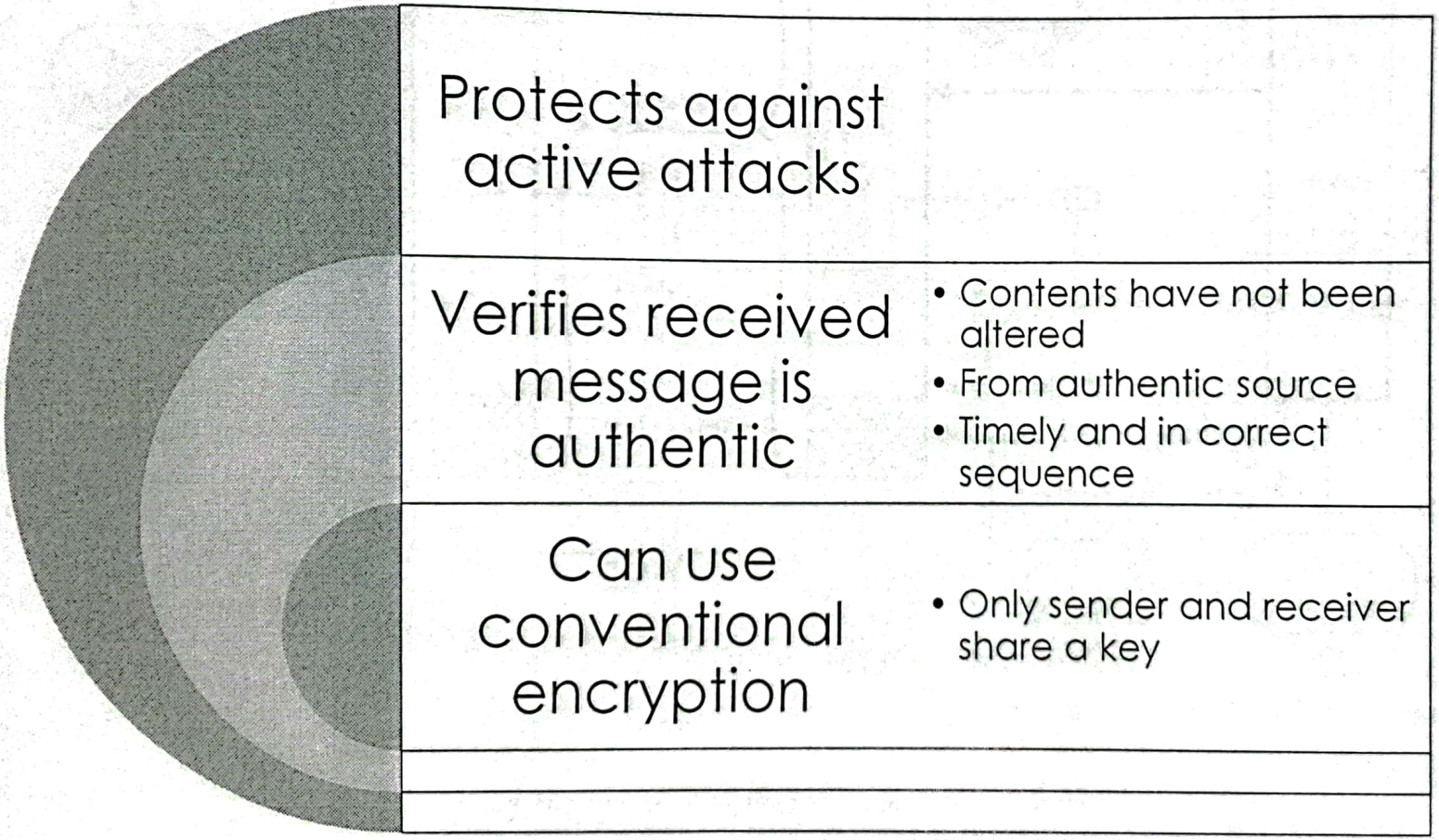
Chapter 2

Cryptographic Tools

Message Authentication

↳ to prove that the subject the one who he claims to be.

- أسباب الحاجة لتأمين confidentiality



Message Authentication Without Confidentiality

- Message encryption by itself does not provide a secure form of authentication
- It is possible to combine authentication and confidentiality in a single algorithm by encrypting a message plus its authentication tag
- Typically message authentication is provided as a separate function from message encryption
- Situations in which message authentication without confidentiality may be preferable include:
  - There are a number of applications in which the same message is broadcast to a number of destinations
  - An exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages
  - Authentication of a computer program in plaintext is an attractive service
- Thus, there is a place for both authentication and encryption in meeting security requirements

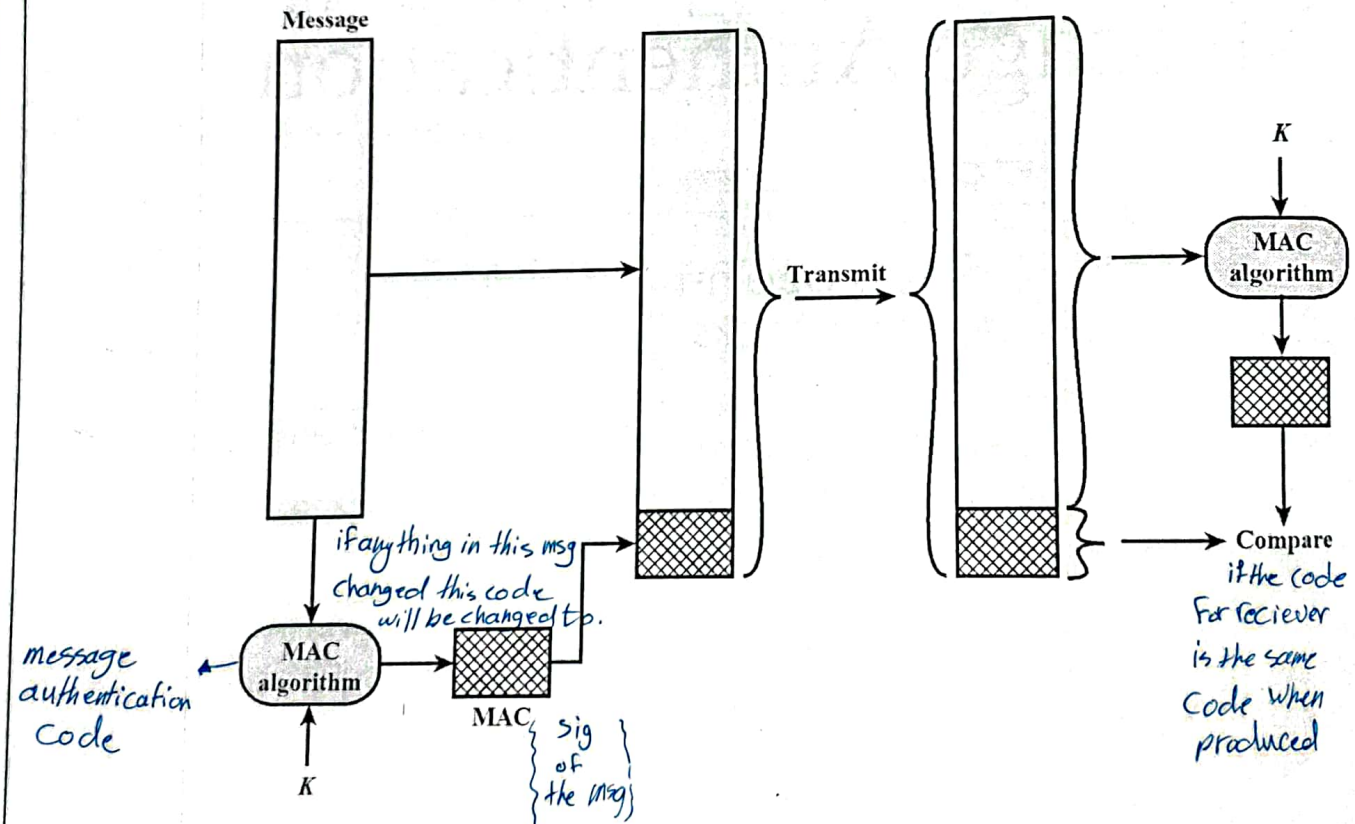
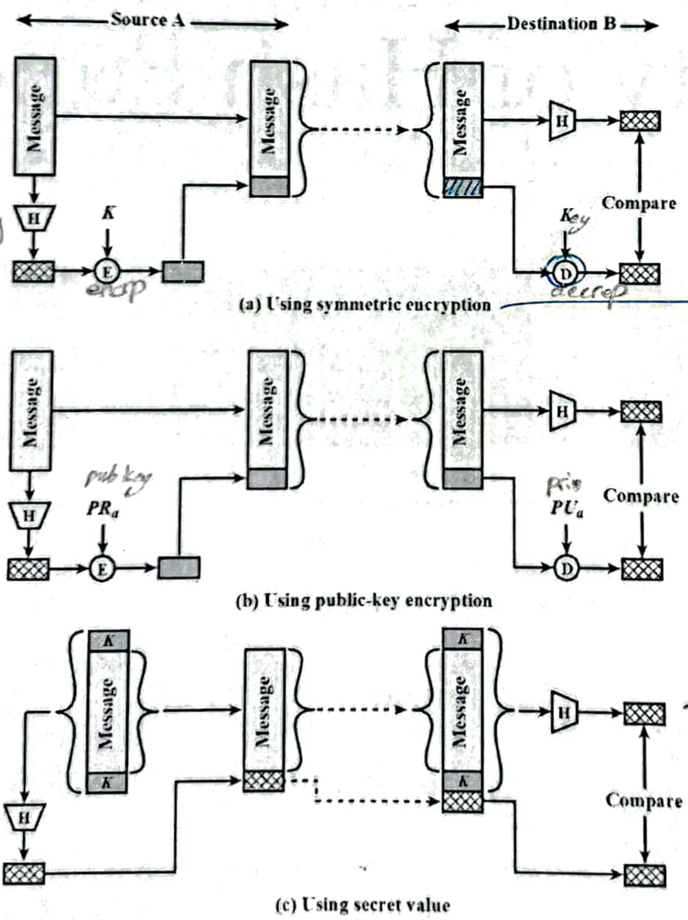


Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).

Hashing: one-way Function it's input [data] & it's output is [hash value]

* hashing: ① ماعشي encryp بالتالي أسرع
② very simple design → against public key process



(a) Using symmetric encryption

(b) Using public-key encryption

(c) Using secret value

Figure 2.5 Message Authentication Using a One-Way Hash Function.

[algorithm in which sender & receiver they share the same key and they will encrp & decrp using the same key]

ولا أحد إلى دكتور سويدان
أحد عنده 2keys + دكتور سويدان
2 keys → public / → private
أحد بعمل encrp باستخدام public key للدكتور سويدان.
[باستخدام الـ public الكل بقدر يرسلك رسالة لكن ما حد بقدر يقرأها إلا اللي عنده الـ priv key الشخص المستقبل]

علية نتفق عليها بين المرسل والمستقبل [not using encryp]
* hashing msg with appended parts that contains secret inform...
* after received check if msg is correct by hashing that msg with that 2 parts then compare it.

[receiver knows that there will be 2 parts]

To be useful for message authentication, a hash function H must have the following properties:

- Can be applied to a block of data of any size
- Produces a fixed-length output
- H(x) is relatively easy to compute for any given x
- One-way or pre-image resistant
  - Computationally infeasible to find x such that H(x) = h
- Computationally infeasible to find y ≠ x such that H(y) = H(x)
- Collision resistant or strong collision resistance
  - Computationally infeasible to find any pair (x, y) such that H(x) = H(y)

* are there any msg's give us the same hash?
- yes, There are but there are no algo gives you the data while you input a hash code

Security of Hash Functions

There are two approaches to attacking a secure hash function:

- **Cryptanalysis**
  - Exploit logical weaknesses in the algorithm
- **Brute-force attack**
  - Strength of hash function depends solely on the length of the hash code produced by the algorithm

SHA most widely used hash algorithm

Additional secure hash function applications:

- **Passwords**
  - Hash of a password is stored by an operating system
- **Intrusion detection**
  - Store H(F) for each file on a system and secure the hash values

pass always stored in hash vale.

all pass's stored in file & this file is hashed

Public-Key Encryption Structure

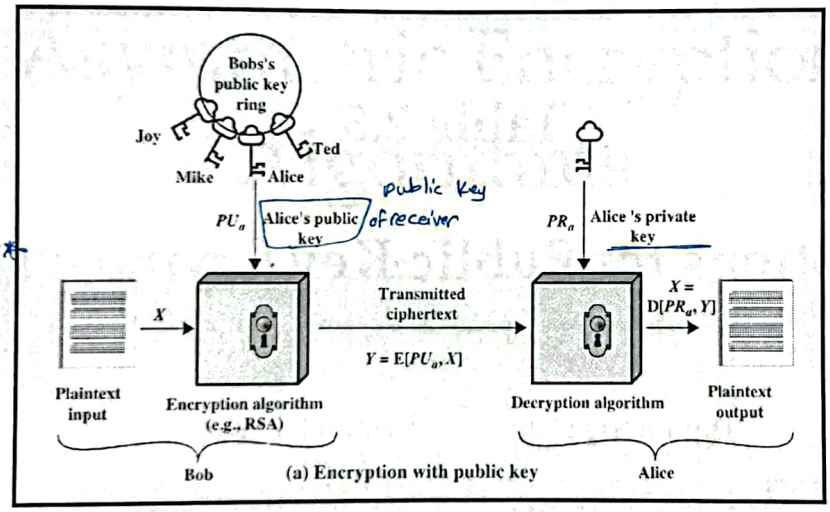
Publicly proposed by Diffie and Hellman in 1976
protocol to solve symmetric key problem

Based on mathematical functions

keyA encryp keyB decryp
Asymmetric
- Uses two separate keys
- Public key and private key
- Public key is made public for others to use

Some form of protocol is needed for distribution

both way :
encryp : priv key ⇔ decryp : public key
encryp : public ⇔ decr : private key



Confidint

- **Plaintext**
  - Readable message or data that is fed into the algorithm as input
- **Encryption algorithm**
  - Performs transformations on the plaintext
- **Public and private key**
  - Pair of keys, one for encryption, one for decryption
- **Ciphertext**
  - Scrambled message produced as output
- **Decryption key**
  - Produces the original plaintext

* every body can know the msg that Bob send [broad cast]

* authintisity of the sender [non-repudiation]

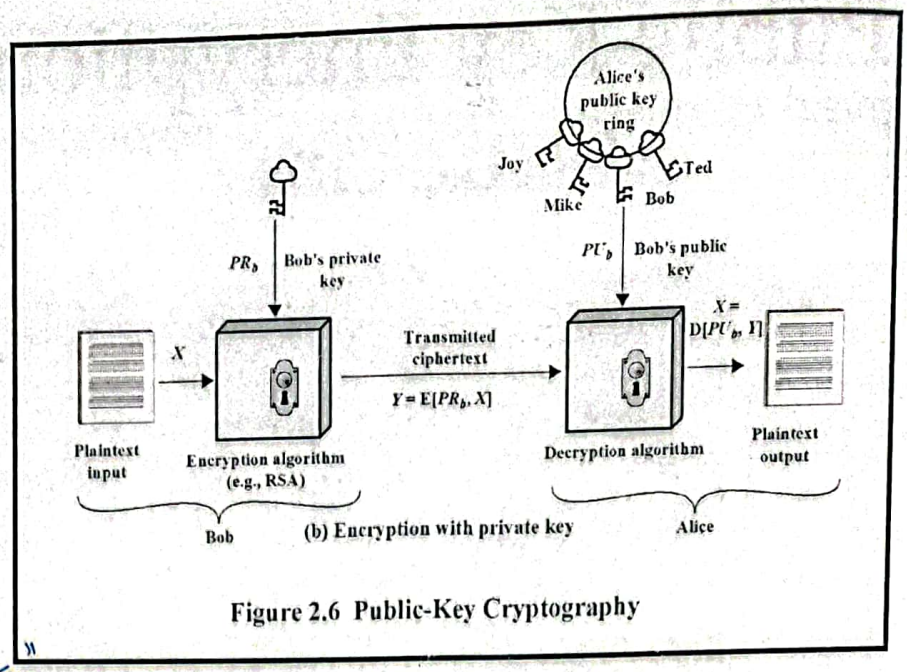


Figure 2.6 Public-Key Cryptography

- User encrypts data using his or her own private key
- Anyone who knows the corresponding public key will be able to decrypt the message

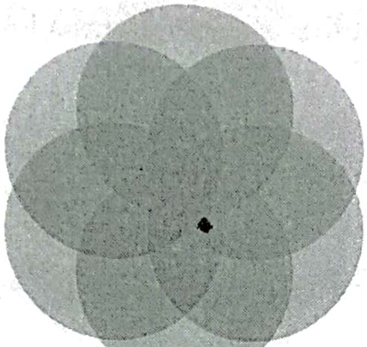
Table 2.3

Applications for Public-Key Cryptosystems

Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
RSA	Yes	Yes	Yes
Diffie-Hellman	No	Yes	No
DSS	Yes	No	No
Elliptic Curve	Yes	Yes	Yes

Commonly

Requirements for Public-Key Cryptosystems



Computationally easy to create key pairs

Computationally easy for sender knowing public key to encrypt messages

Computationally easy for receiver knowing private key to decrypt ciphertext

* أي attacker اذا عرف ال public key لازم مايعرف ال priv key ولا يعرف شو المسج

Computationally infeasible for opponent to determine private key from public key

Computationally infeasible for opponent to otherwise recover original message

Useful if either key can be used for each role

← يقترح ان تكون الالغورثم [in two ways]

* اي مسج encry باستخدام ال public key لازم ينفك بال priv key

* اي مسج encry باستخدام ال priv key لازم تنفك بال public key

Asymmetric Encryption Algorithms

RSA (Rivest, Shamir, Adleman)	Developed in 1977	Most widely accepted and implemented approach to public-key encryption	Block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some *n*.	[encryp + decry]
Diffie-Hellman key exchange algorithm	Enables two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages	Limited to the exchange of the keys		public of key destribution
Digital Signature Standard (DSS)	Provides only a digital signature function with SHA-1	Cannot be used for encryption or key exchange		* بعطي ضمان integrity of content * وضمان من الشخص ← hand written signature
Elliptic curve cryptography (ECC) * encryp/de * hashing	Security like RSA, but with much smaller keys	[encryp + decry]		DSS: مربوط بالشخص + content

Digital Signatures

- NIST FIPS PUB 186-4 defines a digital signature as:

  "The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation."

- Thus, a digital signature is a data-dependent bit pattern, generated by an agent as a function of a file, message, or other form of data block

- FIPS 186-4 specifies the use of one of three digital signature algorithms:
  - Digital Signature Algorithm (DSA)
  - RSA Digital Signature Algorithm
  - Elliptic Curve Digital Signature Algorithm (ECDSA)

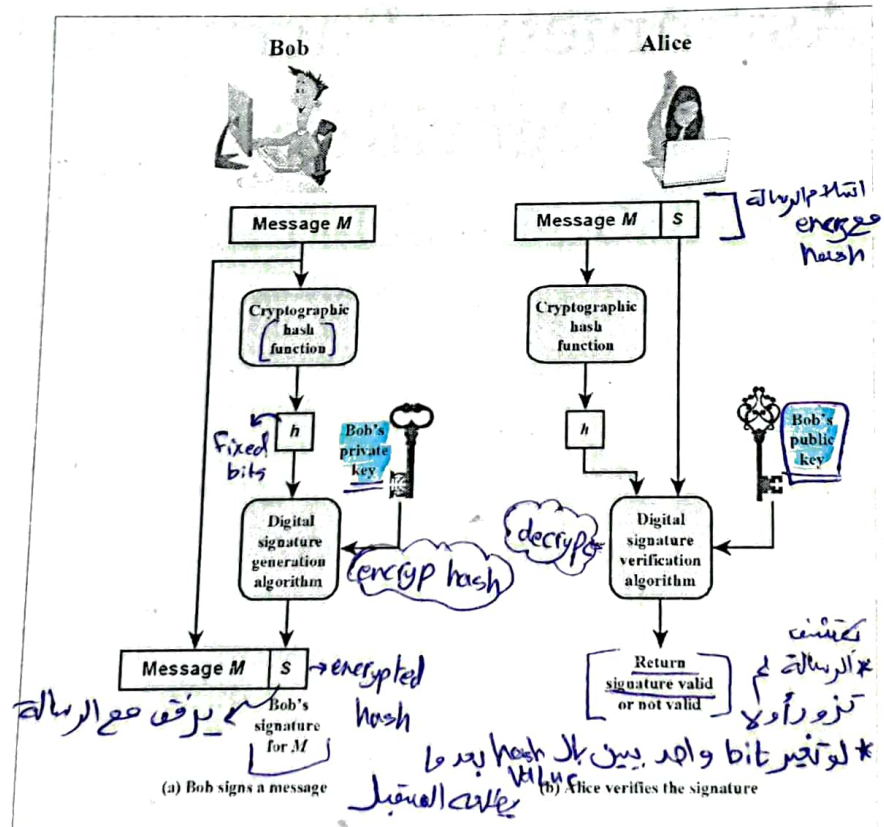


Figure 2.7 Simplified Depiction of Essential Elements of Digital Signature Process

owner, website, user ... Certificate * Use

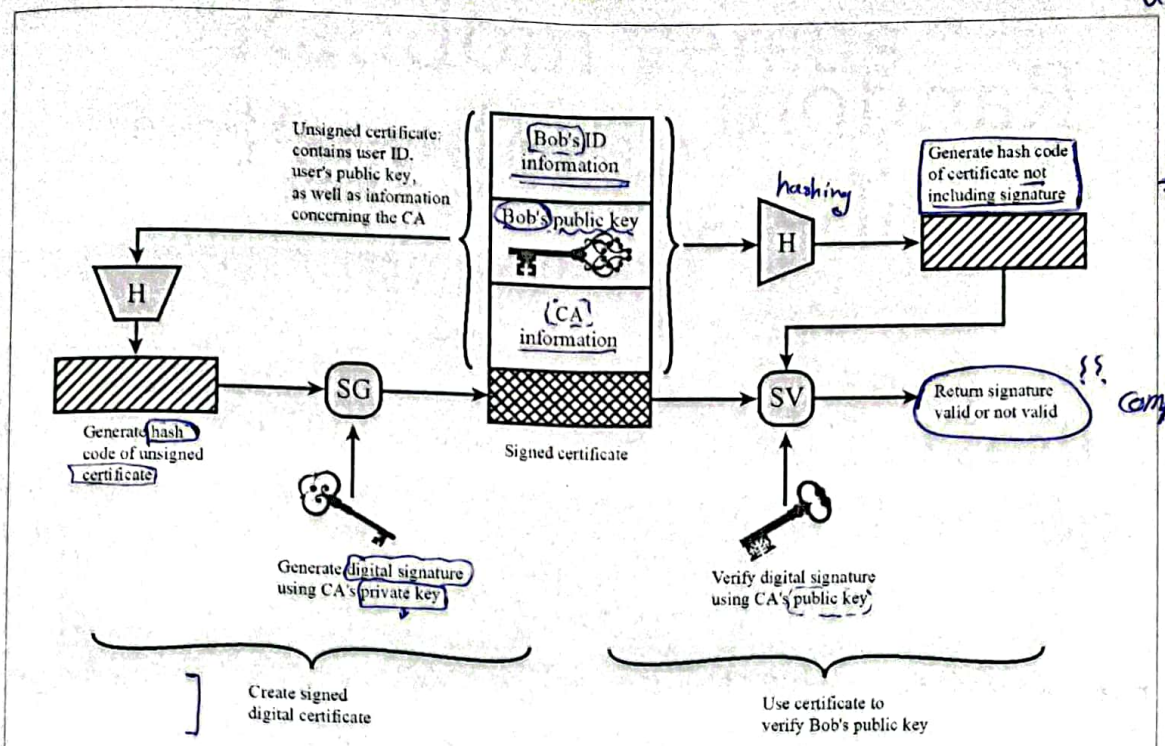


Figure 2.8 Public-Key Certificate Use

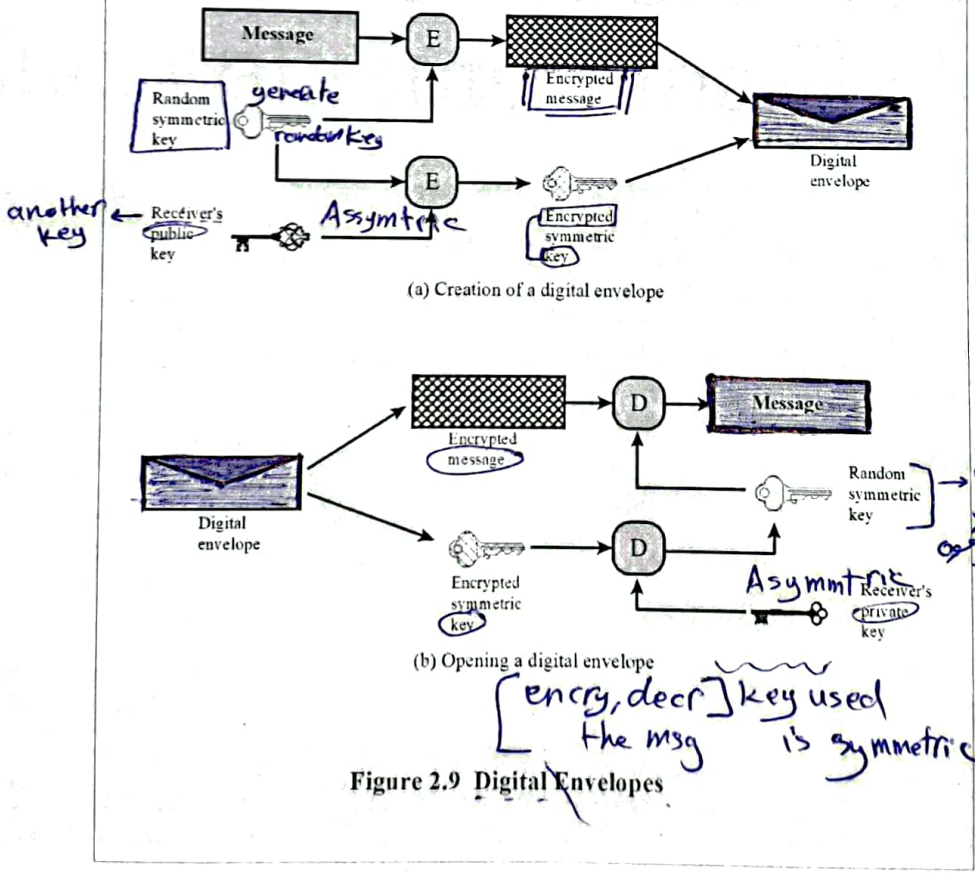
digital signature ↔ public key Uses

[certificate]

all applications Used either

a) encrypt/dec or

b) hashing



[encry, decr] key used the msg is symmetric

Figure 2.9 Digital Envelopes

Random Numbers

Uses include generation of:

- Keys for public-key algorithms
- Stream key for symmetric stream cipher
- Symmetric key for use as a temporary session key or in creating a digital envelope
- Handshaking to prevent replay attacks
- Session key

*random num in security different than random num's in programming.

sudo random :: we generate psudo random in security

*certain structure with certain control that can generate relativly psudo random code

*mostly used in mobile phones

Random Number Requirements

Randomness

- Criteria:
  - Uniform distribution
    - Frequency of occurrence of each of the numbers should be approximately the same
  - Independence
    - No one value in the sequence can be inferred from the others

Unpredictability

- Each number is statistically independent of other numbers in the sequence
- Opponent should not be able to predict future elements of the sequence on the basis of earlier elements

Computer Security: Principles and Practice

Fourth Edition, Global Edition

By: William Stallings and Lawrie Brown

Chapter 3

User Authentication

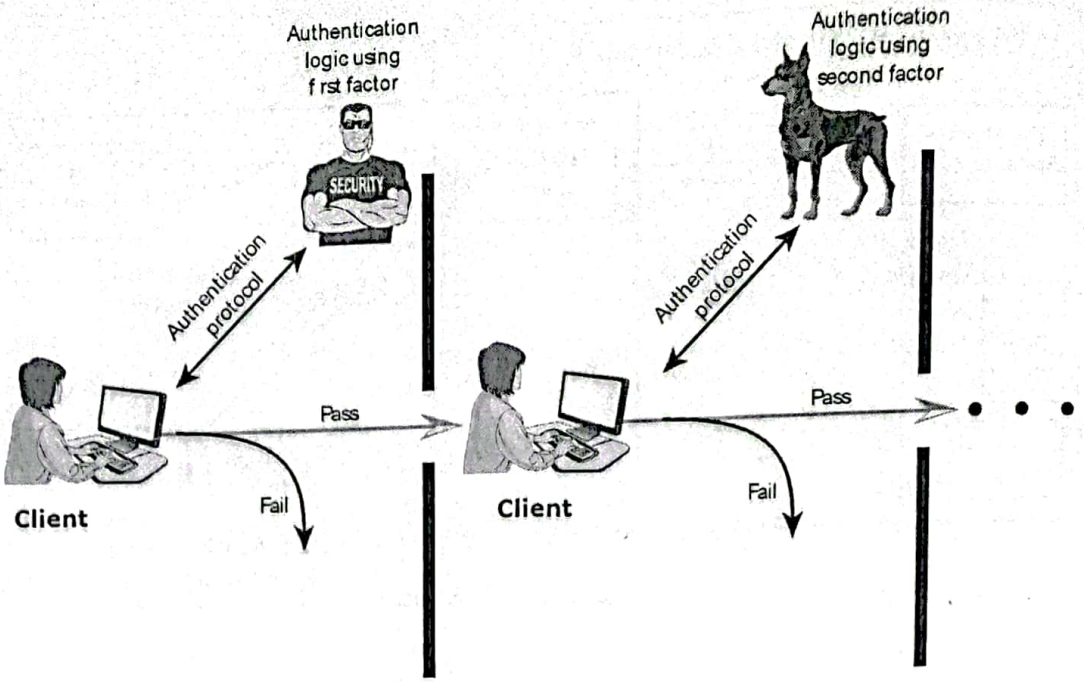
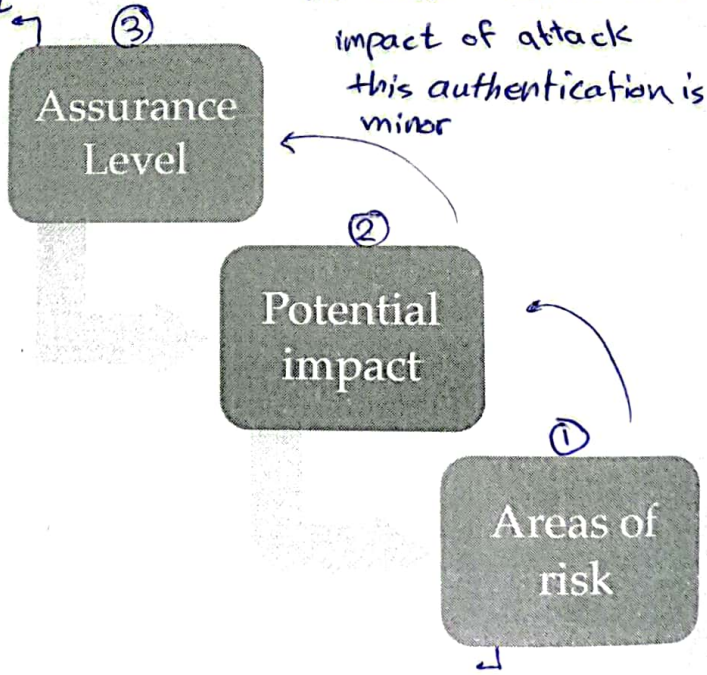


Figure 3.2 Multifactor Authentication

Risk Assessment for User Authentication

idea of How when you are confident, so that this authentication procedure is good & successful

- There are three separate concepts:



Assurance Level

Describes an organization's degree of certainty that a user has presented a credential that refers to his or her identity

More specifically is defined as:

The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued

The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

Four levels of assurance

- Level 1
  - Little or no confidence in the asserted identity's validity
- Level 2
  - Some confidence in the asserted identity's validity
- Level 3
  - High confidence in the asserted identity's validity
- Level 4
  - Very high confidence in the asserted identity's validity

Potential Impact

- FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security:
  1. Low
     - An authentication error could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
  2. Moderate
     - An authentication error could be expected to have a serious adverse effect
  3. High
     - An authentication error could be expected to have a severe or catastrophic adverse effect

Table 3.2

* طبيعة الشركة، تطبيقاتها ← وتطبيقات عليها يكون تأثيرها impact High وممكن impact low

So, that the user assigned to that app, may get diffirent Assure Levels.

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or organization liability	Low	Mod	Mod	High
Harm to organization programs or interests	None	Low	Mod	High
Unauthorized release of sensitive information	None	Low	Mod	High
Personal safety خطر حياة على الناس	None	None	Low	Mod/ High
Civil or criminal violations	None	Low	Mod	High

Maximum Potential Impacts for Each Assurance Level

* most commonly used in authentication : password

Password-Based Authentication

* password file contains all passwords in the system should be hashed.

- Widely used line of defense against intruders
  - User provides name/login and password
  - System compares password with the one stored for that specified login
- The user ID: يقرر privileges of the user
  - Determines that the user is authorized to access the system
  - Determines the user's privileges
  - Is used in discretionary access control

it gives me authority to give others some of my privileges. [access to certain files]

Password Vulnerabilities

Offline dictionary attack

Password guessing against single user

Workstation hijacking

Electronic monitoring

Specific account attack

Popular password attack

Exploiting user mistakes

Exploiting multiple password use

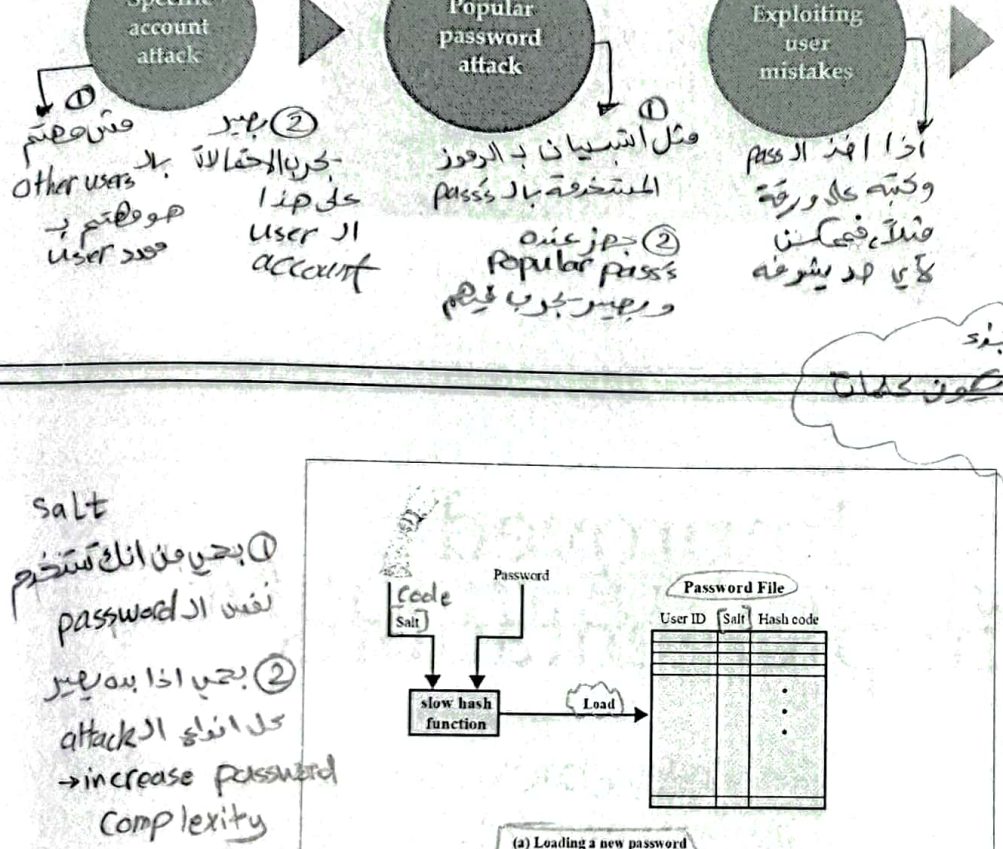
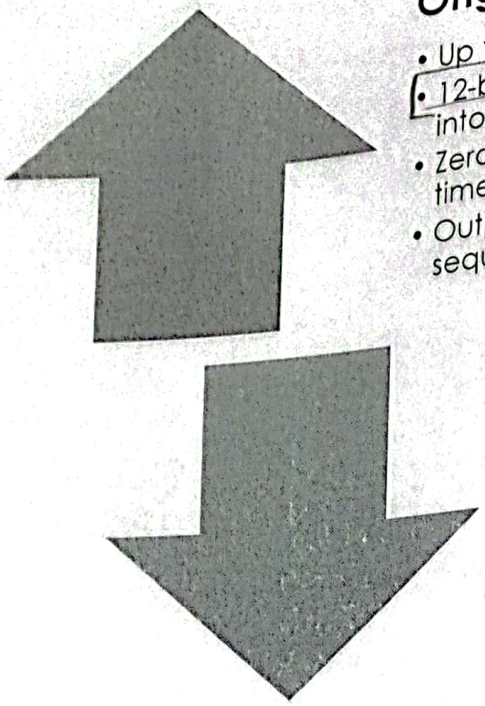


Figure 3.3 UNIX Password Scheme

UNIX Implementation



Original scheme

- Up to eight printable characters in length
- 12-bit salt used to modify DES encryption into a one-way hash function
- Zero value repeatedly encrypted 25 times
- Output translated to 11 character sequence

Now regarded as inadequate

- Still often required for compatibility with existing account management software or multivendor environments

Improved Implementations

Much stronger hash/salt schemes available for Unix

OpenBSD uses Blowfish block cipher based hash algorithm called Bcrypt

- Most secure version of Unix hash/salt scheme
- Uses 128-bit salt to create 192-bit hash value

Recommended hash function is based on MD5

- Salt of up to 48-bits
- Password length is unlimited
- Produces 128-bit hash
- Uses an inner loop with 1000 iterations to achieve slowdown

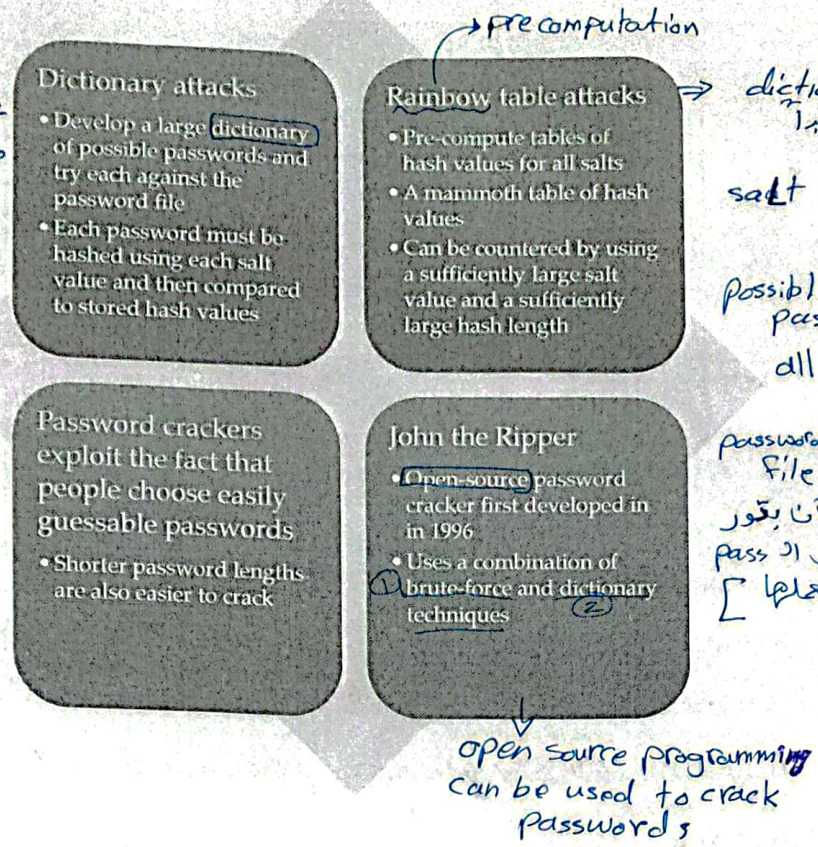
guessing بدون pass

[really extremly difficult]

2^{128} يجرب different salts

Password Cracking

4 approaches :-



dictionary one "offline"

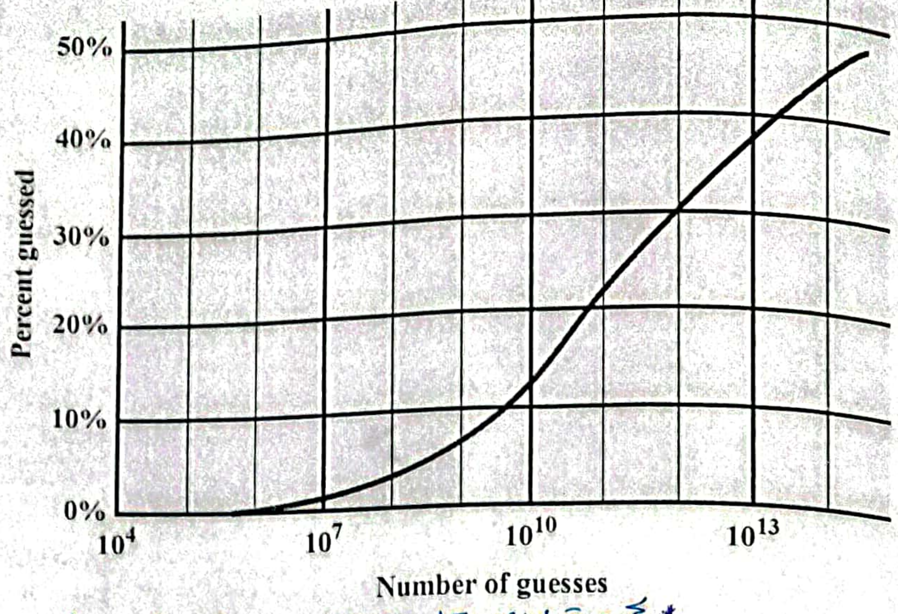
salt

all hashes with all possible salts

open source programming can be used to crack passwords

Modern Approaches

- Complex password policy
  - Forcing users to pick stronger passwords
    - educating
- However password-cracking techniques have also improved
  - The processing capacity available for password cracking has increased dramatically
  - The use of sophisticated algorithms to generate potential passwords
  - Studying examples and structures of actual passwords in use



* كم مرة لازم يعمل guessing → to crack certain password

Figure 3.4 The Percentage of Passwords Guessed After a Given Number of Guesses

* The more you lose. guesses, the more percentage of our probability to guess

---

* windows [or] Linux store the password file in a very secure area. [very confidential file]

Password File Access Contr

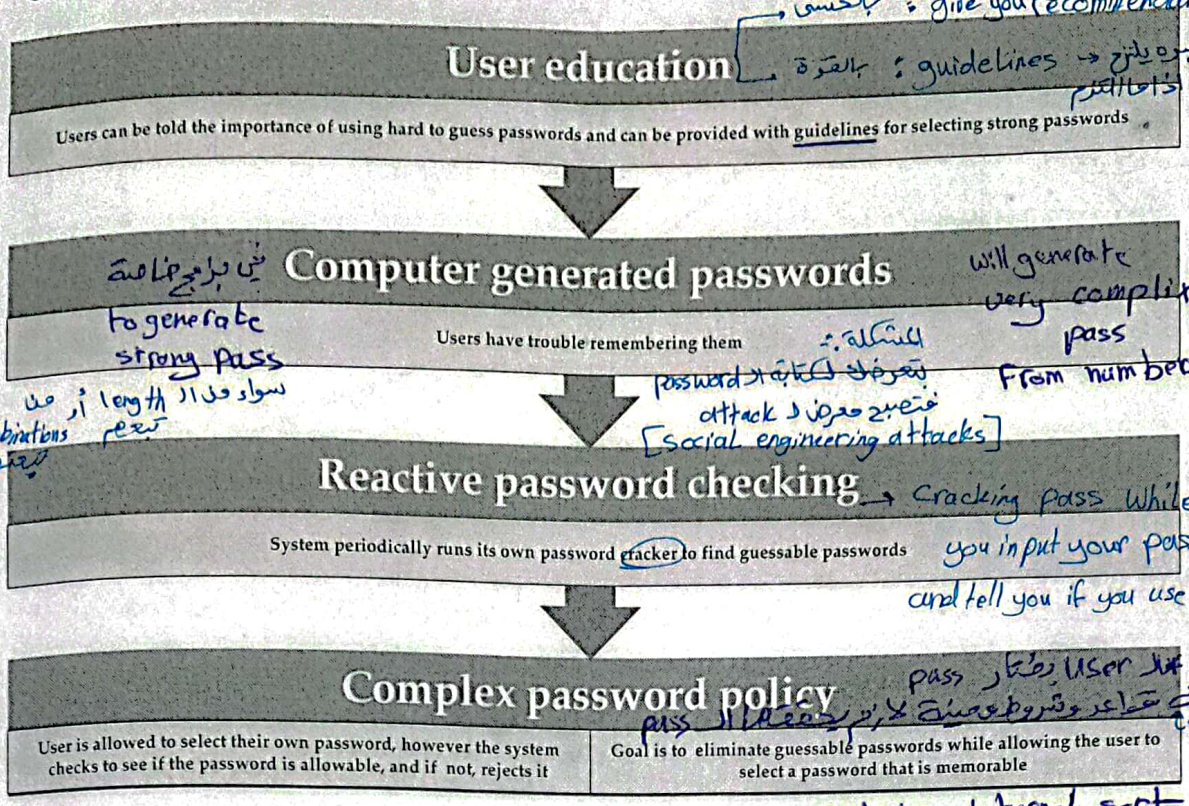
Can block offline guessing attacks by denying access to encrypted passwords

- Make available only to privileged users
- Shadow password file

Vulnerabilities :

- Weakness in the OS that allows access to the file
- Accident with permissions making it readable — by administrator ← عمل privileges لشخص مش لازم يعطيه
- Users with same password on other systems — والسيستم فيه مشكلة أو ثغرة
- Access from backup media — any flashes, CDs for systems لازم تتلف بإجراء خاص
- Sniff passwords in network traffic — يلقط معلومات على الخط

Password Selection Strategies



Proactive Password Checking

- Rule enforcement
  - Specific rules that passwords must adhere to
- Password checker
  - Compile a large dictionary of passwords not to use
- Bloom filter
  - Used to build a table based on hash values
  - Check desired password against this table

bloom filter (k)

$H_i(x_j)$ $1 \le j \le k$ $1 \le j \le D$

→ False positive ÷

→ bloom filter: certain diction used to try, certain num of hash functions

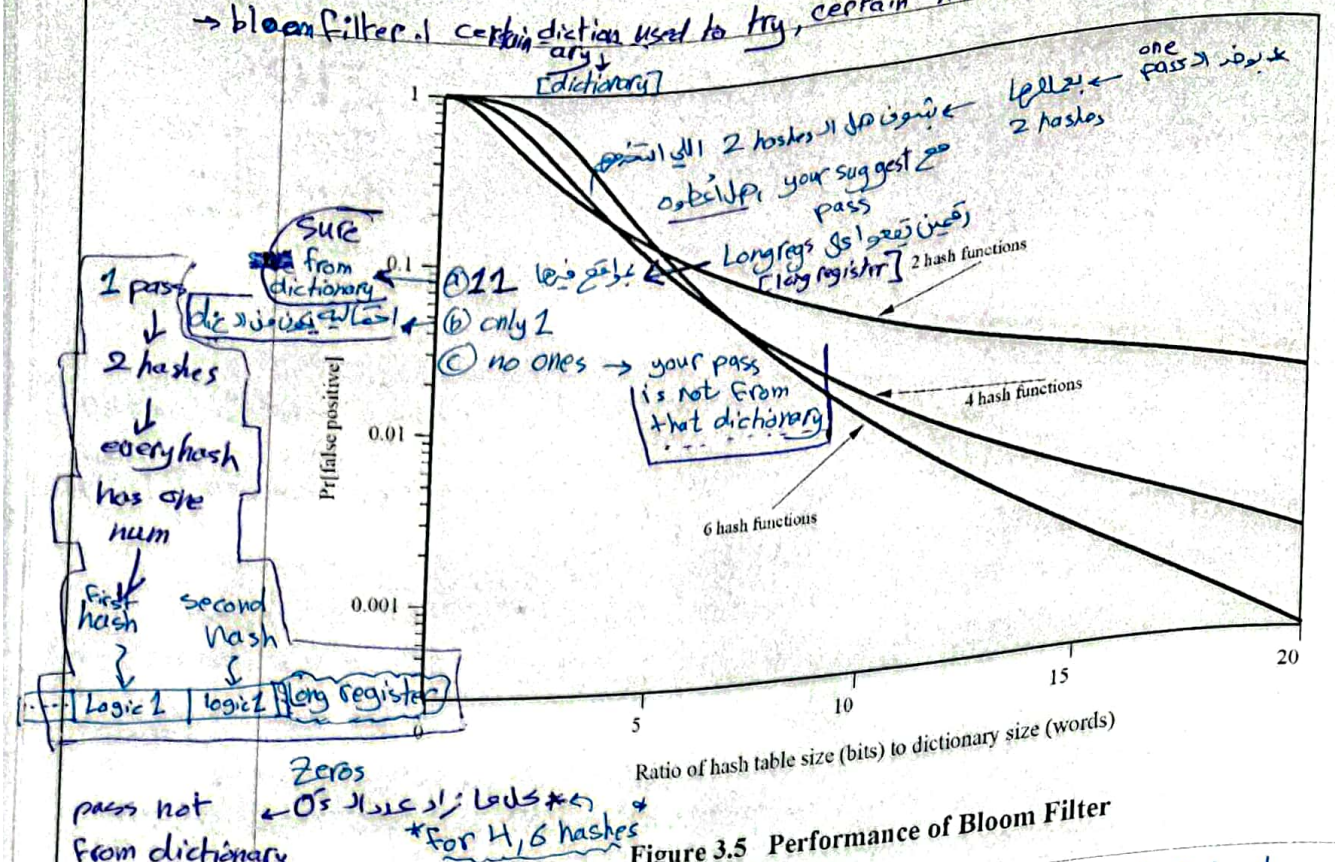


Figure 3.5 Performance of Bloom Filter

pass not from dictionary ← Zeros

→ dic[size]=100 [bits] for register = 1000 ≈ $\frac{1000}{100}$ = 10 and used 2 hashes *

{dictionary size}

bloom Filter:
① not on Line
② need huge register
③ calculations are done prior to the bloom filter work

False positive almost zero [on curve] ← very low probability ← 6 hashes واستخدام ratio = 20

Table 3.3

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart Contact Contactless	Electronic memory and processor inside Electrical contacts exposed on surface Radio antenna embedded inside	Biometric ID card

Types of Cards Used as Tokens

means Tool allow you to access.

→ False positive : احتمالية حدوث

→ bloom filter : certain dictionary used to try, certain num of hash functions [dictionary]

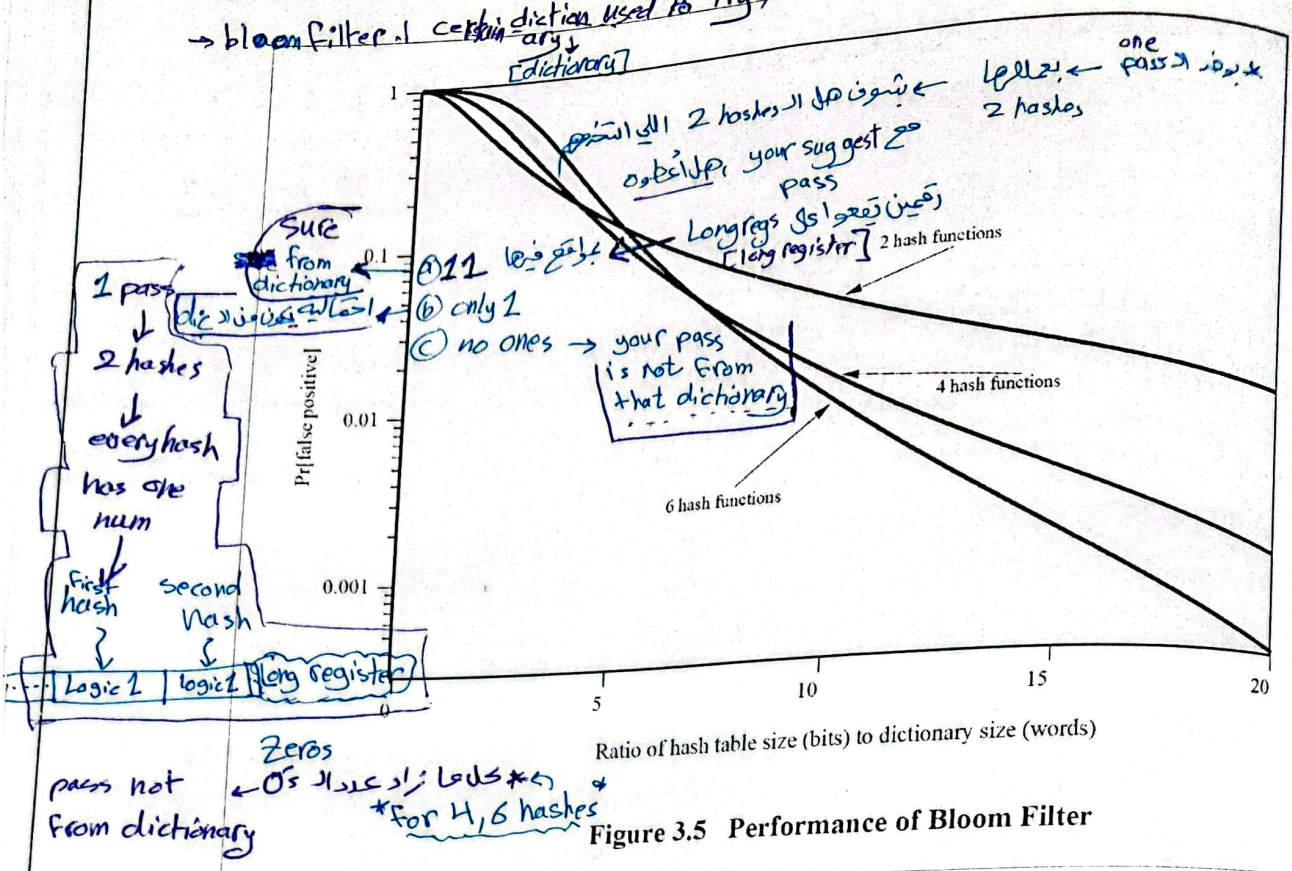


Figure 3.5 Performance of Bloom Filter

→ dic[size]=1000 [bits] for register = 1000 ≈ 1000/100 = 10 and used 2 hashes *

{dictionary size}

احتمالية حدوث false positive ليست عالية

bloom Filter :
① not on Line
② need huge register
③ calculations are done prior to the bloom filter work

False positive almost zero [on curve] ← very low probability ← 6 hashes واستخدام ratio = 20

Table 3.3

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart Contact Contactless	Electronic memory and processor inside Electrical contacts exposed on surface Radio antenna embedded inside	Biometric ID card

Types of Cards Used as Tokens

means Tool allow you to access.

Smart Cards

- Most important category of smart token
  - Has the appearance of a credit card
  - Has an electronic interface
  - May use any of the smart token protocols
- Contain:
  - An entire microprocessor
    - Processor
    - Memory [RoM, EPRoM, RAM] → while calculating certain algorithm
    - I/O ports
- Typically include three types of memory:
  - Read-only memory (ROM) {basic information}
    - Stores data that does not change during the card's life
  - Electrically erasable programmable ROM (EEPROM) {password}
    - Holds application data and programs
  - Random access memory (RAM) {while calculating algorithm}
    - Holds temporary data generated when applications are execute

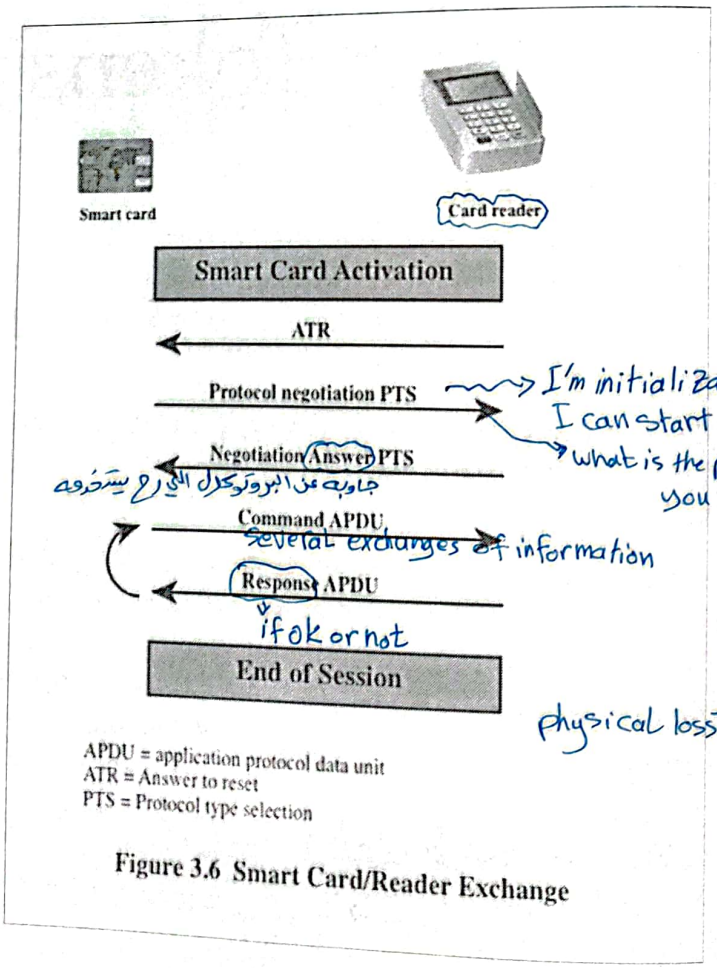


Figure 3.6 Smart Card/Reader Exchange

Memory Cards

top confidentiality = Assurance level 4

- Can store but do not process data
- The most common is the magnetic stripe card
- Can include an internal electronic memory
- Can be used alone for physical access
  - Hotel room → Assurance level no need to be at high level [easily disabled]
  - ATM
- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
  - Requires a special reader
  - Loss of token
  - User dissatisfaction

Smart Tokens

بشبه ال bank card

- Physical characteristics:
  - Include an embedded microprocessor
  - A smart token that looks like a bank card
  - Can look like calculators, keys, small portable objects
- User interface:
  - Manual interfaces include a keypad and display for human/token interaction
- Electronic interface
  - A smart card or other token requires an electronic interface to communicate with a compatible reader/writer
  - Contact and contactless interfaces
- Authentication protocol: → if you want to use that smart card, how you are authticated while you are using such smart card
  - Classified into three categories:
    - Static
    - Dynamic password generator
    - Challenge-response [أقوى واحد] → assur مع أعلى levels 3 or 4

Electronic Identity Cards (eID)

read

Use of a smart card as a national identity card for citizens

Can serve the same purposes as other national ID cards, and similar cards such as a driver's license, for access to government and commercial services

Can provide stronger proof of identity and can be used in a wider variety of applications

In effect, is a smart card that has been verified by the national government as valid and authentic

Most advanced deployment is the German card *neuer Personalausweis*

Has human-readable data printed on its surface

- Personal data
- Document number
- Card access number (CAN)
- Machine readable zone (MRZ)

Function	Purpose	PACE Password	Data	Uses
ePass (mandatory)	Authorized offline inspection systems read the data	CAN or MRZ	Face image; two fingerprint images (optional), MRZ data	Offline biometric identity verification reserved for government access
eID (activation) optional	Online applications read the data or acess functions as authorized	eID PIN	Family and given names; artistic name and doctoral degree: date and place of birth; address and community ID; expiration date	Identification; age verification; community ID verification; restricted identification (pseudonym); revocation query
	Offline inspection systems read the data and update the address and community ID	CAN or MRZ		
eSign (certificate) optional	A certification authority installs the signature certificate online	eID PIN	Signature key; X.509 certificate	Electronic signature creation
	Citizens make electronic signature with eSign PIN	CAN		

Table 3.4

Electronic Functions and Data for eID Cards

CAN = card access number
MRZ = machine readable zone
PACE = password authenticated connection establishment
PIN = personal identification number

all these authentication techiques [access control techi]

Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include:
  - Facial characteristics (3)
  - Fingerprints (2)
  - Hand geometry (3)
  - Retinal pattern (5)
  - Iris (6)
  - Signature (1)
  - Voice (4)

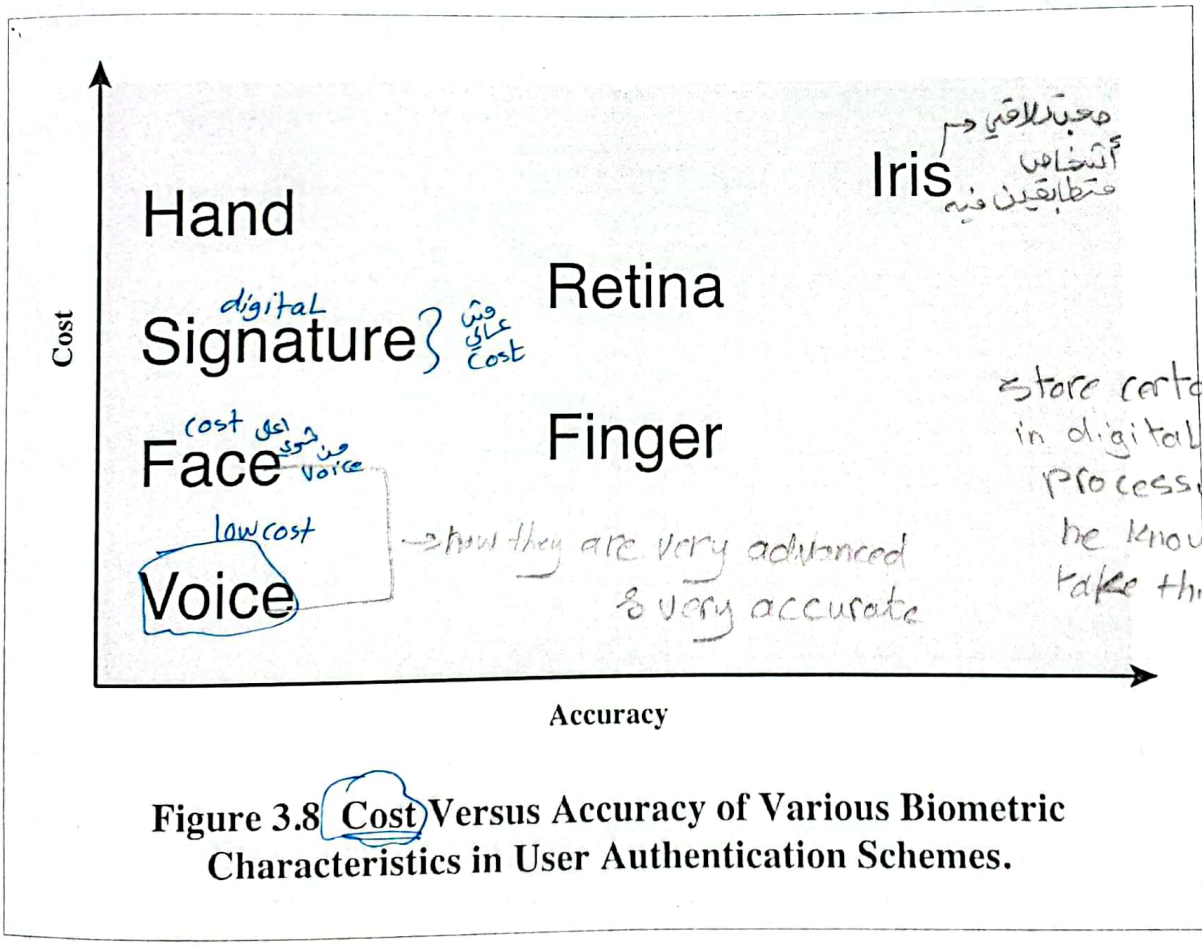


Figure 3.8 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.

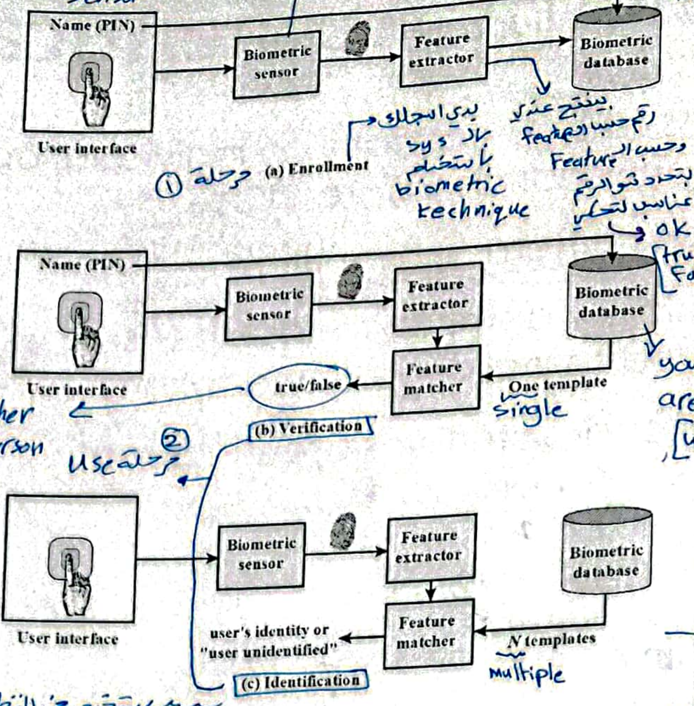


Figure 3.9 A Generic Biometric System. Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.

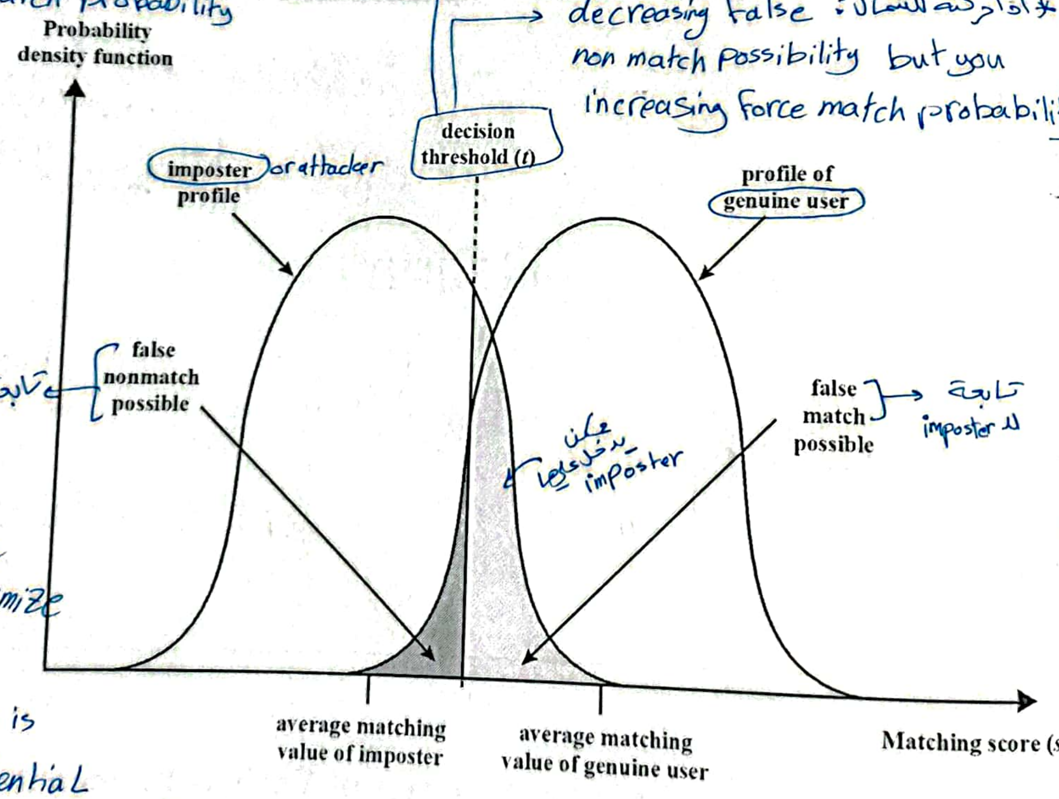


Figure 3.10 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared.

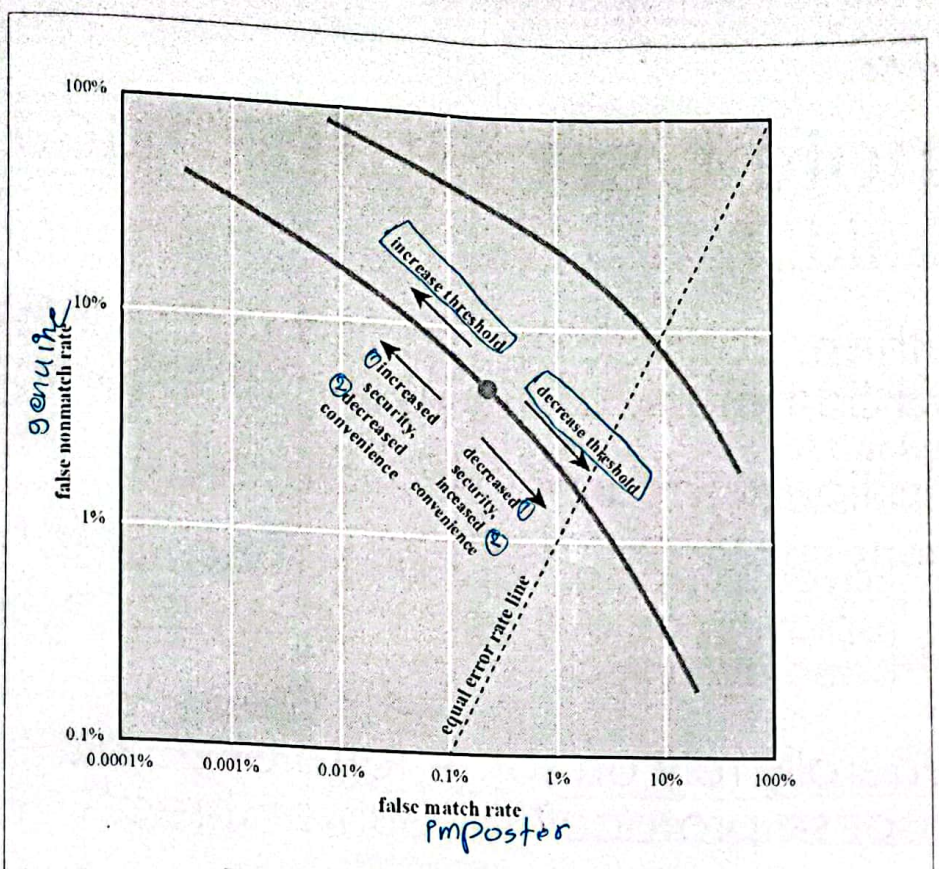


Figure 3.11 Idealized Biometric Measurement Operating Characteristic Curves (log-log scale)

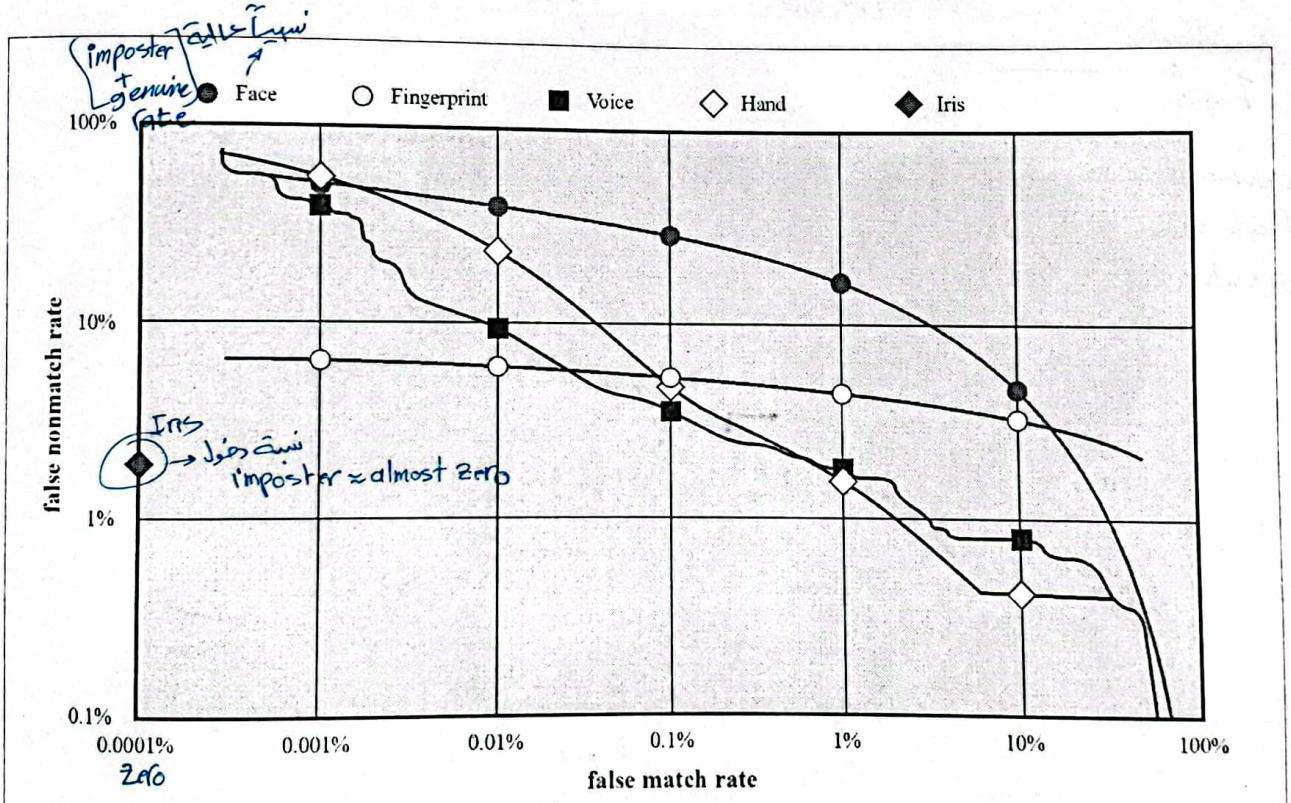


Figure 3.12 Actual Biometric Measurement Operating Characteristic Curves, reported in [MANS01]. To clarify differences among systems, a log-log scale is used.

to get secure

Remote User Authenticati

- Authentication over a network, the Interne or a communications link is more complex
- Additional security threats such as:
  - Eavesdropping, capturing a password, replaying an authentication sequence that h been observed
- Generally rely on some form of a challenge response protocol to counter threats

Valid for all types of authentication

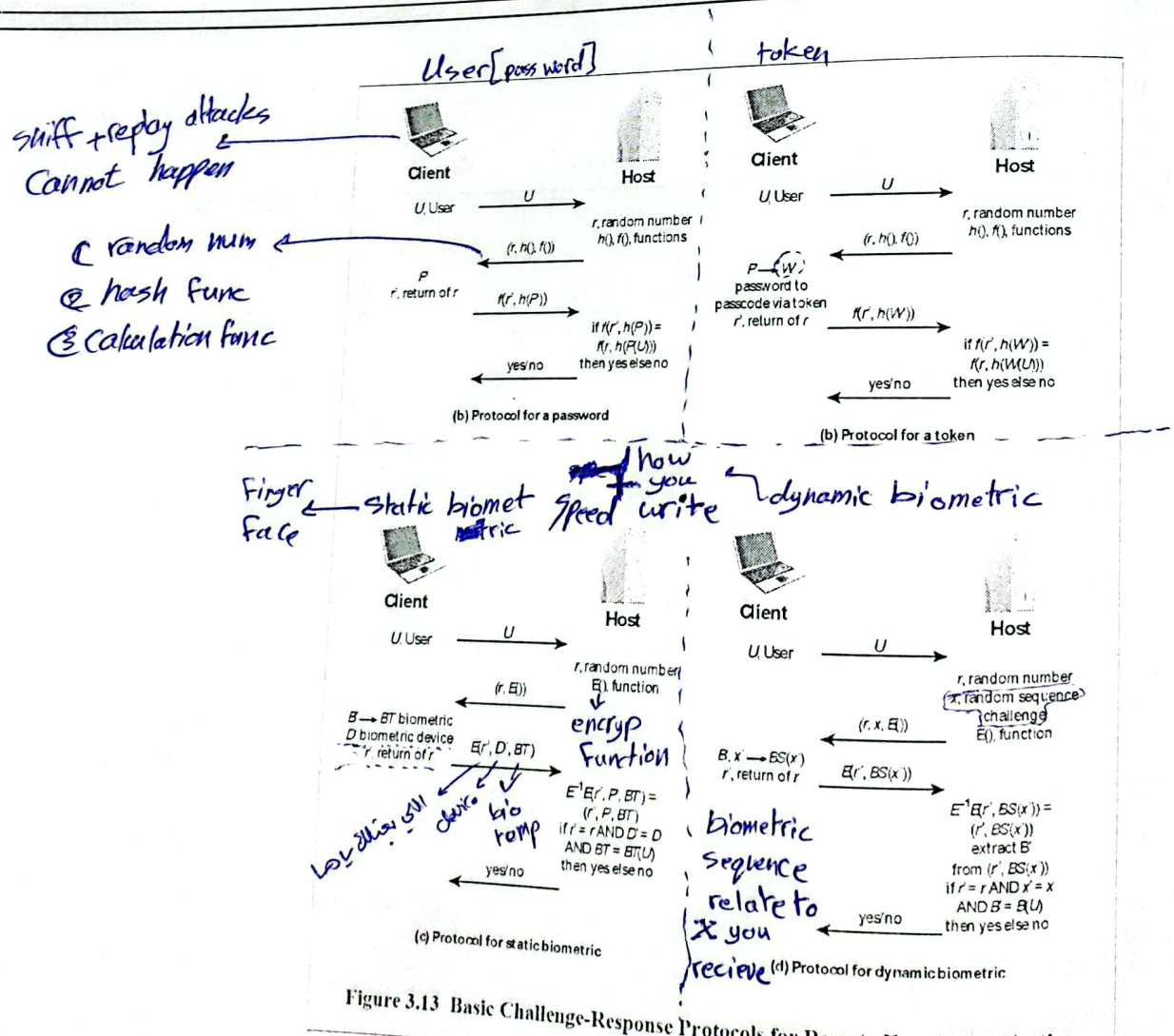


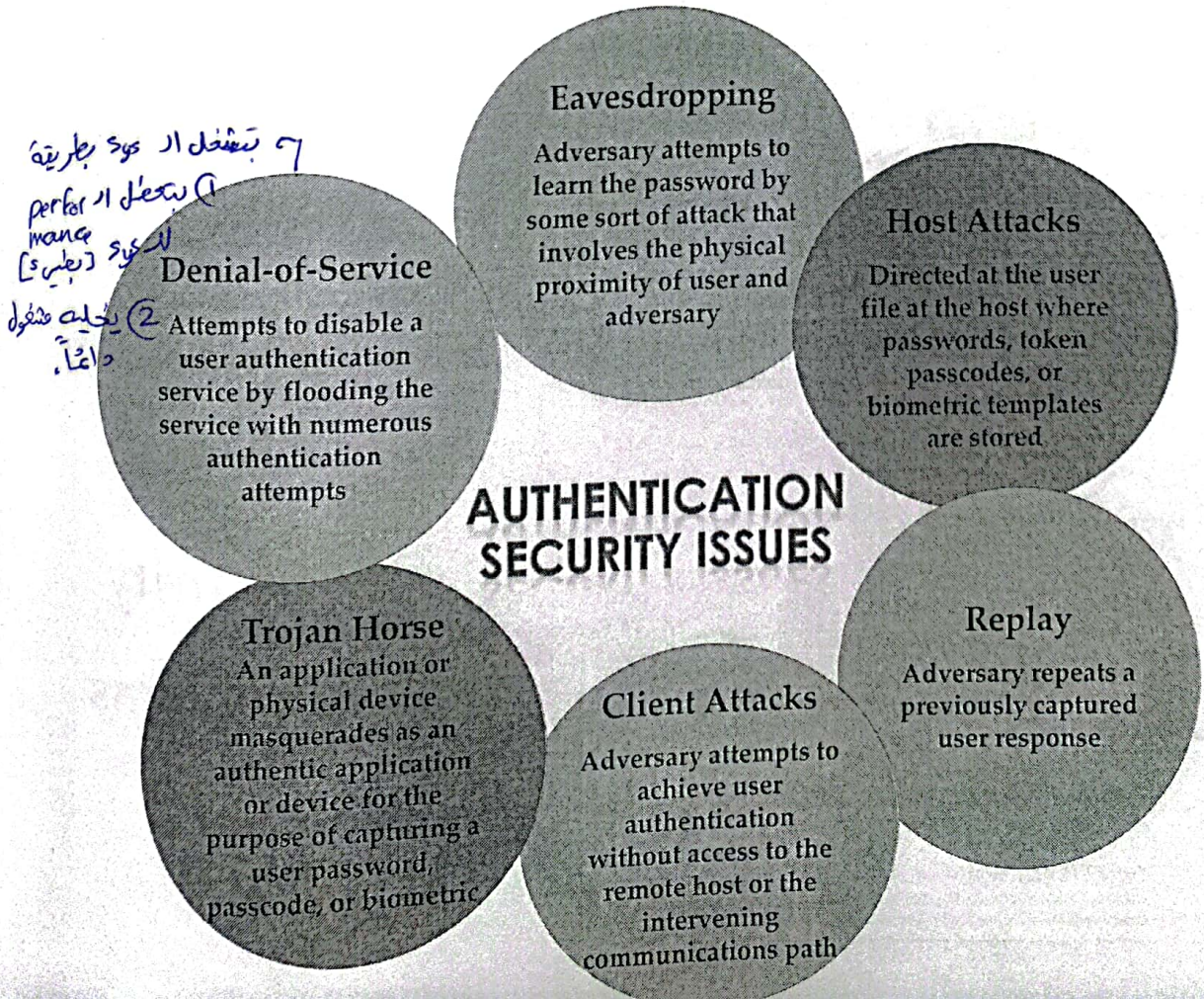
Figure 3.13 Basic Challenge-Response Protocols for Remote User Authentication

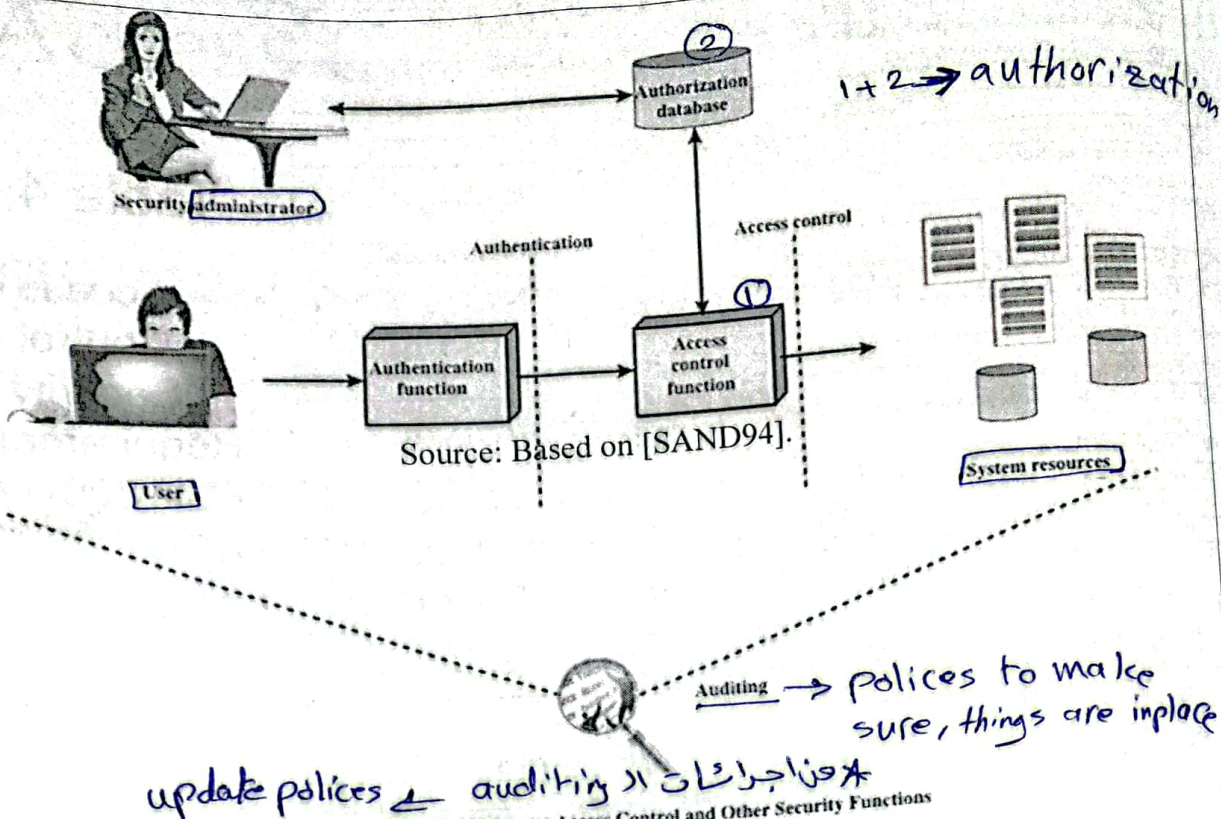
Attacks	Authenticators	Examples	Typical defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts, theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
Denial of service	Password, token, biometric	Lockout by multiple failed authentications	Multifactor with token

Table 3.5

Some Potential Attacks, Susceptible Authenticators, and Typical Defenses

(Table is on page 96 in the textbook)





Source: Based on [SAND94].

1+2 → authorization

Auditing → polices to make sure, things are inplace

update polices ← auditing ← وبناء جراءات ال *

Figure 4.1 Relationship Among Access Control and Other Security Functions

Source: Based on [SAND94].

* subject : user or process done by that user

Access Control Policies

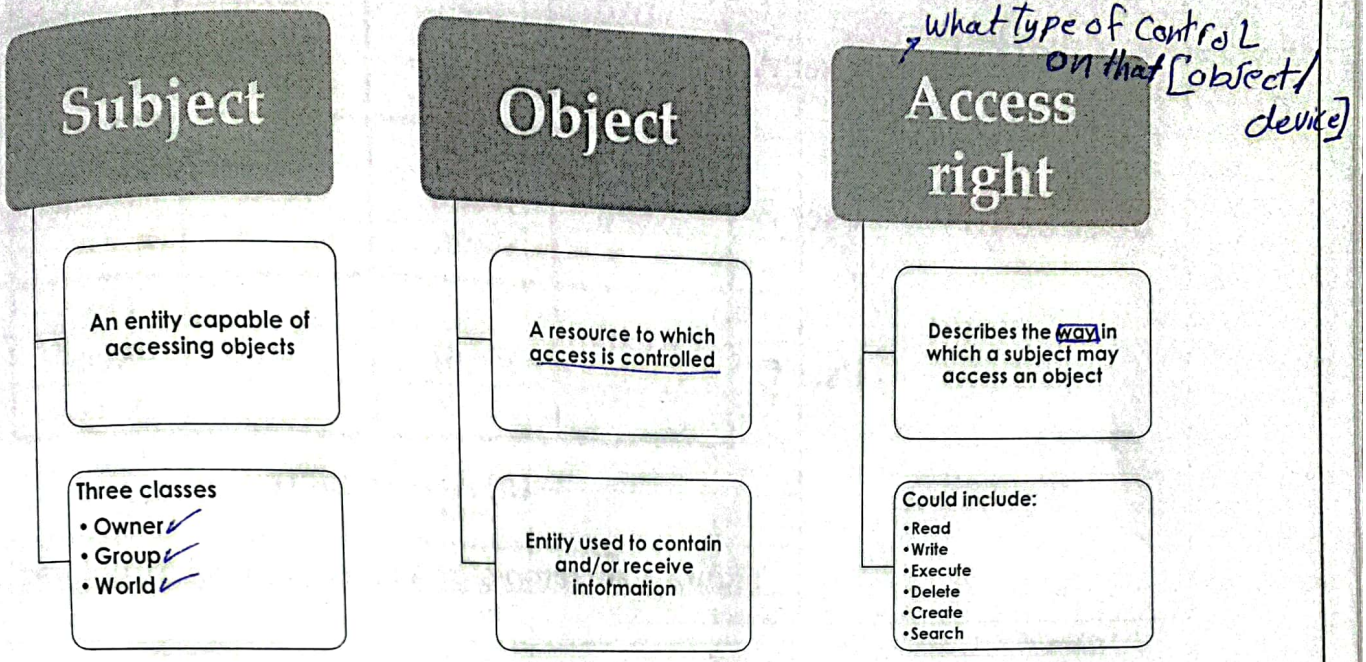
- Discretionary access control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
  - Controls access based on comparing security labels with security clearances
- Role-based access control (RBAC)
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles
- Attribute-based access control (ABAC)
  - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

each subject has certain level of clearances, and each object has certain level of security requirements

* you can have a system in which you can combine two things together

* all these 4 policies are not mutually exclusive

Subjects, Objects, and Access Rights



What type of control on that [object/device]

Discretionary Access Control (DAC)

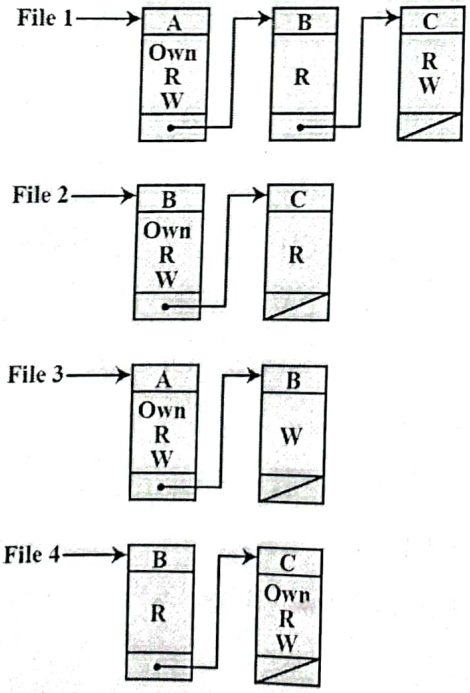
- Scheme in which an entity may be granted access rights that permit the entity, by its own violation, to enable another entity to access some resource
- Often provided using an access matrix
  - One dimension consists of identified subjects that may attempt data access to the resources
  - The other dimension lists the objects that may be accessed
- Each entry in the matrix indicates the access rights of a particular subject for a particular object

OBJECTS

SUBJECTS	File 1	File 2	File 3	File 4
User A	Own Read Write		Own Read Write	
User B	Read	Own Read Write	Write	Read
User C	Read Write	Read		Own Read Write

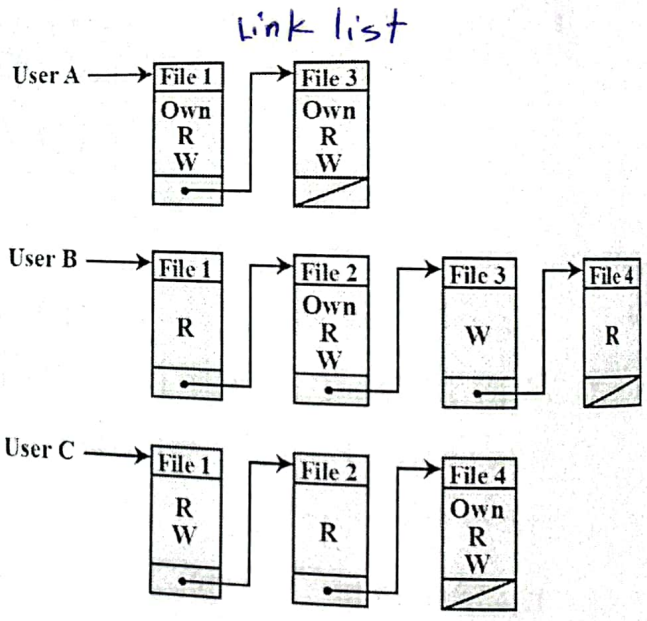
(a) Access matrix

Figure 4.2 Example of Access Control Structures



(b) Access control lists for files of part (a)

objects



(c) Capability lists for files of part (a)

subjects

Figure 4.2 Example of Access Control Structures

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

Table 4.2

Authorization Table for Files in Figure 4.2

(Table is on page 113 in the textbook)

		OBJECTS								
		subjects			files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

* - copy flag set

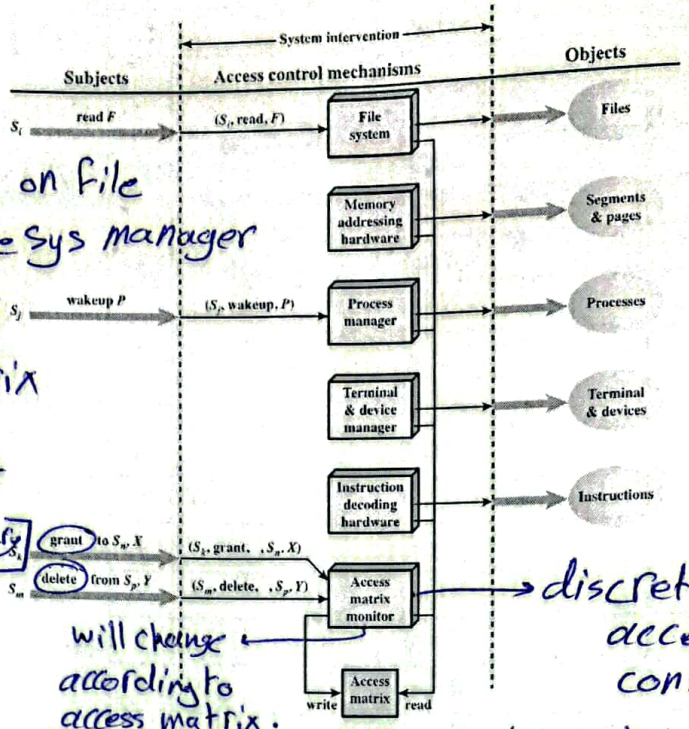
Figure 4.3 Extended Access Control Matrix

* each group of objects, has it's own control.

*any user he wants to do certain operation on file system → enter to file sys manager

*sys manager → can read From access matrix then he decide if read allowed or not

*if these subjects have the right to change access matrix. then access matrix moniter again have the right to write on access matrix



discretionary access control

will change according to access matrix.

then the subject'll have certain control on that object

Figure 4.4 An Organization of the Access Control Function

Rule	Command (by S_0)	Authorization	Operation
R1	**transfer** $\begin{Bmatrix} \alpha^* \\ \alpha \end{Bmatrix}$ **to** S, X	'α^*' in $A[S_0, X]$	store $\begin{Bmatrix} \alpha^* \\ \alpha \end{Bmatrix}$ in $A[S, X]$
R2	**grant** $\begin{Bmatrix} \alpha^* \\ \alpha \end{Bmatrix}$ **to** S, X	'owner' in $A[S_0, X]$	store $\begin{Bmatrix} \alpha^* \\ \alpha \end{Bmatrix}$ in $A[S, X]$
R3	**delete** α **from** S, X	'control' in $A[S_0, S]$ or 'owner' in $A[S_0, X]$	delete α from $A[S, X]$
R4	$w \leftarrow$ **read** S, X	'control' in $A[S_0, S]$ or 'owner' in $A[S_0, X]$	copy $A[S, X]$ into w
R5	**create object** X	None	add column for X to A; store 'owner' in $A[S_0, X]$
R6	**destroy object** X	'owner' in $A[S_0, X]$	delete column for X from A
R7	**create subject** S	none	add row for S to A; execute **create object** S; store 'control' in $A[S, S]$
R8	**destroy subject** S	'owner' in $A[S_0, S]$	delete row for S from A; execute **destroy object** S

Table 4.3 Access Control System Commands

(Table is on page 116 in the textbook)

Protection Domains

- Set of objects together with access rights to those objects
- More flexibility when associating capabilities with protection domains
- In terms of the access matrix, a row defines a protection domain
- User can spawn processes with a subset of the access rights of the user
- Association between a process and a domain can be static or dynamic
- In user mode certain areas of memory are protected from use and certain instructions may not be executed
- In kernel mode privileged instructions may be executed and protected areas of memory may be accessed

*why we need protection domain? @ telling the user, you are allowed within that domain to had certain access.

UNIX File Access Control

UNIX files are administered using inodes (index nodes)

- Control structures with key information needed for a particular file
- Several file names may be associated with a single inode
- An active inode is associated with exactly one file
- File attributes, permissions and control information are sorted in the inode
- On the disk there is an inode table, or inode list, that contains the inodes of all the files in the file system
- When a file is opened its inode is brought into main memory and stored in a memory resident inode table

Directories are structured in a hierarchical tree

- May contain files and/or other directories
- Contains file names plus pointers to associated inodes

Role access control: assign certain authorization for the Rule not for the User.

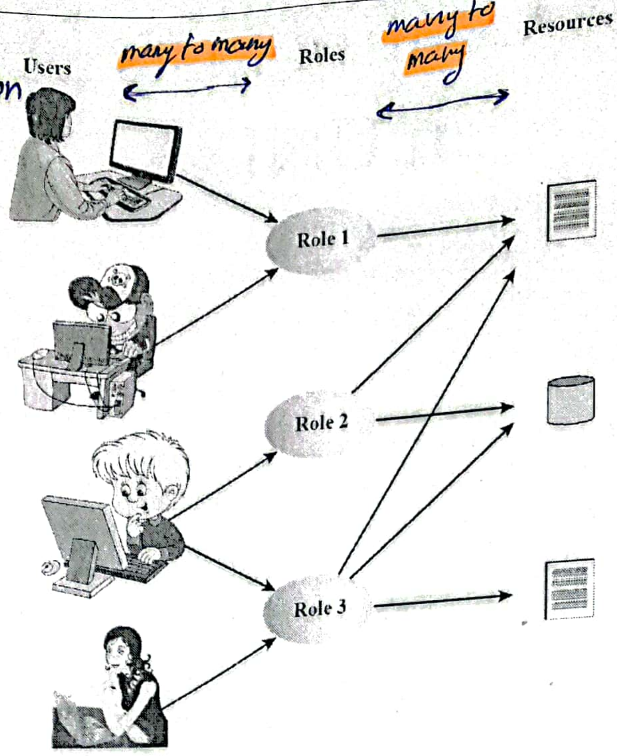


Figure 4.6 Users, Roles, and Resources

one user can play differed Roles, but what preferred in security is to give this Role, very limited number of users ولحتى تقدر تعمل [audit] للأطراف [أشياء]

explain [many to many] relation

	R_1	R_2	• • •	R_n
U_1	×			
U_2	×			
U_3		×		×
U_4				×
U_5				×
U_6				×
• • •				
U_m	×			

if R_1 can delegate R_2 * [this combine Role based and discretionary based]

OBJECTS

ROLES	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
• • •									
R_n			control		write	stop			

Figure 4.7 Access Control Matrix Representation of RBAC

you gave autherization to this Role, to give priv to Role and this Role never had this privilege.

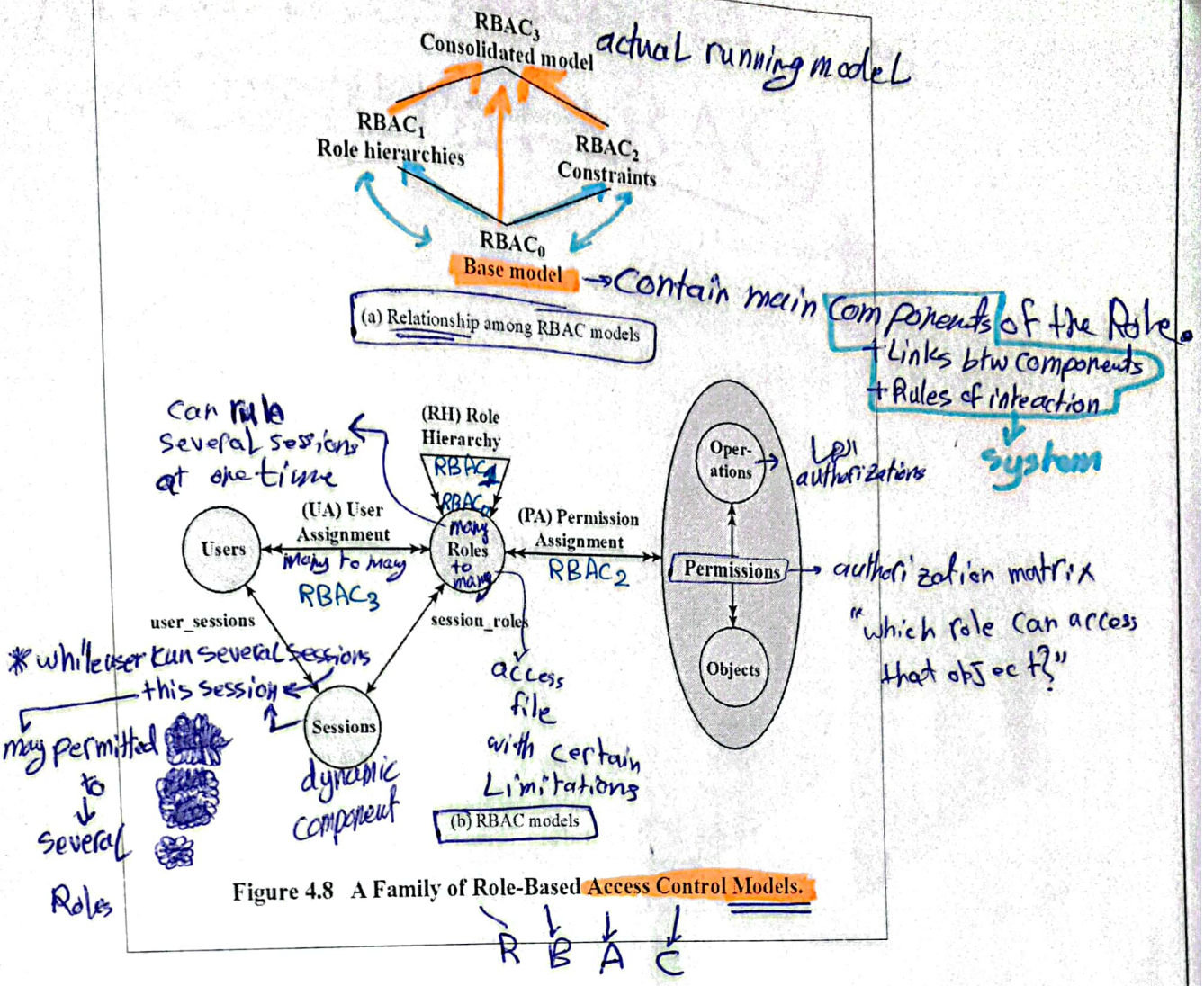


Figure 4.8 A Family of Role-Based Access Control Models.

Table 4.4
Scope RBAC Models

Models	Hierarchies	Constraints
$RBAC_0$	No	No
$RBAC_1$	Yes	No
$RBAC_2$	No	Yes
$RBAC_3$	Yes	Yes

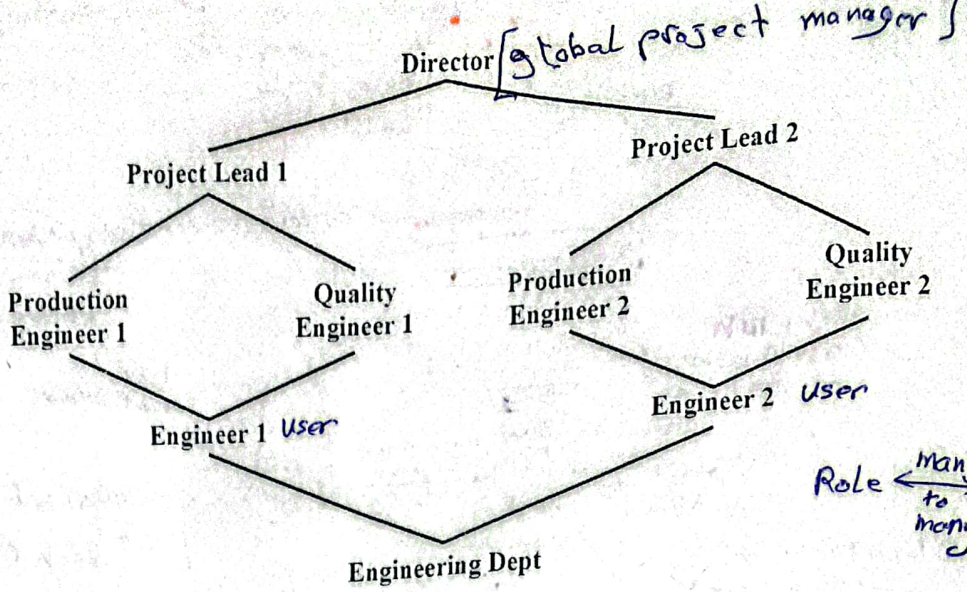


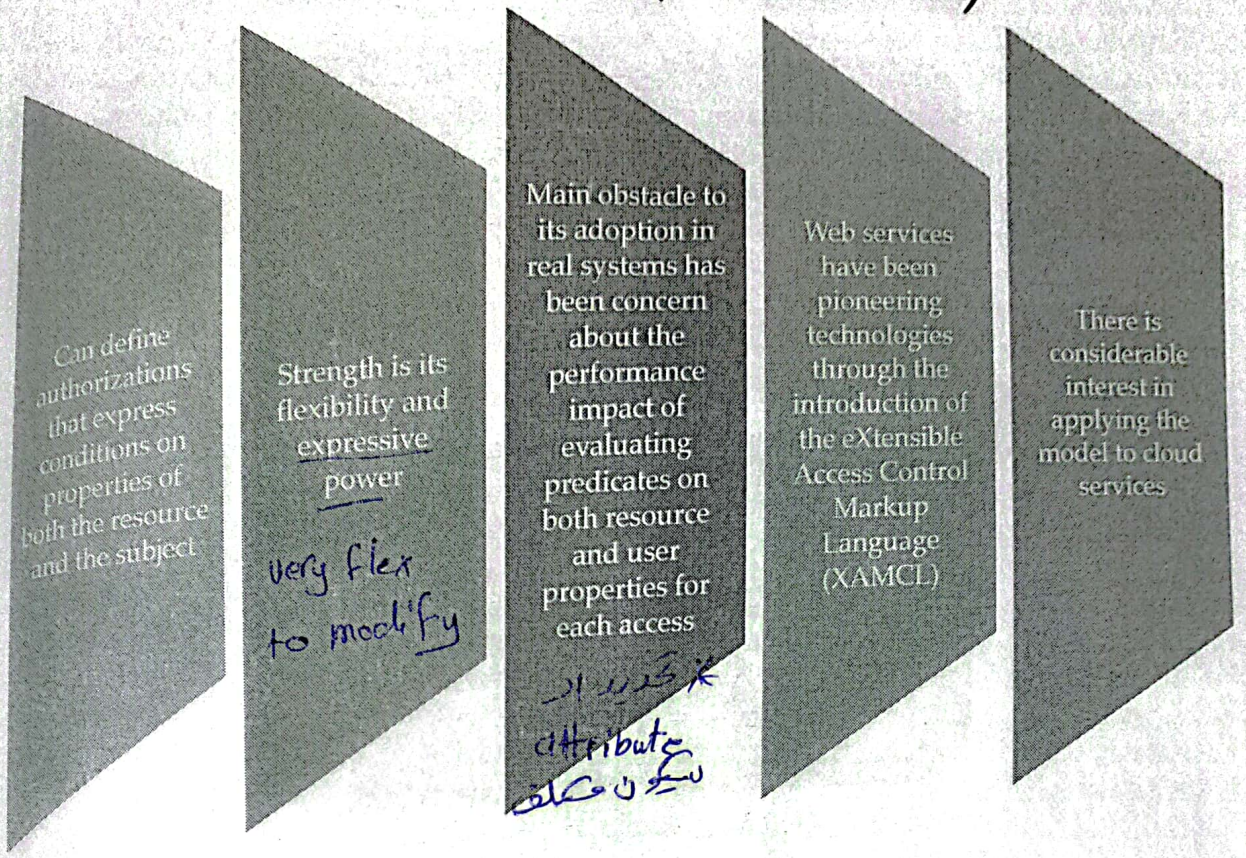
Figure 4.9 Example of Role Hierarchy

Constraints - RBAC

- Provide a means of adapting RBAC to the specifics of administrative and security policies of an organization
- A defined relationship among roles or a condition related to roles
- Types:

Mutually exclusive roles	Cardinality	Prerequisite roles
• A user can only be assigned to one role in the set (either during a session or statically) • Any permission (access right) can be granted to only one role in the set	• Setting a maximum number with respect to roles	• Dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role

Attribute-Based Access Control (ABAC)



ABAC Model: Attributes

Subject attributes

- A subject is an active entity that causes information to flow among objects or changes the system state
- Attributes define the identity and characteristics of the subject

Object attributes

- An object (or resource) is a passive information system-related entity containing or receiving information
- Objects have attributes that can be leverages to make access control decisions

Environment attributes

- Describe the operational, technical, and even situational environment or context in which the information access occurs
- These attributes have so far been largely ignored in most access control policies

موضوع الدرس _____ اليوم _____ التاريخ / /

Chapter 2a

AES : Advanced Encryption standard

block length : 128 bit

Key length ⇒ 128, 192, 256 bits

→ published by NIST

most commonly implemented Key length = 128 bit

→ contains Rounds

- Pre-round
- Main Rounds $N_r - 1$
- Rounds (N_r)

R	Key Size
10	128
12	192
14	256

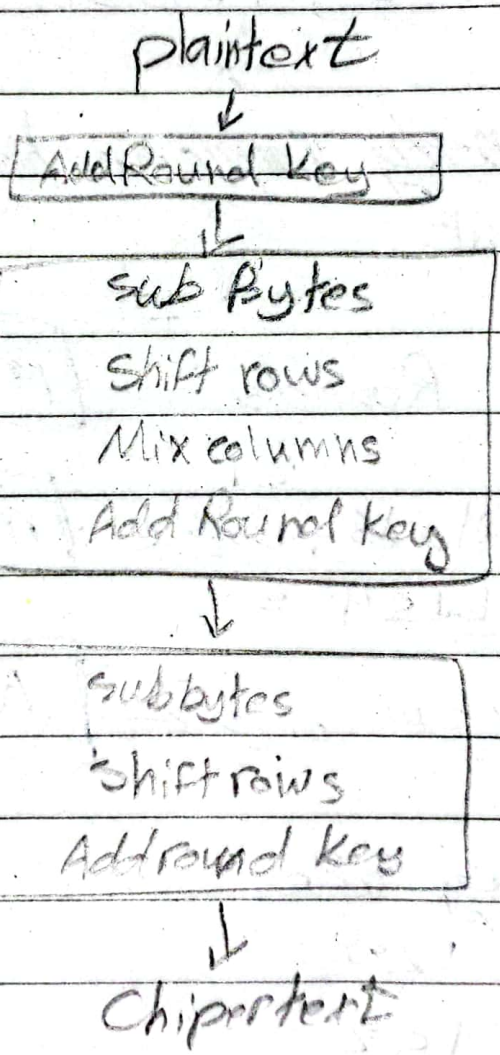
AES operates on 4x4 array of bytes called "state"

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

total = 128 bits

Column-wise order

Encryption



/ / التاريخ _____ اليوم _____ موضوع الدرس _____

→ AES requires a separate 128-bit roundkey block for each round plus one more.
(pre round)

→ Add round key :

128bit "state" XOR 128 bit "round key"

$$\begin{bmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{bmatrix} \oplus \begin{bmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{bmatrix}$$

state =

row col	row col	row col	row col
00	3C	6E	47
1F	4E	22	74
0E	08	1B	31
54	59	0B	1A

0010
0011
0 or 1→0

موضوع الدرس ____ اليوم ____ التاريخ / /

example 69 ⊕ 4B = 22

0110 1001 ⊕ 0100 1011

= 0010 0010

Subbytes : non-linear substitution

Using S-box ("in slides")

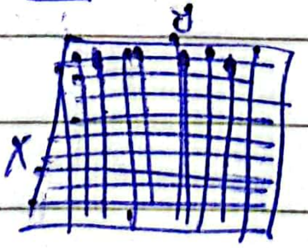
Example: " byte (6E) is substituted by the entry of the S-Box in row 6 and column " E"

ناخد من row = 6 وعامود رقمه "E" في جدول ال S-box

State matrix in previous operation ⇒ when convert it to S_box "state" =

63	EB	9F	A0
C0	2F	93	92
AB	30	AF	C7
20	CB	2B	A2

S_box

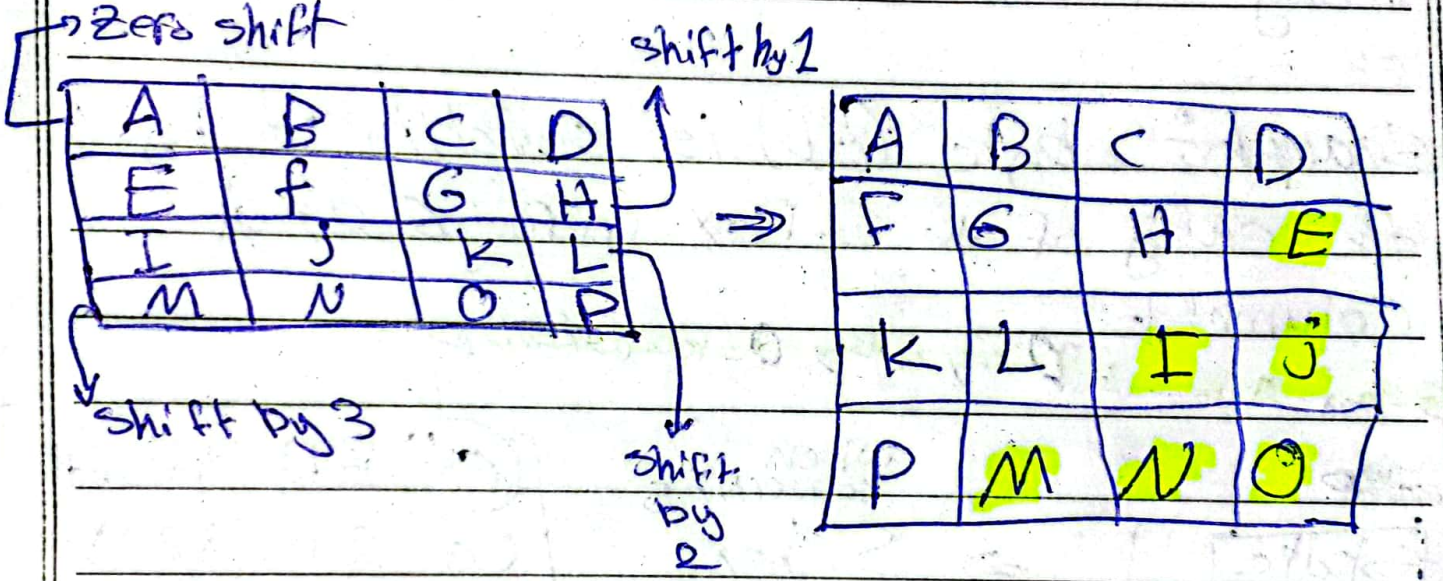


/ / التاريخ _____ اليوم _____ موضوع الدرس _____

S-box ⇒ used for encryption

Inverse S-box ⇒ used for decryption

Shift Rows: transposition step where four rows of state matrix are shifted cyclically to the left by offsets 0, 1, 2, 3.



after shifting =

$$\begin{bmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{bmatrix}$$

Mix columns : linear mixing operation

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} \text{last} \\ \text{state} \\ \text{matrix} \end{bmatrix}$$

fixed matrix in AES Algo

* عزب اول صف في الـ fixed matrix في العامود الأول لـ state matrix

وهكذا

* انتباه انه العملية بعد عزب كل عنصرين هي ليست جمع بل XOR

$$result_{0,0} = (02 \cdot S_{0,0}) \oplus (03 \cdot S_{1,0}) \oplus (01 \times S_{2,0}) \oplus (01 \cdot S_{3,0})$$

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

* The AES Decryption Algorithm :

- AddRound Key : also using XOR op
- Inverse subBytes : using inverse S-Box
- Inv shiftrows : Circular right shift
- Inv Mix columns :

Fixed_matrix_used_decry

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \cdot \begin{bmatrix} \text{last} \\ \text{sate} \\ \text{matrix} \end{bmatrix}$$

(DES) "Data Encryption standard"

Block cipher

→ DES are encrypted in 64-bit blocks using a 56-bit key

DES consists of 1) key schedule

2) round function

3) initial and final permutation

step 1 : plaintext broken into block of length 64 bits

step 2: The 64-bit block undergoes an initial permutation "IP" using initial permutation IP table.

step 3: The 64-bit permuted input is divided into "two 32-bit" blocks : left (L) and Right (R)

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

The initial values of the left & right blocks denoted L_0 & R_0

step 4 : There are 16 rounds of operations on the L & R blocks

Single round Function of the DES

↓ In 32bit . كل واحد من L و R

- Expansion

↓ 48bit

- XOR ← K_1 (48 bits)

↓ 48 bit

- Substitution

↓ 32 bit

- permutation

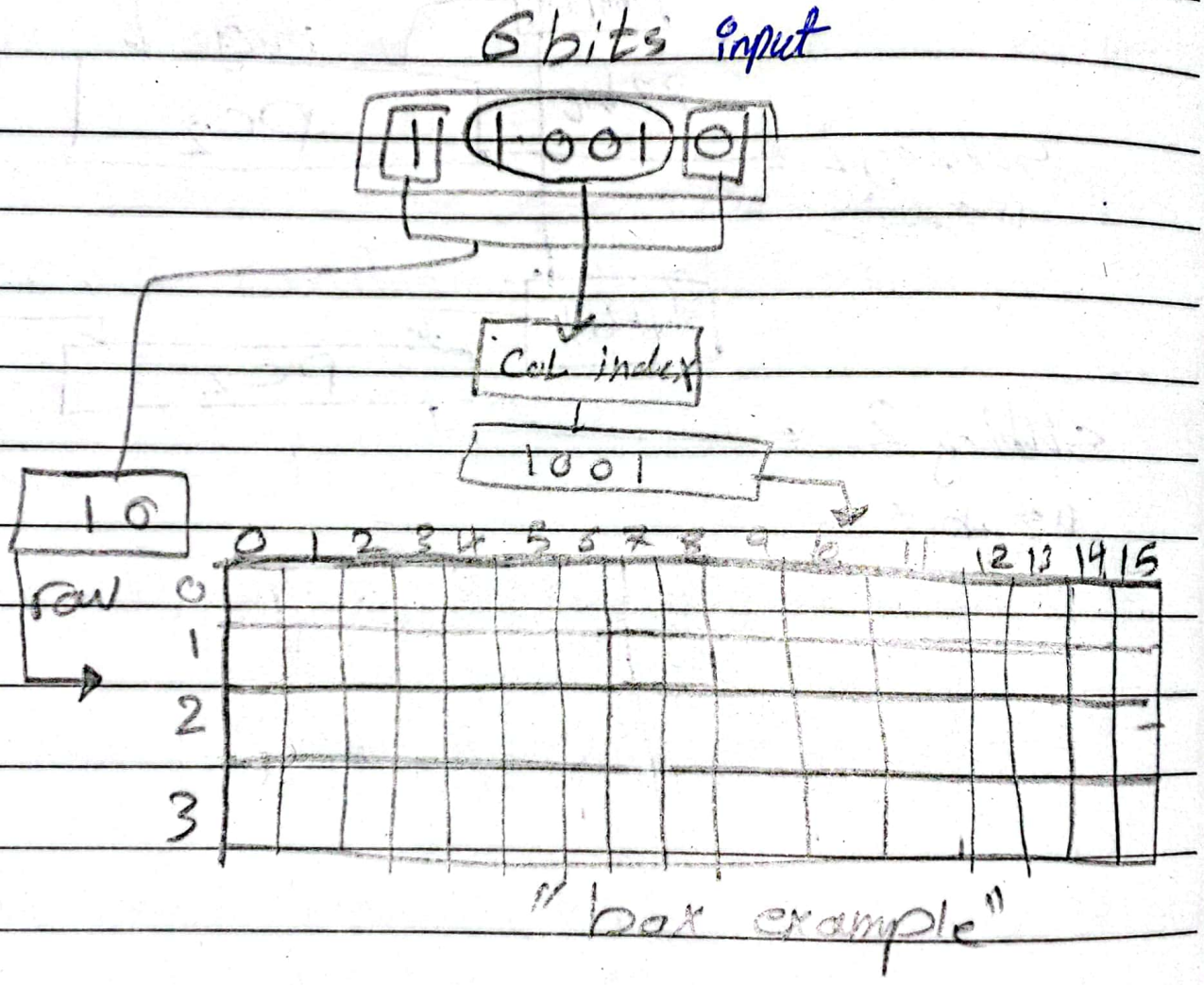
↓ 32 bit

Out

Substitution : 8 boxes

divide 48 bits into 8 boxes = 6 bits

6 x 8 = 32 bits ← 4 بطلع و بطلع 6 bit بدخل كل بوكس



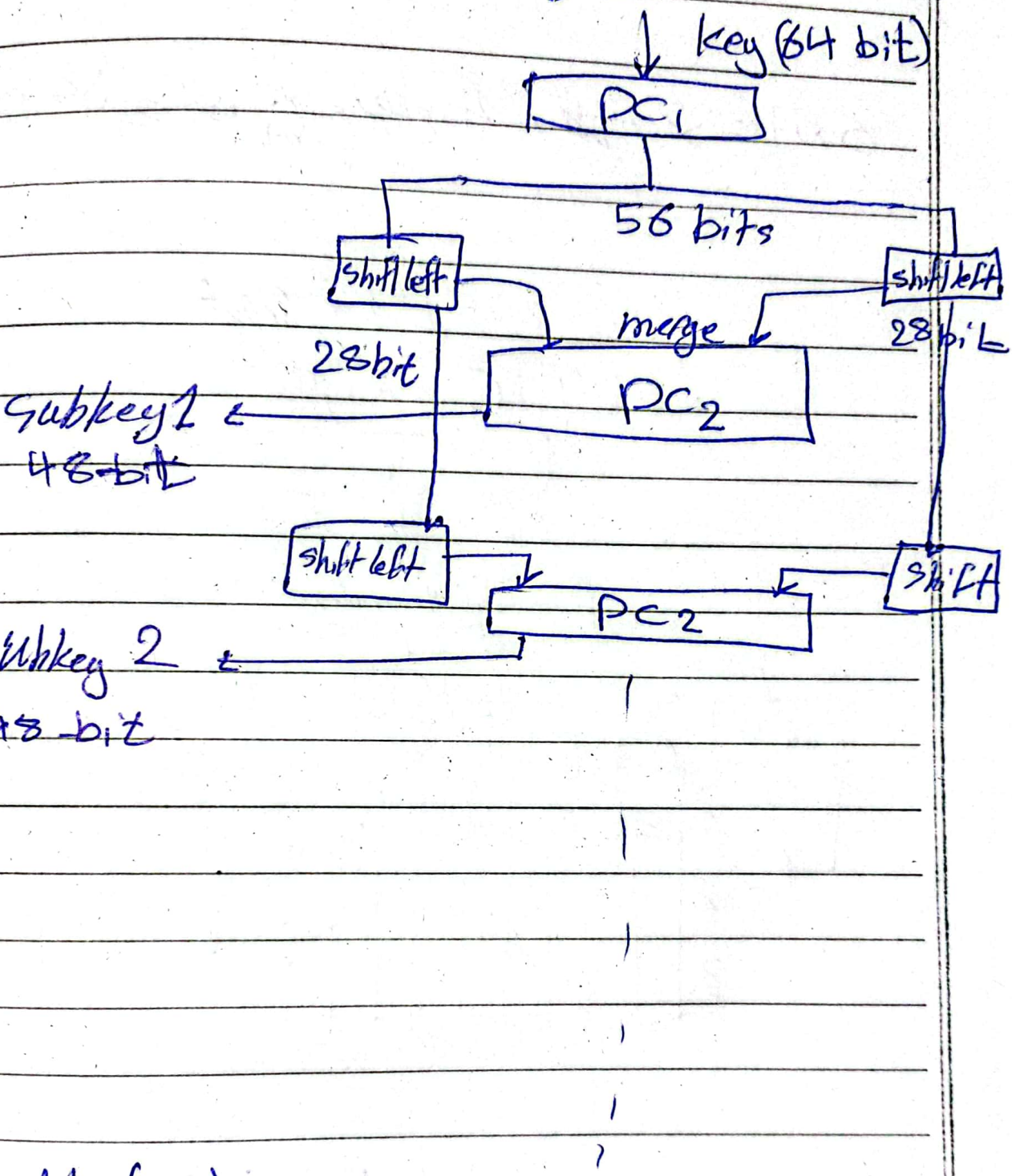
"box example"

output 4 bit digits representation

/ / التاريخ _____ اليوم _____

موضوع الدرس _____

Key schedule (generator)



PC → permuted choice

The 56 selected from initial 64 bit by PC1

Then 56 divided into 2 - 28 bit halves

- The substitution & permutation in DES provide confusion & diffusion.

DES decryption

The difference is in using the Subkeys

"in round 1 use K_{16} instead of K_1"

→ The most used attacks on block cipher are Linear and differential cryptanalysis

→ DES also vulnerable to brute-force attack

موضوع الدرس _____ اليوم _____ التاريخ / /

Triple-DES"

: apply the DES three times to each data block

→ 3-DES use "key bundle", There is 3 keys K_1, K_2, K_3 each of 56 bits

→ Encryption algorithm

$$cipherTx = E_{K3}(D_{K2}(E_{K1}(plaintext)))$$

→ decrypt :

$$plainTx = D_{K1}(E_{K2}(D_{K3}(cipherTx)))$$

→ Each Triple encryption encrypts one Block of 64 bits of data.

/ / التاريخ _____ اليوم _____

موضوع الدرس _____

* Stream cipher : operate on single bit or byte at a time

* implement some form of feedback mechanism , so that the key is constantly changing

* a key input to pseudo random number that produces a stream of n-bit numbers

* out put of generator random called " keystream"

1 byte ⊕ plaintext

stream

→ Encryption $C_i = E_k(P_i) = P_i \oplus K_i$ (plaintext)

→ Decryption $P_i = D_k(C_i) = C_i \oplus K_i$

موضوع الدرس _____ اليوم _____ التاريخ / /

Synchronous stream cipher [key independently of plaintext or state

Asynchronous S. Cipher [updated key based on previous ciphertext digits.

- important design considerations for stream cipher.

1) The encryption sequence should have large period

→ كل ما زادة period for random زادة السيكيورتي للالغوريثم
key generator

2) true random number يجب ان يكون غير تردد

واحد من شروط ان يكون عدد الـ 1 و 0 تقريباً متساوي

3) value of ss pseudo generator اعمى ١
input key

/ / التاريخ _____ اليوم _____

موضوع الدرس _____

problem of stream cipher :

1) practical problem of making large quantity of random keys

2) problem of key distribution & protection

" key of equal length is needed by both sender & reciver "

موضوع الدرس _____ اليوم _____ التاريخ / /

Block cipher Modes of operation :

* عالرسالة متكونة من اكتر من بلوك كيف اتعامل معها

→ "ECB"

encryption : الرسالة بتتقطع كل بلوكات متساوية بالطول كل بلوك باستخدام الـ K بتتشفر وبينتج عندي cipherTxT اعتبارات الـ

- طريقة سريعة بتقدر تشفر رسائل بنفس الوقت لانه كل بلوك بيقدر كل بلوك آخر

decryption : بعكس تشفير كل بلوك باستخدام نفس الـ K وبنتج عندي بلوكات الـ plainTxT اعتبارات

2) CBC

Encryption:-

① XOR بين بلوك الرسالة و الـ cipherKey
الناتج عن البلوك
اللي قبله

② تشفير ما ينتج عن الـ XOR و ينتج عنه chiperblock
نهائي

وهكذا لكل البلوكات

← بالنسبة البلوك الأول لأنه ما له cipher سابق
يستخدم initialization و يعمل XOR مع بلوك الرسالة
block

← العملية تتم Serially أبطأ

Decryption:

① decrypt التشفير مع الـ key

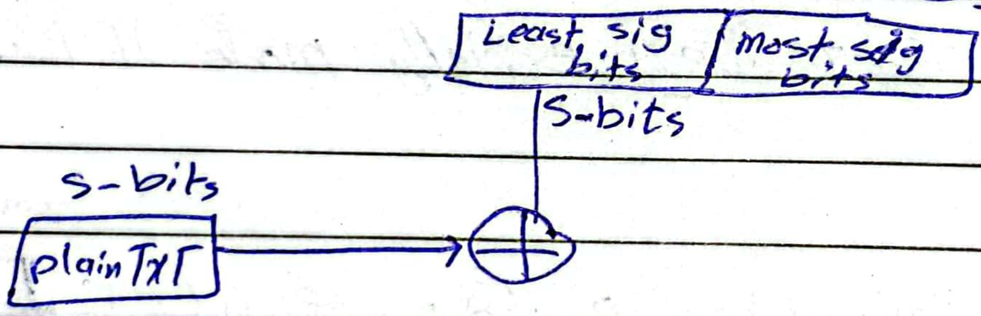
② ناتج فك التشفير XOR مع الـ cipherTxT السابق
و ينتج عنه plainTxT النهائي "

موضوع الدرس ______ اليوم ______ التاريخ / /

3) CFB :

encryption : اول ما نستخدم تشفير الرسالة (بلوكات) رح نبلش بتوليد
initialization vector
هو عبارة عن vector ممكن استخدم اي راندوم فنكشن حتى اولد
فيها الارقام العشوائية [كل ما زادت العشوائية بالارقام كل
ما زادت security الطريقة]

1) تشفير IV باستخدام ال Key وناتج التشفير تقسم
الى جزئين



قسمنا ال p الى أجزاء أصغر من البلوك [هيك كأنك مستخدم stream Mode]

2) ال cipherTxT الناتج بنجعله shift reg

ال shift reg محتوياته الاصلية باخذها من IV الاصلي ونعملها
shift left بمقدار S-bits

بنعملها Shift reg في ال bits والـ المتبقيه بمقدار s-bits
من ال cipher السابق.

وبعمل ال encrypt لـ IV كان في أول عملية على أول بلوك عندي

* Decryption :

- نفس البروسيس لكن الانبوت على XOR بيختلف
بدخل عليها cipherTxt و بيطلع plaintxt

← هذا ال mode serially أيضاً [وقت الحشر أبطأ]

4) OFB :

IV : علان تصدف و تتكرر جزء منه برسالة أخرى

- لكن في ال OFB لازم كل مرة تكون ال random مختلف تماماً وما يتكرر ولا يشبه اي IV استخدمته مسبقاً

"OFB" كل مرة أشفر رسالة جديدة لازم IV مختلف

5) "CTR"

بنبدأ باستخدام Counter بقيمة ابتدائية عشوائية

نبدأ بتشفير الـ counter مع الـ K والناتج نعمله XOR مع أول بلوك من الـ plainTxT والناتج 2 cipher TxT

وما عنعني اي فيديك المستخدمة بالبلوكات القادمة لذلك هي عملية سريعة نوعاً ما " in parallel "

بقدر أوصل لأي بلوك بدون ما انتظر اي بلوك آخر يوصلني.

"refer to slides"

/ / التاريخ ____ اليوم ____ موضوع الدرس

Key distribution

the means of delivering a key to two parties who wish to exchange data without allowing others to see the key.

- استخدام Symm encrypt في حال وجود Trusted Third part والذي هو Key distribution Center [KDC]
- Master key: لازم كل يوزر يعمله يساوي Connection وهو {shared by KDC}
- يطلب اليوزر من KDC لحتى يقدر يعمل Connect مع يوزر آخر ← Session key

موضوع الدرس _____ اليوم _____ التاريخ / /

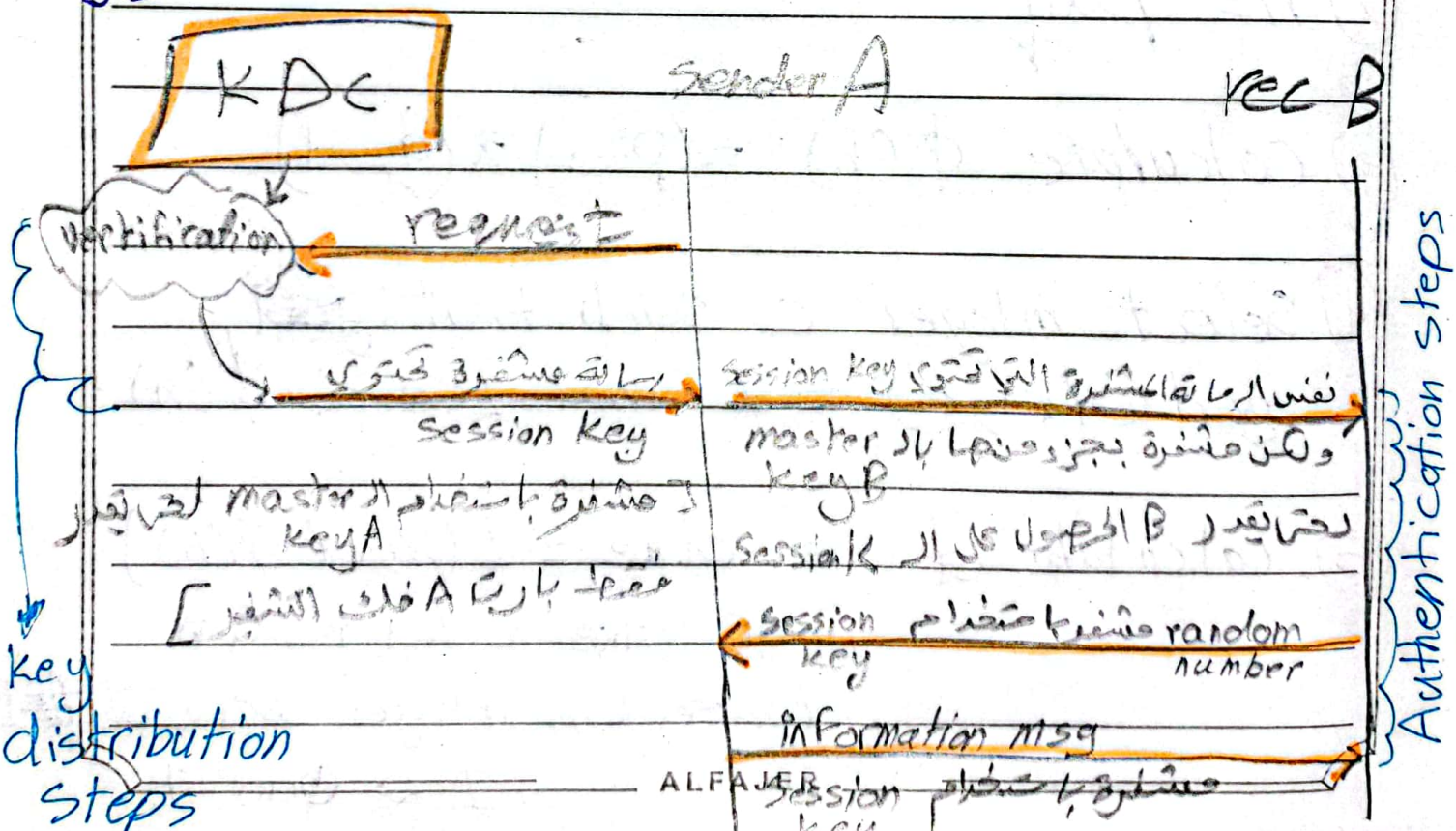
Session key : مسؤول عنه الـ KDC وهو key مؤقت لحتى تحدث عملية الـ connect بنجاح

Level1 ← master key

level2 ← session key

يعني : M.K مسؤول عن تعزيع الـ Ss.k

* أي 2 users بدهم يساووا connection لازم ينبعت request لـ KDC ويعطيهم session key وخصص لهاي التوصيل



/ / التاريخ _____ اليوم _____ موضوع الدرس _____

Chapter 21

RSA public key Cryptography.

RSA can be used for key exchange, digital signature & for encryption of small blocks of data.

To create RSA public/private key pair here are basic steps:

1. Choose 2 prime numbers p & q where $p \neq q$
2. $n = p \times q$
3. Calculate $\phi(n) = (p-1) \times (q-1)$
4. Select integer e such that: $\gcd(\phi(n), e) = 1$ and $1 < e < \phi(n)$
5. Calculate $d \rightarrow d \times e = 1 \pmod{\phi(n)}$
   or $d \times e = 1 + k \phi n$
   where k is integer btw 1 $\leftrightarrow \phi(n) - 1$

* To encrypt msg M with publick k (e, n)
then create cipherTxt using equation

$$C = M^e \bmod n$$

* The receiver then decrypts th cipherTxt with private key (d, n)

$$M = C^d \bmod n$$

/ / التاريخ _____ اليوم _____

موضوع الدرس _____

RSA Example :

① select 2 primes ⇒ $p = 17$ $q = 11$

② calculate $n = 187$

③ $\phi n = 160$

④ select e , we choose $e = 7$

⑤ $d \times e = 1 \pmod{160}$ and $d < 160$

correct value of $d = 23$ where $23 * 7 = 161$

then equal to $= 1 + (1 \times 160)$

finally $PU = \{7, 187\}$ $PR = \{23, 187\}$

موضوع الدرس _____ اليوم _____ التاريخ / /

given $M = 88$ we calculate C

$C = 88^7 \bmod 187$

$= [(88^4 \bmod 187) * (88^2 \bmod 187) * (88^1 \bmod 187)] \bmod 187$

$[132 * 77 * 88] \bmod 187 = 11$

then $M = 11^{23} \bmod 187$

simplify $[(11^1 \bmod 187) * (11^2 \bmod 187) * (11^4 \bmod 187)$

$* (11^8 \bmod 187) * (11^8 \bmod 187)] \bmod 187$

$= [11 * 121 * 55 * 33 * 33] \bmod 187 = 88$ ✓

/ / التاريخ

اليوم

موضوع الدرس

previous modular arithmetic :

① $[(a \bmod n) * (b \bmod n)] \bmod n$

$=$

$(a * b) \bmod n$

② $x^{11} = x^{1+2+8} = (x)(x^2)(x^8)$

موضوع الدرس _____ اليوم _____ التاريخ / /

The Security of RSA :

- Brute force : This involves trying all possible private keys
- mathematical attacks :
- Timing attack : depending on running time of the decryption algorithm
- Hardware fault-based attack : attacker try to make a fault in System hardware to broke this system security specially in processor that generating digital signatures
- Chosen cipher TxT attacks : cipher كل مرة يختار ويحاول يقارنه بـ الـ plainTxT ليوجد العلاقة بينهم الى كل اساليب الـ Keys Private / Public و الـ plain تم اشتقاق

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

Diffie Hellman Key exchange

*protocol enables Two users to establish secret key using a public key schem based on discrete logarithms

*primitive ~~Key~~ Root :

the primitive root of a prime number "p" as one whose powers modulo generate all integers form 1 to p-1

So, if "a" primitive number root
"p" prime number, then

$a^1 \bmod p$, $a^2 \bmod p$ ..... $a^{p-1} \bmod p$

موضوع الدرس _____ اليوم _____ التاريخ / /

for any integer "b" and primitive root "a" of prime number "p", then we can find unique exponent "i" such that

$b = a^i \pmod{p}$ where $0 \leq i \leq p-1$

*The exponent i referred to as the discrete logarithm of "b" for base "a"

steps for the algorithm :

① there Two publicly known numbers: a prime number q and an integer "a" that is primitive root of q

② Users A, B wish to exchang key K

③ User A select a random integer $X_A < q$ and computes Y_A

موضوع الدرس _____ اليوم _____ التاريخ / /

④ User B independently select random integer $X_B < q$ and computes Y_B

⑤ each side keep X value private and makes Y available publicly

Global public Elements ⇒ q, a

user A key generation ⇒ $X_A < q$, $y_A = a^{X_A} \bmod q$

user B key generation ⇒ $X_B < q$, $y_B = a^{X_B} \bmod q$

Calculation of secret key by "A" ⇒ $K = (y_B)^{X_A} \bmod q$

calculate secret key by B ⇒ $K = (y_A)^{X_B} \bmod q$

Example :

$q = 353$ Primitive root = 3

$X_A = 97$ $X_B = 233$, compute each public keys?

$Y_A = 3^{97} \bmod 353 = 40$

$Y_B = 3^{233} \bmod 353 = 248$

then the secret keys

$A \rightarrow K = (Y_B)^{X_A} \bmod 353 = 248^{97} \bmod 353 = 160$

$B \rightarrow K = (Y_A)^{X_B} \bmod 353 = 40^{233} \bmod 353 = 160$

Secret key should by the same.

موضوع الدرس _____ اليوم _____ التاريخ / /

Man in-middle Attack:

→ suppose Alice & Bob wish to exchange keys, and Darth (man in the middle) is the adversary.

attack process :

① Darth prepares for the attack by generating Two random private keys X_{D_1} , X_{D_2} and then computing the public keys Y_{D_1} Y_{D_2}

② Alice transmits Y_A to Bob as usual

③ Darth intercepts Y_A , and transmit Y_{D_1} to Bob instead of y_A transmiting

Darth also calculate $K_2 = (Y_A)^{X_{D_2}} \bmod q$

Alice — Darth — Bob

Y_A ~~Y_A~~ Y_{D_1}

④ Bob recieves Y_{D_1} and calculate

$$K_1 = (Y_{D_1})^{X_B} \bmod q$$

⑤ Bob transmit Y_B to Alice

⑥ Darth intercepts Y_B and transmit Y_{D_2} to Alice, Darth calculate $(Y_B)^{X_{D_1}} \bmod q$ (K_1)

⑦ Alice recieves Y_{D_2} and calculate

$$K_2 = (Y_{D_2})^{X_A} \bmod q$$

At this point Alice & Bob think that they share secret key, but instead Bob and Darth share K_1, and Alice & Darth share K_2

موضوع الدرس _____ اليوم _____ التاريخ / /

All future communicatio btw Bob & Alice is compromised

اي رسالة مشفرة بين Alic, Bob ← Darth قادر على إنه يفكها

Darth ⇒ ممكن يفتح الرسالة المشفرة ويغير كل محتوياتها ← active attack

passive Darth ⇒ فقط يفتح الرسالة ويقرأها attack

موضوع الدرس _____ اليوم _____ التاريخ / /

Extended Euclidean Theorem.

① Using to find the gcd (A_1, D_1)

dividend = Quotient x Divisor + reminder

$A_1 = Q_1 \times D_1 + R_1$

$A_n = Q_n \times D_n + R_n$ {So gcd = D_n

Example GCD(600, 136)

$600 = 4 \cdot 136 + 56$

$136 = 2 \cdot 56 + 24$

$56 = 2 \cdot 24 + 8$

$24 = 3 \cdot 8 + 0$

شرط التوقف اول ما $r_1 = 0$

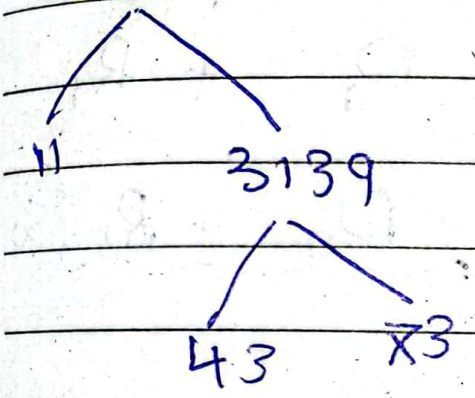
Gcd = 8

/ / التاريخ _____ اليوم _____ موضوع الدرس _____

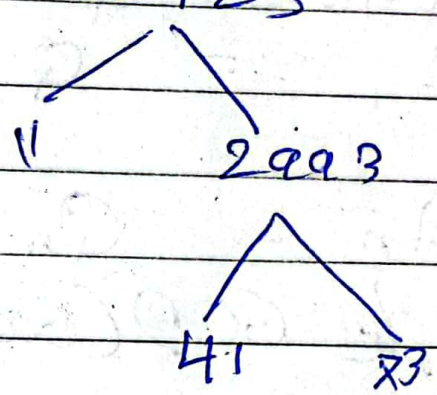
* Factorization

Find Gcd (34529, 32923)

34529



32923



34529 = 11 * 43 * 73

32923 = 11 * 41 * 73

GCD = 11 * 73 = 803

Modular Exponentiation

Allows to evaluate $a^b \equiv c \bmod d$

Methods of computing

- Brute force
- Factoring
- Memory efficient
- Successive squaring
- General fast exponentiation

refer to complementary material

Brute Force

Naïve approach.

Calculate a^b then reduce mod d

Example:

$3^3 \bmod 5 = 27 \bmod 5 = 2$

As the exponent gets larger this becomes harder

Longer time to compute.

Quickly run out of memory.

$3^{1024} \bmod 5$ difficult

Factoring

Better, if we know the factorization of a number.

If **e** factors into e=xyz then

$a^e = a^{xyz} = ((a^x)\text{^}y)\text{^}z$

Example:

Number theory

1. The integers

The set of integers $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is denoted by the symbol $\mathbb{Z}$.

Definition: Let **a**, **b** be integers. Then a divides b (equivalently: **a** is a divisor of **b**, or **a** is a factor of **b**) if there exists an integer **c** such that **b** = **ac**.

If **a** divides **b**, then this is denoted by **a**|**b**.

Example : −3|18, since 18 = (−3)(−6). (ii) 173|0, since 0 = (173)(0).

The following are some elementary properties of divisibility.

Facts (properties of divisibility)

refer to complementary material

For all **a**, **b**, **c** ∈ Z, the following are true:

(i) a|a.

(ii) If **a**|**b** and **b**|**c**, then **a**|**c**.

(iii) If **a**|**b** and **a**|**c**, then **a**|(**b**x + **c**y) for all x, y ∈ Z.

(iv) If **a**|**b** and **b**|**a**, then **a** = ±**b**.

Definition (division algorithm for integers)

If **a** and **b** are integers with **b** ≥ 1, then ordinary lon division of **a** by **b** yields integers **q** (the quotient) an **r** (the remainder) such that **a** = **qb** + **r**, where 0 ≤ r <

Introduction to Blockchain

ASSEMBLED BY: PROF. ANDRAWS SWIDAN
DESIGNED BY: MOHAMMAD SALAMEH

Block chains

refer to slides

- Data structure
- Coupled, therefore can't be altered or removed
- Distributed database

How does Blockchain Technology work?

- Cryptocurrency
- Transactions are protected through digital signature
- **Distributed Database**