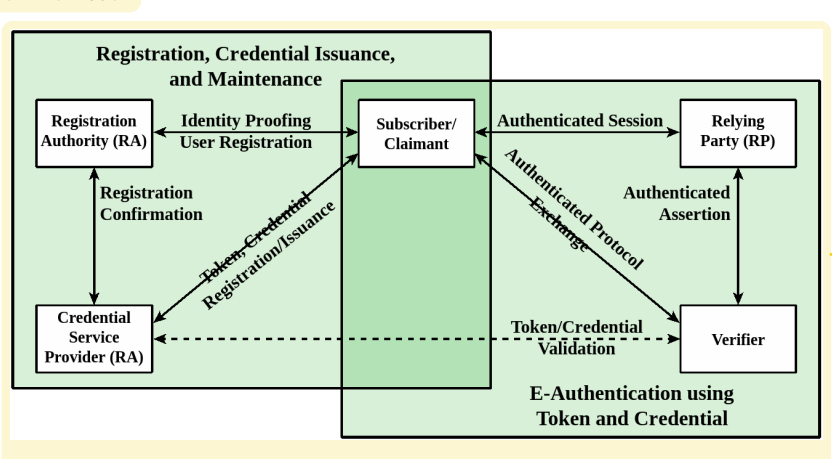
Information Security Systems

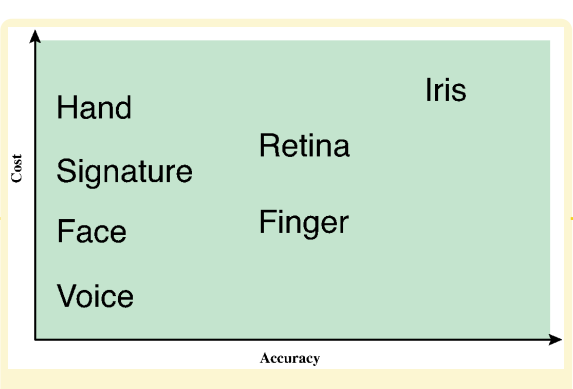
User Authentication

- **defintion**
  - The process of establishing confidence in user identities
    - that are presented electronically to an information system
- identification & authentication **requirements**
  - basic requirements
    - identify information system users
      - processes acting on behalf of users or devices
    - verify the identities of those
      - users
      - processes
      - devices
      - as a prerequisite to allowing access to organizational information systems
  - derived requirements
    - using multifactor authentication
      - for local & network access to privileged accounts
      - & for network access to non-privileged accounts
    - employ replay-resistant authentication mechanisms
      - for network access to privileged & non-privilged accounts
    - prevent reuse of identifiers for a defined preiod
    - disable identifiers after a defined period of inactivity
    - enforce a minimum password complexity
      - and change of characters when new passwords are created
    - prohibit password reuse for a specified number of generations
    - allow temporary password reuse for a specified number of generations
    - store & transmit only crytographically-protected passwords
    - obscure feedback of authentication information


Registration, Credential Issuance, and Maintenance
Registration Authority (RA)
Identity Proofing User Registration
Subscriber/ Claimant
Registration Confirmation
Tokens/Credential Registration/Issuance
Credential Service Provider (RA)
Authenticated Session
Relying Party (RP)
Authenticated Protocol Exchange
Authenticated Assertion
Token/Credential Validation
Verifier
E-Authentication using Token and Credential

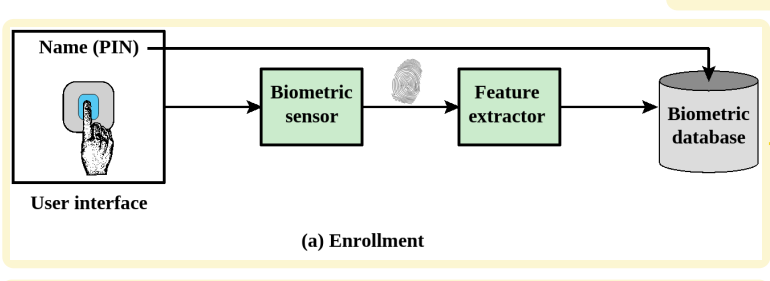
NIST Authentication Architecture Model

- **authenticating user identity is based on**
  - Something the individual knows
  - Something the individual possesses (token)
  - Something the individual is (static biometrics)
  - Something the individual does (dynamic biometrics)
- **password-based authentication**
  - Widely used line of defense against intruders
    - User provides name/login and password
    - System compares password with the one stored for that specified login
      - or the hash of it
  - the user ID
    - Determines that the user is authorized to access the system
    - Determines the user's privileges
    - Is used in discretionary access control
- **Password Vulnerabilities**
  - Offline dictionary attack
  - Specific account attack
  - Popular password attack
  - Password guessing against single user
  - Workstation hijacking
  - Exploiting user mistakes
  - Exploiting multiple password use
  - Electronic monitoring
- **Password Selection strategies**
  - User education
    - Users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords
  - Computer generated passwords
    - Users have trouble remembering them
  - Reactive password checking
    - System periodically runs its own password cracker to find guessable passwords
  - Complex password policy
    - User is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it
    - Goal is to eliminate guessable passwords while allowing the user to select a password that is memorable

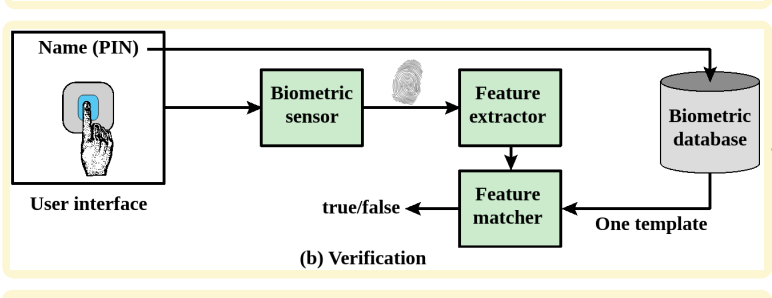


Cost & **Accuracy** in **Biometric authentication**

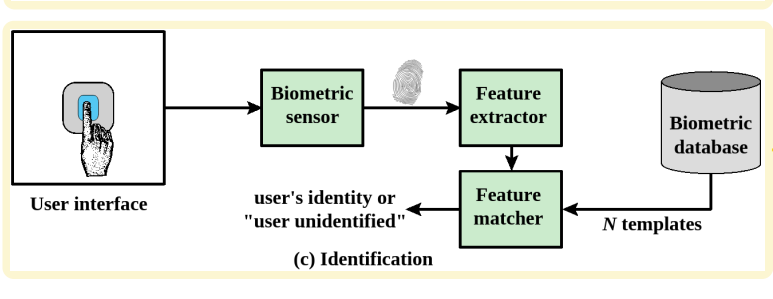
- example on biometric verification


Name (PIN)
User interface
Biometric sensor
Feature extractor
Biometric database

(a) Enrollment

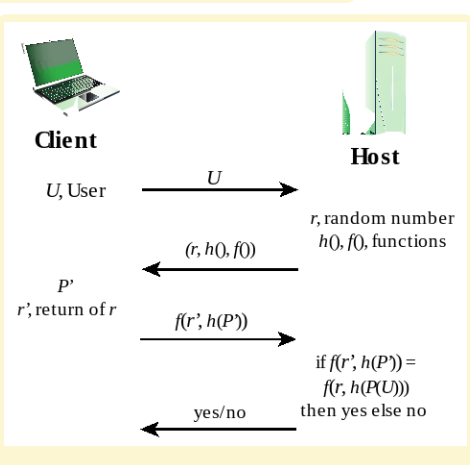

Name (PIN)
User interface
Biometric sensor
Feature extractor
Biometric database
true/false
Feature matcher
One template

(b) Verification

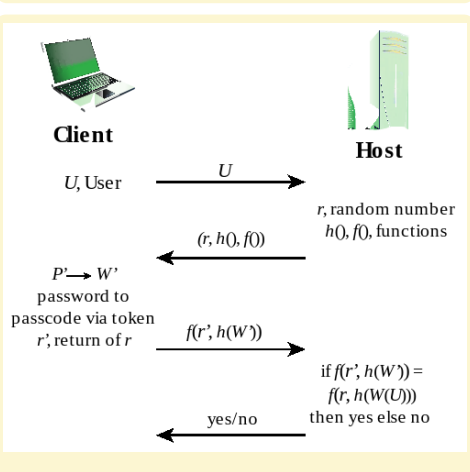

User interface
Biometric sensor
Feature extractor
Biometric database
user's identity or "user unidentified"
Feature matcher
N templates

(c) Identification

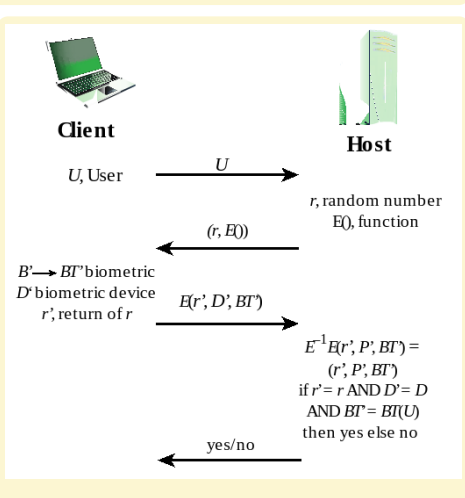
- **Remote User Authentication**
  - definition
    - Authentication over a network
  - adds
    - Additional security threats such as
      - Eavesdropping
      - capturing a password
      - replaying an authentication sequence that has been observed
  - basic protocols for remote auth.


Client
Host
U, User
U
r, random number
h(), f(), functions
(r, h(), f())
P'
r', return of r
f(r', h(P'))
if f(r', h(P')) = f(r, h(P(U))) then yes else no
yes/no

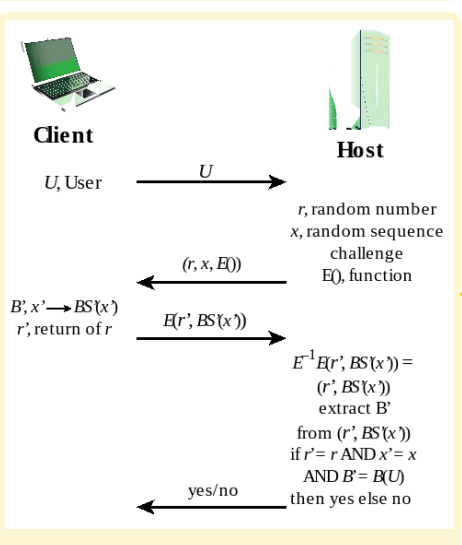
Protocol for a password


Client
Host
U, User
U
r, random number
h(), f(), functions
(r, h(), f())
P' → W'
password to passcode via token
r', return of r
f(r', h(W'))
if f(r', h(W')) = f(r, h(W(U))) then yes else no
yes/no

Protocol for a token


Client
Host
U, User
U
r, random number
E(), function
(r, E())
B' → BT' biometric
D' biometric device
r', return of r
E(r', D', BT')
E⁻¹E(r', P', BT') = (r', P', BT')
if r' = r AND D' = D AND BT' = BT(U) then yes else no
yes/no

Protocol for static biometric

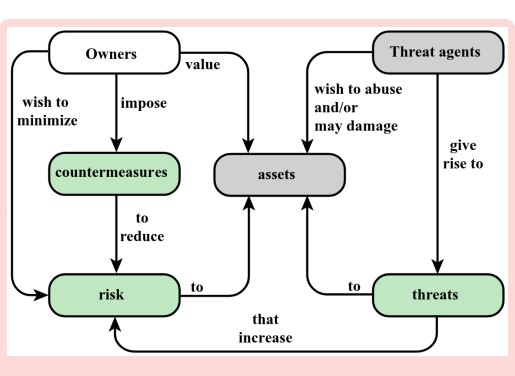

Client
Host
U, User
U
r, random number
x, random sequence challenge
E(), function
(r, x, E())
B', x' → BS'(x')
r', return of r
E(r', BS'(x'))
E⁻¹E(r', BS'(x')) = (r', BS'(x'))
extract B' from (r', BS'(x'))
if r' = r AND x' = x AND B' = B(U) then yes else no
yes/no

Protocol for static biometric

- **Authentication Security Issues**
  - **Eavesdropping**
    - attempts to learn the password by some sort of attack that involves the physical proximity of user and adversary
  - **Replay**
    - repeats a previously captured user response
  - **Host Attacks**
    - Directed at the user file at the host
      - where passwords, token passcodes, or biometric templates are stored
  - **Client Attacks**
    - attempts to achieve user authentication
      - without access to the remote host or the intervening communications path
  - **Trojan Horse**
    - application or physical device
      - masquerades as an authentic application
      - for the purpose of capturing a user password, passcode, or biometric
  - **Denial-of-Service**
    - disable a user authentication service
      - by flooding the service with numerous authentication attempts

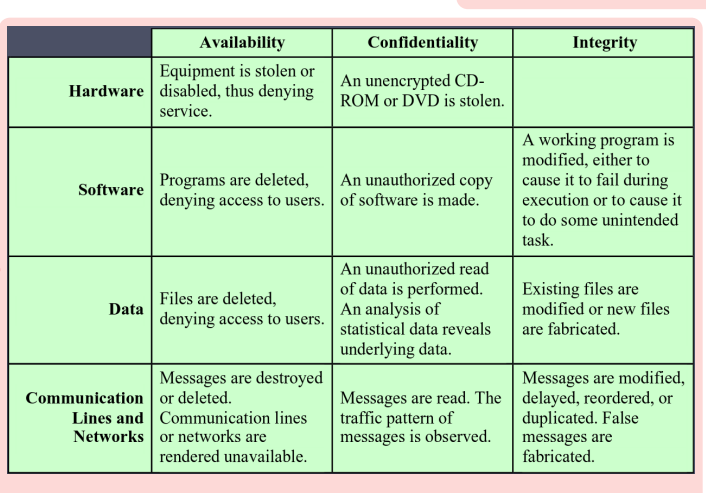
Overview

- Key Security Concepts
  - **Confidentiality** — Preserving authorized restrictions on information access
  - **Integrity** — Guarding against improper information modification or destruction
  - **Availability** — Ensuring timely and reliable access to and use of information
- Levels of Impact
  - **Low** — The loss could be expected to have a **limited** adverse effect
  - **Medium** — The loss could be expected to have a **serious** adverse effect
  - **High** — The loss could be expected to have a **severe** adverse effect


Owners
value
wish to minimize
impose
countermeasures
to reduce
risk
to
assets
Threat agents
wish to abuse and/or may damage
give rise to
threats
to
that increase

Important **Terminology**

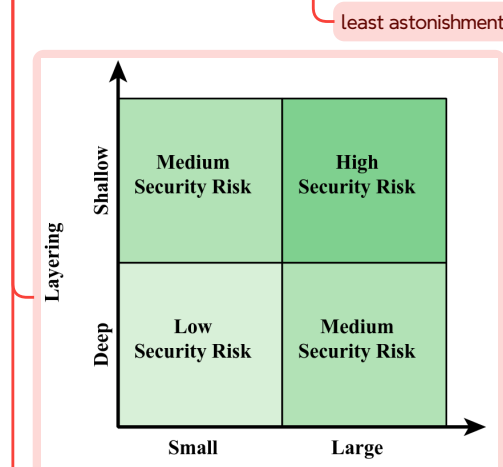
- **Attack** — Any kind of malicious activity — that attemps to
  - collect
  - disrupt
  - deny
  - degrade
  - destroy
  - information or system resources
- **Countermeasure** — device or techniques
  - that counter the undesirable or adversarial activity
  - or to prevent
    - espionage
    - sabotage
    - theft
    - unauthorized access
    - use of
    - sensitive information or information system
- **Risk**
  - measure of the extent to which an entity is threatened by a potential circumstance or event
  - consists of
    - the impact if the risk happened
    - likelihood of occurrence
- **Security Policy** — set of criteria for the provision of security services
- **Assets**
  - Hardware
  - Software
  - Data
  - Communication facilities & networks
- **Threat** — Any circumstance or event with the potential to adversely impact organizational operations, assets, individuals via
  - unauthorized access
  - destruction
  - disclosure
  - modification of information
  - denial of service
- **Vulnerability** — Weakness in an information system — could be exploited or triggered by a threat source
- Categories of **vulnerabilities**
  - **Corrupted** — loss of integrity
  - **Leaky** — loss of confidentiality
  - **Unavailable or very slow** — loss of availability
- **Attacks**
  - **Passive**
    - attempt to learn or make use of information from the system that does not affect system resources
    - 2 types
      - Release of message contents
      - Traffic analysis
  - **Active**
    - attempt to alter system resources or affect their operation
    - 4 types
      - Replay
      - Masquerade
      - Modification of messages
      - Denial of service
  - **Insider** — initiated by an entity inside the security parameter
  - **Outsider** — initiated from outside the perimeter
- **Countermeasures**
  - means used to deal with security attacks
    - prevent
    - detect
    - recover
  - may itself introduce new vulnerabilities
  - Goal is to minimize residual level of risk to the assets
  - Residual vulnerabilities may remain
- **Threat types**
  - **Unautherized disclosure**
    - accessing data where it's not authorized
    - **Exposure** — Sensitive data are directly released to unauthorized entity
    - **Interception** — unauthorized entity directly accesses sensitive data traveling between authorized sources & destinations
    - **Inference** — like exposure but it's an indirect threat
    - **Intrusion** — like exposure but it gains access by circumventing a system security protection
  - **Deception**
    - receiving false data and believe it to be true
    - **Masquerade** — unauthorized entity gains access to a system by posing as autherized entity
    - **Falsification** — False data deceive an authorized entity
    - **Repudiation** — Entity deceives another by falsely denying responsibility for an act
  - **Disruption**
    - preventing the correct operation of system services and functions
    - **Incapacitation** — prevents or interrupts system operation by disabling a system component
    - **Corruption** — Undesirably alters system operation by adversely modifying system function or data
    - **Obstruction** — threat action that interrupts delivery of system services by hindering system operation
  - **Usurpation**
    - controlling of system services or functions by unauthorized access
    - **Misappropriation** — assuming unauthorized logical or physical control of a system resource
    - **Misuse** — Causes a system to perform a function or a service by hindering system operation



	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Computer & Network Assets

- **Security Requirements**
  - **access control** — limit information system access to authorized users (or processes)
  - **awareness & training** — ensure that users are aware of security risks
  - **Audit & accountability** — record to be able to report
  - **Certification & accreditation & security assessements** — for validation
  - **Configuration management**
    - make & maintain base configs
    - make & enforce security
  - **Contengency planning** — make & maintain & implement plans for emergency
  - **Identification & authentication** — for verification
  - **Incident response** — make sure we can handle incidents & report them
  - **Maintenance** — periodic maintenance in effective way
  - **Media Protection**
    - protection
    - limiting access
    - sanitize — before disposal
    - Media
  - **Physical & environmental protection**
    - limiting physical access to information
    - protecting physical infrastructure
    - protecting against environmental hazards
  - **Planning** — developing & documenting & implementing security plans
  - **Personnel security** — ensure that we can trust the employees and meet the security criteria
  - **Risk assessment** — periodically assess the risk to organizational assets & individuals
  - **Systems & services acquisition** — allocating sufficient resources to protect information systems
  - **System & communication protection**
    - monitor & control & protect communications
    - design architecture & techniques
    - for effective security
  - **System & information integrity**
    - identify
    - report
    - correct
    - information & information systems
    - protect against malicious code
    - monitor security alerts — take appropriate actions in response
- **Security Design Principles**
  - Economy of mechanism
  - fail-safe defaults
  - complete mediation
  - open design
  - seperation of privilage
  - least privilege
  - least common mechanism
  - psychological acceptability
  - isolation
  - encapsulation
  - modularity
  - layering
  - least astonishment

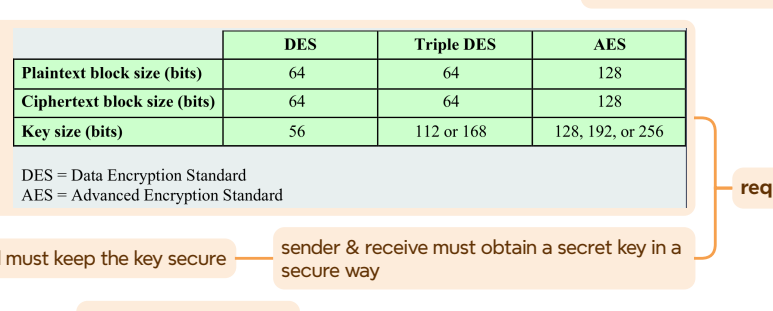

Layering
Shallow
Deep
Medium Security Risk
High Security Risk
Low Security Risk
Medium Security Risk
Small
Large
Attack Surface

Attack Surfaces Categories

- **Network** Attack Surface — vulnerabilities over the network
- **Software** Attack Surface — vulnerabilities in
  - applications
  - utility
  - operating system
- **Human** Attack Surface — vulnerabilities created by personnel or outsiders — like social engineering or human error
- **Computer Security Strategy**
  - **Security Policy** — rules & practices the regulate how system or organization provides security services
  - **Security Implementation**
    - prevention
    - detection
    - response
    - recovery
  - **Assurance** — to make sure we implement what we designed
  - **Evaluation** — examining computer product or system with respect to certain criteria

Cryptographic Tools

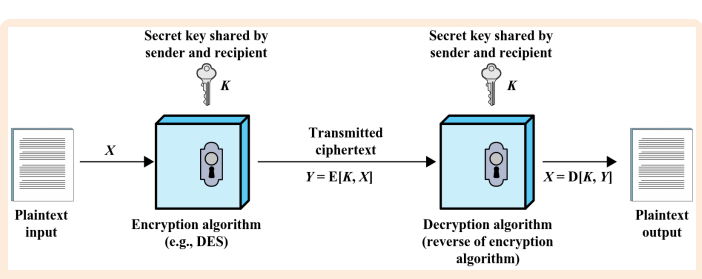
- definition
  - the universal technique for providing confidentiality for transmitted or stored data
  - aka
    - conventional encryption
    - single-key encryption
- **requirements** for secure use
  - strong encryption algorithm like



	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

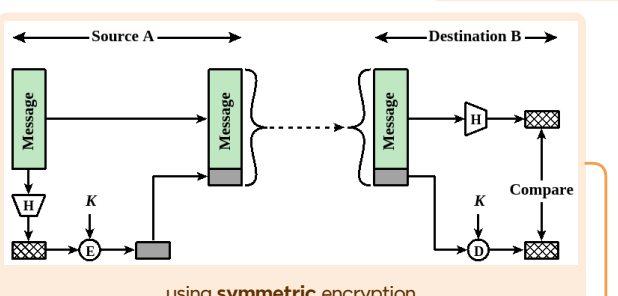
DES = Data Encryption Standard
AES = Advanced Encryption Standard

  - sender & receive must obtain a secret key in a secure way
    - and must keep the key secure
- **attacking** symmetric encryption
  - **cryptanalysis** attacks
    - rely on
      - Nature of the algorithm
      - Some knowledge of the general characteristics of the plaintext
      - Some sample plaintext-ciphertext pairs
    - it exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
      - if successful all future and past messages encrypted with that key are compromised
  - **brute-force** attacks
    - trying all possible keys on some ciphertext until one succeed

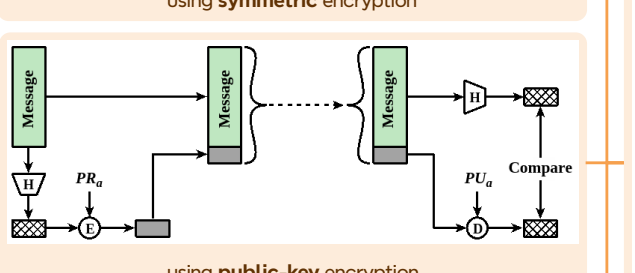

Secret key shared by sender and recipient
K
Plaintext input
X
Encryption algorithm (e.g., DES)
Transmitted ciphertext
Y = E[K, X]
Decryption algorithm (reverse of encryption algorithm)
X = D[K, Y]
Plaintext output

Symmetric Encryption

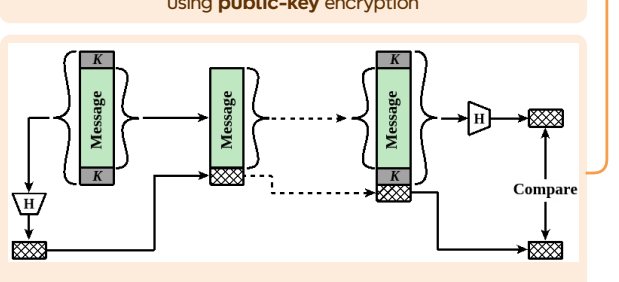
- **DES (Data Encryption Standard)**
  - it was the most widely used encryption scheme
  - uses 64 bit plaintext block
    - and uses a 56 bit key
      - the key size here is small to the day standards of computing
  - **3DES (Triple DES)**
    - repeats DES 3 times
    - using 2 or 3 keys
    - kinda slow as software
- **AES (Advanced Encryption Standard)**
  - replacement for 3DES
  - 128 bit data
  - 128/192/256 bit keys
- **Block & Stream ciphers**
  - **Block ciphers**
    - processes the input one block at a time
    - outputs one at a time too
    - can reuse keys
    - common
  - **Stream ciphers**
    - processes input continuously
    - produces output one element at a time
    - faster and use less code
    - encrypts plaintext one byte at a time
    - pseudorandom stream is unpredicatable without knowledge of the input key
- **Message Authentication**
  - what does it do?
    - protect against active attacks
    - verifies recieved message is authentic
      - contents have not been altered
      - from authentic source
      - timely & in correct sequence
    - can use conventional encryption
  - authentication without confidentiality
    - message encryption may not provide a secure form of authentication
      - so typically message authentication is provided as seperate function from message encryption
    - cases
      - when the message is broadcasted
      - exchange during heavy load


Source A
Destination B
Message
H
K
E
D
Compare

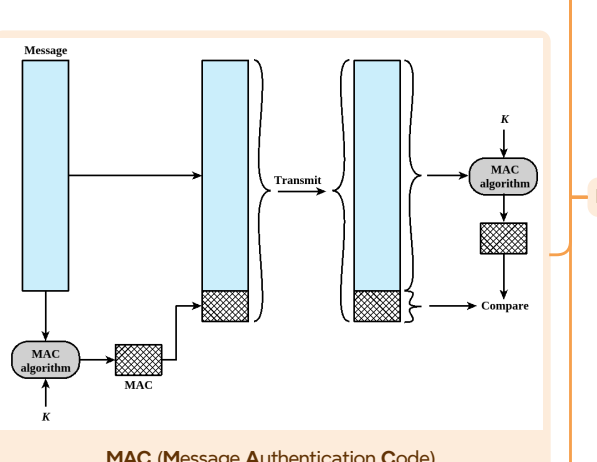
using **symmetric** encryption


Message
H
PRa
E
PUa
D
Compare

using **public-key** encryption

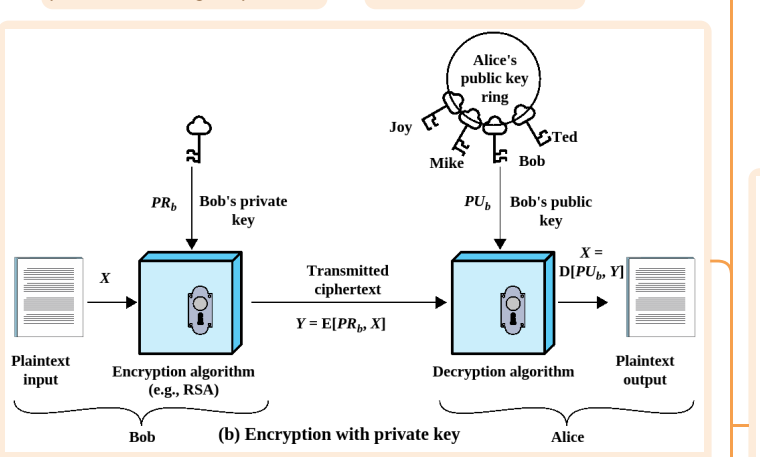

Message
K
H
Compare

using **secret value**


Message
K
MAC algorithm
MAC
Transmit
Compare

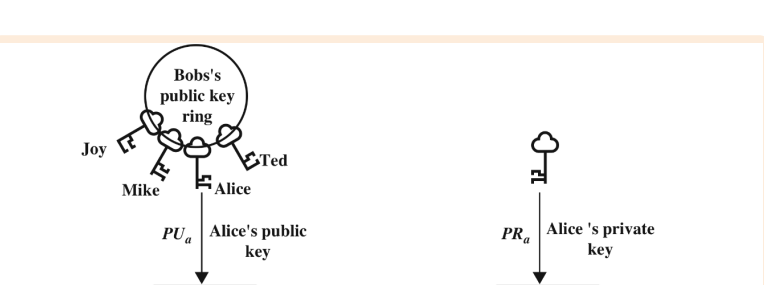
MAC (**M**essage **A**uthentication **C**ode)

  - hash function for message authentication 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
      - computationally infeasible to find x such that H(x) = h
    - computationally infeasible to find y != x such that H(y) = H(x)
    - computationally infeasible to find any pair (x,y) such that H(x) = H(y)
- what is it?
  - proposed by diffie & hellman
  - based on mathematical functions
  - **asymmetric**
    - uses 2 separate keys
      - public key — public to others
      - private key — only owner know it
  - a protocol is needed for distribution
- **scheme**
  - **Plaintext** — readable message or data fed into an algorithm as input
  - **encryption algorithm** — performs transformations on the plaintext
  - **public & private key** — pair of keys
    - one for encryption
    - one for decryption
  - **ciphertext** — scrambled message produced as output
  - **decryption algorithm** — produces the original plaintext


Alice's public key ring
Joy
Mike
Bob
Ted
PRb
Bob's private key
PUb
Bob's public key
Plaintext input
X
Encryption algorithm (e.g., RSA)
Transmitted ciphertext
Y = E[PRb, X]
Decryption algorithm
X = D[PUb, Y]
Plaintext output
Bob
Alice

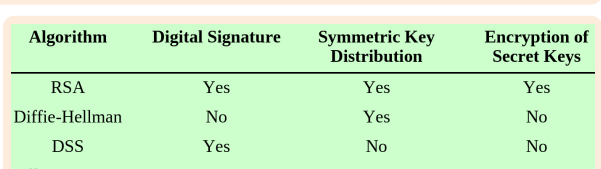
(b) Encryption with private key

Public-Key Encryption but we encrypt with private key


Bobs's public key ring
Joy
Mike
Alice
Ted
PUa
Alice's public key
PRa
Alice 's private key
Plaintext input
X
Encryption algorithm (e.g., RSA)
Transmitted ciphertext
Y = E[PUa, X]
Decryption algorithm
X = D[PRa, Y]
Plaintext output
Bob
Alice

(a) Encryption with public key

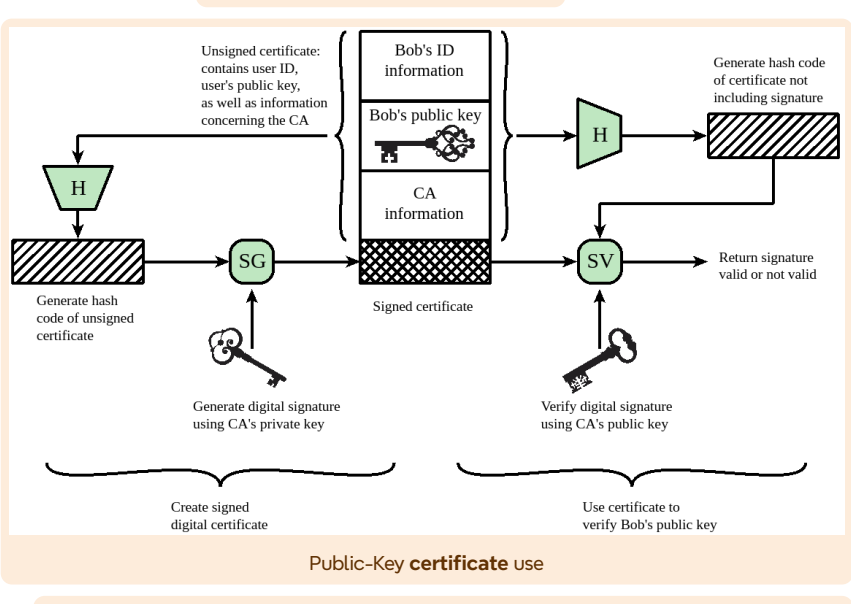
Public-Key Encryption



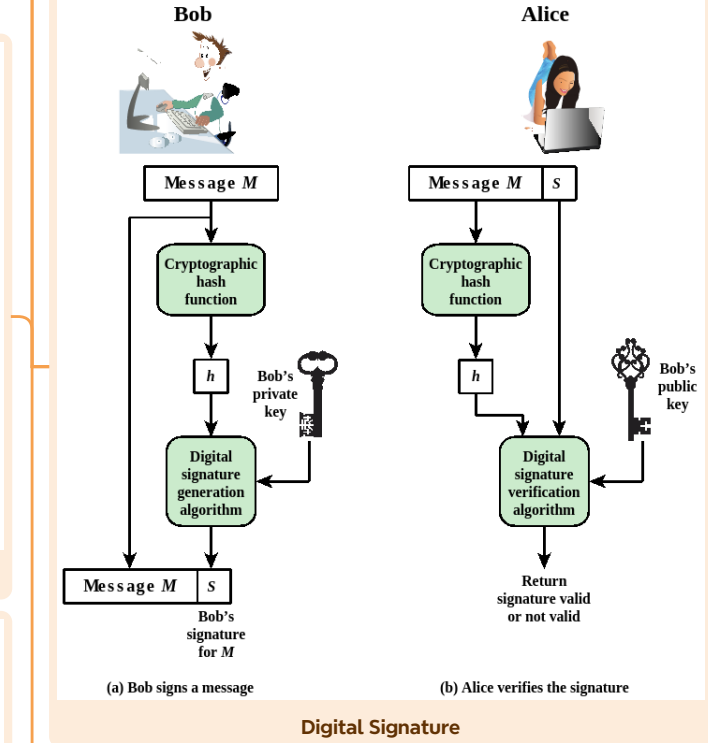
Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
RSA	Yes	Yes	Yes
Diffie-Hellman	No	Yes	No
DSS	Yes	No	No
Elliptic Curve	Yes	Yes	Yes

applications for public-key cryptosystems

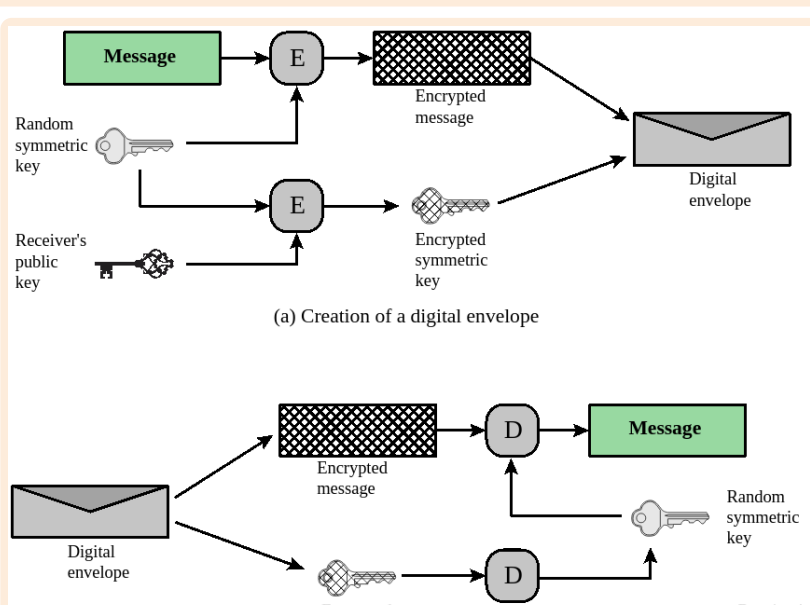
- **Requirements**
  - Computationally **easy** to **create key** pairs
  - Computationally **easy** for sender knowing public key to **encrypt** messages
  - Computationally **easy** for receiver knowing private key to **decrypt** ciphertext
  - Useful if either **key** can be used for **each role**
  - Computationally **infeasible** for opponent to **determine private** key from public key
  - Computationally **infeasible** for opponent to otherwise **recover** original message
- **Encryption Algorithms**
  - **RSA** (**R**ivest, **S**hamir, **A**dleman) — widely accepted & implemented approach in public-key encryption
  - **Diffie-Hellman** key exchange algorithm
    - enables 2 users to securely reach agreement about a shared secret key
    - limited to the exchange of the keys
  - **DSS** (**D**igital **S**ignature **S**tandard) — provides a digital signature function with SHA-1
  - **ECC** (**E**lliptic **C**urve **C**ryptograohy) — security like RSA but with much smaller keys
- to verify
  - origin authentication
  - data integrity
  - signatory non-repudiation
- we have 3 digital signature
  - **DSA** (**D**igital **S**ignature **A**lgorithm)
  - RSA Digital Signature Algorithm
  - **ECDSA** (**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm)


Unsigned certificate: contains user ID, user's public key, as well as information concerning the CA
Bob's ID information
Bob's public key
CA information
H
SG
SV
Generate hash code of unsigned certificate
Signed certificate
Generate hash code of certificate not including signature
Return signature valid or not valid
Generate digital signature using CA's private key
Verify digital signature using CA's public key
Create signed digital certificate
Use certificate to verify Bob's public key

Public-Key **certificate** use


Bob
Alice
Message M
Cryptographic hash function
h
Bob's private key
Digital signature generation algorithm
Message M
S
Bob's signature for M
Bob's public key
Digital signature verification algorithm
Return signature valid or not valid
(a) Bob signs a message
(b) Alice verifies the signature

Digital Signature


Message
E
Encrypted message
Random symmetric key
Receiver's public key
Encrypted symmetric key
Digital envelope
D
Receiver's private key

(a) Creation of a digital envelope

Digital Envelopes

- **Random Numbers**
  - **use cases**
    - keys for public-key algorithms
    - stream keys for symmetric stream cipher
    - digital envelope
    - Handshaking to prevent replay attacks
    - session key
  - **requirements**
    - randomness
      - 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
      - Opponent should not be able to predict future elements of the sequence on the basis of earlier elements
  - Random versus Pseudorandom
    - Algorithms are deterministic and therefore produce sequences of numbers that are not statistically random
    - Pseudorandom numbers
      - Sequences produced that satisfy statistical randomness tests
      - Likely to be predictable
    - **TRNG** (**T**rue **R**andom **N**umber **G**enerator)
      - Uses a nondeterministic source to produce randomness
      - Most operate by measuring unpredictable natural processes
      - Increasingly provided on modern processors

For more MindMaps
Check our Blitz Website
https://blitz.deveopix.com/

Created by
Omar Alkhateeb

Presented with xmind