Computer Security

CS433

Chapter 2:

Authentication, Access Control, and Cryptography

Objectives

- Survey authentication mechanisms
- List available access control implementation options
- Explain the problems encryption is designed to solve
- Understand the various categories of encryption tools as well as the strengths, weaknesses, and applications of each
- Learn about certificates and certificate authorities

Authentication

Authentication

The act of proving that a user is who she says she is

Methods:

- ✓ Something the user *knows*
- ✓ Something the user *is*
- ✓ Something user *has*

Identification is asserting who a person is.

Authentication is proving that asserted identity.

Something You Know

Can be:

- Passwords
- Security questions

Attacks on "something you know":

- Dictionary attacks
- Inferring likely passwords/answers
- Guessing
- Defeating concealment
- Exhaustive or brute-force attack
- Rainbow tables

Every password can be guessed; password strength is determined by how many guesses are required.

Password Storage

Plaintext

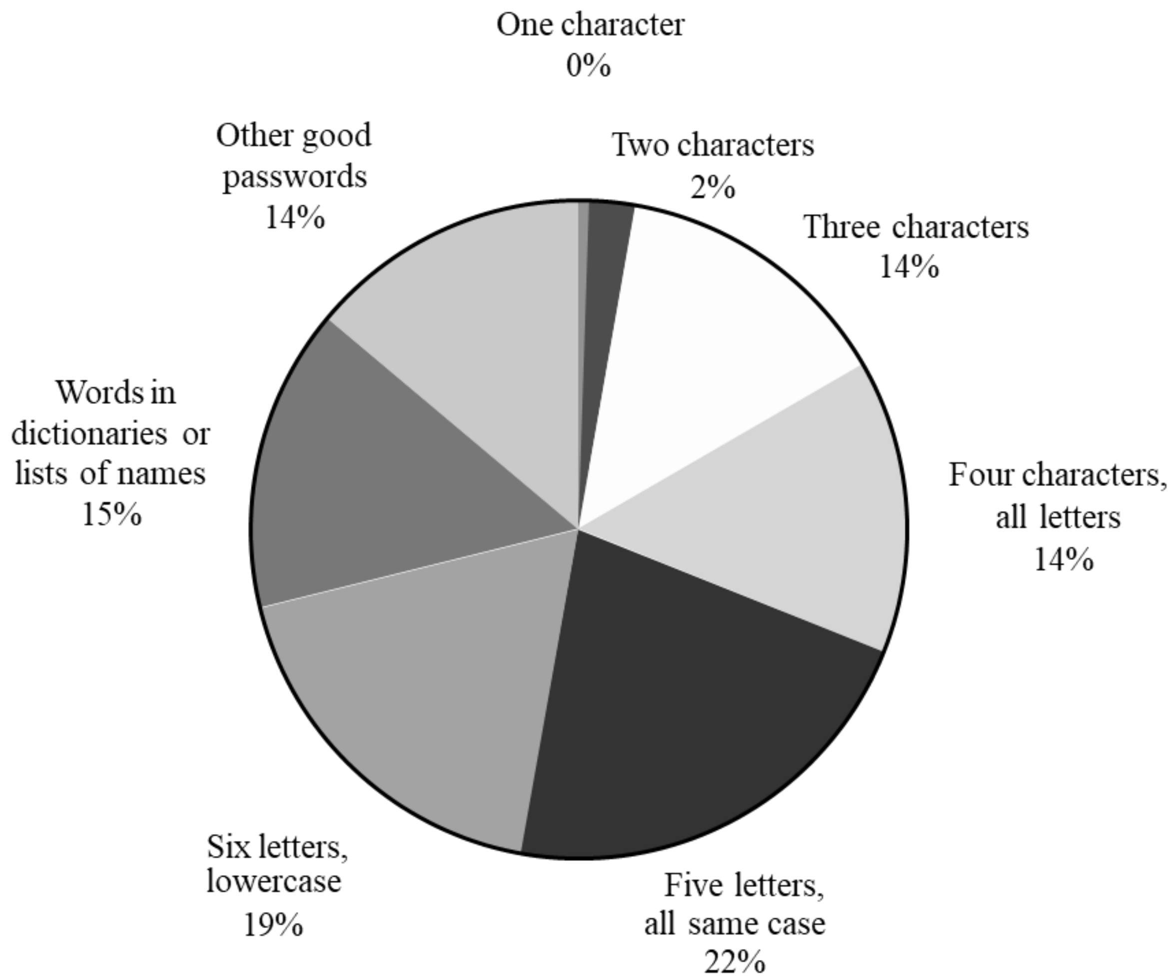
Identity	Password
Jane	qwerty
Pat	aaaaaa
Phillip	oct31witch
Roz	aaaaaa
Herman	guessme
Claire	aq3wm$oto!4

Concealed

Identity	Password
Jane	0x471aa2d2
Pat	0x13b9c32f
Phillip	0x01c142be
Roz	0x13b9c32f
Herman	0x5202aae2
Claire	0x488b8c27

Passwords should never be stored in plaintext but rather should always be concealed

Distribution of Password Types



Good Password

- Use characters other than just a–z
- Choose long passwords.
- Avoid actual names or words.
- Use a string you can remember.
- Use variants for multiple passwords
- Change the password regularly.
- Don’t write it down.
- Don’t tell anyone else. The easiest attack is social engineering

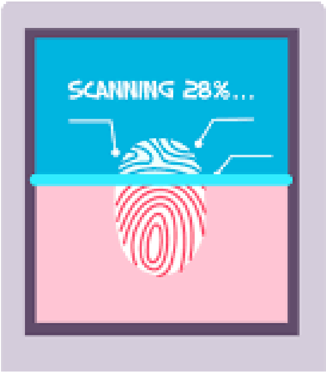
Something You Are

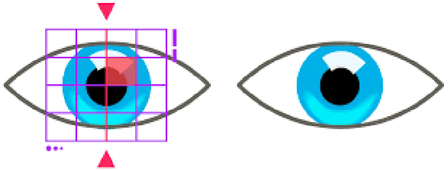
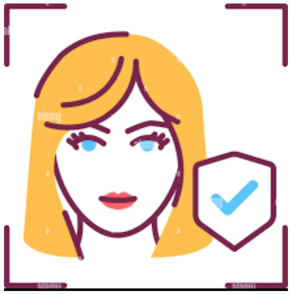
Biometrics

Biological properties, based on some physical characteristic of the human body.

Can be:

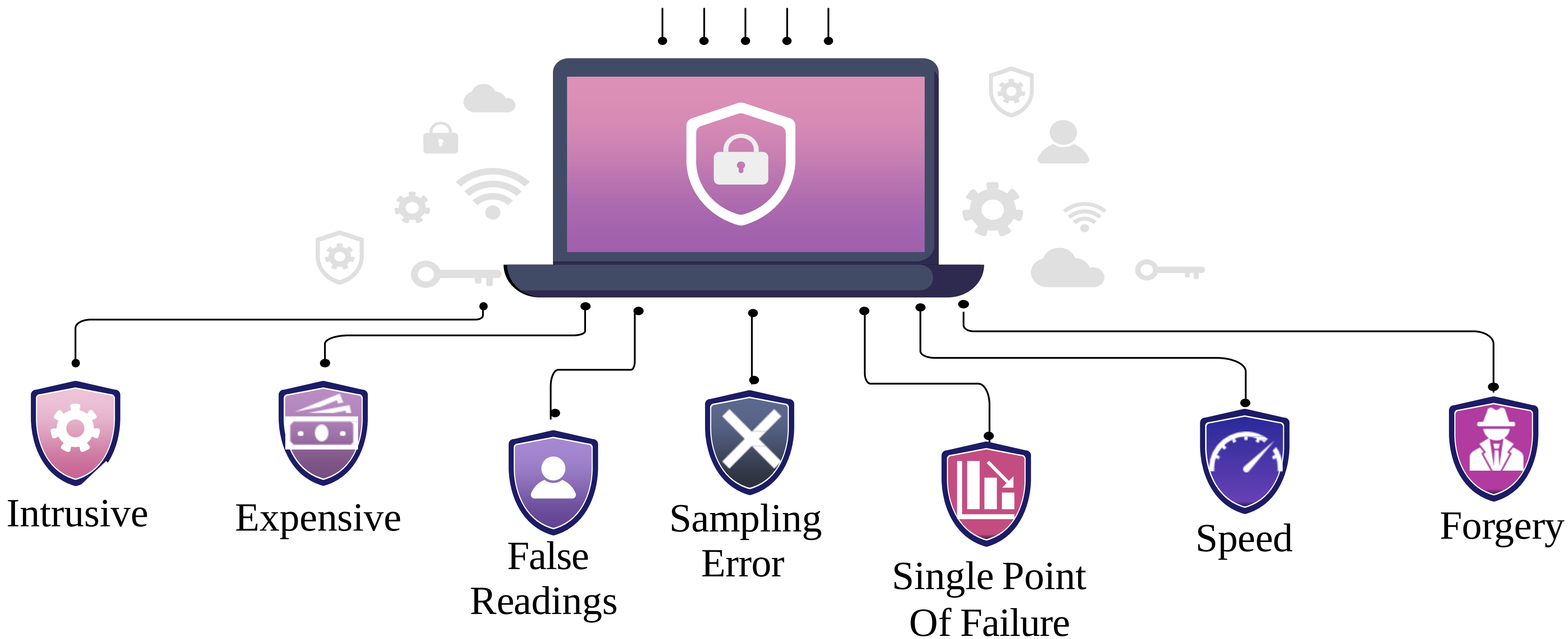
- fingerprint
- hand geometry (shape and size)
- retina and iris (parts of the eye)
- voice
- handwriting, signature, hand motion
- typing characteristics
- blood vessels in the finger or hand
- face
- facial features, such as nose shape or eye spacing



Biometrics

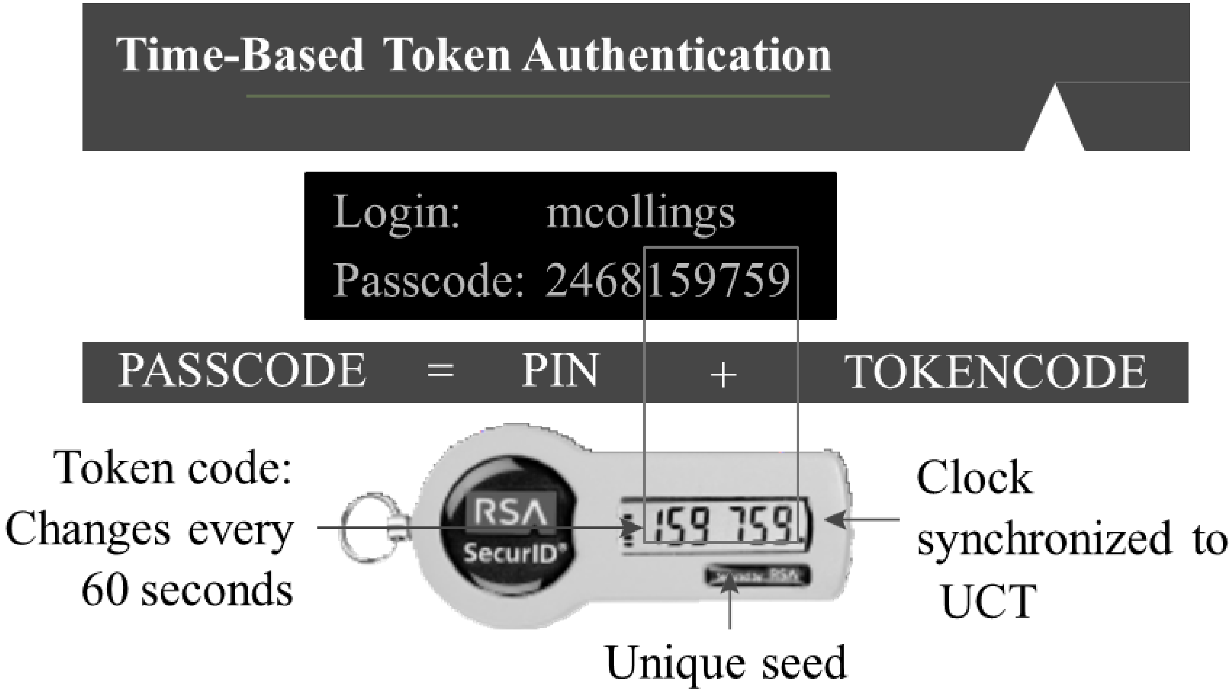
Problems with Biometrics



Something You have

Something you have can be:

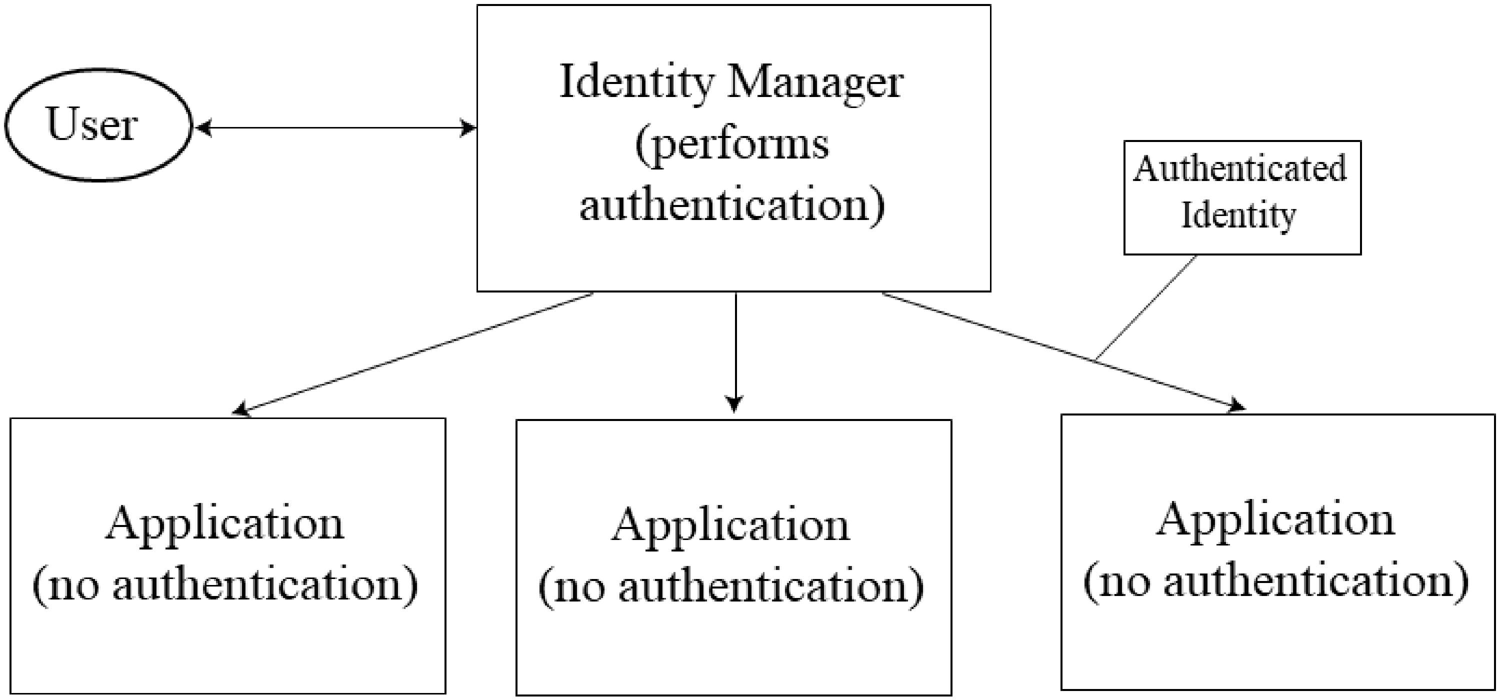
- Passive or active
- Static or dynamic



Federated Identity Management

- FIM : is a union of separate identification and authentication systems.
- Instead of maintaining separate user profiles, a federated scheme maintains one profile with one authentication method.
- Separate systems share access to the authenticated identity database.
- Authentication is performed in one place, and separate processes and systems determine that an already authenticated user is to be activated.

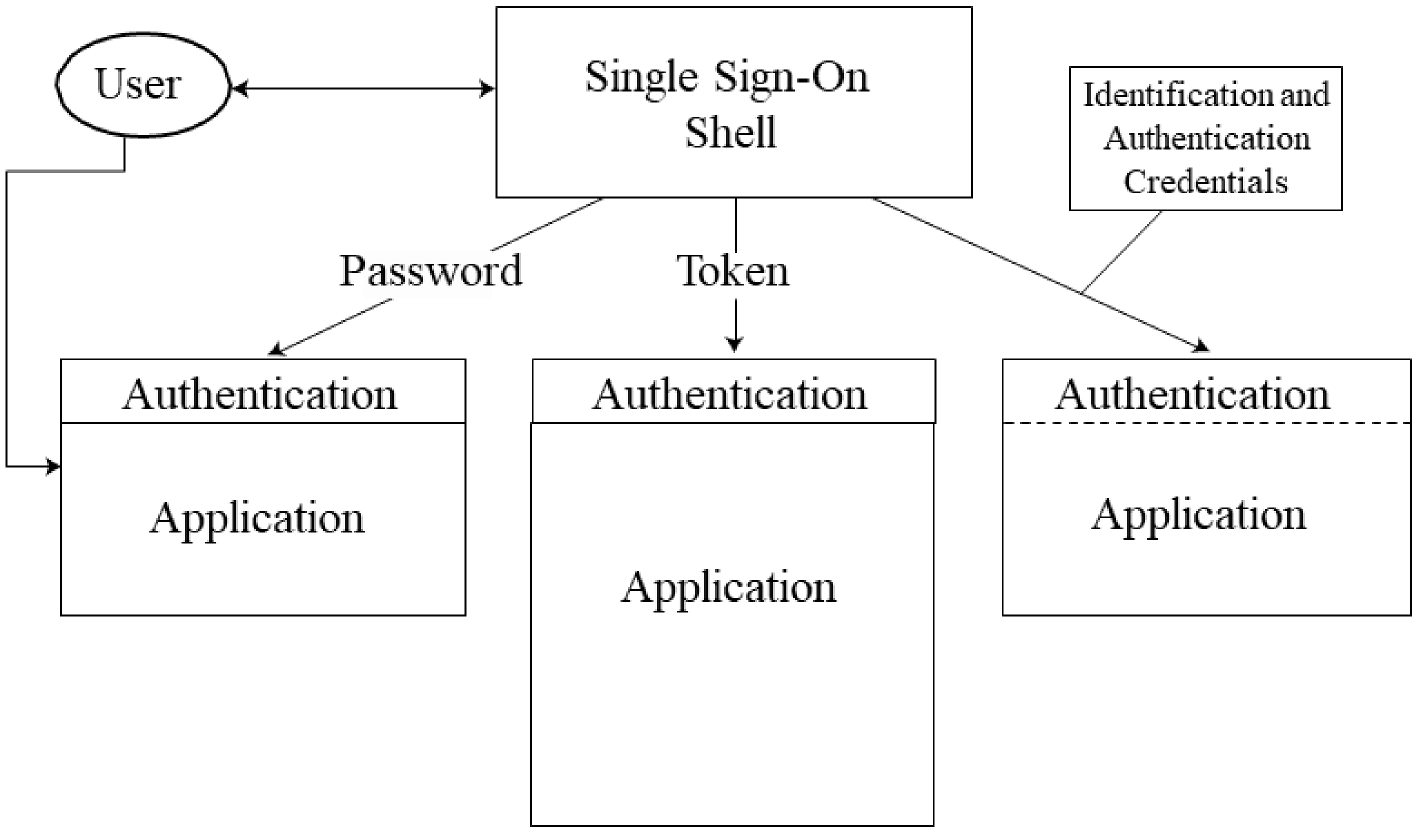
Federated Identity Management



Single sign-on

- ✓ Single sign-on lets a user log on once per session but access many different applications/systems.
- ✓ It often works in conjunction with federated identity management, with the federated identity provider acting as the source of authentication for all the applications.

Single sign-on



FID VS SSO

Federated identity management

- ✓ Involves a single identity management module that replaces identification and authentication in all other systems.
- ✓ All these systems invoke the identity management module.

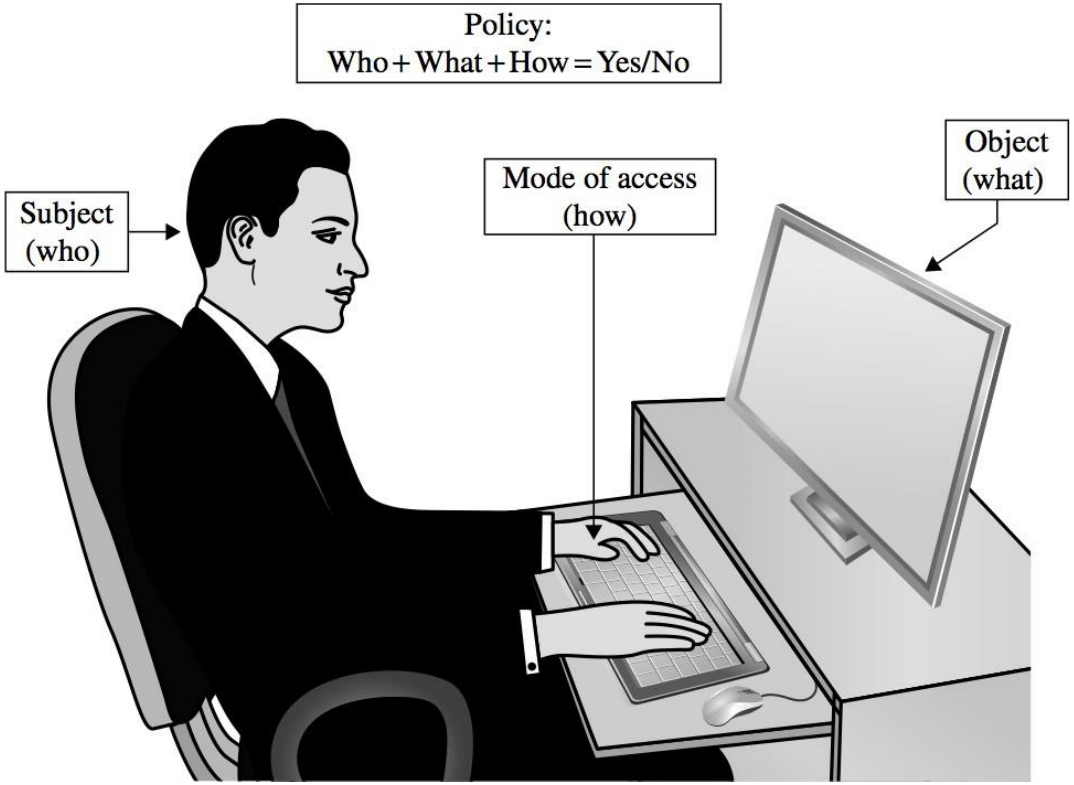
Single sign-on,

- ✓ An umbrella procedure to which you log in once per session
- ✓ The umbrella procedure maintains your identities and authentication codes for all the different processes
- ✓ You access systems still call for individual identification and authentication, but the umbrella task performs those interactions on behalf of the user.

Access Control

Access Control

Access control: limiting who can access what in what ways



Access Policies

- **Protecting objects involves several complementary goals:**
  - ✓ Check every access
    - If we have previously authorized the user to access the object, we do not necessarily intend that the user should retain indefinite access to the object.
  - ✓ Enforce least privilege
    - A subject should have access to the smallest number of objects necessary to perform some task.
  - ✓ Verify acceptable usage
    - Ability to access is a yes-or-no decision
- Track users' access
- Enforce at appropriate granularity
- Use audit logging to track accesses

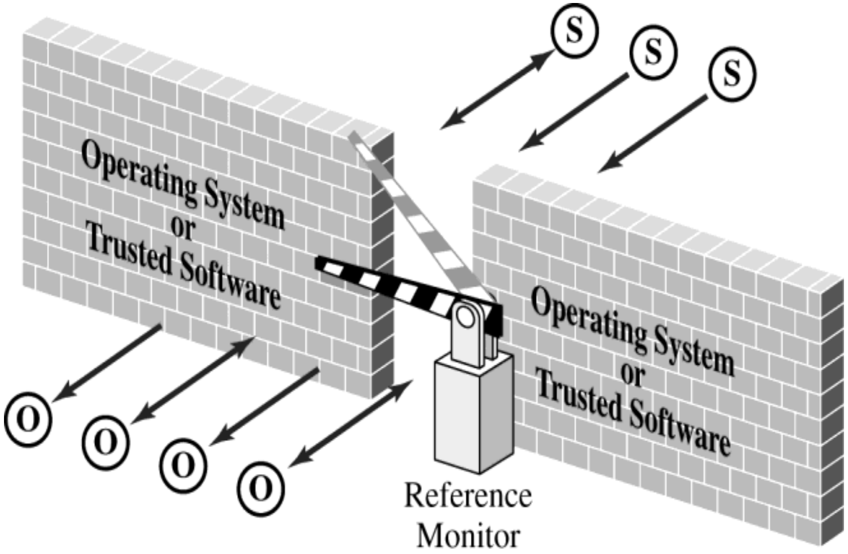
Implementing Access Control

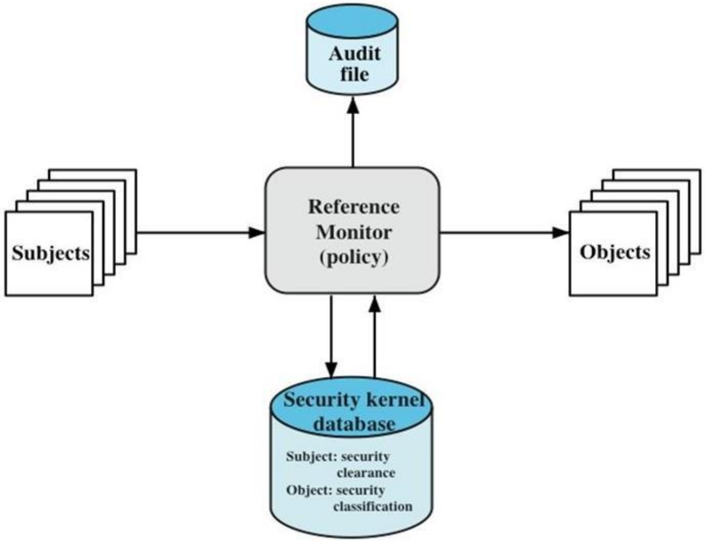
- **Reference monitor**
  - To have an effective reference monitor, we need to consider effective and efficient means to translate policies.
  - It could be embedded in an application, part of the operating system, or part of an appliance.

- **Access rights models implemented by the reference monitor**:
  - Access control directory
  - Access control matrix
  - Access control list
  - Privilege list
  - Capability
  - Procedure-oriented access control
  - Role-based access control

Reference Monitor

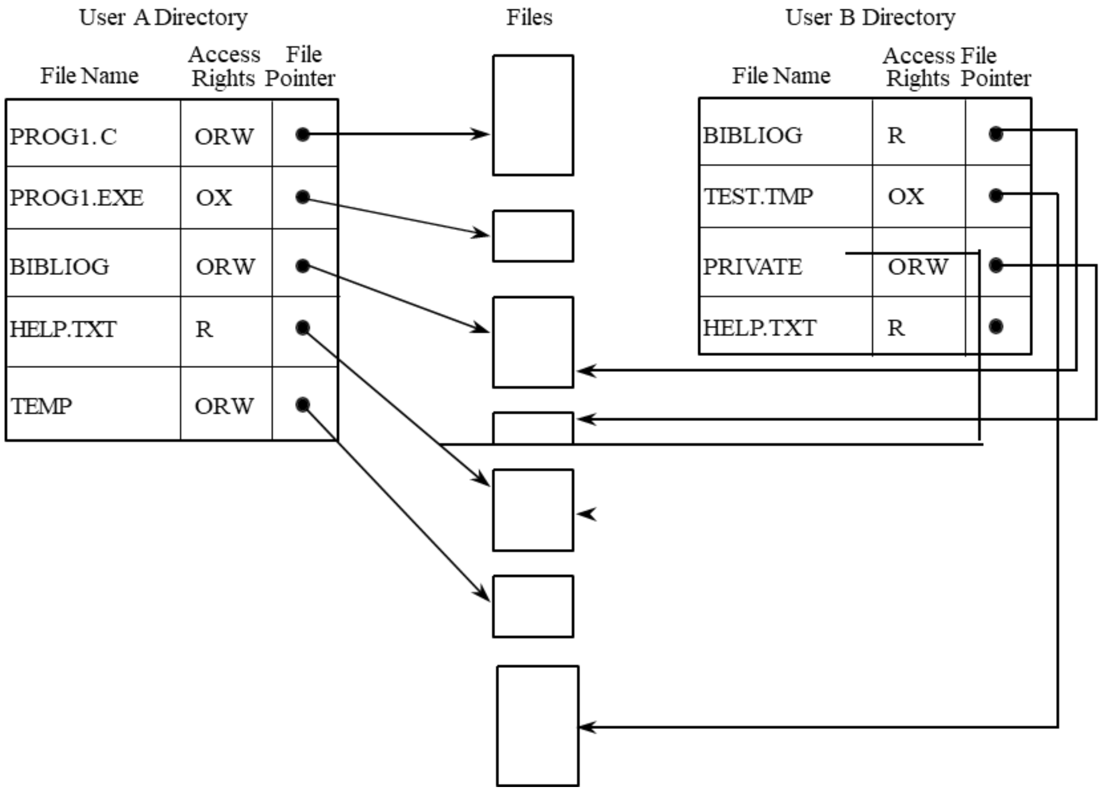
- Access control that is always invoked, tamperproof, and verifiable
- A reference monitor is the primary access control enforcement mechanism of the operating system





Access Control Directory

- We can think of the directory as a listing of objects accessible by a single subject, and the access list as a table identifying subjects that can access a single object.



Pros:
- Easy to implement

Cons:
- Long list
- Revocation of access
- Pseudonyms

Access Control Matrix

Access Control Matrix is a table in which:

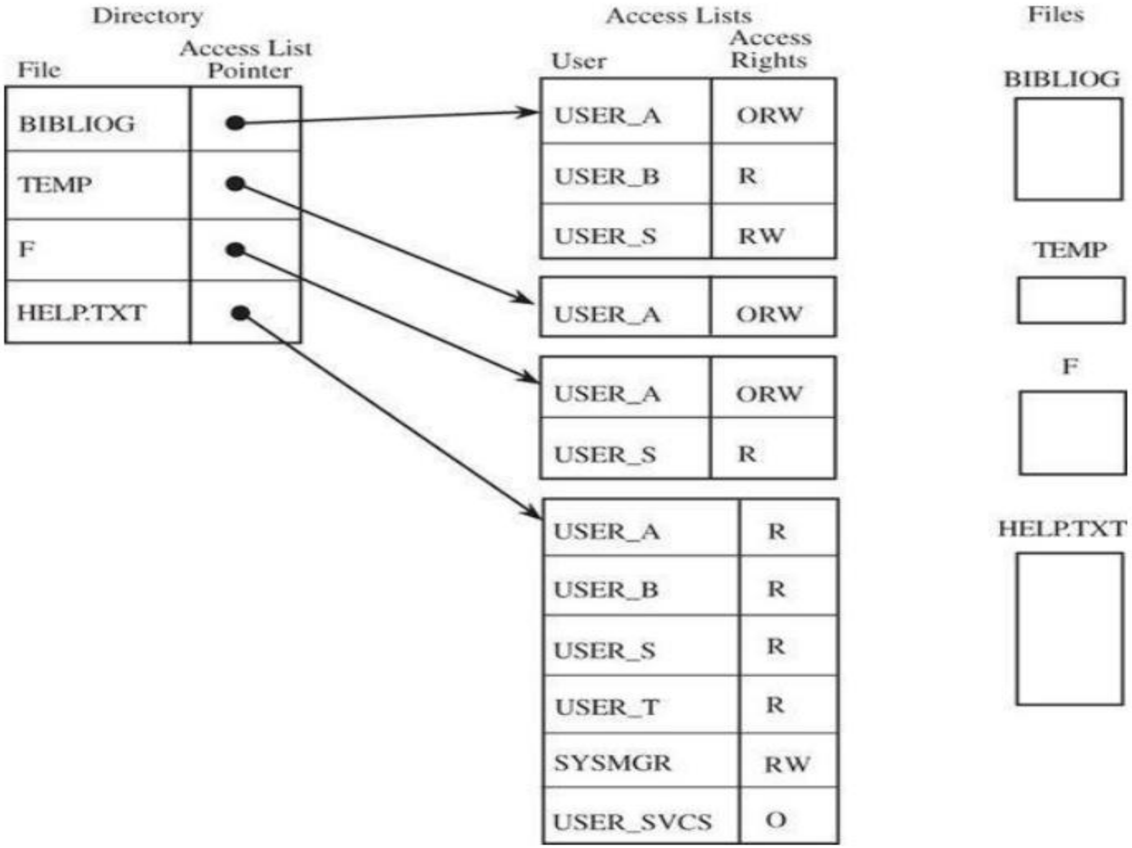
- Row represents a subject
- Column represents an object
- Entry is the set of access rights for that subject to that object.
- Can be represented as a list of triples: <subject, object, rights >

	BIBLIOG	TEMP	F	HELP.TXT	C_COMP	LINKER	SYS_CLOCK	PRINTER
USER A	ORW	ORW	ORW	R	X	X	R	W
USER B	R	-	-	R	X	X	R	W
USER S	RW	-	R	R	X	X	R	W
USER T	-	-	-	R	X	X	R	W
SYS_MGR	-	-	-	RW	OX	OX	ORW	O
USER_SVCS	-	-	-	O	X	X	R	W

Subject	Object	Right
USER A	Bibliog	ORW
USER B	Bibliog	R
USER S	Bibliog	RW
USER A	Temp	ORW
USER A	F	ORW
USER S	F	R
etc.		

Access Control List

- There is one such list for each object, and the list shows all subjects who should have access to the object and what their access is.
- The access control list allows default rights



Privilege Control List

Privilege List: is a row of the access matrix, showing all those privileges or access rights for a given subject

- One advantage of a privilege list is ease of revocation

	File A	Printer	System Clock
User W	Read Write Own	Write	Read
Admin		Write Control	Control

Capability

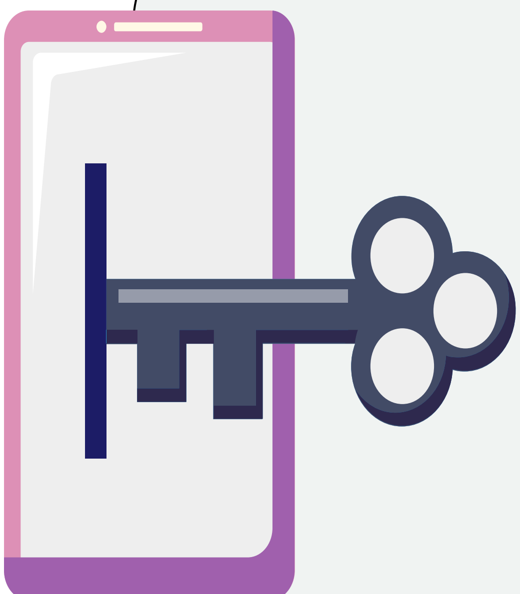
- Capability is an unforgeable token that gives the possessor certain rights to an object

	File A	Printer	System Clock
User W	Read Write Own	Write	Read
Admin		Write Control	Control

Capability: Single- or multi-use ticket to access an object or service

Implementing Access Control

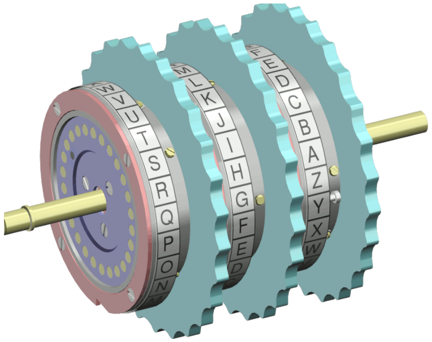
- **Reference monitor**
  - To have an effective reference monitor, we need to consider effective and efficient means to translate policies.
- **Access rights models implemented by the reference monitor**:
  - Access control directory
  - Access control matrix
  - Access control list
  - Privilege list
  - Capability
  - **Procedure-oriented access control**
  - **Role-based access control**



Cryptography

Cryptography

- ✓ Encryption or cryptography means secret writing
- ✓ Cryptography conceals data against unauthorized access
- ✓ A transformation makes data difficult for an outsider to interpret
  - The purpose is to make data unreadable (meaningless).
- ✓ Probably the strongest defence in computer security
- ✓ Encryption is like a machine
  - You insert a plaintext and the output is an encrypted text.
- ✓ Old encryption devices uses rotor machines. Now they are substituted by computer algorithms.



Problems Addressed by Encryption

Suppose a sender ***S*** wants to send a message ***M*** to a recipient ***R***.

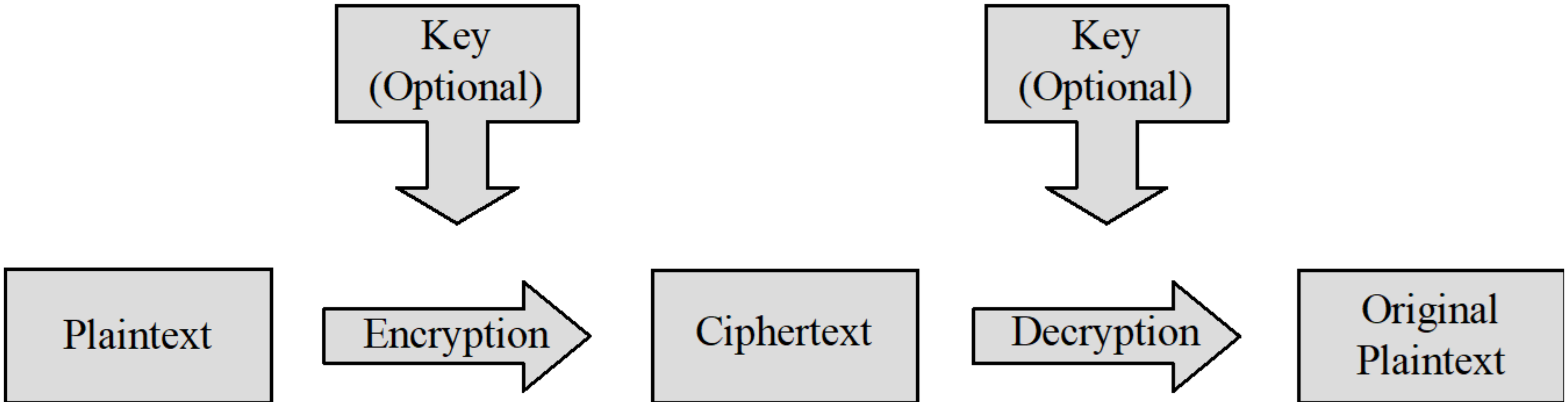
An attacker may attempt to:

block **it**	preventing M from reaching R ➔ ~~availability~~
intercept **it -**	reading or listening to M ➔ ~~confidentiality~~
modify **it -**	intercepting and changing M ➔ ~~integrity~~
fabricate **an authentic-looking M`**	~~integrity, availability~~

Encryption Terminology

- Sender
- Recipient
- Transmission medium
- Interceptor/intruder
- Encrypt, encode, or encipher
- Decrypt, decode, or decipher
- Cryptosystem
- Plaintext
- Ciphertext

Encryption/Decryption Process



Cryptographic Systems

Cryptographic systems can be characterized by:

Type of encryption operations used

- Substitution
- Transposition
- Product

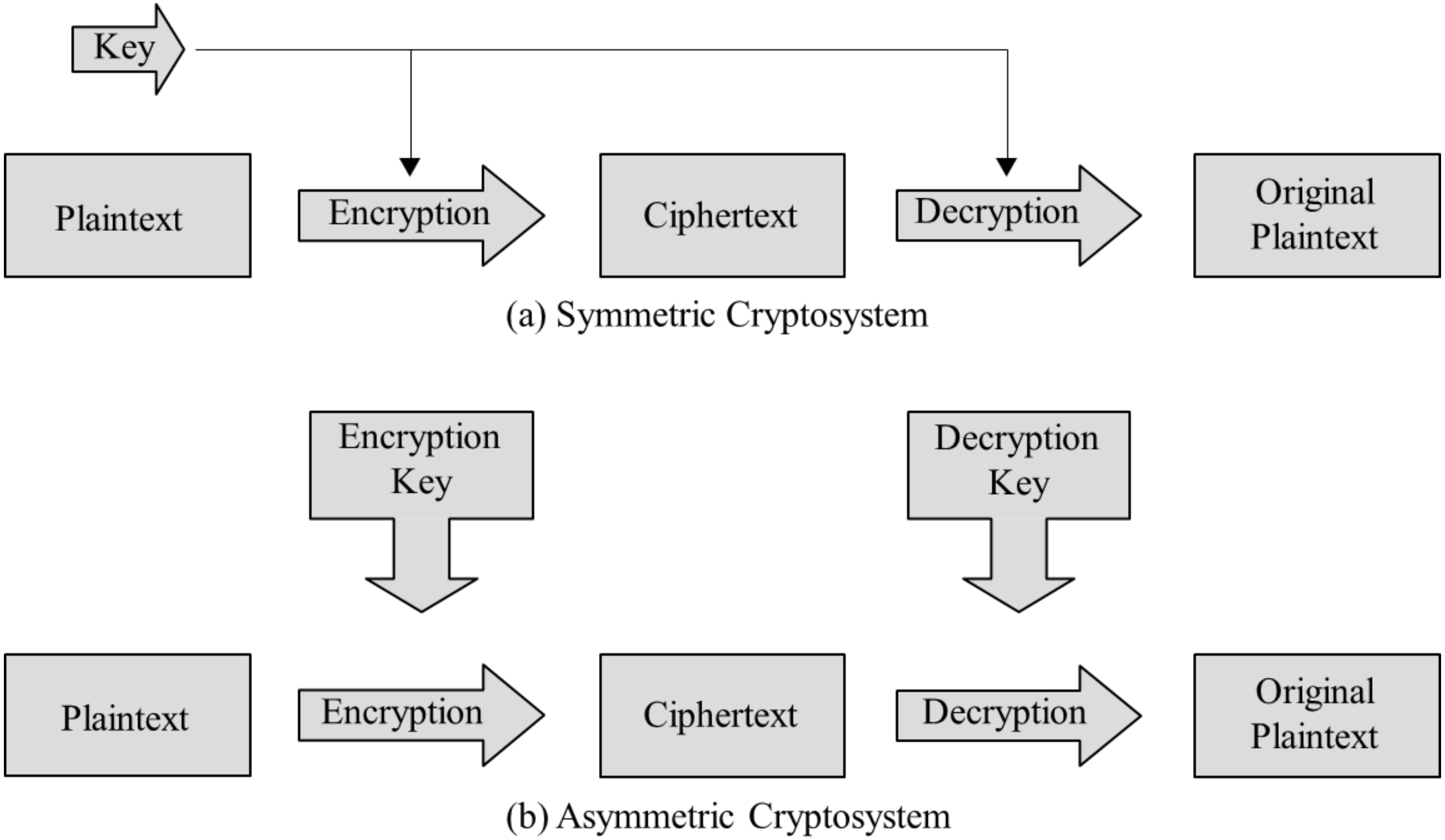
Number of keys used

- Single-key or private/secret-key
- Two-key or public-key

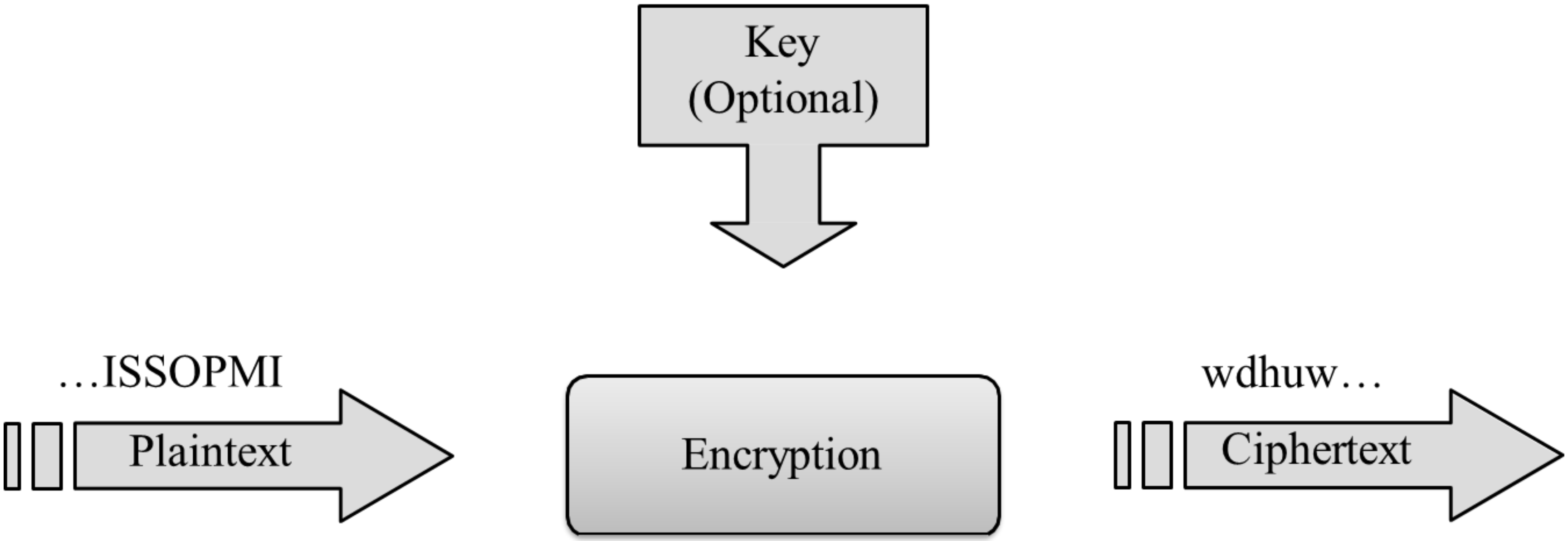
Way in which plaintext is processed

- Block
- Stream

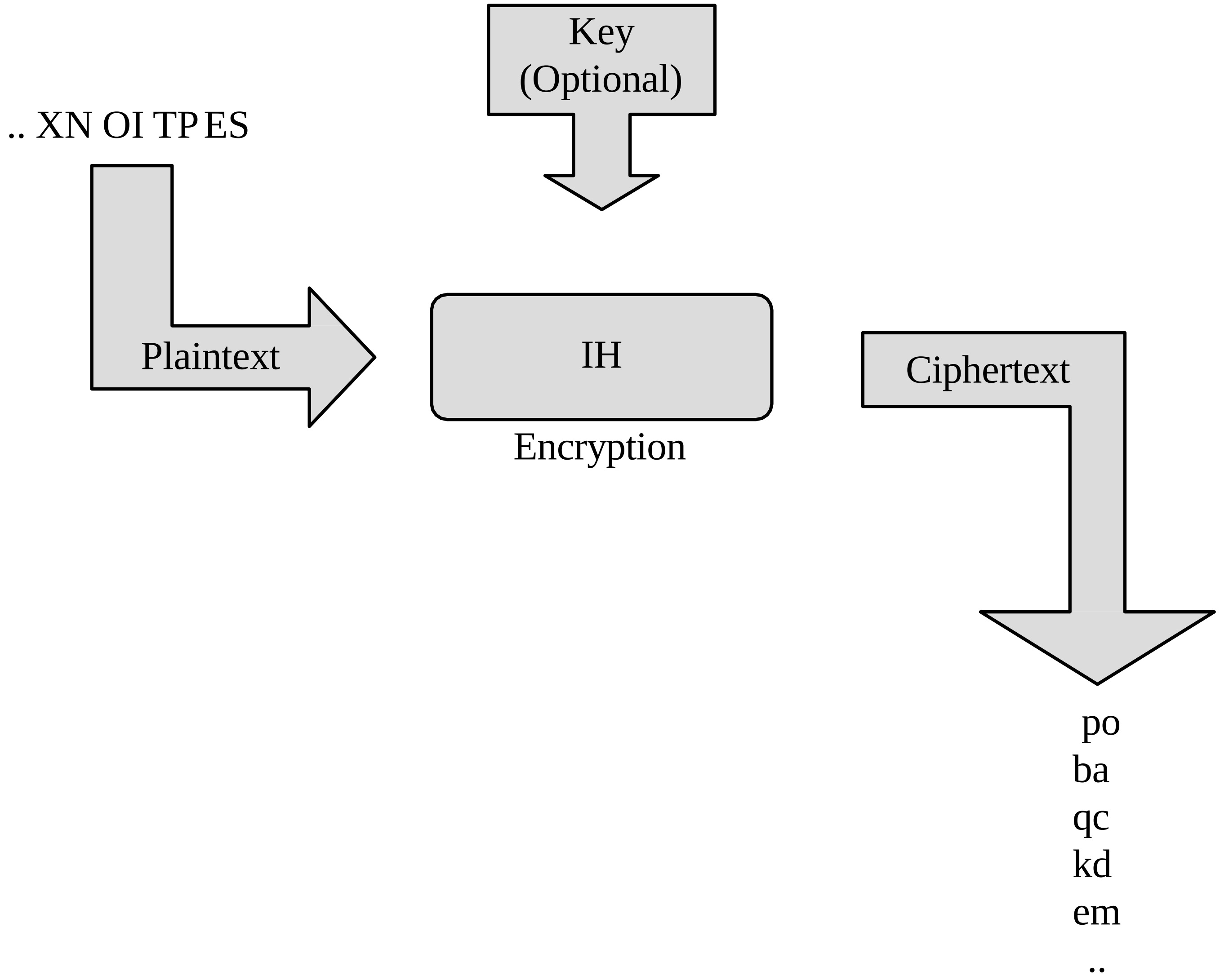
Symmetric vs. Asymmetric



Stream Ciphers



Block Ciphers



Stream vs. Block

	Stream	Block
Advantages	• Speed of transformation • Low error propagation	• High diffusion • Immunity to insertion of symbol
Disadvantages	• Low diffusion • Susceptibility to malicious insertions and modifications	• Slowness of encryption • Padding • Error propagation

DES

The Data Encryption Standard

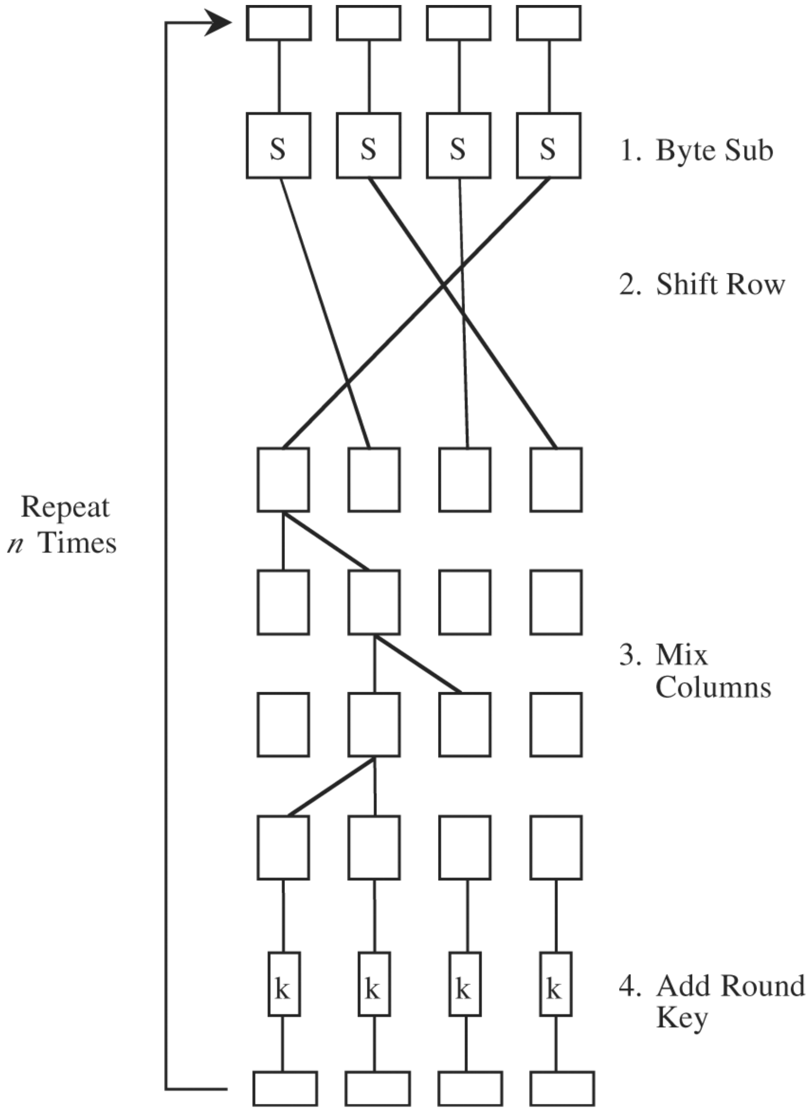
Symmetric block cipher

Developed in 1976 by IBM for the US National Institute of Standards and Technology (NIST)

Form	Operation	Properties	Strength
DES	Encrypt with one key	56-bit key	Inadequate for high-security applications by today's computing capabilities
Double DES	Encrypt with first key; then encrypt result with second key	Two 56-bit keys	Only doubles strength of 56-bit key version
Two-key triple DES	Encrypt with first key, then encrypt (or decrypt) result with second key, then encrypt result with first key (E-D-E)	Two 56-bit keys	Gives strength equivalent to about 80-bit key (about 16 million times as strong as 56-bit version)
Three-key triple DES	Encrypt with first key, then encrypt or decrypt result with second key, then encrypt result with third key (E-E-E)	Three 56-bit keys	Gives strength equivalent to about 112-bit key about 72 quintillion ($72*10^{15}$) times as strong as 56-bit version

AES

Advanced Encryption System

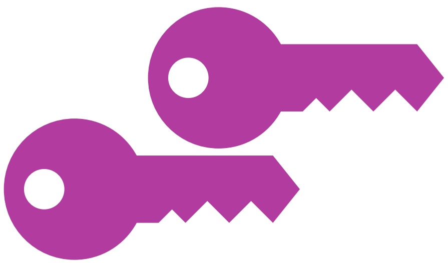


- ✓ Symmetric block cipher
- ✓ Developed in 1999 by independent Dutch cryptographers
- ✓ Still in common use

DES vs. AES

	DES	AES
Date designed	1976	1999
Block size	64 bits	128 bits
Key length	56 bits (effective length); up to 112 bits with multiple keys	128, 192, 256 (and possibly more) bits
Operations	16 rounds	10, 12, 14 (depending on key length); can be increased
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but open public comments and criticisms invited
Source	IBM, enhanced by NSA	Independent Dutch cryptographers

Public Key (Asymmetric) Cryptography



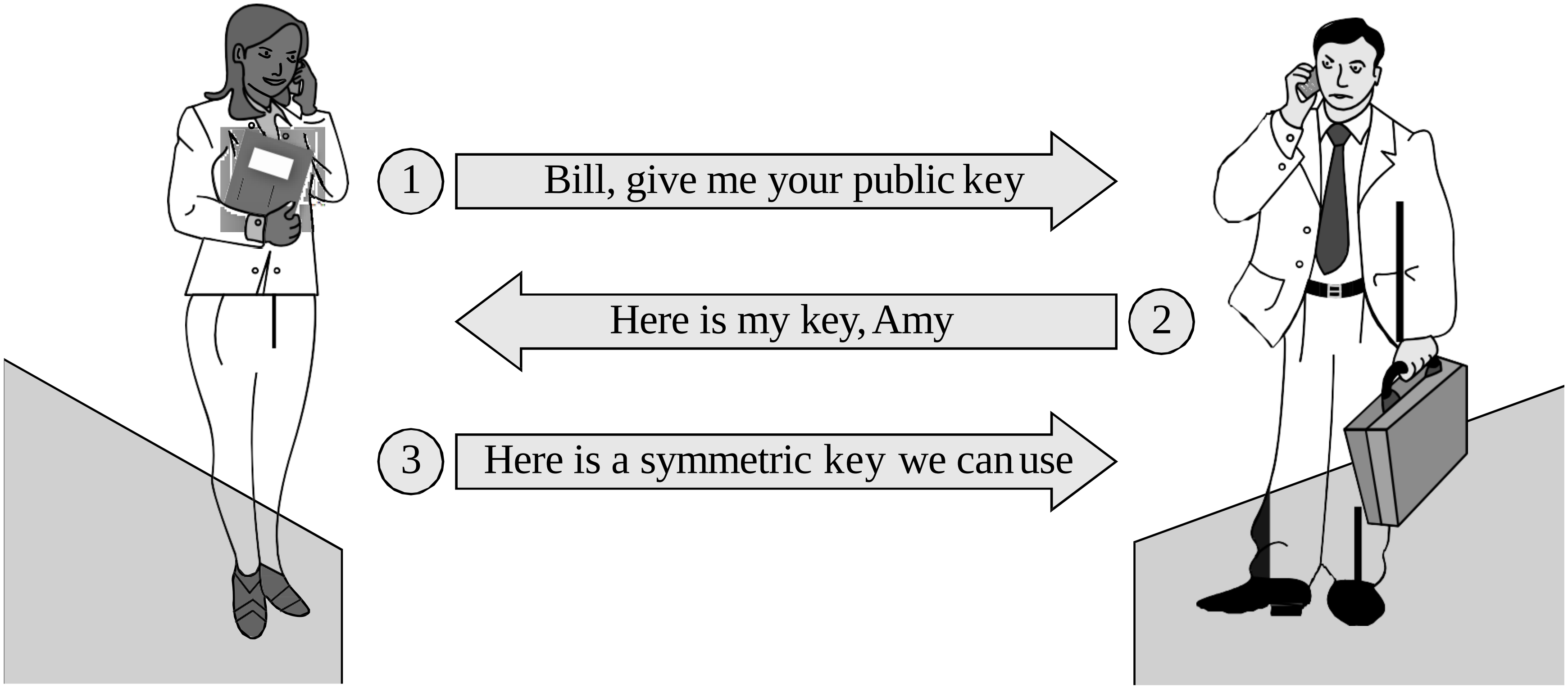
Instead of two users sharing one secret key, each user has two keys: one public and one private

Messages encrypted using the user’s public key can only be decrypted using the user’s private key, and vice versa

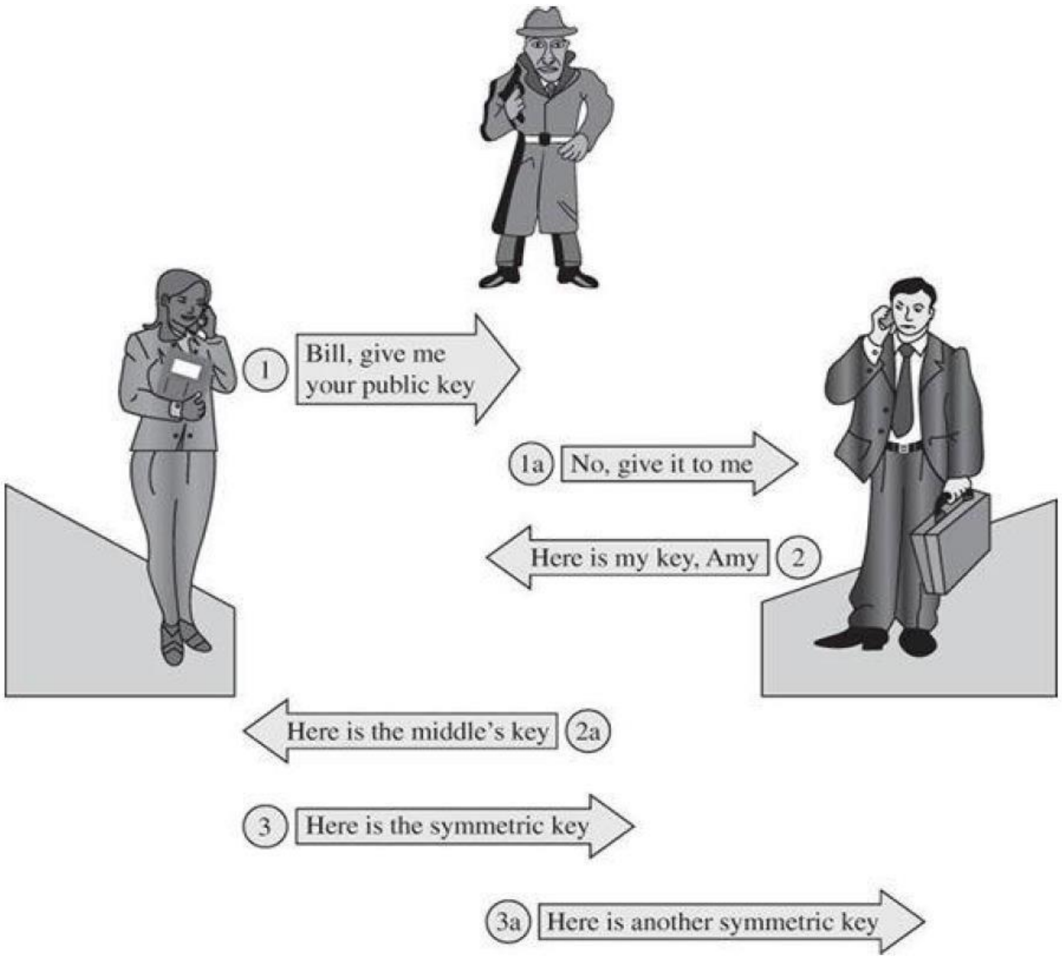
Secret Key vs. Public Key Encryption

	Secret Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Key size (bits)	56–112 (DES), 128–256 (AES)	Unlimited; typically no less than 256; 1000 to 2000 currently considered desirable for most uses
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse. Secrecy and integrity of data, from single characters to blocks of data, messages and files	Key exchange, authentication, signing
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow, typically by a factor of up to 10,000 times slower than symmetric algorithms

Public Key to Exchange Secret Keys



Key Exchange Man in the Middle



Error Detecting Codes

Demonstrates that a block of data has been modified

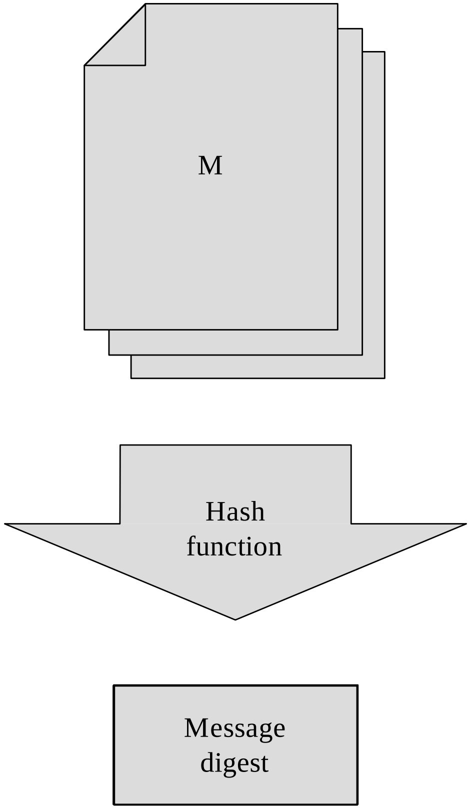
- **Simple error detecting codes:**
  - ✓ Parity checks
    - Odd vs Even
  - ✓ Cyclic redundancy checks
    - A short check value attached to the message, based on the remainder of a polynomial division of message

- **Cryptographic error detecting codes:**
  - ✓ One-way hash functions- invers is hard(infeasible) to compute
  - ✓ Cryptographic checksums- prevents attackers from modifying:
    - the error detection mechanism
    - the data bits
  - ✓ Digital signatures- a protocol produces the same effect as a real signature

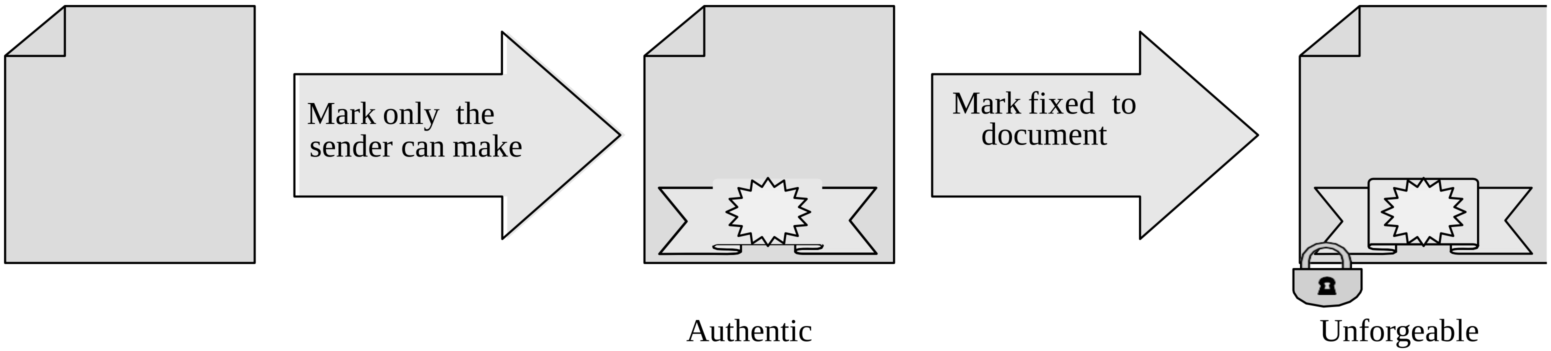
Parity Check

Original Data	Parity Bit	Modified Data	Modification Detected?
0 0 0 0 0 0 0 0	1	0 0 0 0 0 0 0 1	Yes
0 0 0 0 0 0 0 0	1	1 0 0 0 0 0 0 0	Yes
0 0 0 0 0 0 0 0	1	1 0 0 0 0 0 0 1	No
0 0 0 0 0 0 0 0	1	0 0 0 0 0 0 1 1	No
0 0 0 0 0 0 0 0	1	0 0 0 0 0 1 1 1	Yes
0 0 0 0 0 0 0 0	1	0 0 0 0 1 1 1 1	No
0 0 0 0 0 0 0 0	1	0 1 0 1 0 1 0 1	No
0 0 0 0 0 0 0 0	1	1 1 1 1 1 1 1 1	No

One-Way Hash Function



Digital Signature

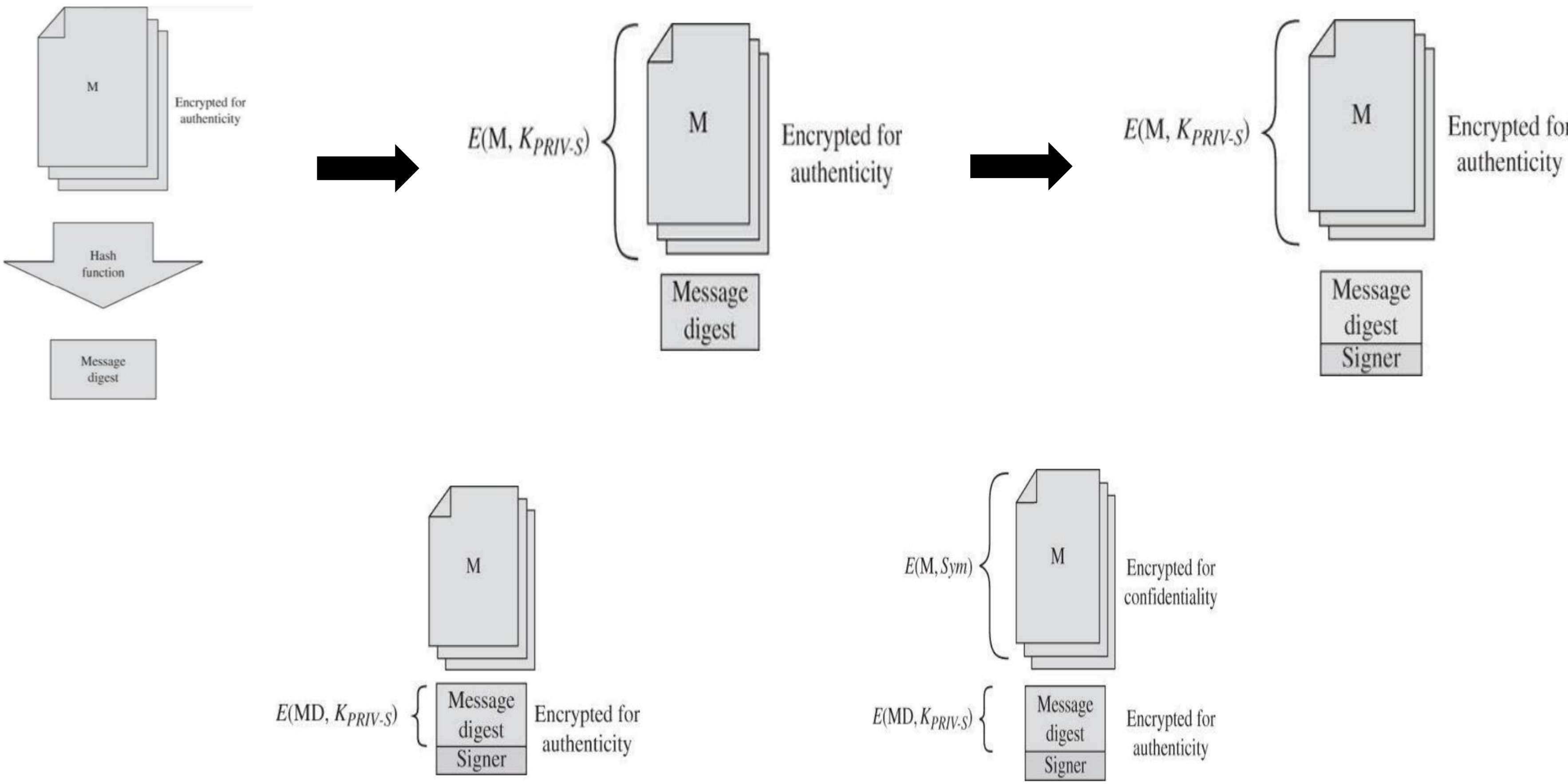


A digital signature must meet two primary conditions:

- It must be unforgeable.
  - If person S signs message M with signature Sig(S,M), no one else can produce the pair [M,Sig(S,M)].

- It must be authentic.
  - If a person R receives the pair [M, Sig(S,M)], R can check that the signature is really from S. Only S could have created this signature, and the signature is firmly attached to M.

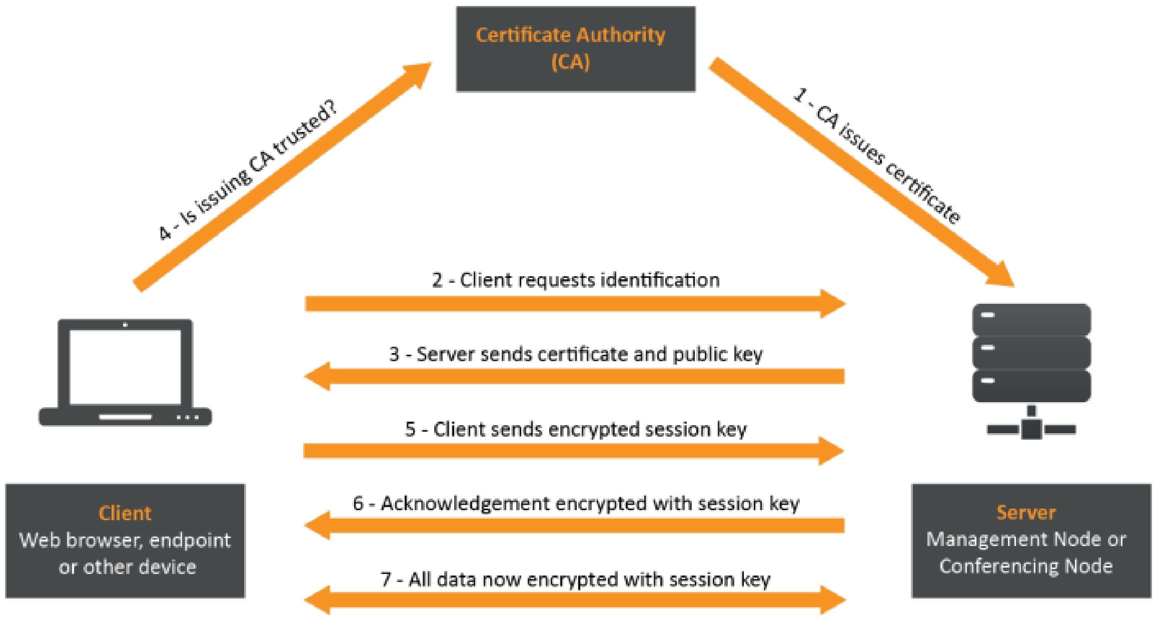
Example:
Construct digital signature for a file



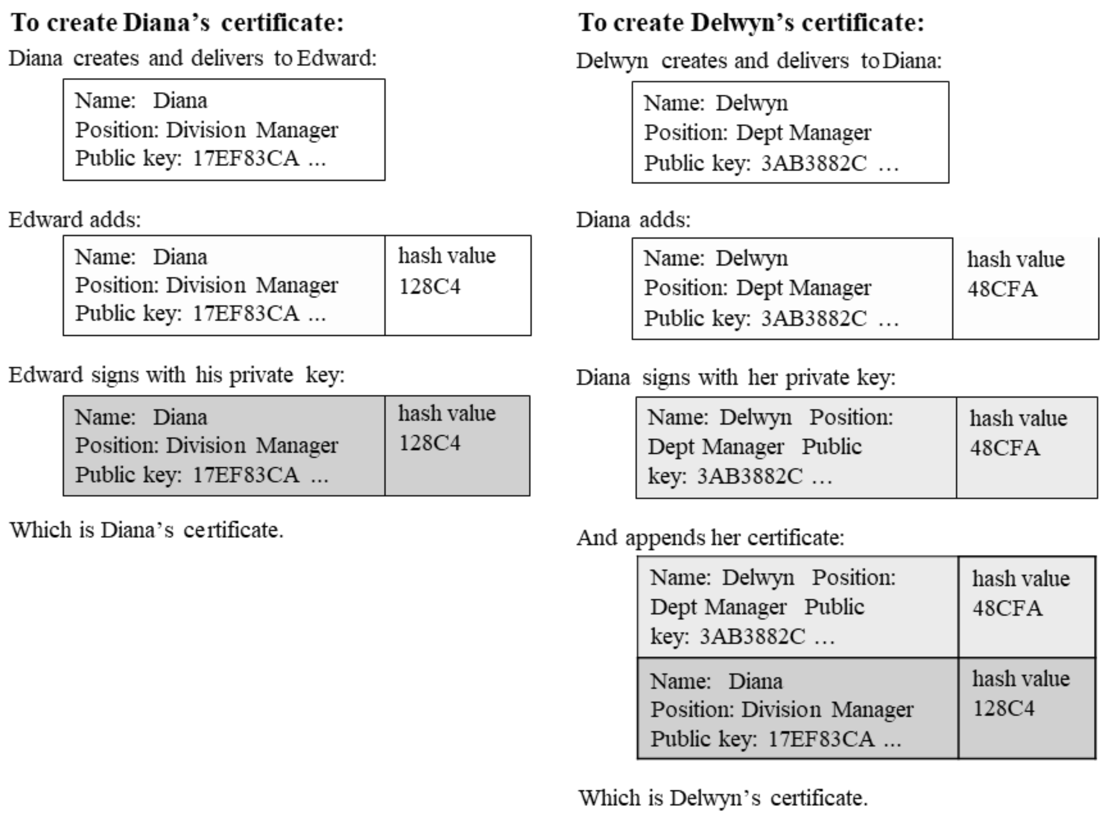
Certificates

Trustable Identities and Public Keys

- A **certificate** is a public key and an identity bound together and signed by a **certificate authority.**
- A **certificate authority** is an authority that users trust to accurately verify identities before generating certificates that bind those identities to keys.



Certificate Signing and Hierarchy



- Diana's certificate is made using Edward's signature.
- Delwyn's certificate includes Diana's certificate so that it can effectively be tied back to Edward, creating a chain of trust.

Cryptographic Tool Summary

Tool	Uses
Secret key (symmetric) encryption	Protecting confidentiality and integrity of data at rest or in transit
Public key (asymmetric) encryption	Exchanging (symmetric) encryption keys Signing data to show authenticity and proof of origin
Error detection codes	Detect changes in data
Hash codes and functions (forms of error detection codes)	Detect changes in data
Cryptographic hash functions	Detect changes in data, using a function that only the data owner can compute (so an outsider cannot change both data and the hash code result to conceal the fact of the change)
Error correction codes	Detect and repair errors in data
Digital signatures	Attest to the authenticity of data
Digital certificates	Allow parties to exchange cryptographic keys with confidence of the identities of both parties

Summary

- Users can authenticate using something they know, something they are, or something they have

- Systems may use a variety of mechanisms to implement access control

- Encryption helps prevent attackers from revealing, modifying, or fabricating messages

- Symmetric and asymmetric encryption have complementary strengths and weaknesses

- Certificates bind identities to digital signatures

Quick Quiz

Zain and Noor use asymmetric cryptographic system, which of the following is NOT true?

A> Noor can decrypt any message that is encrypted using Zain's private kay	**B> If Zain used her private key for encryption then Noor can use Zain's public key for decryption**
C> If Zain used her public key to encrypt a message, then Noor can use her private key for decryption	**D> Noor cannot decrypt any message that is encrypted using Zain's public kay** **E> Other:**

[redacted]

Quick Quiz

One of the advantages of public key cryptography is that, if implemented properly, the algorithms generally run much faster than symmetric key cryptography algorithms.

A> true	**B> false**

[redacted]

Quick Quiz

Zain and Noor want to establish a secure communication channel between them. They do not care about the confidentiality of the messages being transmitted, but they do want to ensure the integrity and authenticity of the messages.

A> they cannot achieve that! Why?	B> they can achieve that! How?

[redacted]

Quick Quiz

Implementing a symmetric cryptographic system, How many key are required in each of the following cases?

A> 5 team members want to keep their discussions secret from other teams in the class	**B> 5 team members want to keep their discussions secret from each other**

[redacted]

Quick Quiz

The number of keys required to establish pair-wise secure communications among a group of 30 people using symmetric-key cryptography is less than the number of keys required using asymmetric cryptography

A> true	**B> false**