Security Objectives

- **Confidentiality**: prevent/detect/deter improper **disclosure** of information
- **Integrity**: prevent/detect/deter improper modification of information
- **Availability**: prevent/detect/deter improper **denial of access** to services

Commercial Example

- **Confidentiality**: patient's medical information should not be improperly disclosed
- **Integrity**: patient's medical information should be correct
- **Availability**: patient's medical information can be accessed when needed for treatment

Fourth Objective

- Securing **computing resources**: prevent/detect/deter improper **use** of computing resources
  - Hardware
  - Software
  - Data
  - Network

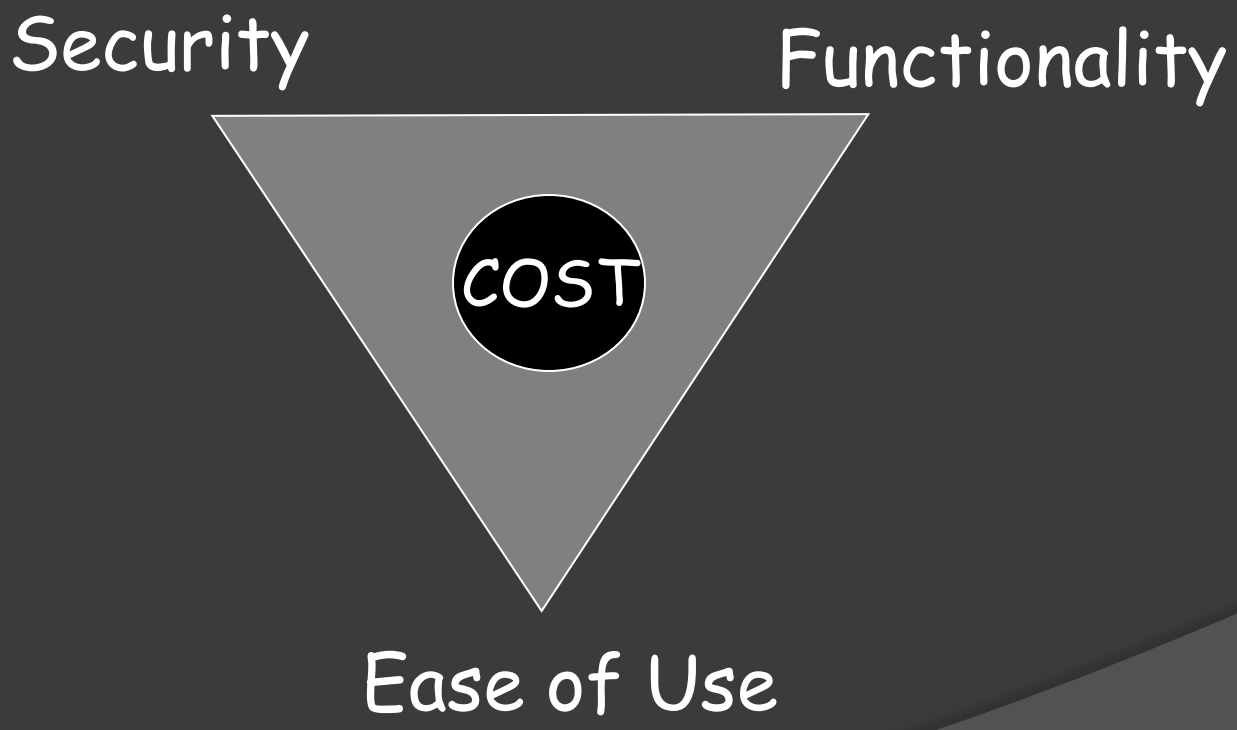
Security Mechanism

- Prevention
- Detection
- Tolerance/Recovery

Security by Legislation

- Instruct users how to behave
- Not good enough!
  - Important
  - Only enhance security
  - Targets only some of the security problems

Security Tradeoffs



Threat, Vulnerability, Risk

- **Threat**: **potential occurrence** that can have an undesired effect on the system
- **Vulnerability**: **characteristics** of the system that makes is possible for a threat to potentially occur
- **Attack**: **action of malicious** intruder that exploits vulnerabilities of the system to cause a threat to occur
- **Risk**: measure of the possibility of security breaches and severity of the damage

Types of Threats (1)

- Errors of users
- Natural/man-made/machine disasters
- Dishonest insider
- Disgruntled insider
- Outsiders

Types of Threats (2)

- **Disclosure** threat – **dissemination** of unauthorized information
- **Integrity** threat – **incorrect modification** of information
- **Denial of service** threat – **access to a system** resource is blocked

Types of Attacks (1)

- **Interruption** – **an asset** is destroyed, unavailable or unusable (*availability*)
- **Interception** – unauthorized party gains **access to an asset** (*confidentiality*)
- **Modification** – unauthorized party **tampers with asset** (*integrity*)
- **Fabrication** – unauthorized party **inserts counterfeit object** into the system (*authenticity*)
- **Denial** – person denies taking an **action** (*authenticity*)

Computer Criminals

Any crime that involves computers or aided by the use of computers

- **Amateurs**: **regular users,** who exploit the vulnerabilities of the computer system
  - Motivation: **easy access** to vulnerable resources
- **Crackers**: **attempt to access** computing facilities for which they do not have the authorization
  - Motivation: **enjoy challenge**, curiosity
- **Career criminals: professionals** who understand the computer system and its vulnerabilities
  - Motivation: **personal gain** (e.g., **financial**)

Methods of Defense

- **Prevent**: block attack
- **Deter**: make the attack harder
- **Deflect**: make other targets more attractive
- **Detect**: identify misuse
- **Tolerate**: function under attack
- **Recover**: restore to correct state

Cryptographic Protocols

- Only the recipient should see it
- Only the recipient should get it

Terminology

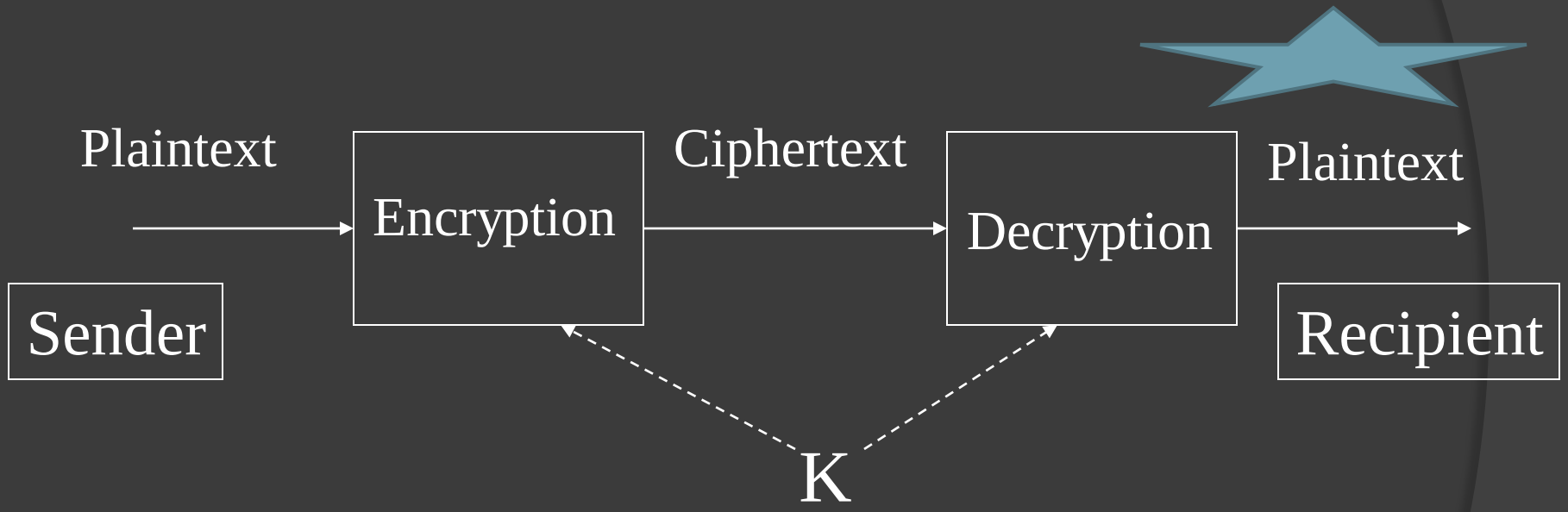
- **Plaintext (cleartext):** a message in its original form
- **Ciphertext (cyphertext):** an encrypted message
- **Encryption:** transformation of a message to hide its meaning
- **Cipher:** cryptographic algorithm.

Terminology

- **Decryption**: recovering meaning from ciphertext
- **Cryptography**: art and science of keeping messages secure
- **Cryptanalysis**: art and science of breaking ciphertext
- **Cryptology**: study of both cryptography and cryptanalysis

Important

Conventional (Secret Key) Cryptosystem



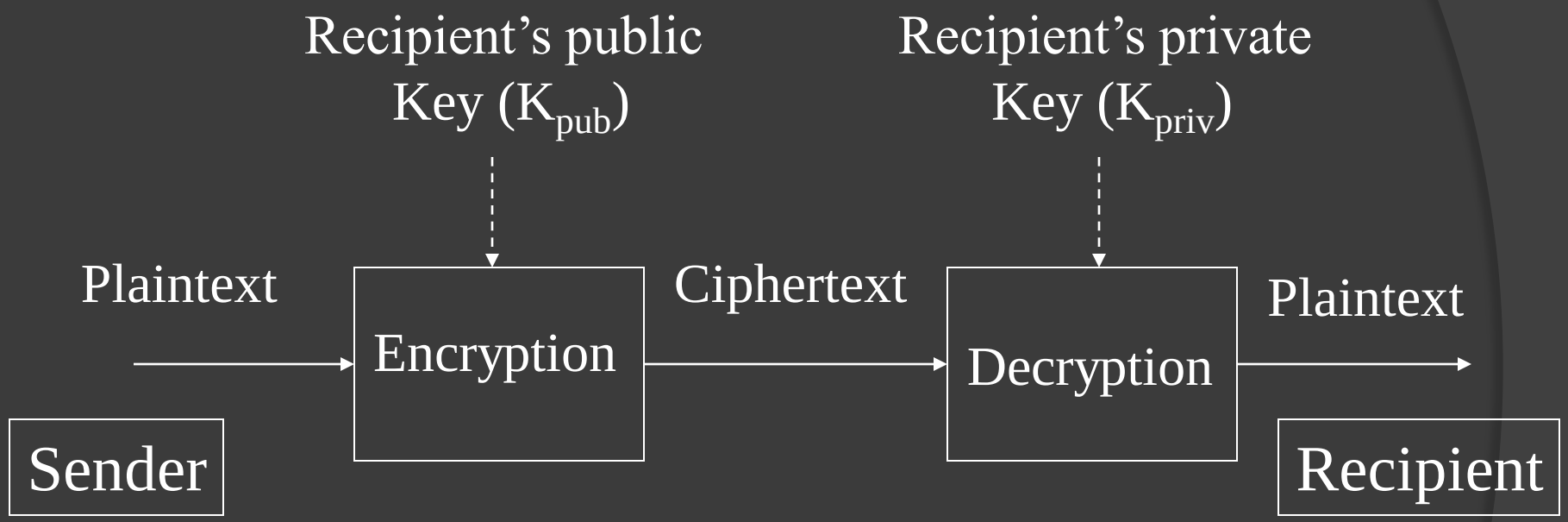
C=E(K,M)

M=D(K,C)

K needs **secure** channel

Important

Public Key Cryptosystem



$C=E(K_{pub},M)$

$M=D(K_{priv},C)$

K_{pub} needs **reliable** channel

Cryptanalysis

- *n* users need *n*(n-1)/2* keys

Cryptanalyst's goal:

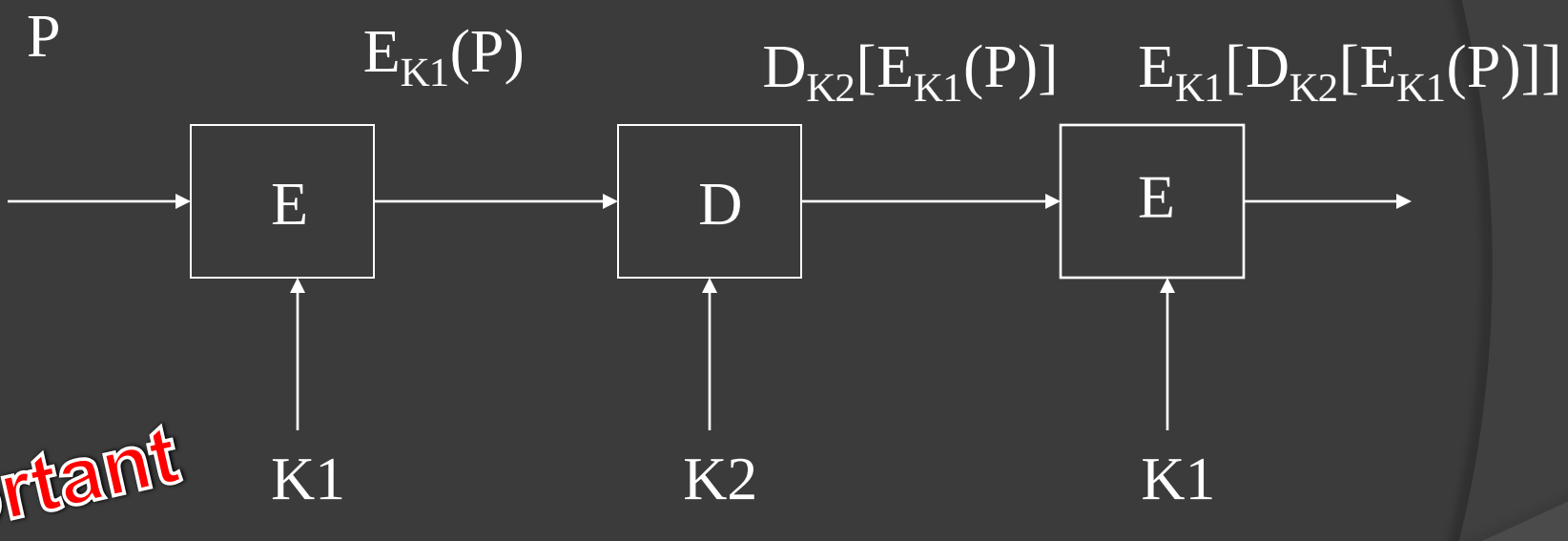
- Break message
- Break key
- Break algorithm

Basic Encryption Techniques

- Substitution
- Permutation
- Combinations and iterations of these

One-Time Pad ..(The best)وامن

DES Multiple Encryption



Important

Tuchman: avoid meet-in-the-middle attack

If K1=K2: single encryption

Important

Signature and Encryption

- We could do the encryption first, followed by the signature.

  Adv. signature first: parties, other than B can verify the signature
- DES can be used for encryption

DES is about 100 times faster than RSA

RSA: used for secure exchange of DES keys

Public-Key Encryption(need reliable channel)

***Slower* than secret-key encryption (10,000 times)**

Hash Functions

Message digest

Used for authenticity and integrity purposes

Algorithms:

- SHA-1MD2,MD4,
- MD5 حرف واحد بخربه Hasn't been disproved yet

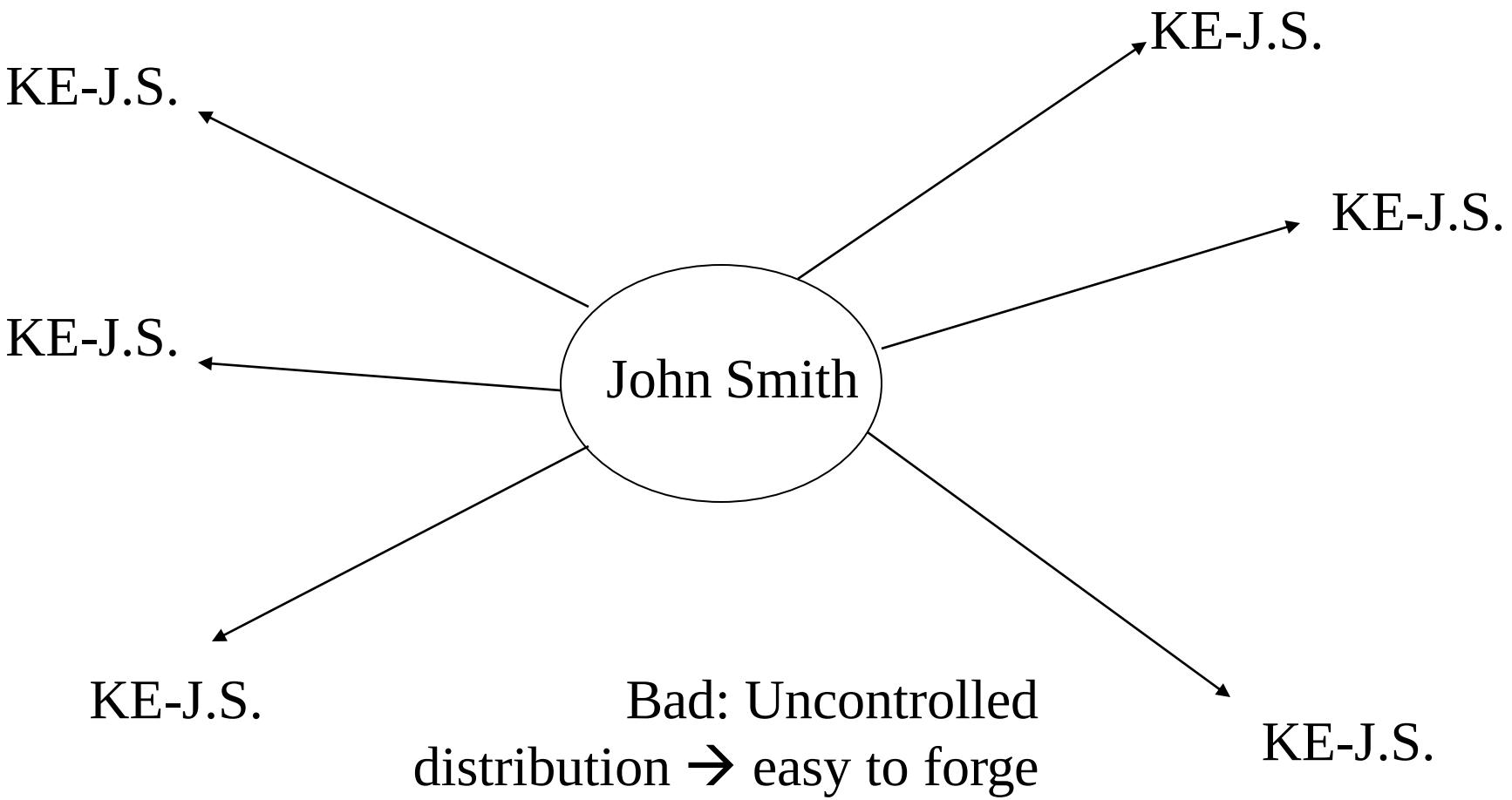
Symmetric-Key Distribution: Symmetric-Key Techniques

- Symmetric-Key without Server
- Symmetric-Key with Server

Asymmetric-Key Exchange

- Without server
  - Broadcasting –
  - Publicly available directory –
- With server
  - Public key distribution center –
  - Certificates –

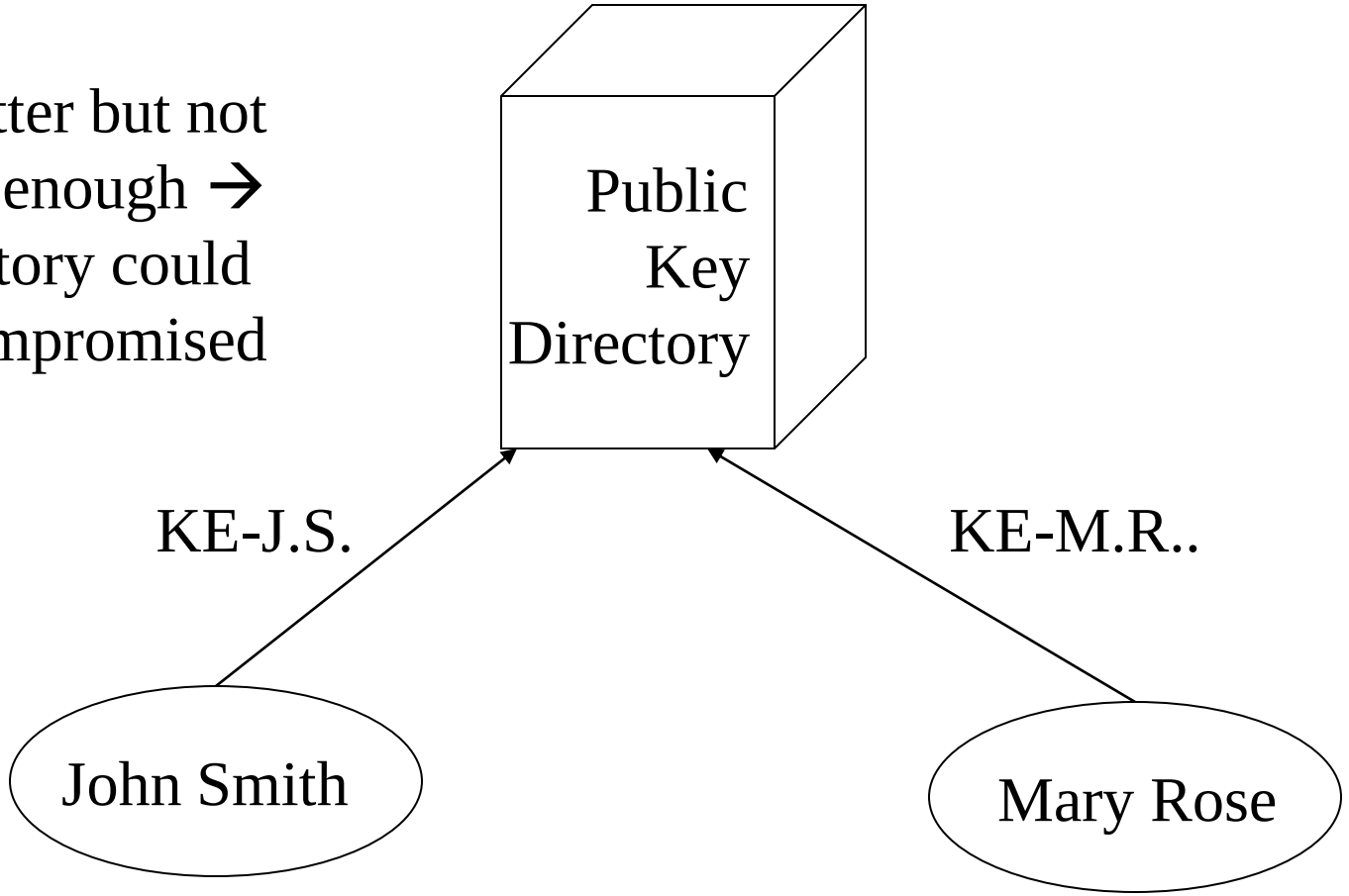
Public announcement



Bad: Uncontrolled distribution → easy to forge

Publicly available directory

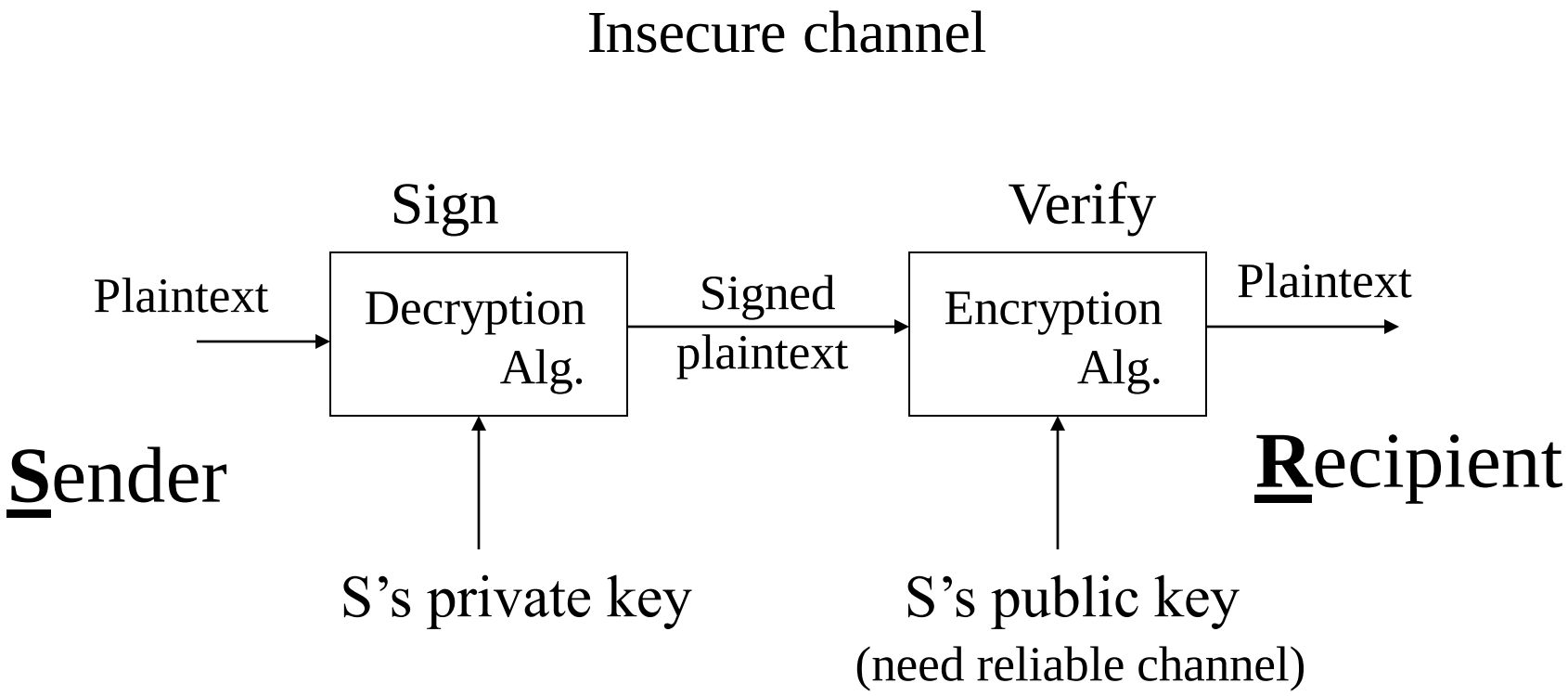
Better but not
Good enough →
Directory could
Be compromised



Digital Signature

- Need the same effect as a real signature
  - Un-forgeable –
  - Authentic –
  - Non-alterable –
  - Not reusable –

Digital Signatures in RSA



Attackers' Capabilities

- Read traffic
- Modify traffic
- Delete traffic
- Perform cryptographic operations
- Control over network principals

Password Management Policy

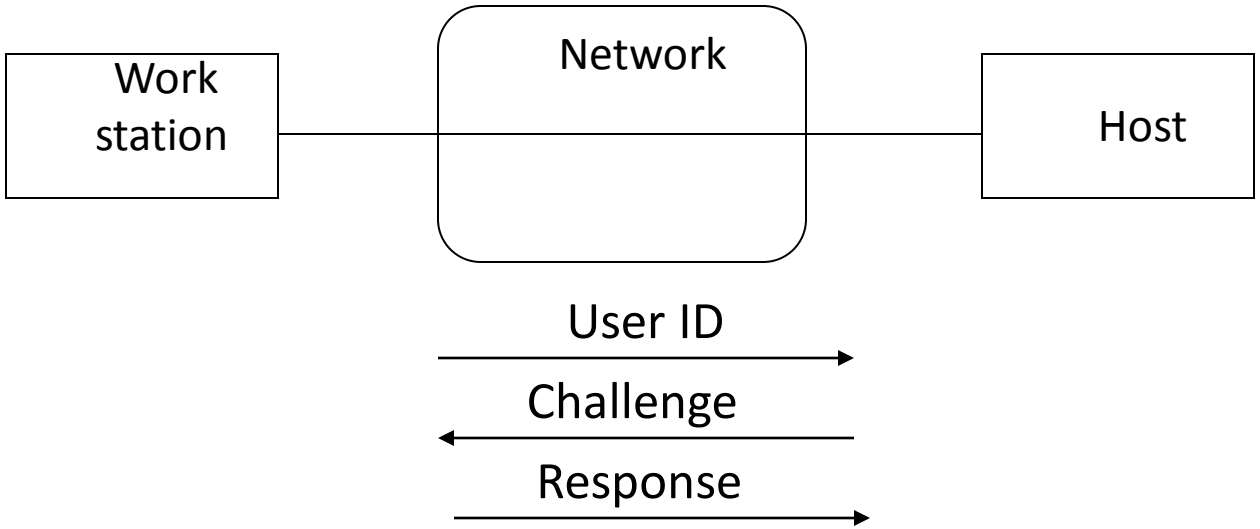
- Educate users to make better choices
- Ask or force users to change their password periodically
- Screen password choices

One-time Password

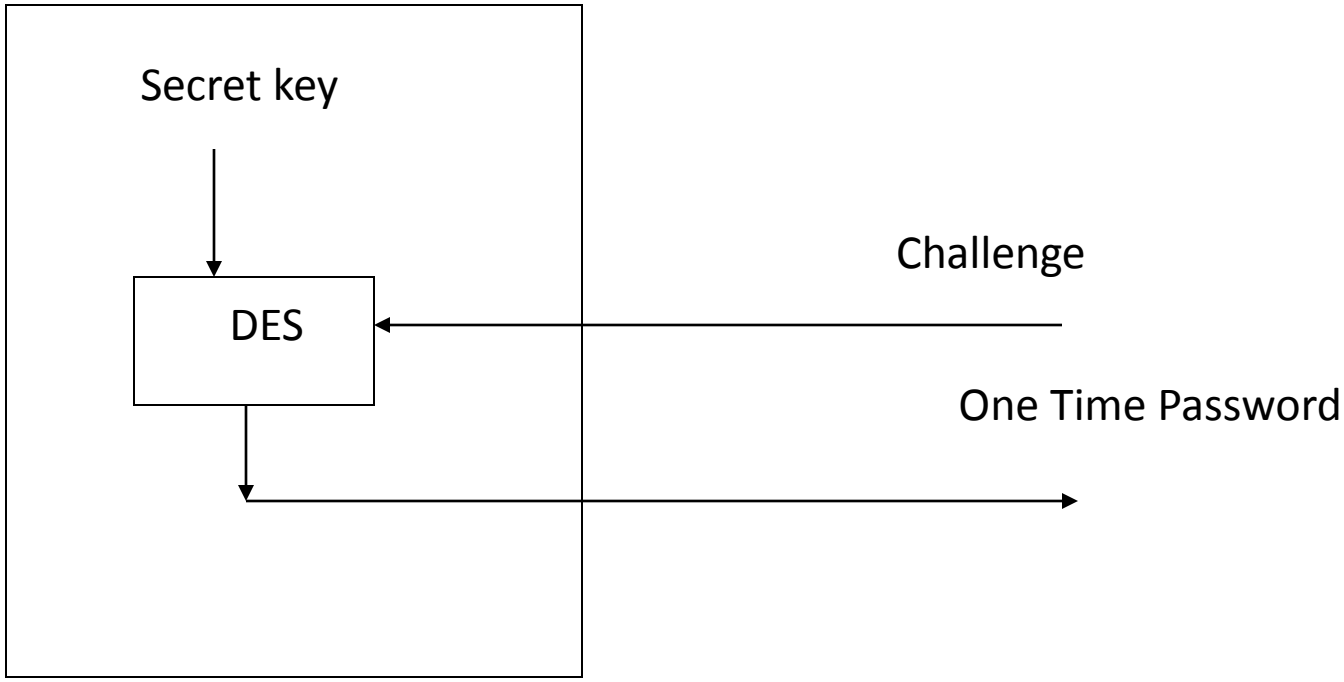
-Use the password exactly once!

Challenge Response

- Non-repeating challenges from the host is used
- The device requires a keypad



Challenge Response



Devices with Personal Identification Number (PIN)

- Devices are subject to theft, some devices require PIN (something the user knows)
- PIN is used by the device to authenticate the user
- Problems with challenge/response schemes
  - Key database is extremely sensitive –
  - This can be avoided if public key algorithms are used –

Biometrics

- Fingerprint
- Retina scan
- Voice pattern
- Signature
- Typing style

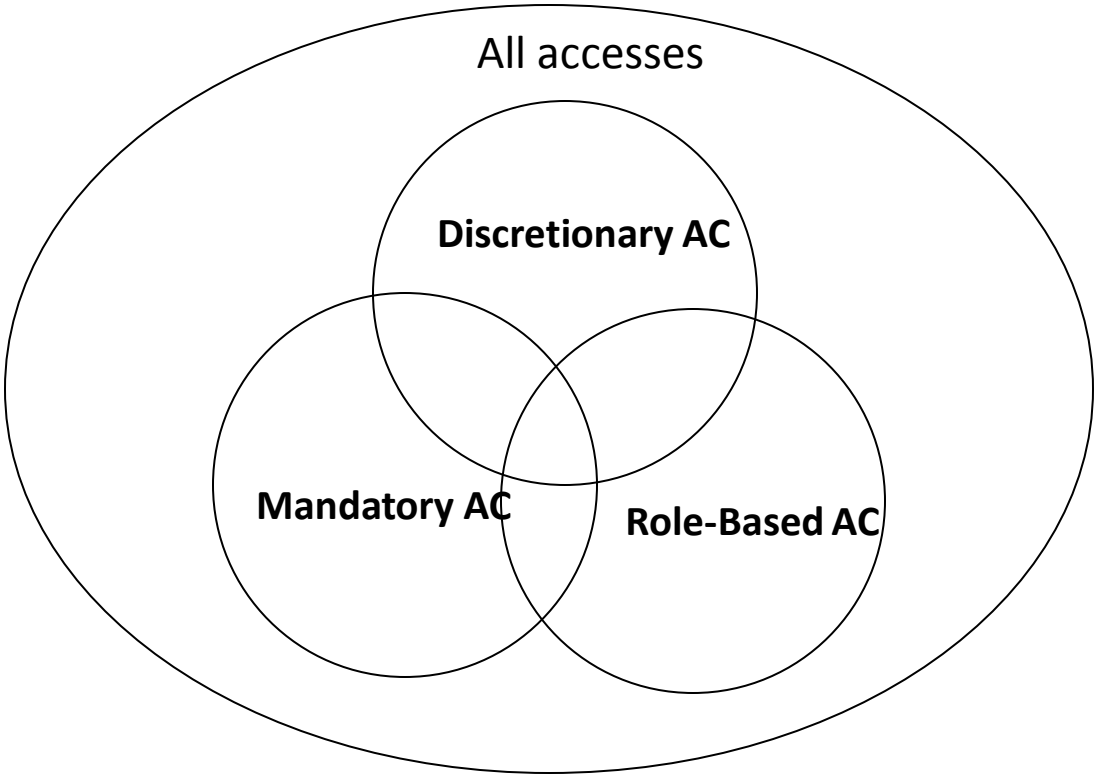
Access Control

- Protection objects: system resources for which protection is desirable
  - Memory, file, directory, hardware resource, software resources, etc.
- Subjects: active entities requesting accesses to resources
  - User, owner, program, etc.
- Access mode: type of access
  - Read, write, execute

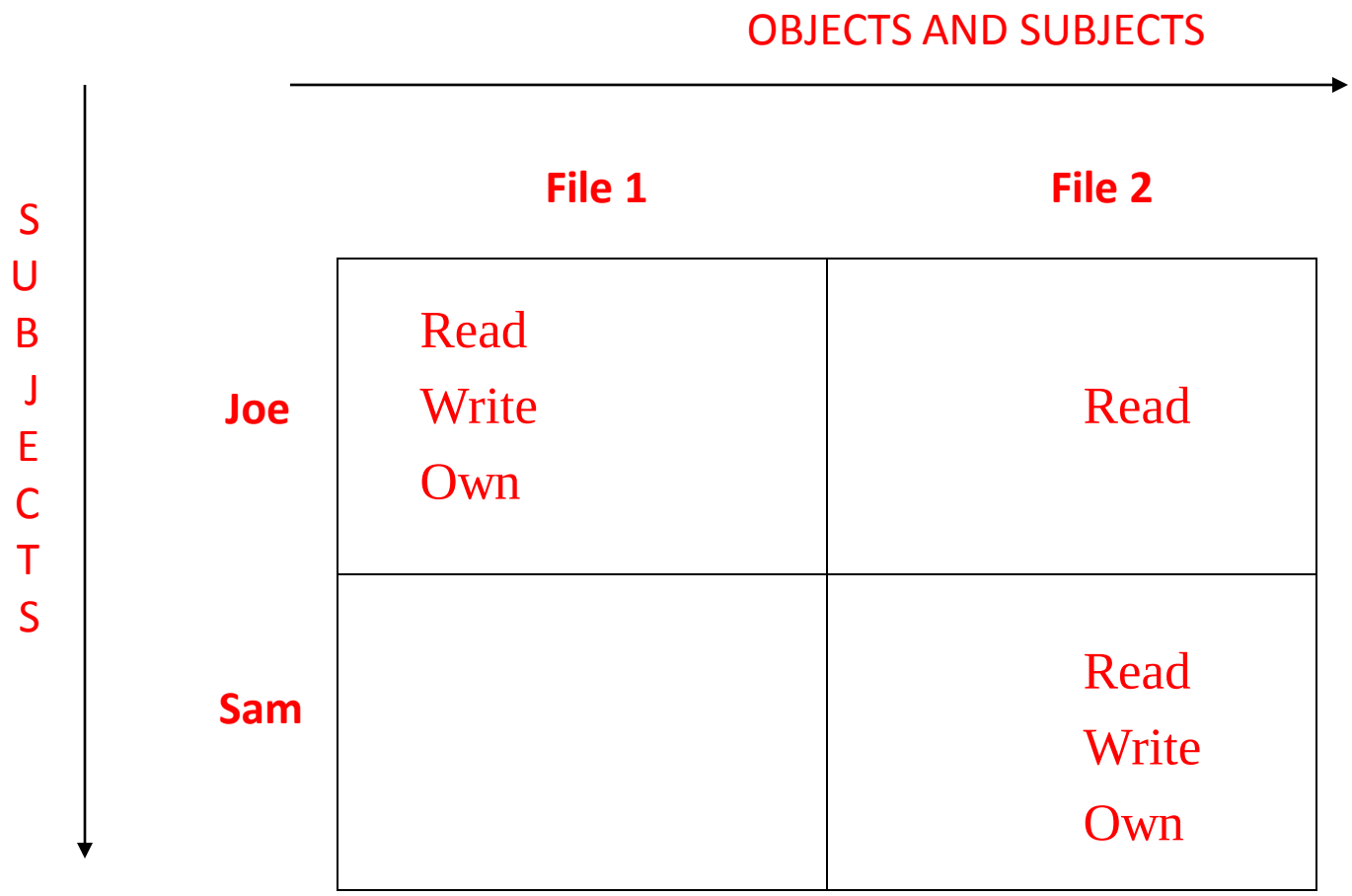
Access Control Requirement

- Cannot be bypassed
- Enforce organizational policy

Access Control Models



Access Matrix Model



Implementation

Access Control List (column) (ACL)

File 2	**File 1**
Joe:Read	Joe:Read
Sam:Read	Joe:Write
Sam:Write	Joe:Own
Sam:Own	

Capability List (row)

Joe: File 1/Read, File 1/Write, File 1/Own, File 2/Read

Sam: File 2/Read, File 2/Write, File 2/Own

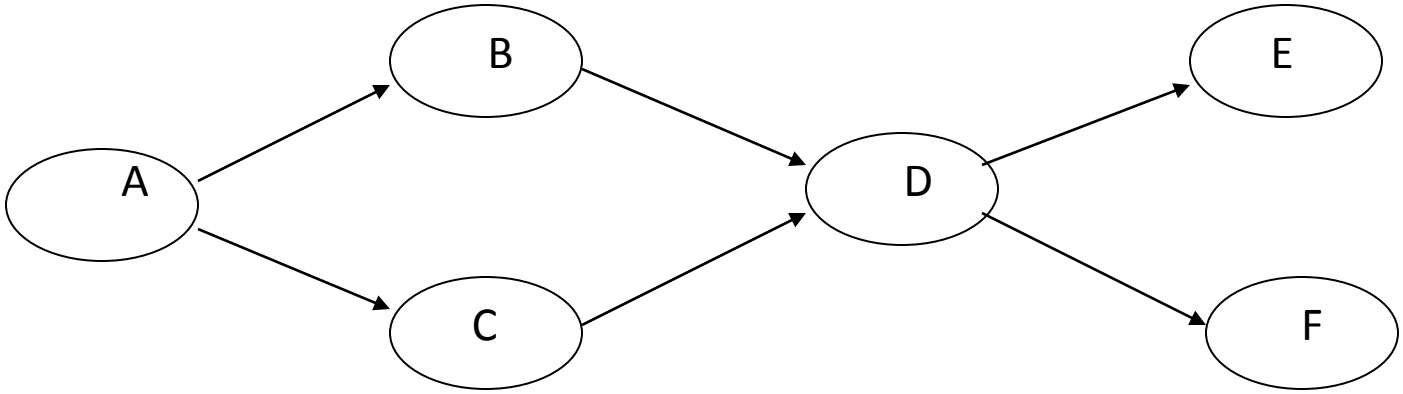
Access Control Triples

Object	Access	Subject
File 1	Read	Joe
File 1	Write	Joe
File 1	Own	Joe
File 2	Read	Joe
File 2	Read	Sam
File 2	Write	Sam
File 2	Own	Sam

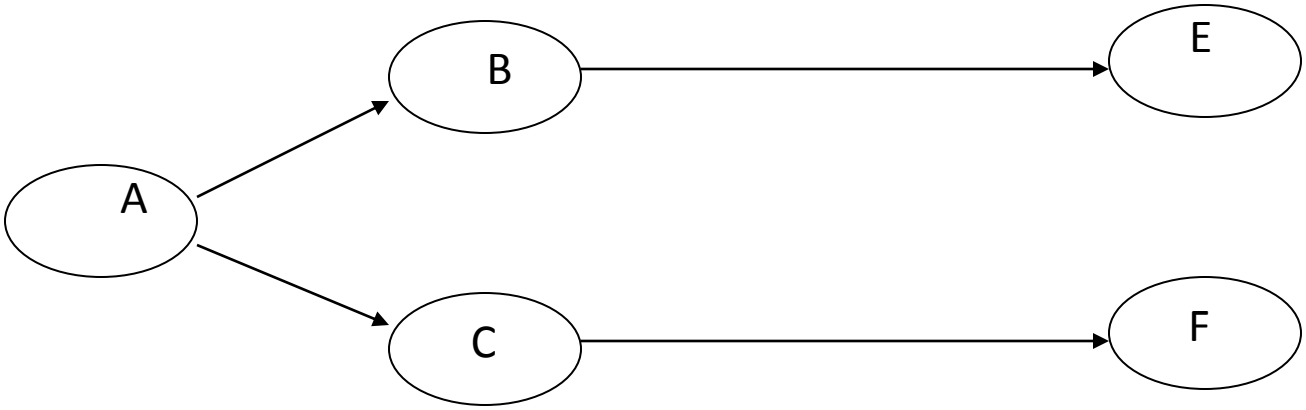
ACL v.s. Capabilities

- ACL:
  - Per object based –
  - Good for file systems –
- Capabilities:
  - Per subject based –
  - Good for environment with dynamic, short-lived subjects –

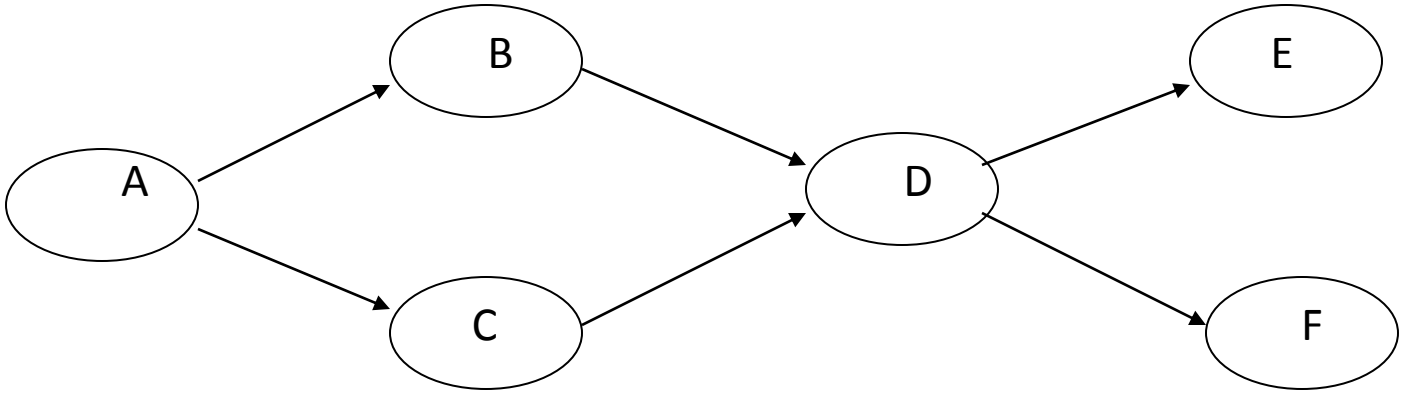
Non-cascading Revoke



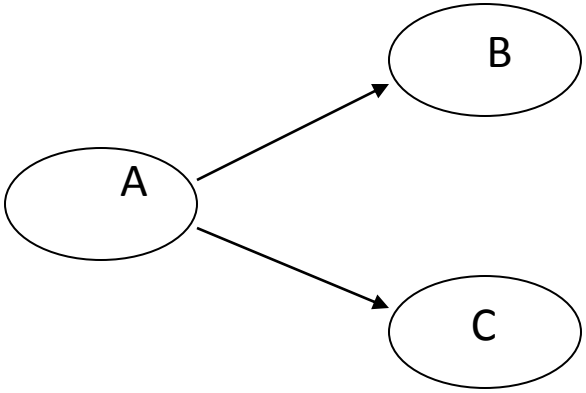
A revokes D's privileges



Cascading Revoke



A revokes D's privileges



DAC Overview

- Advantages:
  - Intuitive –
  - Easy to implement –
- Disadvantages:
  - Inherent vulnerability –
  - Maintenance of Grant/Revoke –

BLP Axioms 1.

- No read up
- Applies to *all subjects*

BLP Axioms 2.

- No write down
- Applies to *un-trusted subjects* only