Key terms

- **Exposure**
- **Vulnerability**
- **Attack**
- **Threat**
- **Control**
- **Major assets of computing:**
  - Hardware, Software, Data

Terminologies

- **Plaintext:** Message or data which are in their normal, readable (not crypted) form.
- **Encryption:** Encoding the contents of the message in such a way that hides its contents from outsiders.
- **Ciphertext**: The encrypted message

Terminologies

- **Decryption:** The process of retrieving the plaintext back from the ciphertext.

- **Key:** Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key.

Terminologies

- **Cryptography** is the art or science of keeping messages secret. It deals with all aspects of secure messaging, authentication, digital signatures, electronic money, and other applications.

- **Cryptosystems:** A cryptographic system (cryptosystem) consists of a pair of data transformations, namely encryption and decryption.

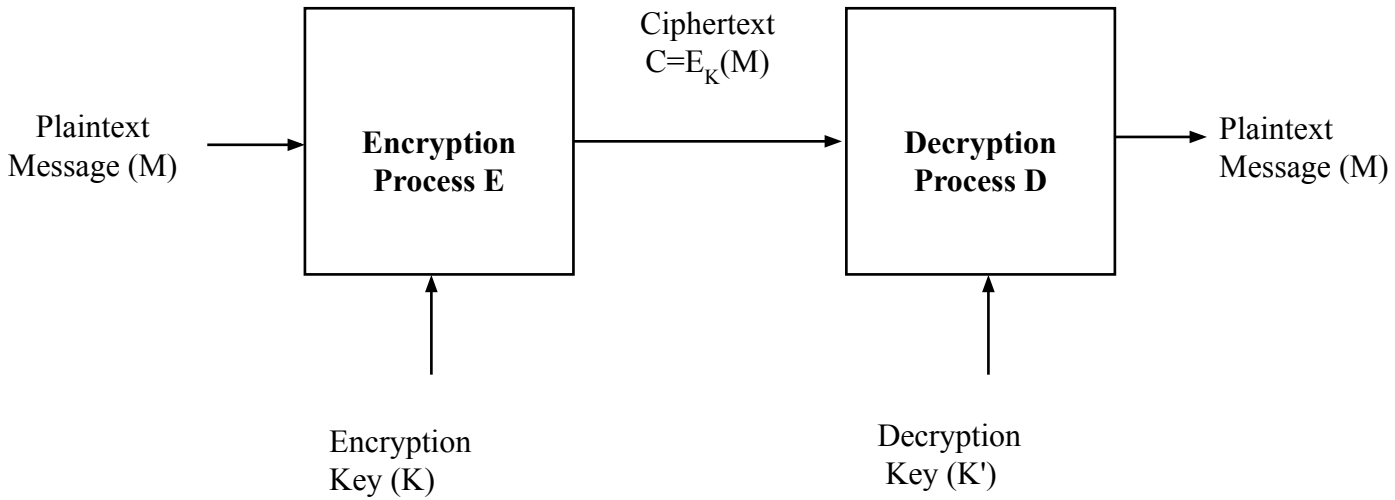
Terminologies

- **Cryptanalysis:** The art of **breaking** ciphers, i.e. retrieving the plaintext without knowing the proper key.
- **Cryptographers:** People who do cryptography
- **Cryptanalysts:** practitioners of cryptanalysis

Conventional Cryptosystem Principles

- **An cryptosystem has the following five ingredients:**
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm
- **Security depends on the secrecy of the key, not the secrecy of the algorithm**

Conventional Cryptosystem Principles

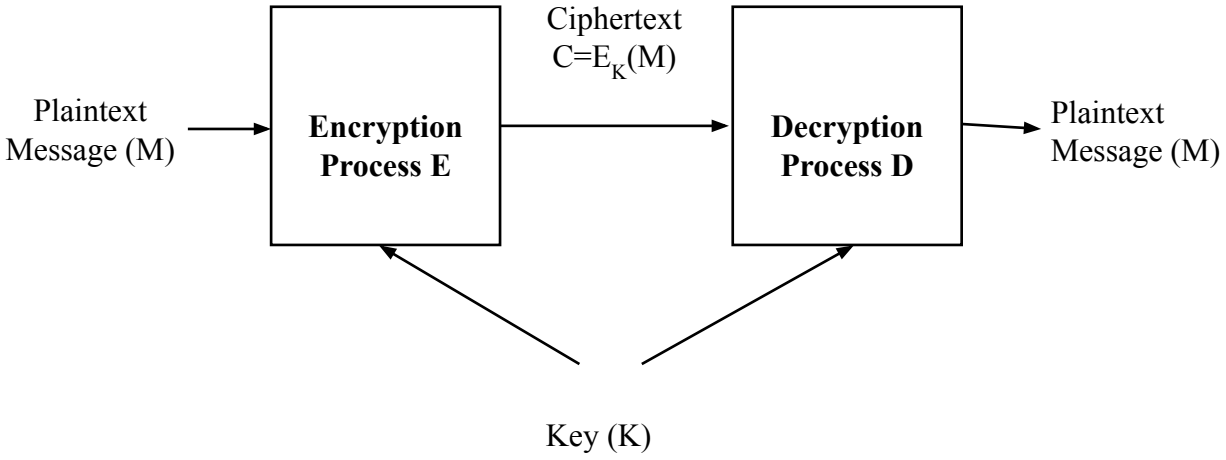


Classifications

- **Classification of cryptosystems**
  - Symmetric cryptosystems
  - Asymmetric cryptosystems

Symmetric Cryptosystem

- The same key is used for both encryption and decryption purposes



Symmetric Cryptosystem

- Examples of symmetric cryptosystem are Data Encryption Standard (DES)

- Problem : How do we distribute the key securely?

Key Distribution

- A key could be selected by A and physically delivered to B.
- A third party could select the key and physically deliver it to A and B.
- If A and B have previously used a key, one party could transmit the new key to the other, encrypted using the old key.

Key Distribution

- If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.

- **Session key:**
  - Data encrypted with a one-time session key.At the conclusion of the session the key is destroyed

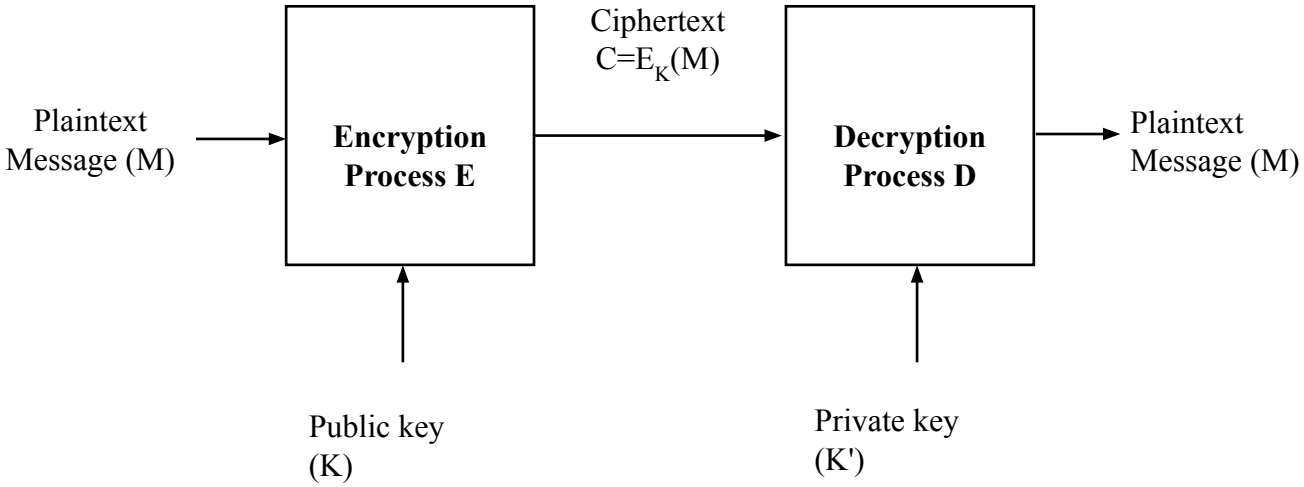
Assymmetric Cryptosystem

- Different keys are used for encryption and decryption purposes.
- The pair of keys are mathematically related and consist of a public key that can be published without doing harm to the system's security and a private key that is kept secret.
- Also known as public key cryptosystems

Assymmetric Cryptosystem

- The public key is used for encryption purposes and lies in the public domain.
- Anybody can use the public key to send an encrypted message.
- The private key is used for decryption purposes and remains secret.
- An example of a public cryptosystem is the RSA cryptosystem.

Assymmetric Cryptosystem



Encyption – can it be broken?

- Theoretically, it is possible to devise unbreakable cryptosystems
- However, practical cryptosystems almost always are breakable, given adequate time and computing power
- The trick is to make breaking a cryptosystem hard enough for the intruder

Types of Ciphers

- Ciphers can be broadly classified into the following two categories depending upon whether
  (i) a symbol of plaintext is immediately converted into a symbol of ciphertext (Stream Ciphers)
  (ii) or a group of plaintext symbols are converted as a block into a group of ciphertext symbols (Block Ciphers)

Stream Ciphers

- A symbol of plaintext is immediately converted into a symbol of ciphertext
- **Advantages**
  - Speed of transformation
  - Low error propagation
- **Disadvantages**
  - Low diffusion
  - Susceptible to malicious insertions and modifications

Block Ciphers

- A group of plaintext symbols are converted as a block into a group of ciphertext symbols
- **Advantages**
  - Diffusion
  - Immunity to insertions
- **Disadvantages**
  - Slowness of encryption
  - Error propagation

General Types of Ciphers

- **Substitution ciphers**
  - Letters of the plaintext messages are replaced with other letters during the encryption

- **Transposition ciphers**
  - The order of plaintext letters is rearranged during encryption

General Types of Ciphers

- **Product ciphers**
  - Combine two or more ciphers to enhance the security of the cryptosystem

Trends

- **Block size:** larger block sizes mean greater security
- **Key Size:** larger key size means greater security
- **Number of rounds:** multiple rounds offer increasing security

Monoalphabetic Substitution Ciphers

- **Caesar cipher**

  $c_i = E(p_i) = p_i + 3 \bmod 26$

  Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

  Ciphertext: d e f g h i j k l m n o p q r s t u v w x y z a b c

- **Example**

  Plaintext: CRYPTOGRAPHY IS GREAT FUN

  Ciphertext: fubswrjudskb lv juhdw

Polyalphabetic Substitution Ciphers

- Flatten the frequency distribution of letters by combining high and low distributions

- **Example:**

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Ciphertext1: a d g j m p s v y b e h k n q t w z c f i l o r u x

Ciphertext2: n s x c h m r w b g l q v a f k p u z e j o t y d i

Plaintext: VIGENERE TABLEAUX

Ciphertext: lbshnhzh fndqmniy

Transposition Ciphers

- Rearrangement of the letters or a message

Columnar transposition

Plaintext	**Ciphertext**
W H Y D O	welrnel
E S I T A	hswatta
L W A Y S	yiaihhn
R A I N I	dtyneed
N T H E N	oasinrs
E T H E R	
L A N D S	

Characteristics of good cipher

- **Shannon characteristics**
  - The amount of secrecy should determine the amount of labor appropriate for the encryption and decryption
  - The set of keys and encryption algorithm should be free of complexity
  - The implementation of the process should be as simple as possible

Characteristics of good cipher

- Errors in encryption should not propagate and cause corruption of further information in the message.
- Ciphertext size should not be larger than plaintext

- **Confusion**
  - The change in ciphertext triggered by an alteration in the plaintext should be unpredictable

Characteristics of good cipher

- **Diffusion**
  - Change in the plaintext should affect many parts of the ciphertext
- **Other issues**
  - Perfect secrecy vs. Effective secrecy
  - Redundancy of languages
  - Unicity distance

Methods of attack

- **Ciphertext-only attack**
  - The attacker gets a ciphertext and tries to find the corresponding plaintext.

- **Known-plaintext attack**
  - The attacker has some plaintext and its matching ciphertext. The task is to find a key corresponding to this match.

Methods of attack

- **Chosen-plaintext attack**
  - Here, the attacker selects a plaintext and ciphers it using the cryptotechinque he attacks. The plaintext may be chosen to ease the task of key finding.

Application of Cryptography

- Confidentiality
- Authentication
- Message Integrity
- Digital Signature

Confidentiality

- Confidentiality of a message can be achieved by encrypting it with a key (symmetric/asymmetric).
- Only the authorized recipients of the message possessing the decryption can decrypt the message.
- It will become difficult for an intruder to see the content of the message in the absence of the appropriate key.

Authentication

- Authentication is the process of reliably verifying the identity of a distributed entity amidst threats arising from the environment.

- In a computer system there are generally three different levels of authentication that are involved as given below
  - User Authentication

Authentication

- Authentication of a distributed entity (e.g. remote computer, smart card, remote process etc.)

- Authentication of the system to the entity - System Authentication.

Authentication

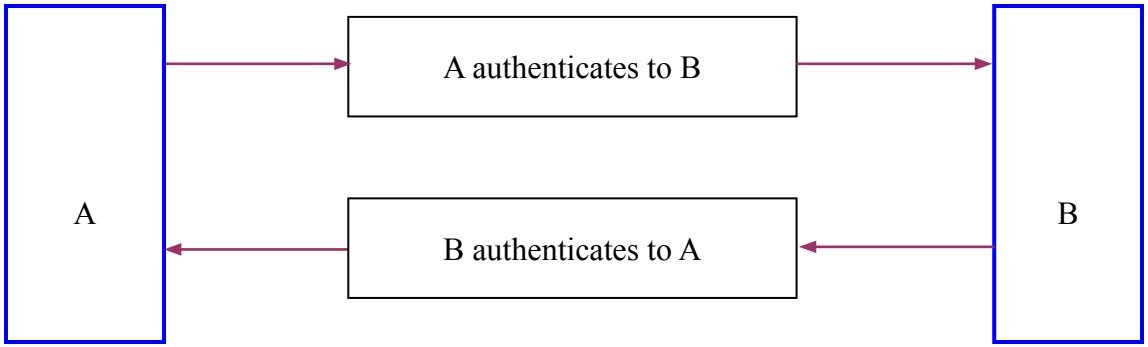
- Most of the mutual authentication protocol addresses the following two different issues:
  - Authentication of distributed entities.
  - Establishment of a random session key between the authenticated entities

Authentication

- For any claimant entity to authenticate itself to a verifier entity two different strategies exist namely:
  - Direct authentication
  - Authentication via a trusted third party

Authentication

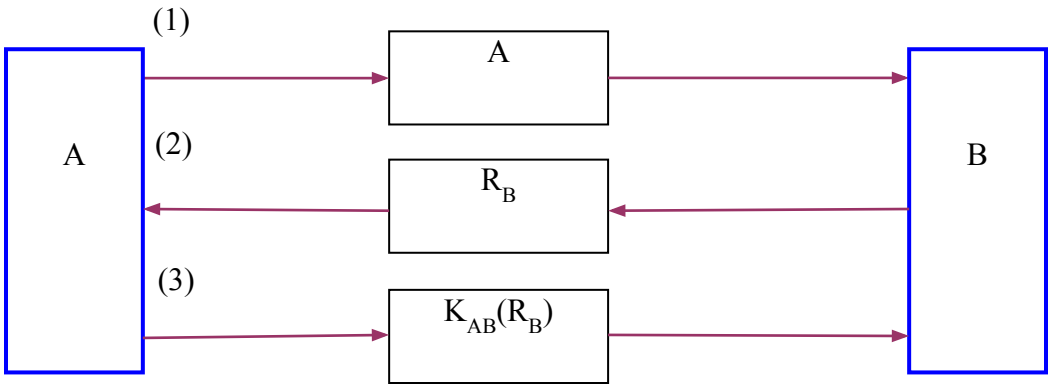
- **Direct authentication**



- **Limitations** - Key management is relatively complex, e.g. for a distributed entity to communicate securely with *n* other entities, it needs to maintain a minimum of *n* keys.

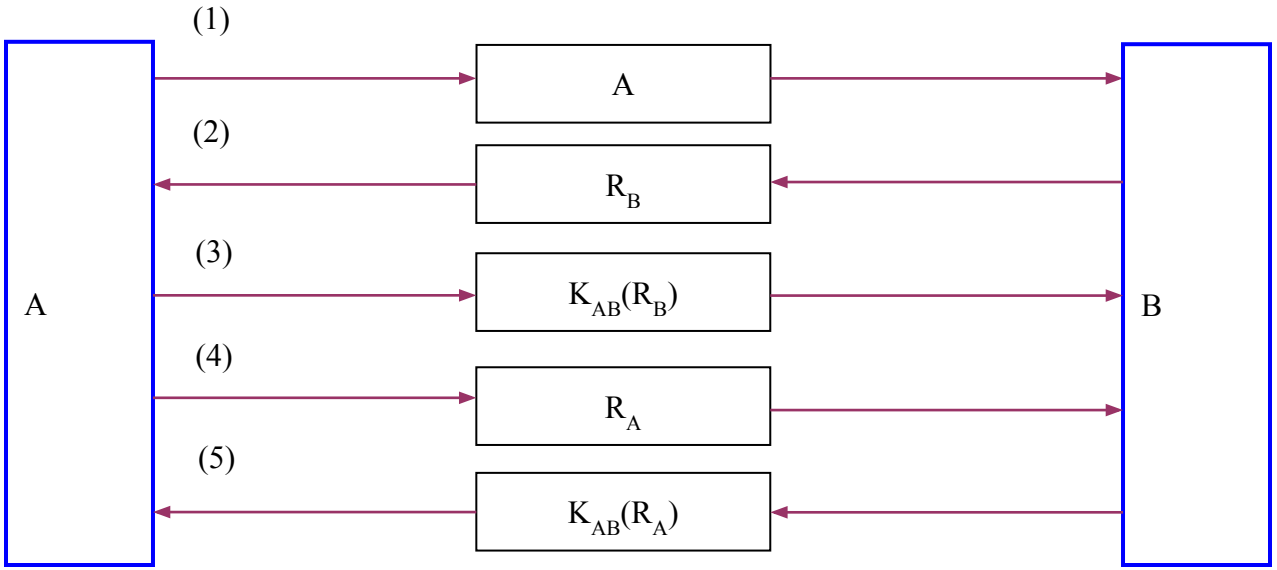
Authentication

- Example – Unidirectional Authentication



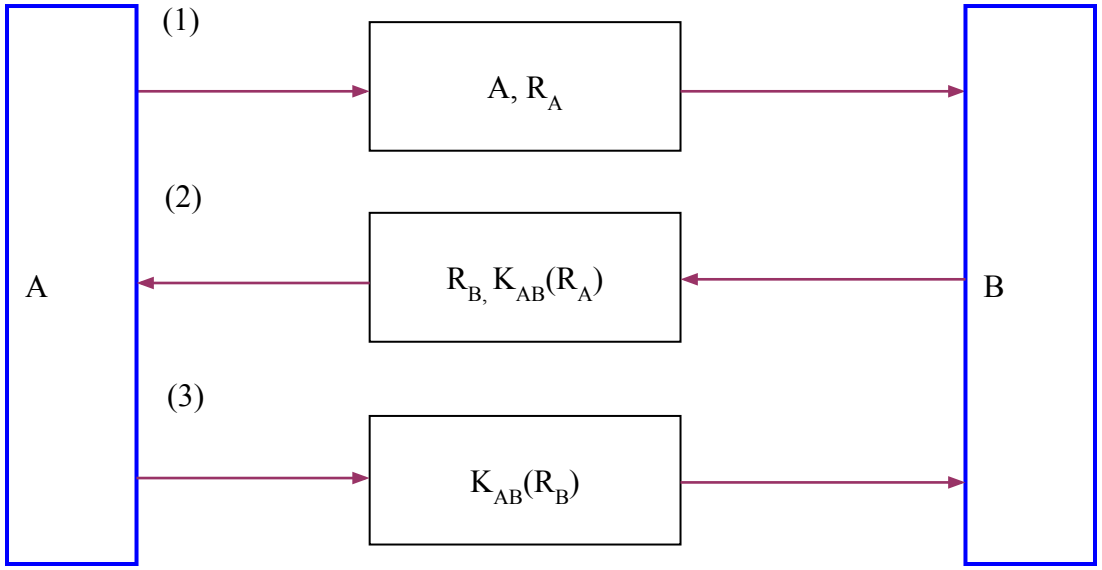
Authentication

- Example – Mutual Authentication



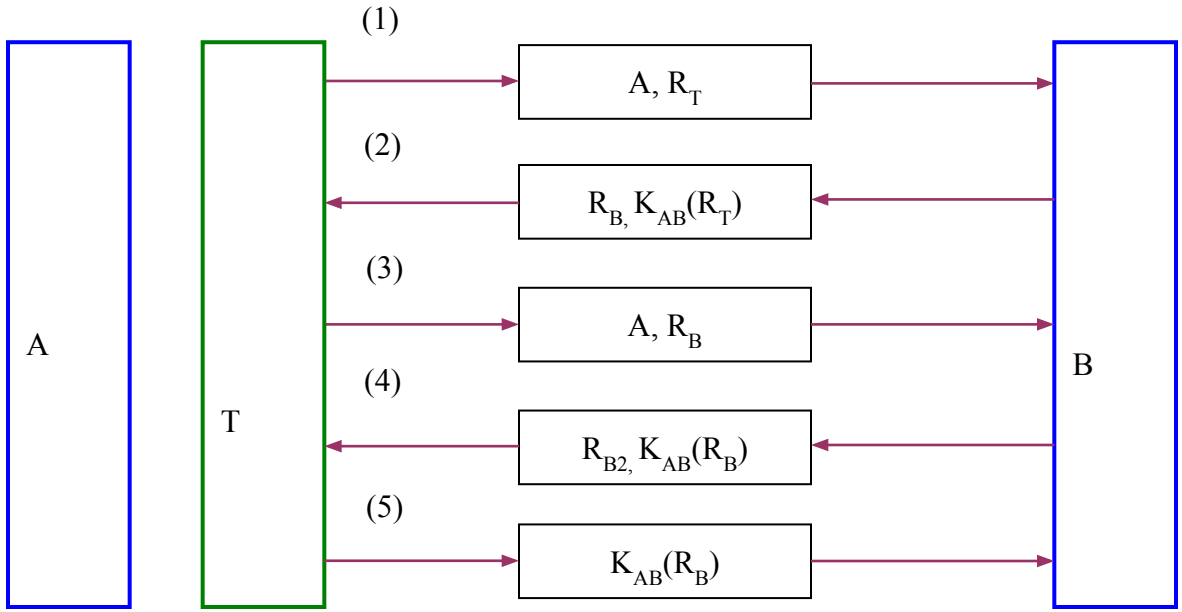
Authentication

- Example – Optimized Mutual Authentication



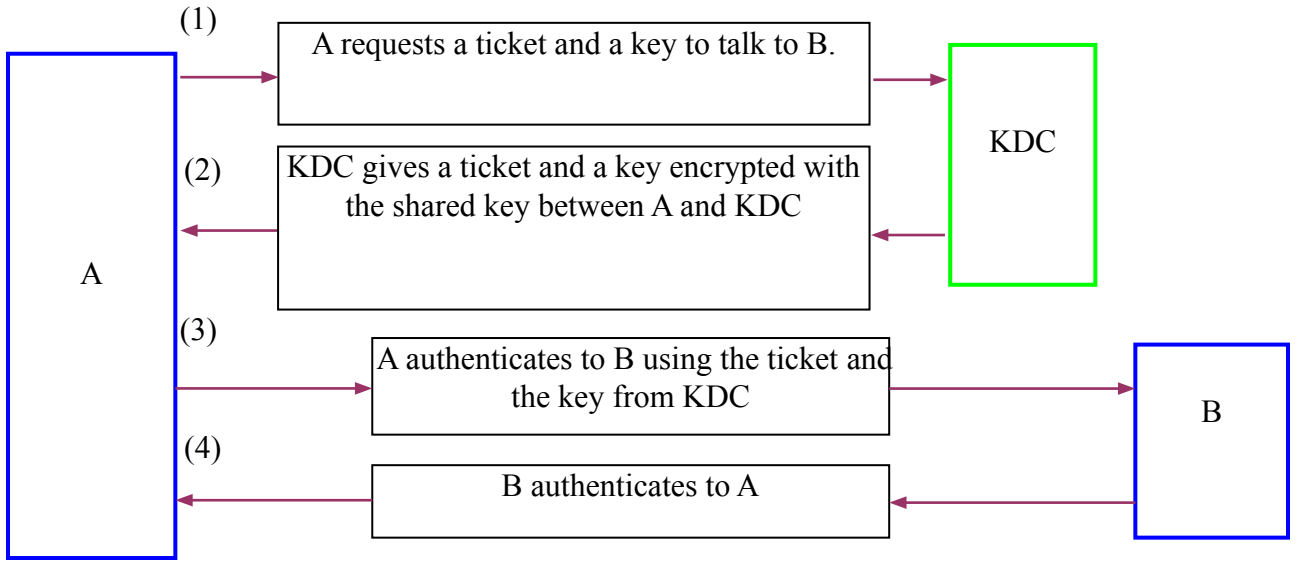
Authentication

- Problem !!!



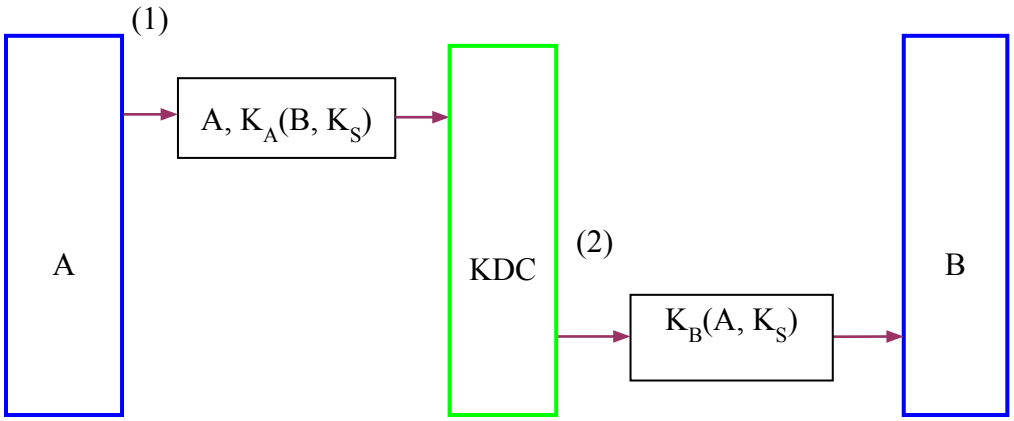
Authentication

- **Authentication via a trusted third party**



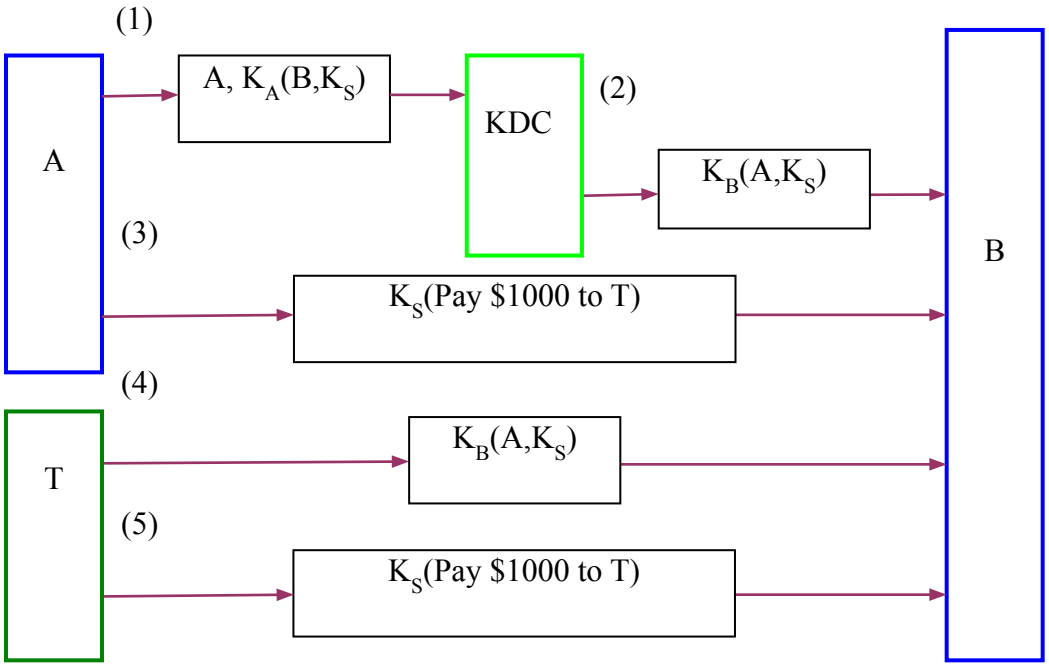
Authentication

- Example



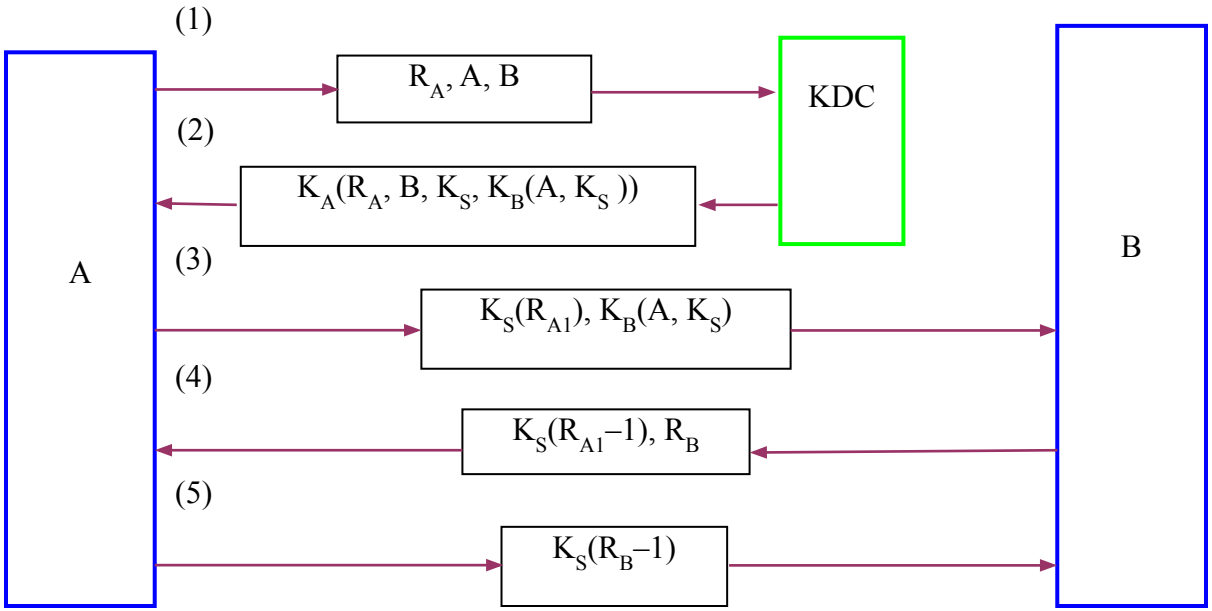
Authentication

- Problem – Replay attack



Authentication

- Another Example ??



Authentication

- Problem
  - Old session keys can be valuable. If T can manage to get hold of an old session key, it can launch a successful **replay attack** by replaying the sequence from message (3) and convince B that it is A.
  - If the key shared between A and the KDC is ever compromised, the consequences can be drastic. T can use the key to obtain session keys to talk with anyone.

Authentication

- **Message**
  - Authentication Protocols are very hard to design.

Message Authentication

- **Objective:**
  - Contents have not been altered
  - A hash function is used

- Hash Functions
  - A hash function is a one way function that maps values from a large domain into a comparatively small range known as a digest.

Message Authentication

- **Properties of a HASH function H :**
  - H can be applied to a block of data at any size
  - H produces a fixed length output
  - H(x) is easy to compute for any given x.
  - For any given block x, it is computationally infeasible to find x such that H(x) = h
  - For any given block x, it is computationally infeasible to find with H(y) = H(x).
  - It is computationally infeasible to find any pair (x, y) such that H(x) = H(y)

Message Authentication

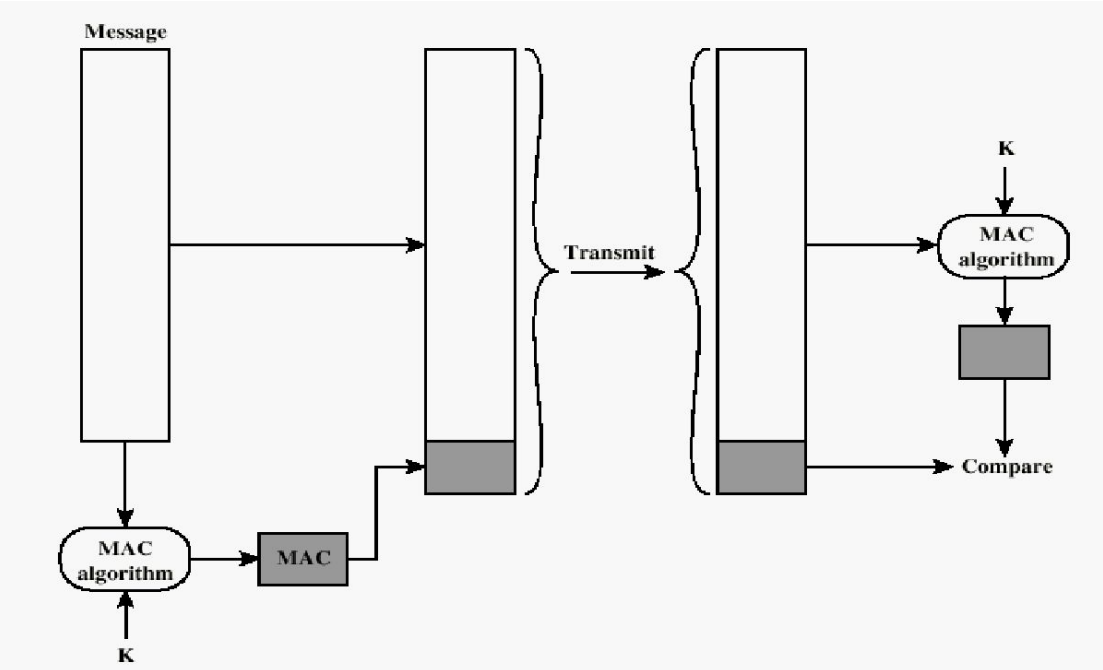


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

Digital Signature

- A message can be attached a digital signature to guarantee authenticity, integrity and non-repudiation.
- Asymmetric Cryptography is used.
- A digital signature is a block of data that is generated by the sender of a message using his/her secret key. The public key of the user is later used by the receiver to verify whether the message was *signed* by that particular user.

Digital Signature

- The following are the features of digital signature
  - Verification of a correct signature will succeed
  - Modification of a signed message will be detected
  - Signature will not help divulge signer's private key
  - Only parties in the possession of a secret key will be able to produce a valid signature

Software Security

- **Why are software flawed?**
  - Controls apply at individual program or programmer level
  - Software engineering techniques evolve much faster than security techniques
  - Malicious software vs. accidental errors

Malicious code

- **Type** **Characteristics**

  Virus Attaches itself to programs and propagates copies of itself to other programs

  Trojan horse Contains unexpected functionality

  Logic bomb Triggers action when a condition occurs

  Time bomb Triggers action at a certain time

  Trapdoor Allows unauthorized access to functionality

Malicious code

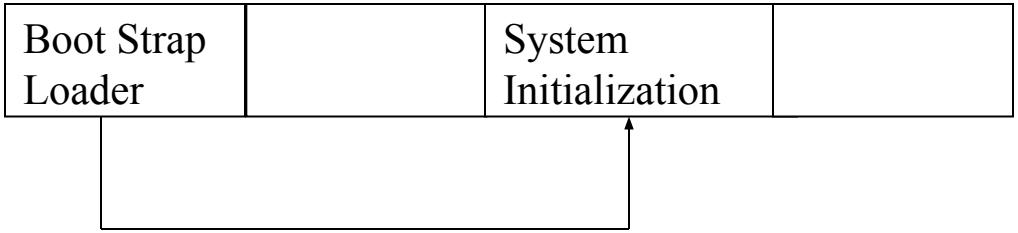
Type	Characteristics
Worm	Propagates copies of itself through a network
Rabbit	Replicates without limit to exhaust resources

”Good viruses”

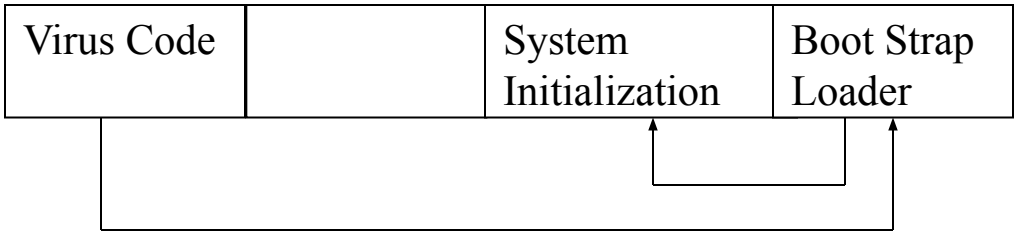
- Are hard to detect
- Are hard to destroy
- Spread widely
- Can re-infect cleaned files
- Are easy to create
- Are machine independent

Hiding places

- Boot sector



Normal Process



Infection

Hiding places

- Memory- resident viruses
- Macro, library etc. viruses

Effects and causes

Effect	How caused?
Attach to executable Program	• Modify file directory • Write to executable file
Attach to data or control	• Modify directory • Rewrite data • Append to data • Append data to itself

Effects and causes

Effect	How caused?
Remain in memory	• Intercept interrupts and modify handlers
Infect disks	• Intercept interrupt • Intercept OS call • Modify system file • Modify ordinary executables

Effects and causes

Effect	How caused?
Spread infection	• Infect boot sector • Infect system program • Infect ordinary program • Infect data that controls ordinary programs

How to prevent infections?

- Make sure you know the source of software
- Test new software on an isolated computer
- Make backups of bootable disks, store safely
- Keep backups of system files
- Use detectors
- Be careful with macro scripts

Outline

- Network threats
- Network controls
- Firewalls
- Internet security

Network threats

- Causes of security problems:
  - Sharing of resources and workload
  - Complexity of systems and interconnection mechanisms
  - Unknown security perimeter
  - Multiple points of attacks
  - Anonymity of attackers
  - Unknown access paths to resources

What could be attacked?

- *local nodes* connected via *local communications links* to a *local area network* which also has *local data storage, local processes* , and *local devices*. The LAN is also connected to a *network gateway* that gives access via *network communications links* to *network control resources , network routers*, and *network resources*, such as databases.

What can an attacker do?

- Intercept data in transit
- Modify data in transit
- Gain unauthorized access to programs or data in remote hosts
- Modify programs or data in remote hosts
- Insert communications
- Replay previous communication
- Block selected traffic
- Block all traffic
- Run a program at a remote host

By what means?

- Wiretapping
- Impersonation
- Message confidentiality violations
- Message integrity violations
- Hacking
- Code integrity violations
- Denial of service

Wiretapping

- Passive vs. active wiretapping
  - Cable
  - Microwave
  - Satellite communications
  - Optical fibre

Message confidentiality violations

- Mis-delivery
- Exposure in processing systems

Message integrity violations

- Change content of a message
- Change part of the content of a message
- Replace a message
- Reuse an old message
- Change the apparent source of a message
- Redirect a message
- Destroy or delete a message

Hacking

- hacker vs. cracker
- Hacking tools
- Automated attacks
- Distributed automated attacks
- Are they a real threat?

Code integrity violations

- User is typically unaware of the content of the downloaded file
- File downloading may happen without user's permission

Denial of service

- Connectivity
- Flooding
- Routing problems
- Disruption of service

Firewalls

- In the good ol' days, cities were protected by thick walls, and houses were separated from each other by firewalls that prevented of, for example, spread of fire throughout the city.

- Single point of control where network traffic is examined, could help in the maintenance of security

Firewalls

- Physical world analogies:
  - Passport (and visa) checking at borders
  - Apartments are often locked at the entrance in addition to each door
- Properties:
  - All traffic from inside to outside, and vice versa, must pass through a firewall

Firewalls

- Only authorized traffic, as defined by the local security policy, will be allowed to pass
- The firewall itself is immune to penetration