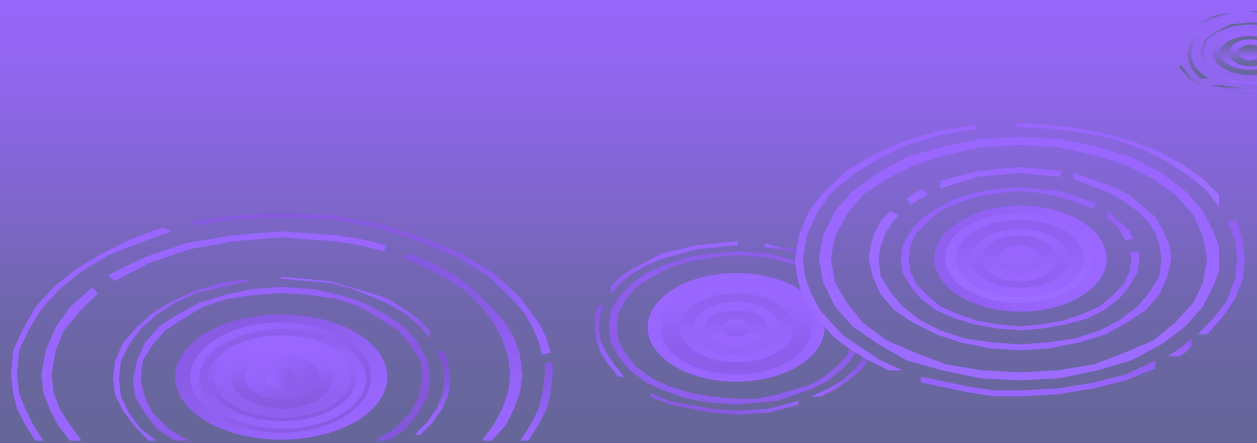
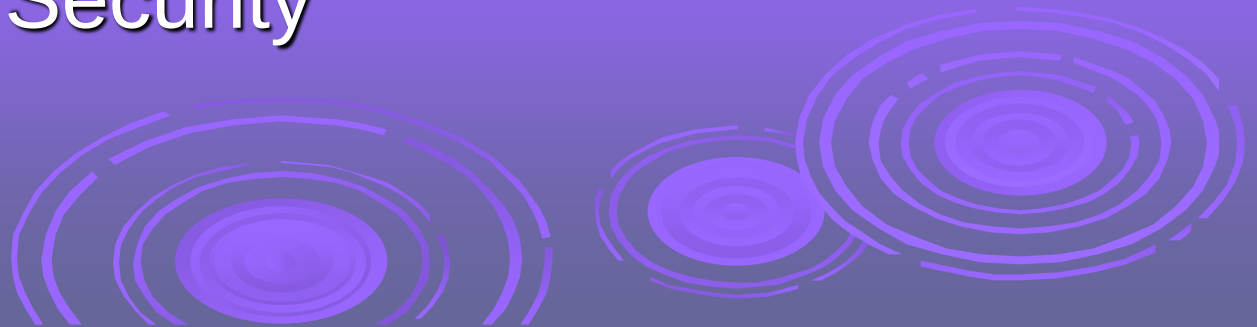
Cryptography for Blockchain



Roadmap

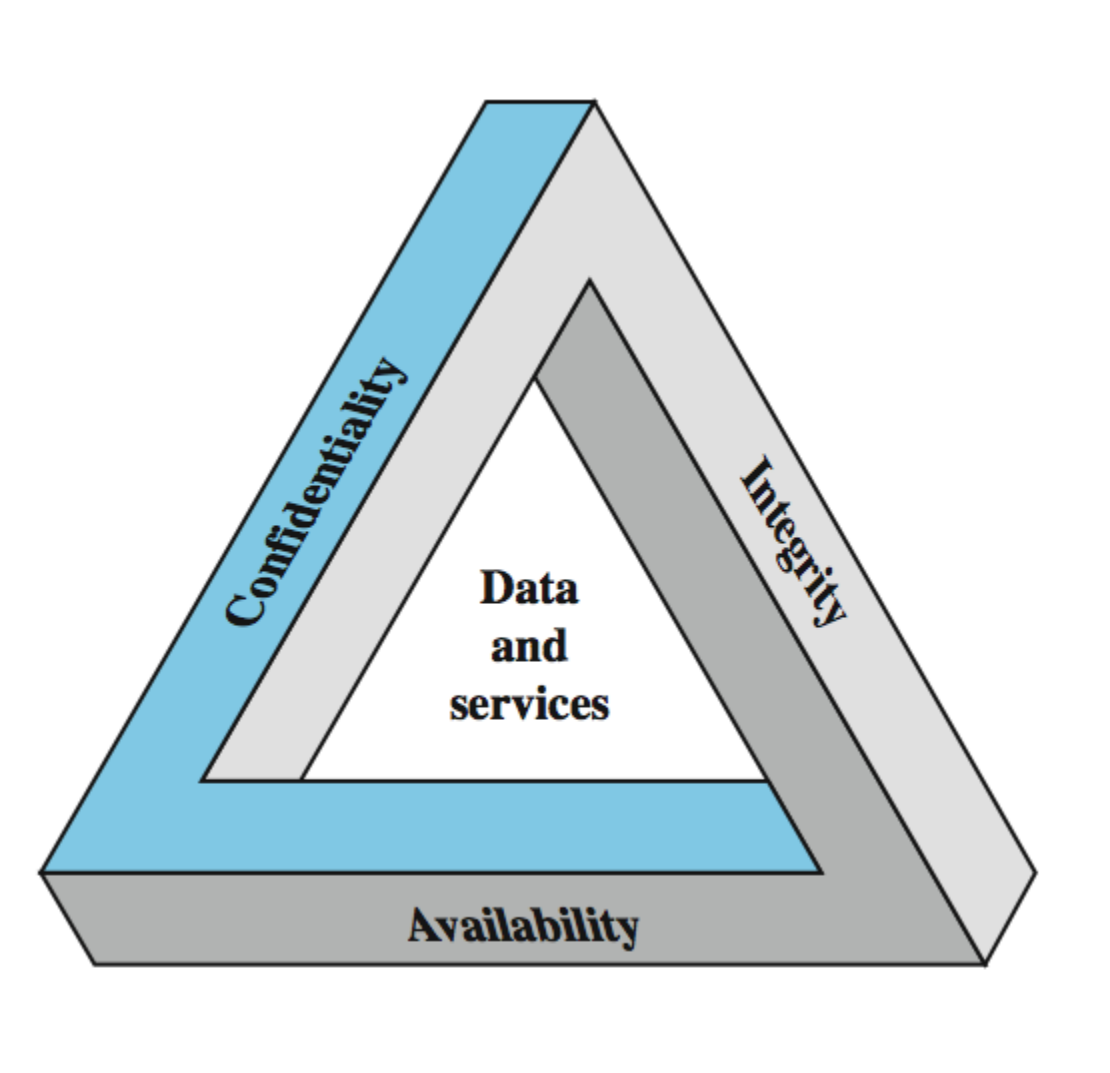
- Cryptographic algorithms
  - symmetric ciphers
  - asymmetric encryption
  - hash functions
- Mutual Trust
- Network Security
- Computer Security



Standards Organizations

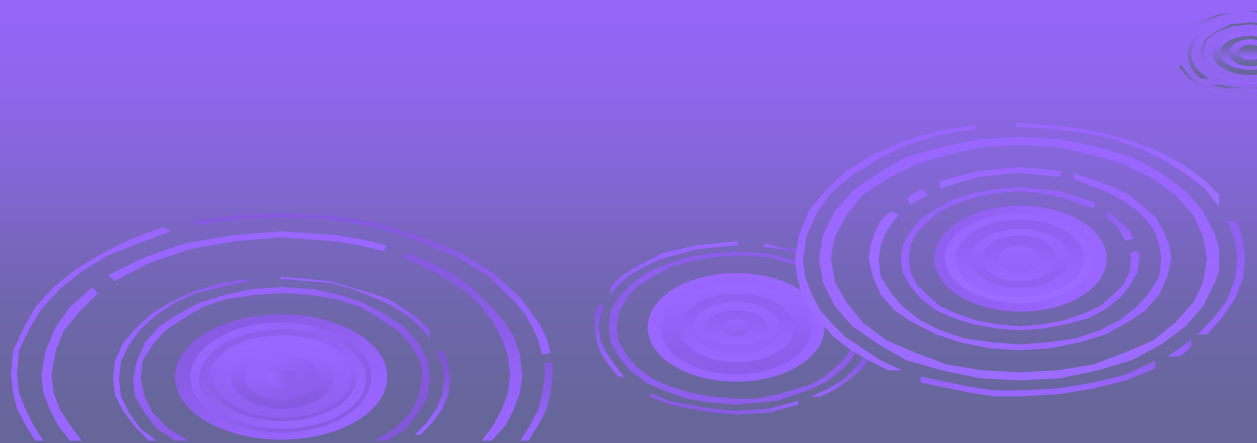
- National Institute of Standards & Technology (NIST)
- Internet Society (ISOC)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)
- RSA Labs (de facto)

Key Security Concepts



Levels of Impact

- can define 3 levels of impact from a security breach
  - Low
  - Moderate
  - High



Low Impact

- The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might
  - (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
  - (ii) result in minor damage to organizational assets;
  - (iii) result in minor financial loss; or
  - (iv) result in minor harm to individuals.

Moderate Impact

- The loss could be expected to have a serious adverse effect on organizational operations, assets, or individuals.
- A serious adverse effect means that, e.g., the loss might
  - (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
  - (ii) result in significant damage to organizational assets;
  - (iii) result in significant financial loss; or
  - (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

High Impact

- The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- A severe or catastrophic adverse effect means that, for example, the loss might
  - (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
  - (ii) result in major damage to organizational assets;
  - (iii) result in major financial loss; or
  - (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

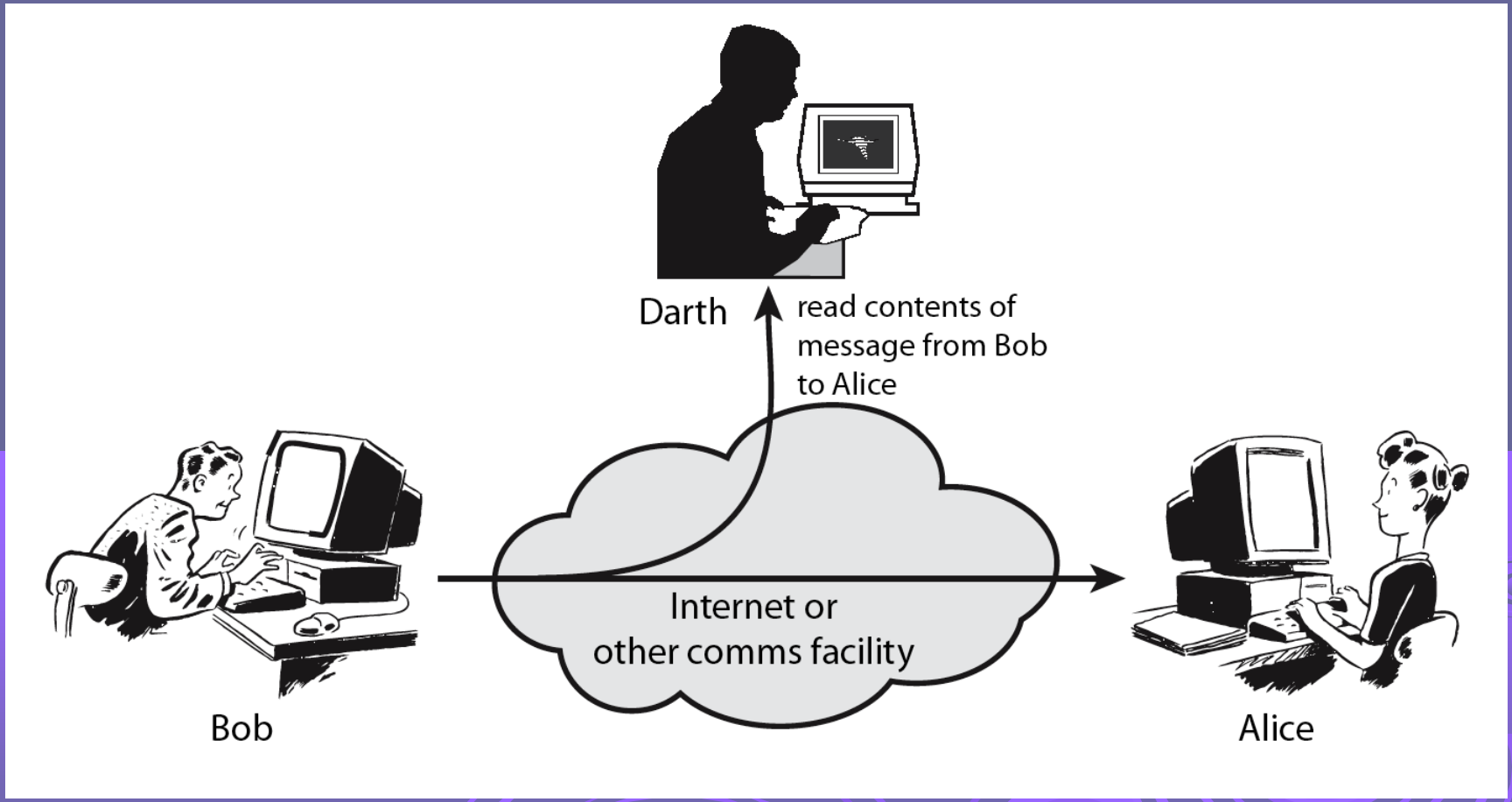
Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – authentication service
- authenticity – admission ticket
- non-repudiation – stock sell order

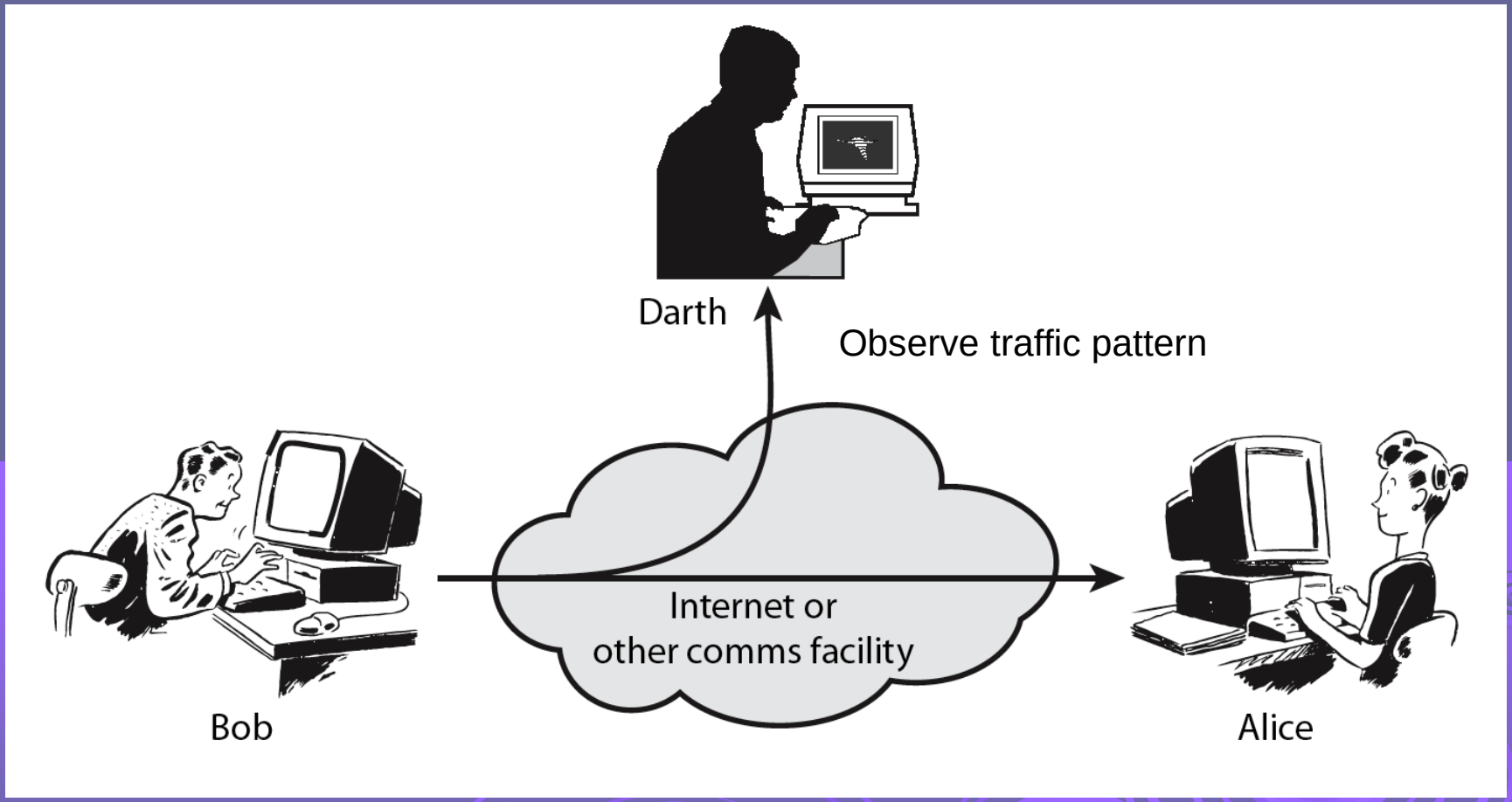
Aspects of Security

- consider 3 aspects of information security:
  - **security attack**
  - **security mechanism (control)**
  - **security service**
- note terms
  - *threat* – a potential for violation of security
  - *vulnerability* – a way by which loss can happen
  - *attack* – an assault on system security, a deliberate attempt to evade security services

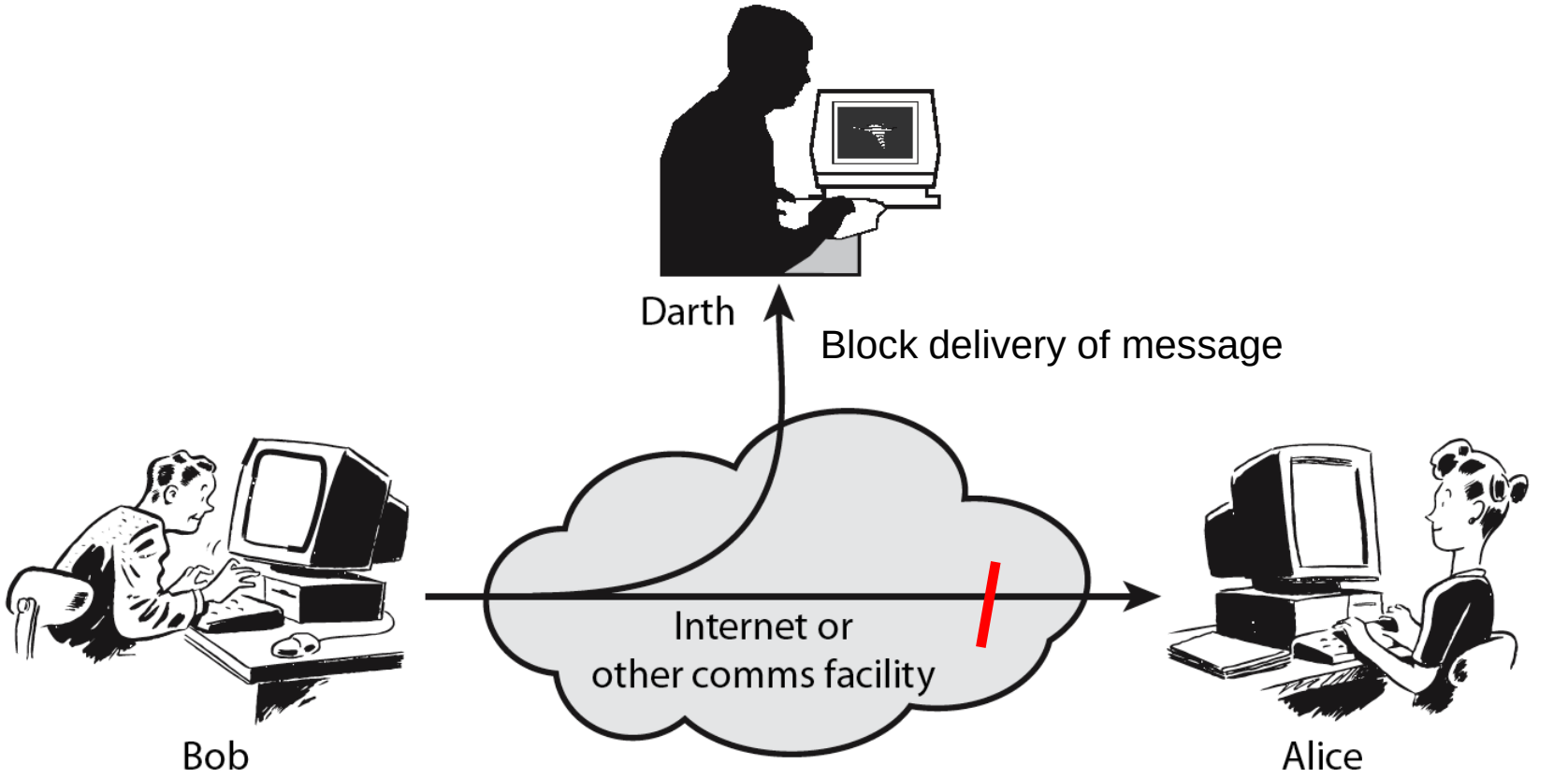
Passive Attack - Interception



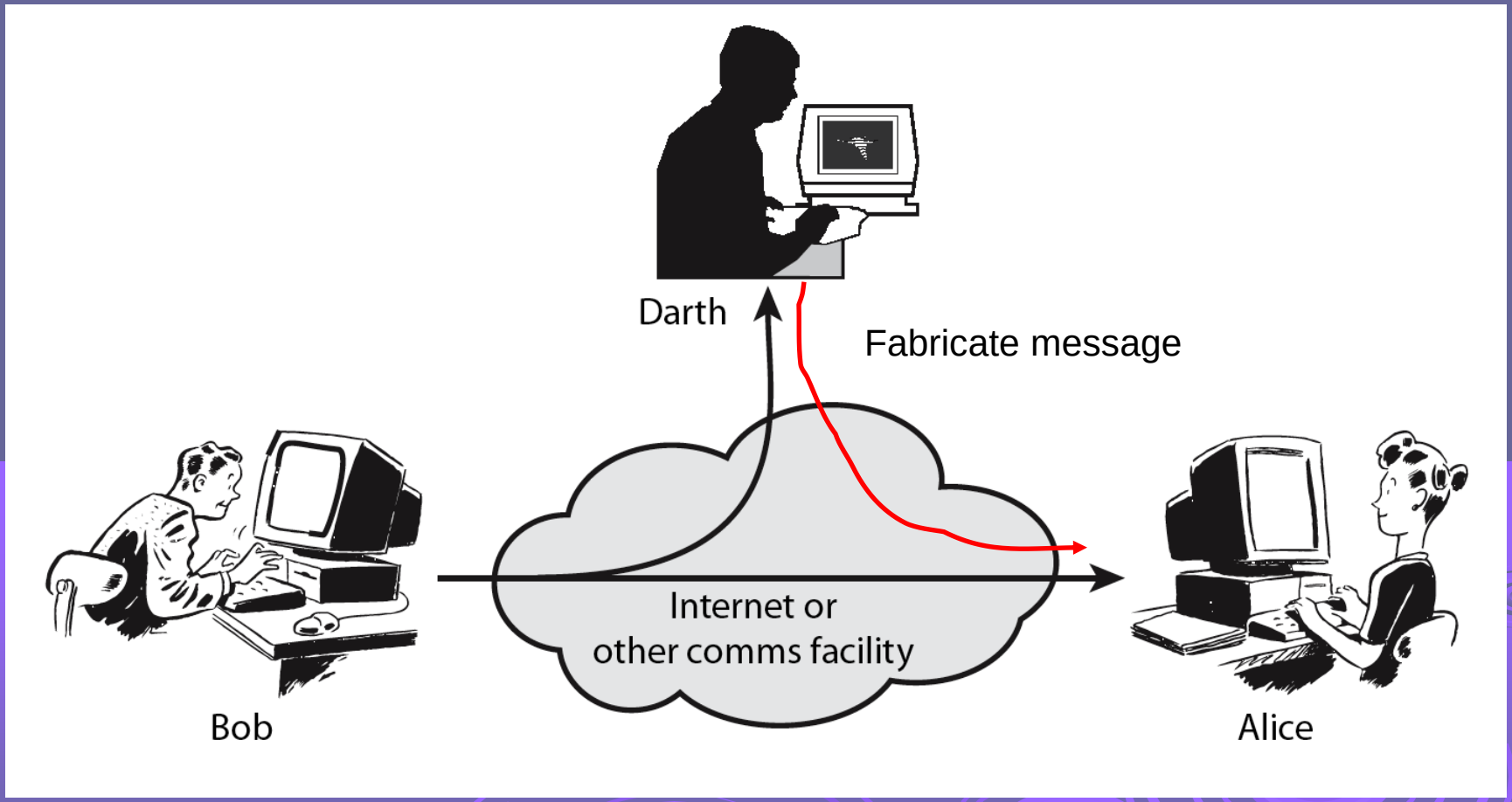
Passive Attack: Traffic Analysis



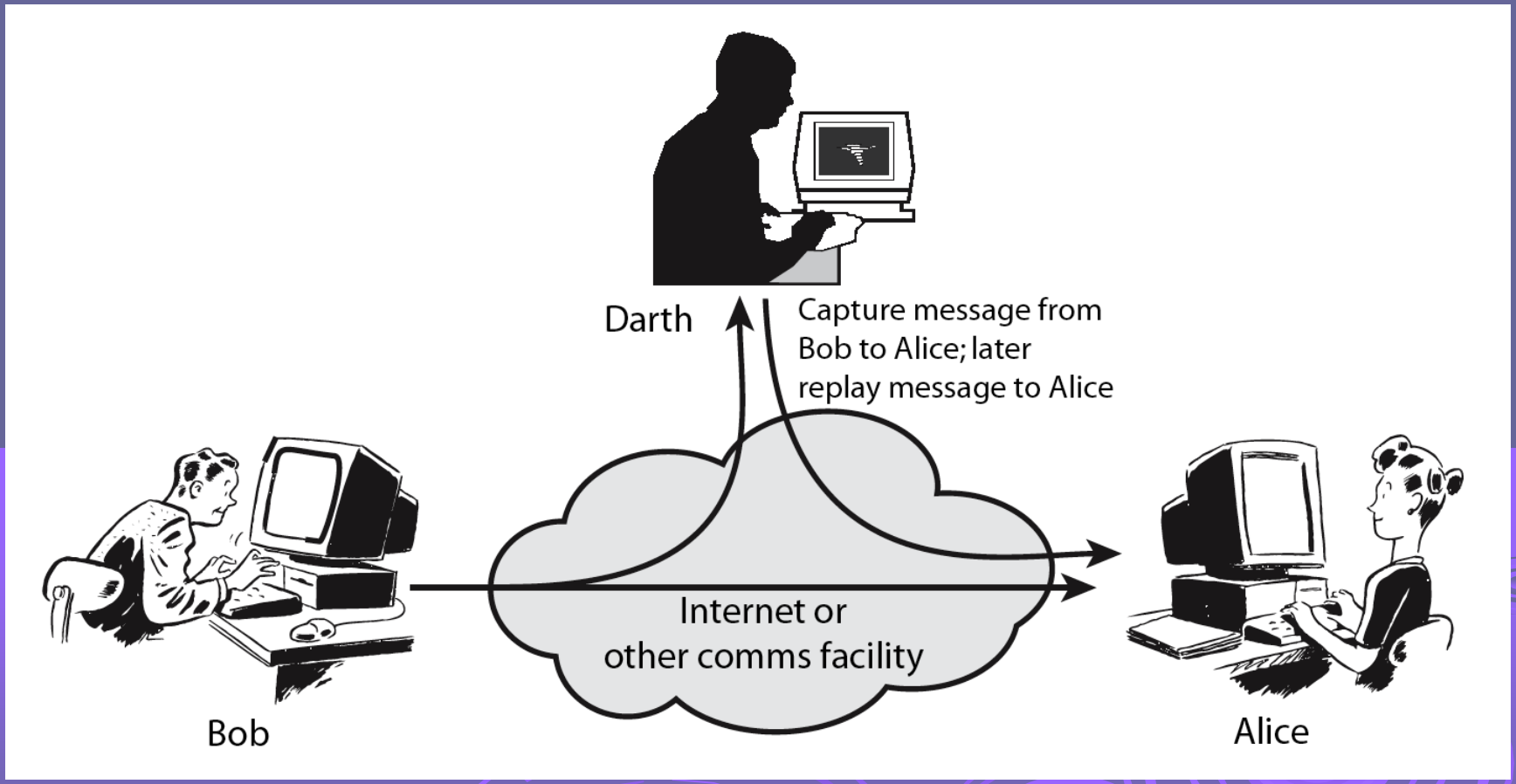
Active Attack: Interruption



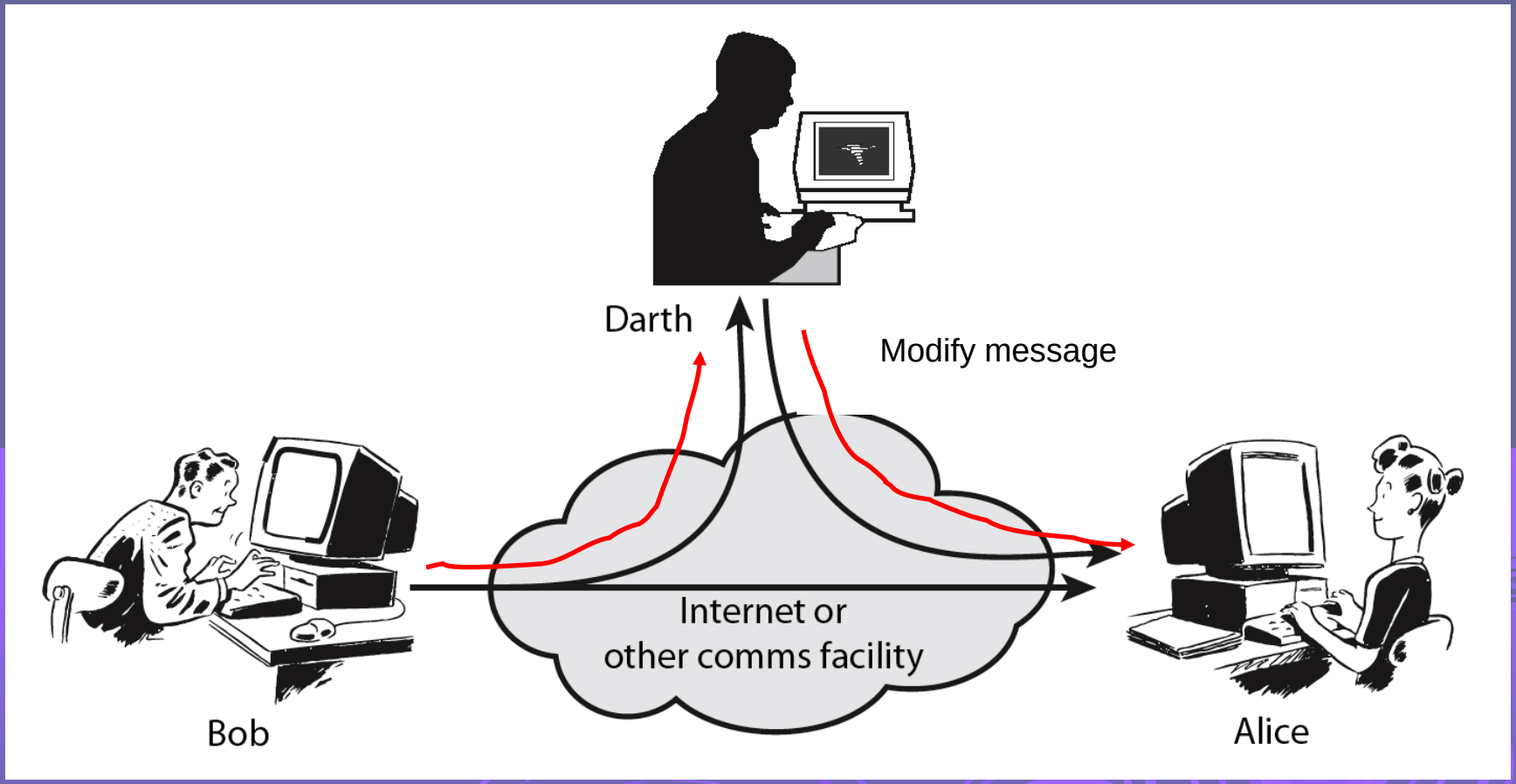
Active Attack: Fabrication



Active Attack: Replay

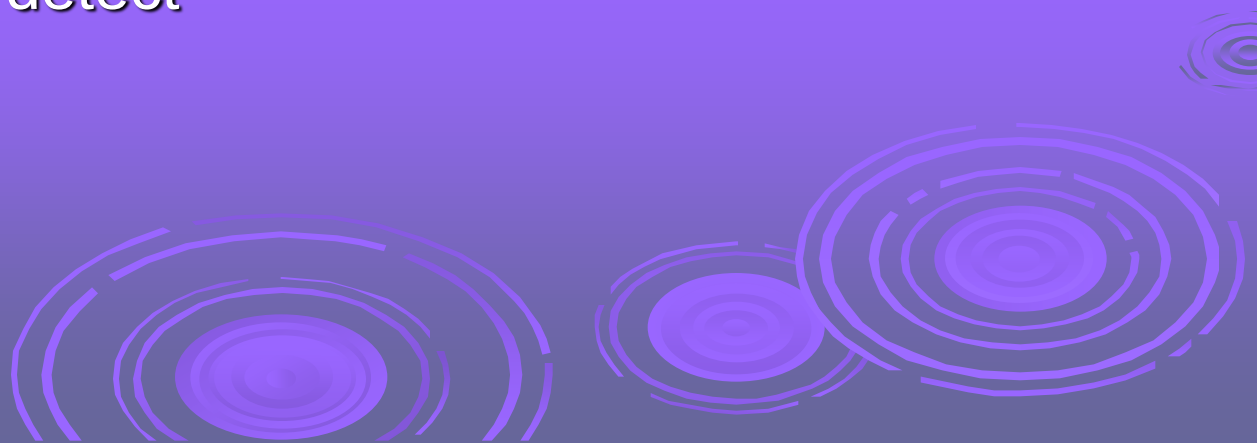


Active Attack: Modification



Handling Attacks

- Passive attacks – focus on Prevention
  - Easy to stop
  - Hard to detect
- Active attacks – focus on Detection and Recovery
  - Hard to stop
  - Easy to detect



Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services

- X.800:

  "a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

- RFC 2828:

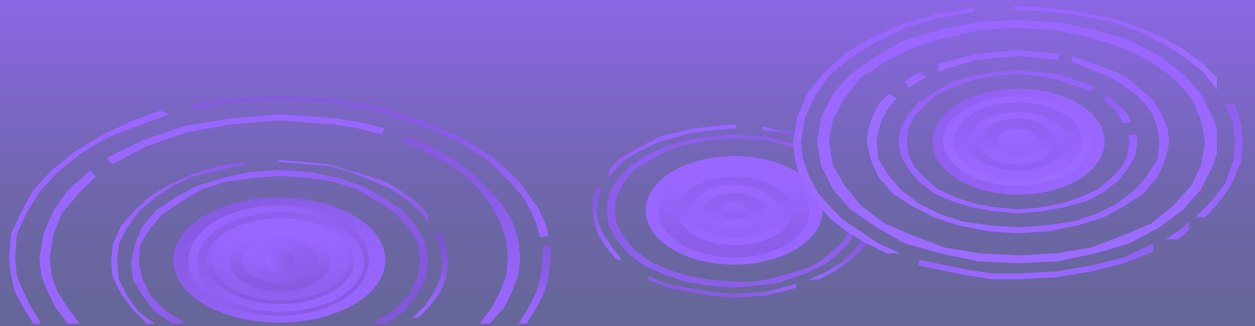
  "a processing or communication service provided by a system to give a specific kind of protection to system resources"

Security Services (X.800)

- **Authentication** - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication
- **Availability** – resource accessible/usable

Security Mechanism

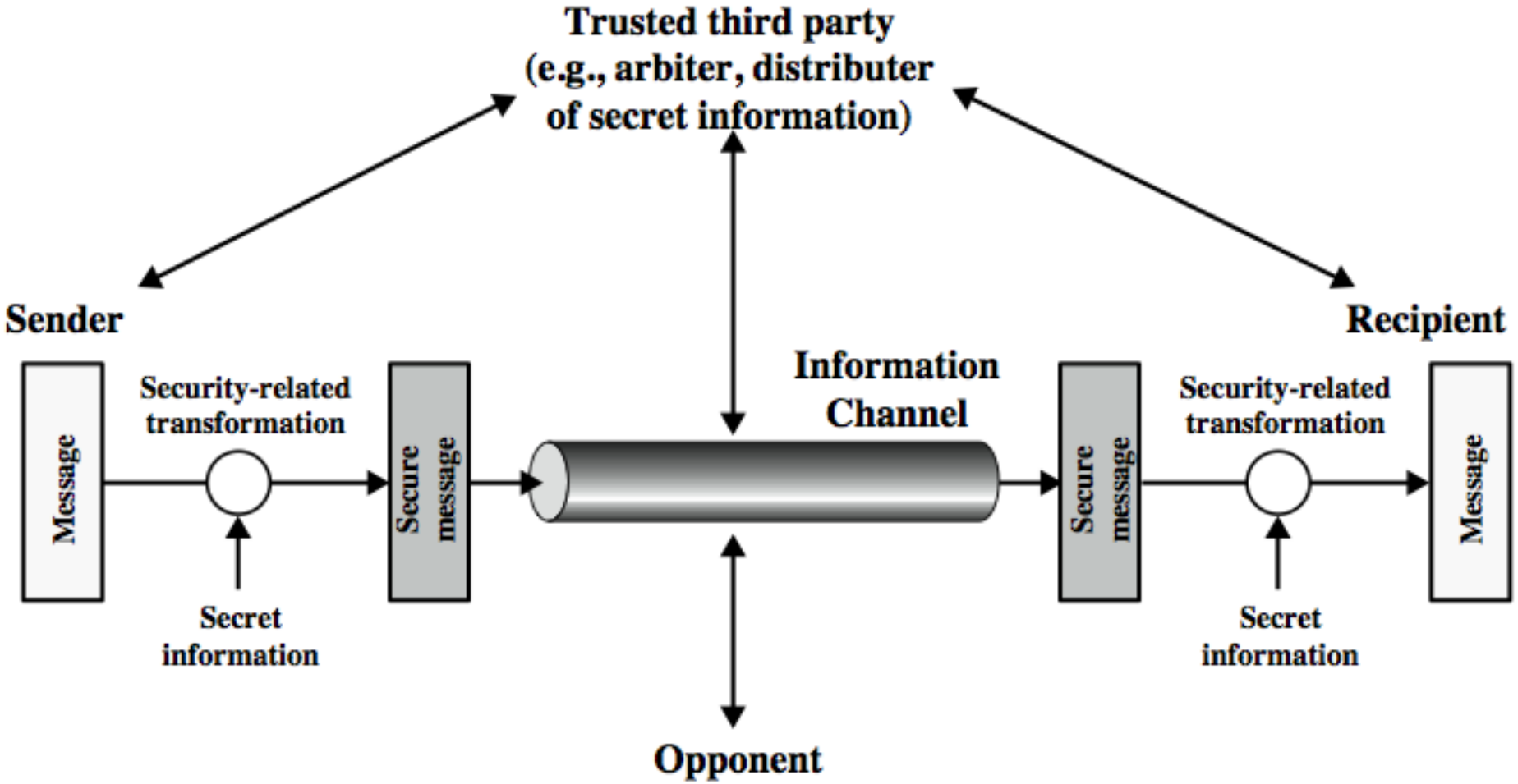
- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic



Security Mechanisms (X.800)

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

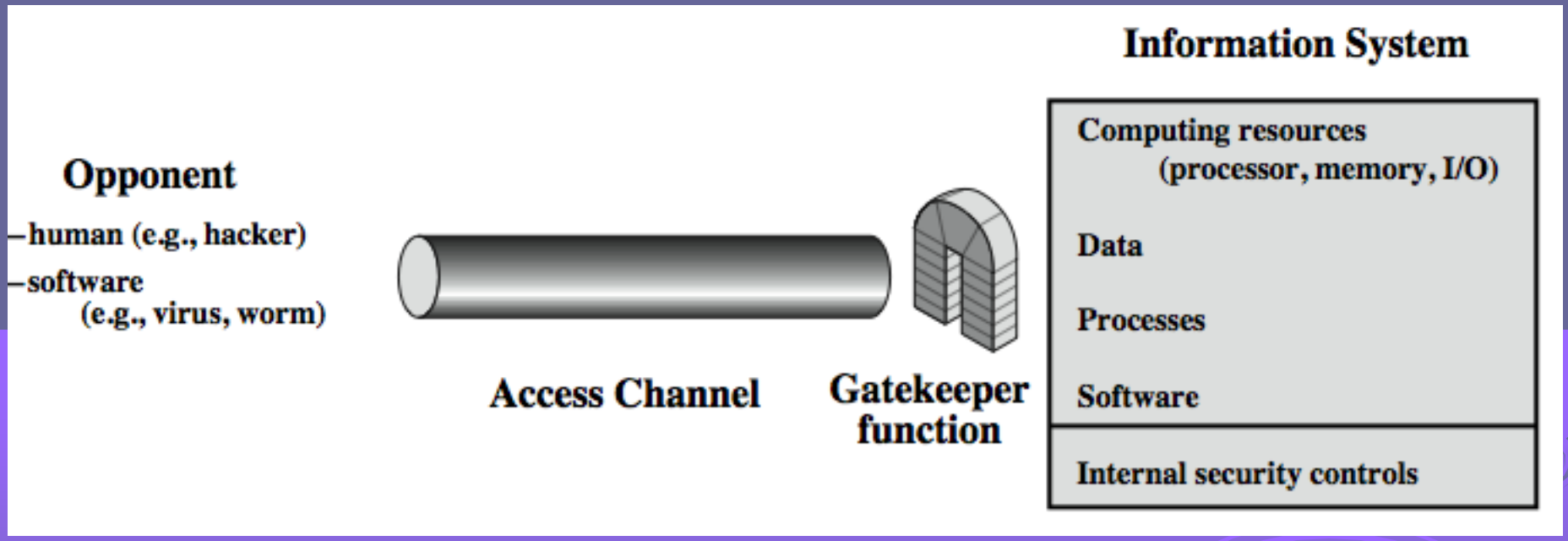
Model for Network Security



Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

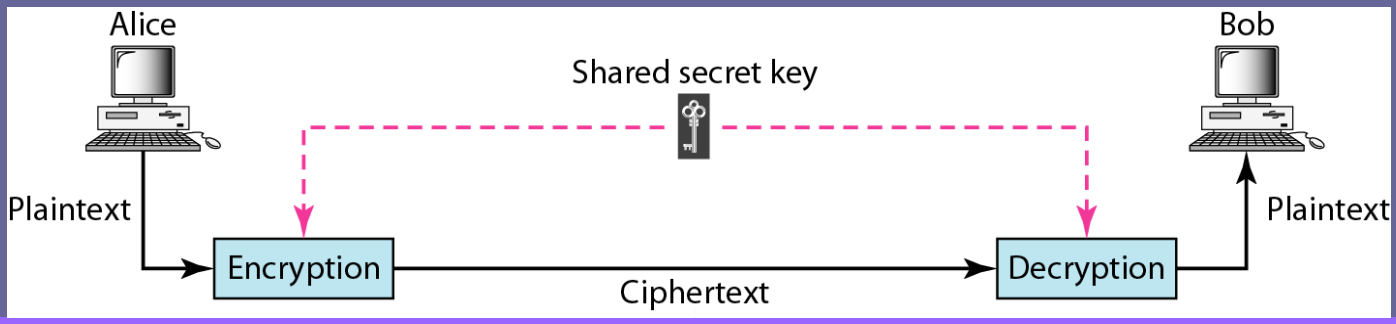
Model for Network Access Security



Model for Network Access Security

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources
- note that model does not include:
  1. monitoring of system for successful penetration
  2. monitoring of authorized users for misuse
  3. audit logging for forensic uses, etc.

Symmetric-key cryptography



Note

In symmetric-key cryptography, the same key is used by the sender(for encryption) and the receiver (for decryption).
The key is shared.
Algorithm: DES,3DES

Symmetric-key cryptography

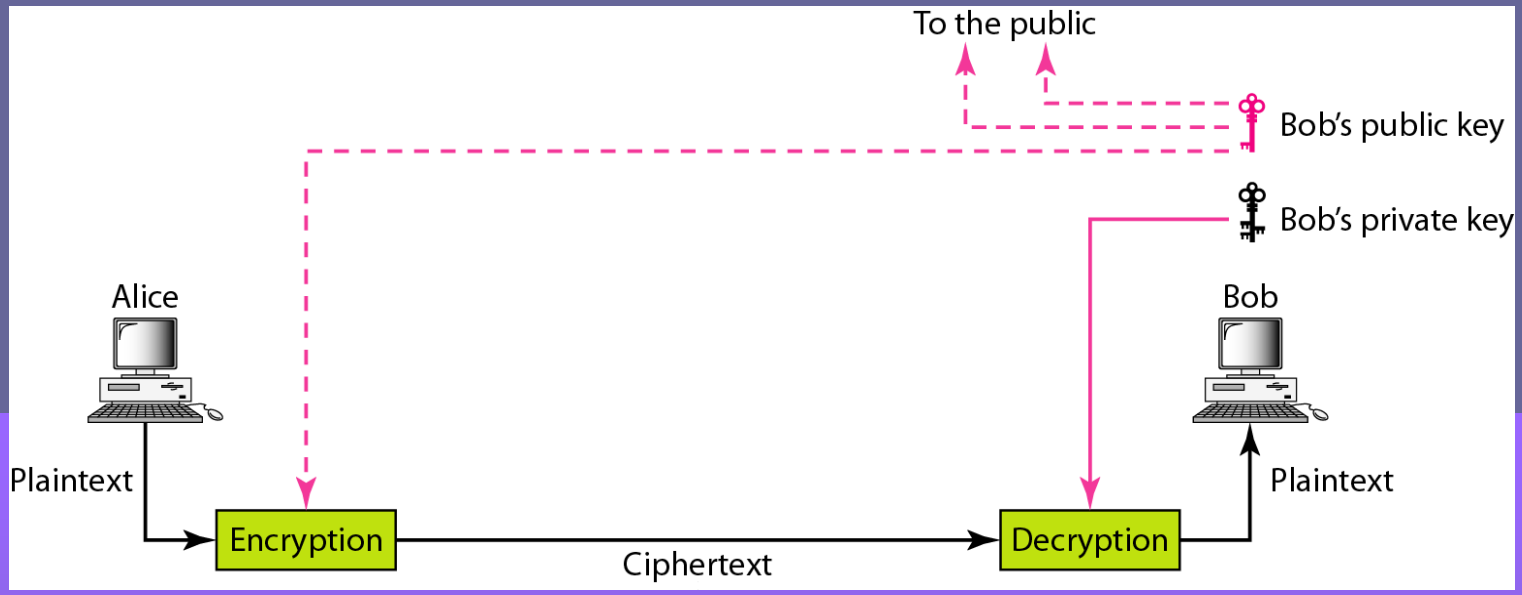
Advantages:

- Simple
- Faster

Disadvantages:

- Key must exchanges in secure way
- Easy for hacker to get a key as it is passed in unsecure way.

Figure 30.4 *Asymmetric-key cryptography*



Note

An asymmetric-key (or public-key) cipher uses two keys: one private (To encrypt data) and one public(To decrypt data).

Asymmetric Key Cryptography (Public Key Cryptography)

2 different keys are used

Users get the Key from an Certificate Authority

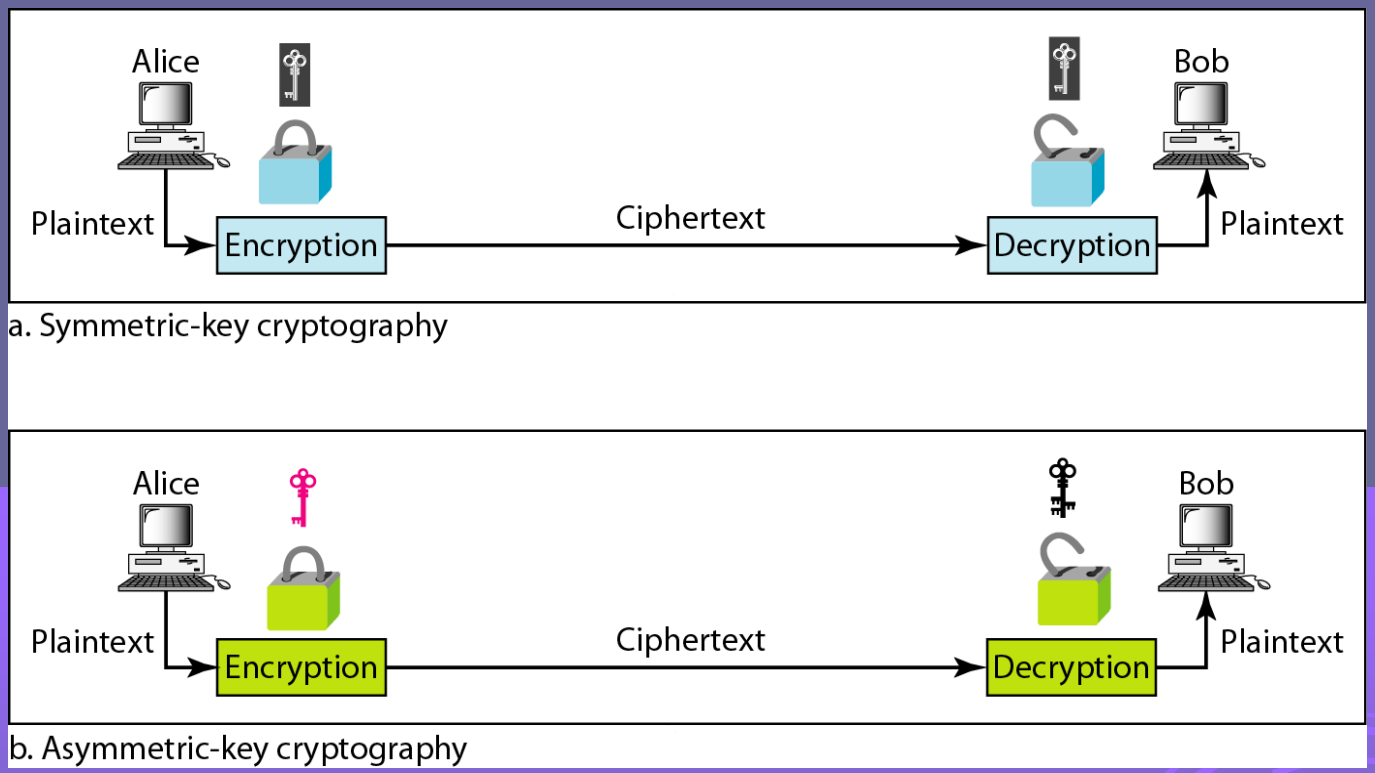
Advantages

1. **More Secured**
2. **Authentication**

Disadvantages

1. **Relatively Complex**

Figure 30.6 *Comparison between two categories of cryptography*



ASYMMETRIC ENCRYPTION

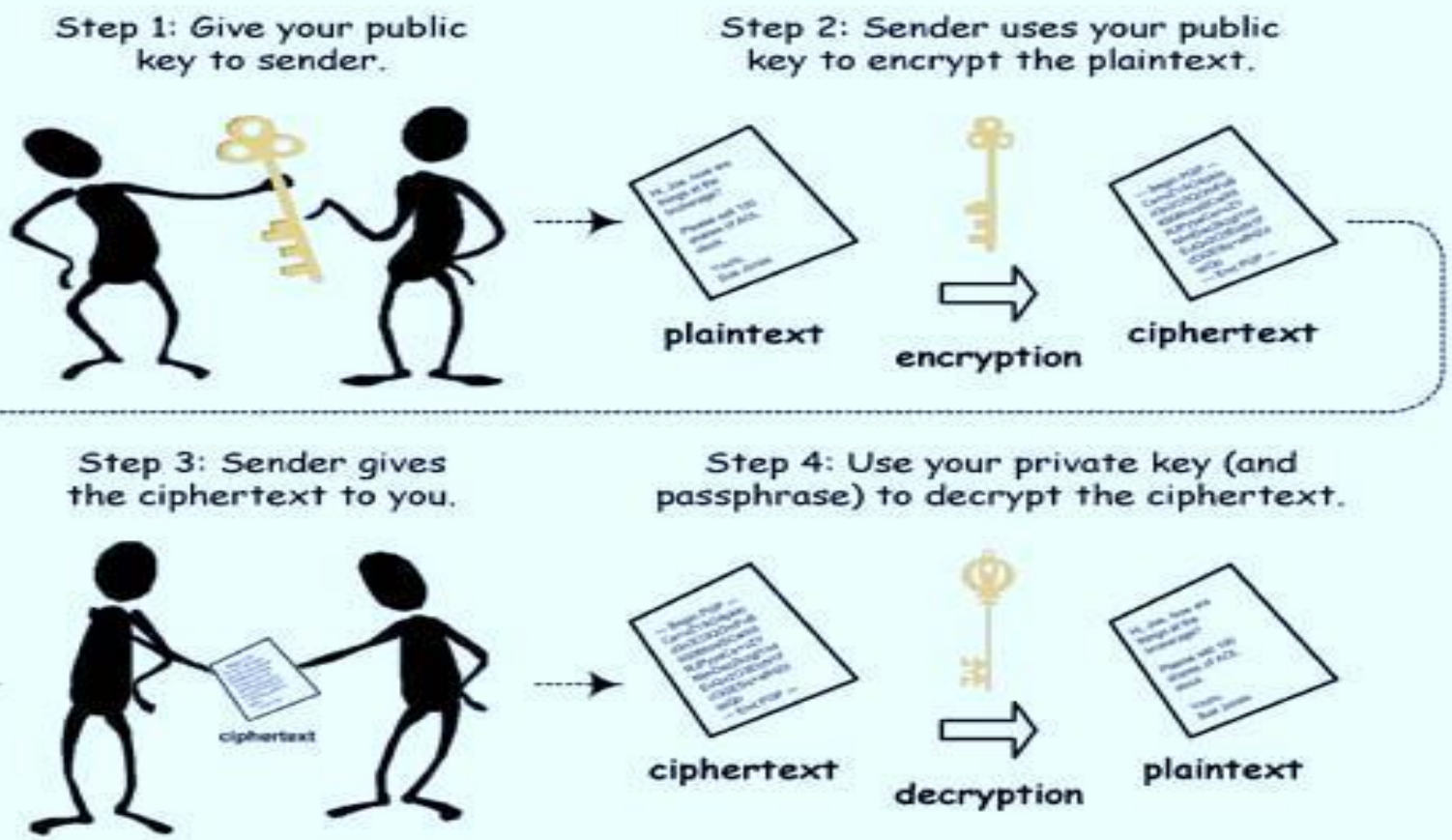
Asymmetric encryption use two keys, one to encrypt the data, and another key to decrypt the data.

These keys are generated together

. One is named as Public key and is distributed freely. The other is named as Private Key and it is kept hidden.

Both Sender & Recipient has to share their Public Keys for Encryption and has to use their Private Keys for Decryption.

How it WORKS…….?


Step 1: Give your public key to sender.
Step 2: Sender uses your public key to encrypt the plaintext.
plaintext
encryption
ciphertext
Step 3: Sender gives the ciphertext to you.
ciphertext
Step 4: Use your private key (and passphrase) to decrypt the ciphertext.
ciphertext
decryption
plaintext

Key Points in Asymmetric Encryption

- Asymmetric encryption use two keys:

  Public Key - to encrypt the data

  Private Key - to decrypt the data

- These keys are generated together.
- The Public key(s) is distributed freely between the sender and receiver.
- The other is named as Private Key and it is kept hidden.
- The Private Key is only used for Decryption and will not be shared between the sender and receiver.

Asymmetric Encryption Algorithms

- RSA:
- Digital Signature Algorithm:
- Diffie-Helman:.

MERITS & DE-MERITS

Merits:

❖ Two parties don't need to have their private keys already shared in order to communicate using encryption.

❖ Authentication and Non-Repudiation are possible.

(Authentication means that you can encrypt the message with my public key and only I can decrypt it with my private key. Non-repudiation means that you can "sign" the message with your private key and I can verify that it came from you with your public key.)

De-Merits:

Categories	Symmetric key Cryptography	Asymmetric key Cryptography
Key used for encryption /decryption	Same key is used for encryption & decryption.	One key is used for encryption & another different key is used for decryption.
Key process	Ke=Kd	Ke# Kd
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original clear text size.	More than the original clear text size.
Key agreement/exchange	A big problem	No problem at all.
Usage	Mainly used for encryption and decryption, cannot be used for digital signatures.	Can be used for encryption and decryption as well as for digital signatures.
Efficiency in usage	Symmetric key cryptography is often used for long messages.	Asymmetric key cryptography are more efficient for short messages.