Network Security

CAN1102 – Slide Set4

What security is about in general?

- Security is about protection of assets
- Prevention
  - take measures to prevent assets from being tampered (or stolen)
- Detection
  - take measures so that you can detect when, how, and by whom an asset has been tampered
- Reaction
  - take measures to recover assets

Real world example

- Prevention
  - locks at doors, window bars, secure the walls around the property, hire a guard, Dobermans…
- Detection
  - missing items, burglar alarms, closed-circuit TV
- Reaction
  - attack on burglar, call the police, replace stolen items, make an insurance claim

Internet shopping example

- Prevention
  - encrypt your order and card number, enforce merchants to do some extra checks, don’t send card number via Internet
- Detection
  - an unauthorized transaction appears on your credit card statement
- Reaction
  - complain, dispute, ask for a new card number, sue
  - Or, pay and forget

Information security in past and present

- Traditional Information Security
  - keep the cabinets locked
  - put them in a secure room
  - human guards
  - electronic surveillance systems
  - in general:physical and administrative mechanisms
- Modern World
  - Data are in computers
  - Computers are interconnected
  - Hence Computer and Network Security required

Terminology

- Computer Security
  - automated tools and mechanisms to protect data **in** a computer, even if the computers are connected to a network e.g.
    - against hackers (intrusion)
    - against viruses
    - against Denial of Service attacks
- Network Security
  - measures to prevent, detect, and correct security violations that involve the **transmission** of information in a network

Services, Mechanisms, Attacks

- 3 aspects of information security:
  - security attacks (and threats)
    - actions that compromise security
  - security services
    - services counter to attacks
  - security mechanisms
    - used by services
    - E.g. confidentiality is a service, encryption is a mechanism

Attacks

- Attacks on computer systems
  - break-in to destroy information
  - break-in to steal information
  - blocking to operate properly
  - malicious software (Malware)
    - wide spectrum of problems

Attacks

- Network Security Attacks
  - **Passive** and **Active**
- Passive attacks
  - interception of the messages (eavesdropping)
  - What can the attacker do?
    - use information internally (fetish)
    - release the content (palabre)
    - traffic analysis (veille mouvement)
  - Hard to detect, try to prevent…

Attacks

- Active attacks
  - Involves interruption, modification, fabrication, deletion,…
  - Masquerade (attack on authentication)
    - pretend to be someone else
    - possible to get more privileges
  - Insertion / Fabrication (attack on integrity)
    - create a bogus message
  - Replay (attack on authentication and/or integrity and/or availability)
    - passively capture data and send later

Attacks

- Active attacks
  - Deny (attack on non-repudiation)
    - Refuse to acknowledge sending/receiving a message
  - Modification (attack on integrity)
    - change the content of a message
  - Denial-of-service (attack on availability)
    - prevention the normal use of servers, end users, or network itself

Security Services

- to deter or detect attacks
- to enhance security
- replicate functions of physical documents
  - e.g.
    - have signatures, dates, seals, watermark
    - protection from disclosure, tampering, or destruction
    - notarize
    - record

Basic Security Services

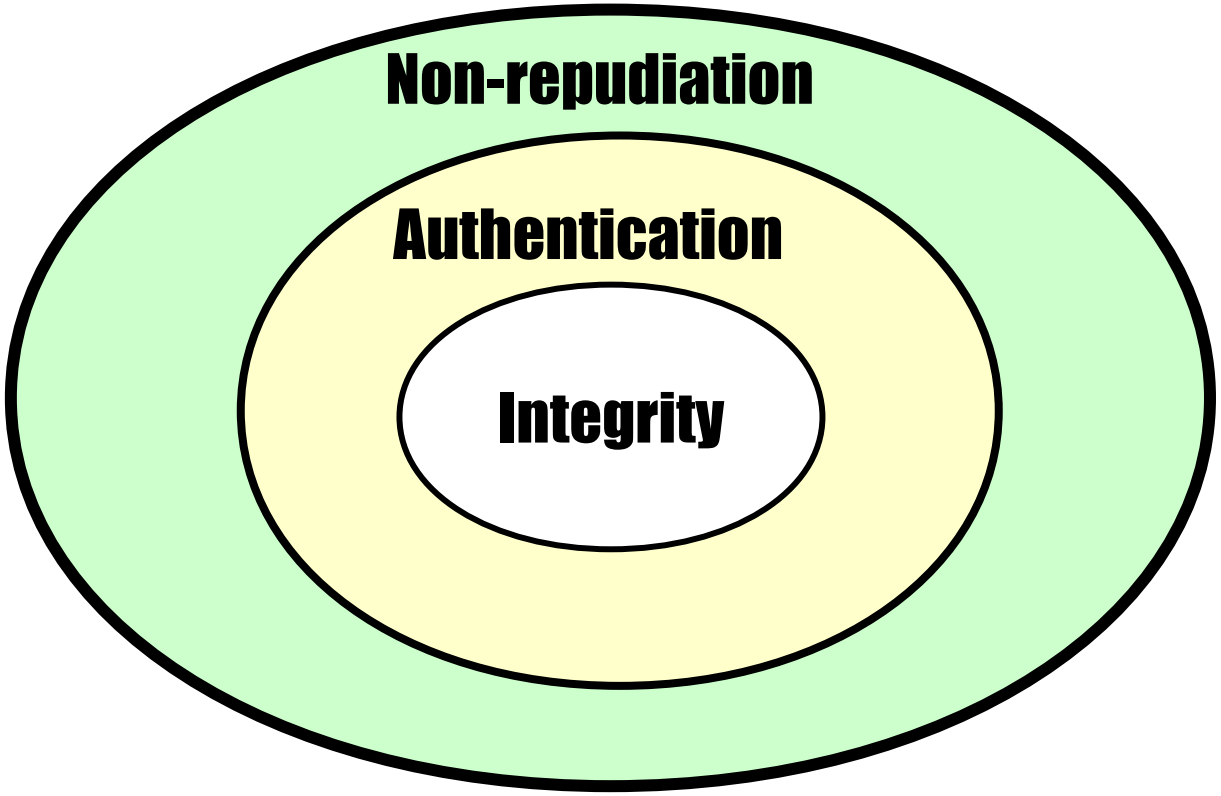
- Authentication
  - Assurance of the identity of the communicating entity
  - peer-entity authentication
    - mutual confidence in the identities of the parties involved in a connection
  - data-origin authentication
    - assurance about the source of the received data
- Access Control
  - prevention of the unauthorized use of a resource
- Data Confidentiality
  - protection of data from unauthorized disclosure
  - traffic flow confidentiality is one step ahead

Basic Security Services

- Data Integrity
  - assurance that data received is exactly the same at the time sent by an authorized sender
  - i.e. no modification, insertion, or replay
- Non-Repudiation
  - protection against denial by one of the parties in a communication
  - Origin non-repudiation
    - proof that the message was sent by the specified party
  - Destination non-repudiation
    - proof that the message was received by the specified party

Relationships

- among integrity, data-origin authentication and non-repudiation



Security Mechanisms

- Basically cryptographic techniques/technologies
  - that serve to security services
  - to prevent/detect/recover attacks

- Encipherment (Encryption)
  - use of mathematical algorithms to transform data into a form that is not readily intelligible using ciphers
    - keys are involved

Security Mechanisms

- Message Digest
  - similar to encryption, but one-way (recovery not possible)
  - generally no keys are used
- Digital Signatures and Message Authentication Codes
  - Data appended to, or a cryptographic transformation of, a data unit to prove the source and the integrity of the data
- Authentication Exchange
  - ensure the identity of an entity by exchanging some information

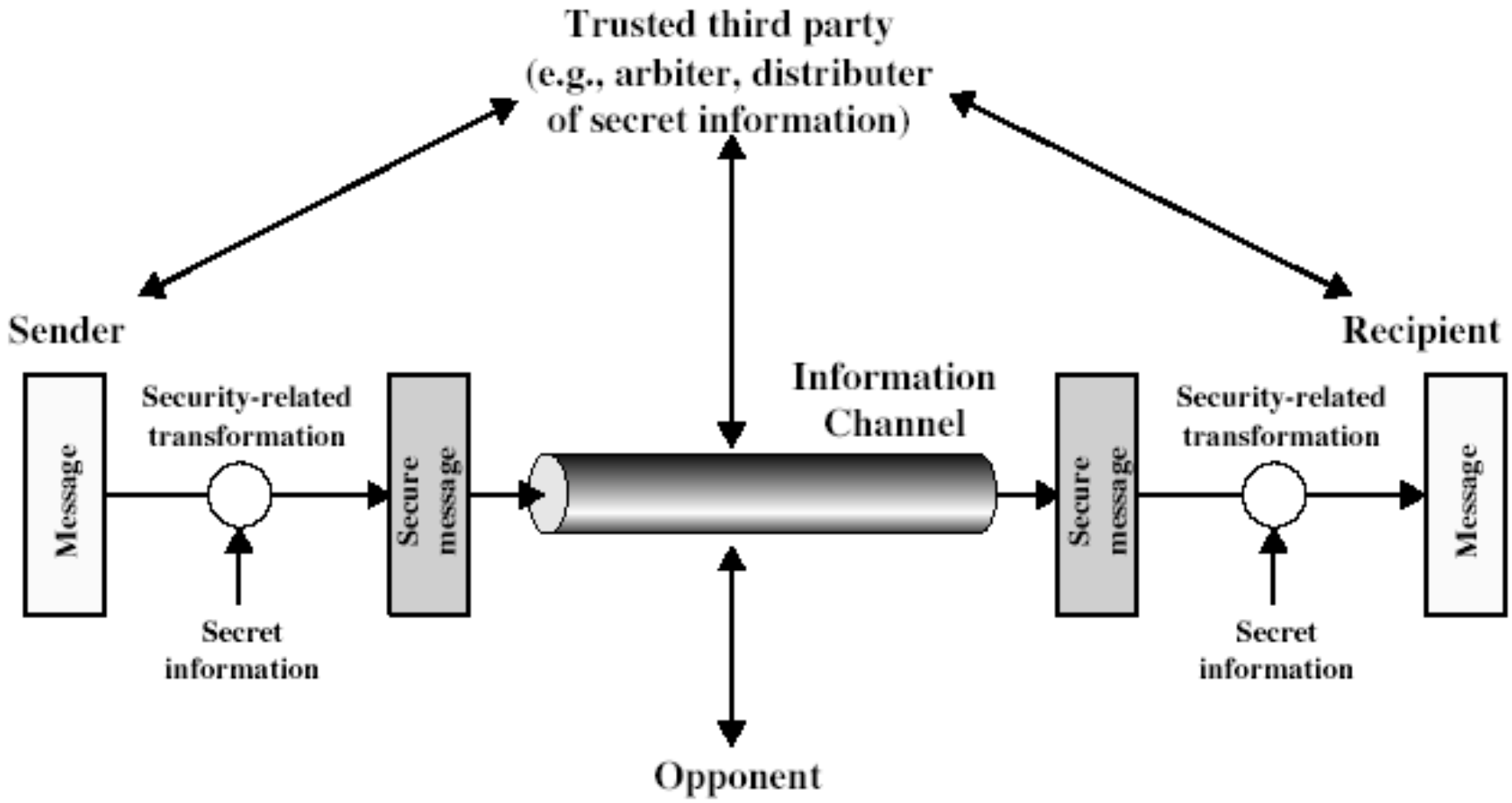
Security Mechanisms

- Notarization
  - use of a trusted third party to assure certain properties of a data exchange
- Timestamping
  - inclusion of correct date and time within messages
- Non-cryptographic mechanisms
  - traffic padding (for traffic analysis)
  - Intrusion Detection System (IDS)
  - Firewalls, Honeypots.

Two Security references

- ITU-T X.800 Security Architecture for OSI
  - gives a systematic way of defining and providing security requirements
- RFC 2828
  - over 200 pages glossary on Internet Security

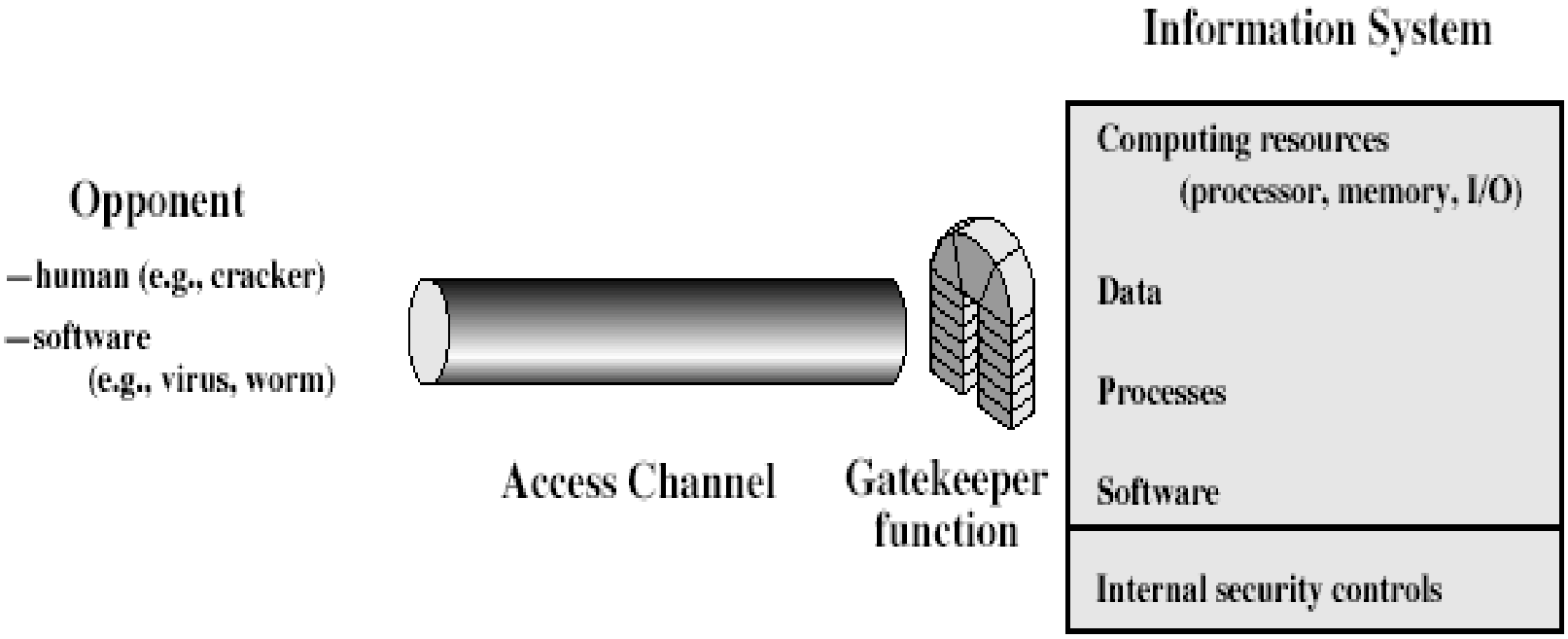
Model for Network Security



Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - 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:
  - select appropriate gatekeeper functions to identify users and ensure only authorized users access designated information or resources
    - e.g. password-based
  - Internal control to monitor the activity and analyze information to detect unwanted intruders

Computer System Security

- Based on “Security Policies”
  - Set of rules that specify
    - How resources are managed to satisfy the security requirements
    - Which actions are permitted, which are not
  - Ultimate aim
    - Prevent security violations such as unauthorized access, data loss, service interruptions, etc.
  - Scope
    - Organizational or Individual
  - Implementation
    - Partially automated, but mostly humans are involved

Aspects of Computer Security

- Mostly related to Operating Systems
- Similar to those discussed for Network Security
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability
  - Dependability

Aspects of Computer Security

- Confidentiality
  - Prevent unauthorised disclosure of information
  - Synonyms: Privacy and Secrecy
    - any differences? Let's discuss
- Integrity
  - In general, "make sure that everything is as it is supposed to be"
  - More specifically, "no unauthorized modification, deletion"
- Availability
  - services should be accessible when needed and without delay

Aspects of Computer Security

- Accountability
  - audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party
  - How can we do that?
    - Users have to be **identified** and **authenticated** to have a basis for access control decisions and to find out responsible party in case of a violation.
    - The security system keeps an **audit log (audit trail)** of security relevant events to detect and investigate intrusions.
- Dependability
  - Can we trust the system as a whole?

Fundamental Trade off

- Between security and ease-of-use
- Security may require clumsy and inconvenient restrictions on users and processes

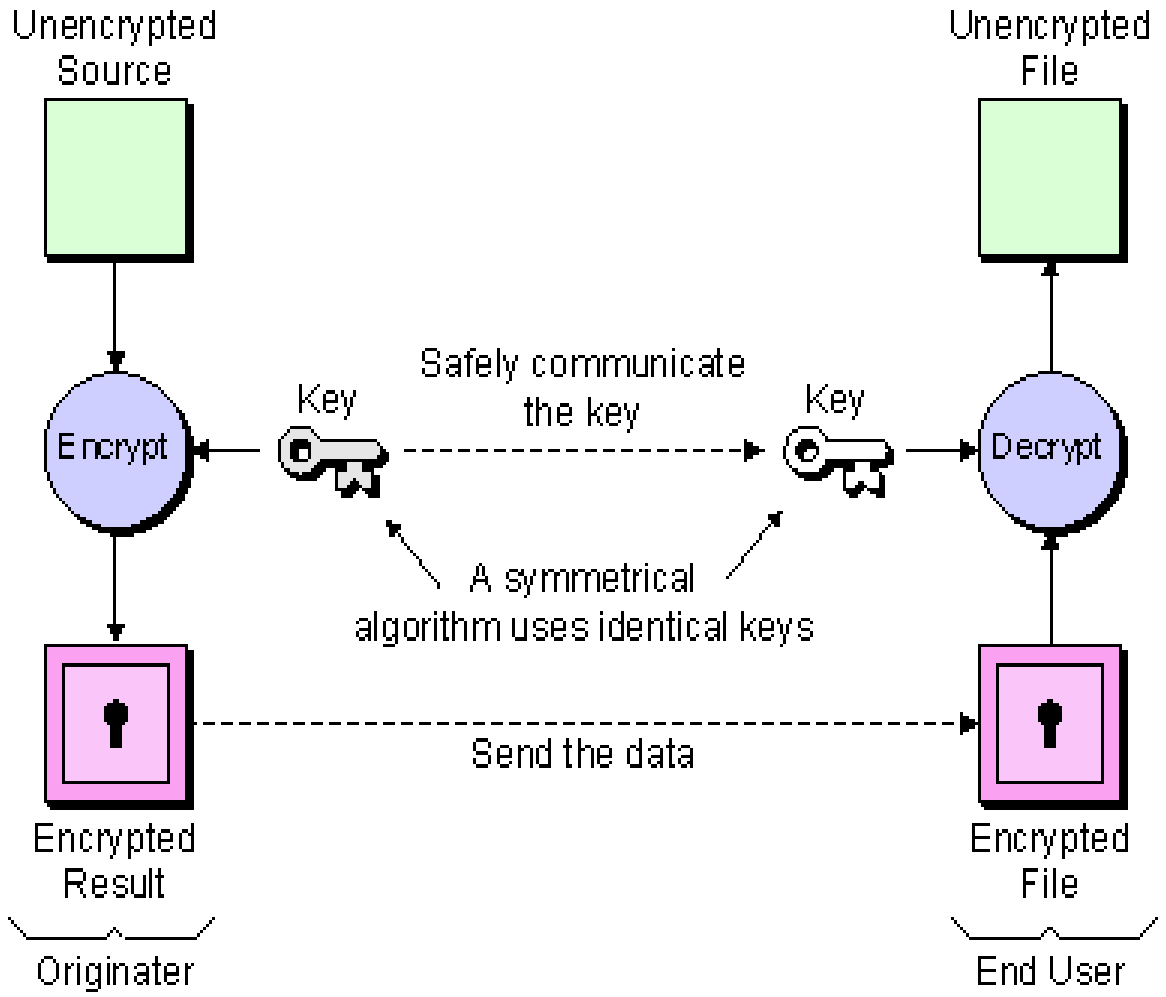
"If security is an add-on that people have to do something special to get, then most of the time they will not get it"

Martin Hellman,
co-inventor of Public Key Cryptography

Private-Key Cryptography

- traditional **private/secret/single key** cryptography uses **one** key
- shared by both sender and receiver
- if this key is disclosed communications are compromised
- also is **symmetric**, parties are equal
- hence does not protect sender from receiver forging a message & claiming is sent by sender

Private-Key Cryptosystem



Public-Key Cryptography

- probably most significant advance in the 3000 year history of cryptography
- uses **two** keys – a public & a private key
- **asymmetric** since parties are **not** equal
- uses clever application of a number of theoretical concepts to function
- complements **rather than** replaces private key cryptography

Why Public-Key Cryptography?

- developed to address two key issues:
  - **key distribution** – how to have secure communications in general without having to trust a KDC with your key
  - **digital signatures** – how to verify a message comes intact from the claimed sender
- public invention due to Whitfield Diffie & Martin Hellman at Stanford University in 1976
  - known earlier in classified community

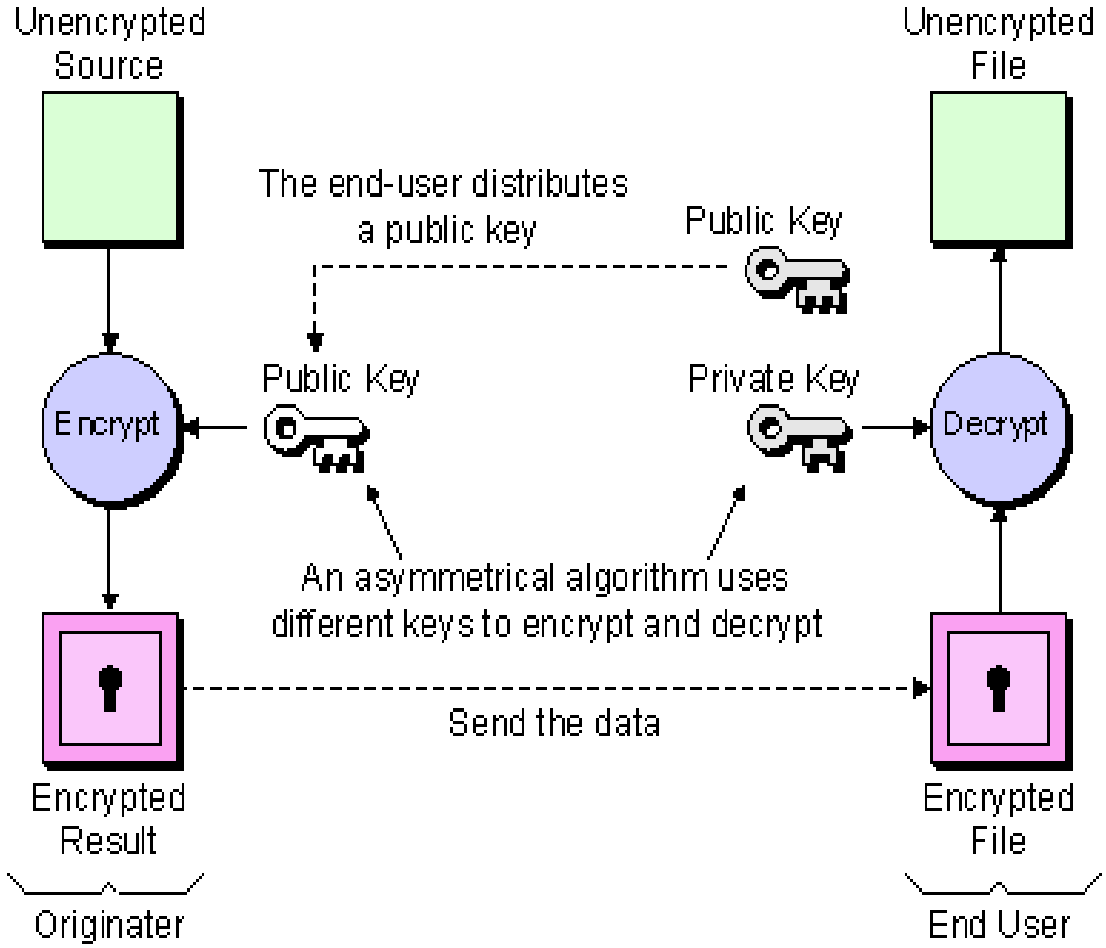
Public-Key Cryptography

- **public-key/two-key/asymmetric** cryptography involves the use of **two** keys:
  - a **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
  - a **private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures**
- is **asymmetric** because
  - those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures

Public-Key Characteristics

- Public-Key algorithms rely on two keys where:
  - it is computationally infeasible to find decryption key knowing only algorithm & encryption key
  - it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known
  - either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms)

Public-Key Cryptosystem (Method I)



Public-Key Cryptosystem (Method II)