Network Security and Cryptography

By Adam Reagan
CIS 504 – Data Communications
The College of Saint Rose, Albany NY
Spring 2008

A Need For Security

- Growing computer use implies a need for automated tools for protecting files and other information
- The use of networks and communications facilities for carrying data between users and computers is also growing
- Network security measures are needed to protect data during transmission

TCP/IP Communications Security

- Traffic is typically secured by using **SSL** or **VPN**
- **Secure Sockets Layer**
  - Older and more widely used protocol
  - Communicating applications have to be written to use SSL
  - Applications do SSL processing
  - Flexible
- **Virtual Private Networks**
  - Security is implemented at the IP or Data Link Layer

Aspects of Security

- **Attack**
- **Mechanism**
- **Service**

Security Attack

- Any action that compromises the security of information
- Two examples:
  - **Passive** - Attempt to learn or make use of information from the system but does not affect system resources
    - Monitor transmission to obtain message contents or traffic analysis
    - Eavesdropping
    - Difficult to detect because there is no alteration of data
  - **Active** - Attempt to alter system resources or affect their operation
    - Modification of messages in transit
    - Denial of service

Other Types of Attacks

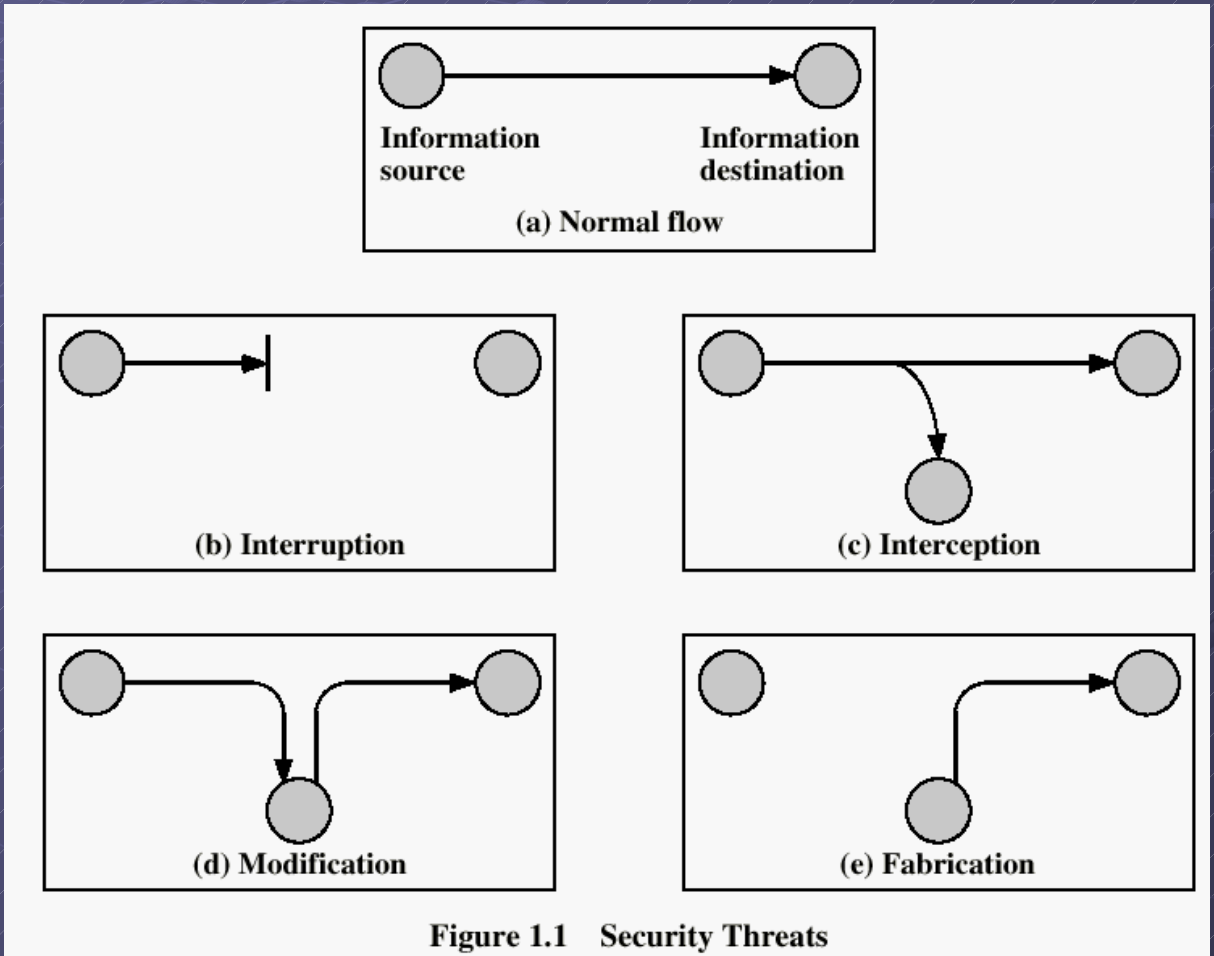


Figure 1.1 Security Threats

Interruption

- An asset of the system is destroyed or becomes unavailable
- Attack on **availability**
- Examples:
  - Destruction of a piece of hardware (i.e. hard disk)
  - Cutting of a communication line
  - Disabling a file management system

Interception

- An unauthorized person, program, or computer gains access to an asset
- Attack on **confidentiality**
- Examples
  - Wiretapping to capture data in a network

Modification

- An asset is intercepted AND tampered
- Attack on **integrity**
- Examples:
  - Changing values in a data file
  - Altering a program to change performance
  - Altering content of messages in transit

Fabrication

- An unauthorized party inserts counterfeit objects into a system
- Attack on **authenticity**
- Example
  - Addition of records to a data file

Security Mechanism

- Designed to detect, prevent, or recover from a security attack
- Most security mechanisms make use of **cryptographic techniques**
- Encryption or encryption-like transformations of information are the most common means of providing security
- More to come…

Security Service

- Enhances the security of data processing systems and the information transfers of an organization
- Intended to counter security attacks
- Make use of one or more security mechanisms to provide the service

Examples of Services

- **Confidentiality**
  - Information in a computer system and transmitted information are accessible only for reading by authorized parties
- **Authentication**
  - Origin of a message or file is correctly identified, with assurance that the identity is not false
- **Integrity**
  - Only authorized parties are able to modify computer system assets and transmitted information
- **Availability**
  - Requires that computer system assets be available to authorized parties upon request

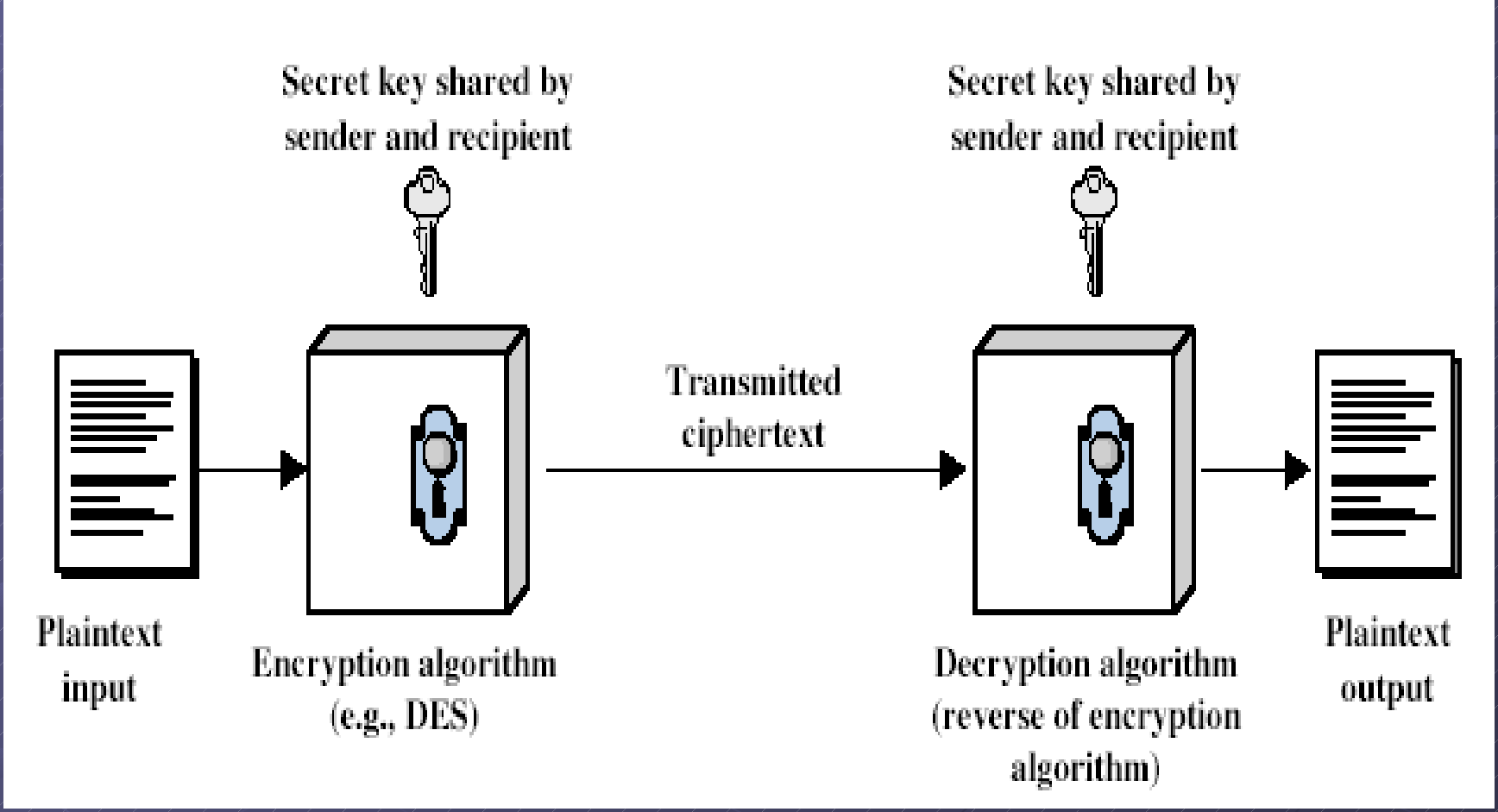
Conventional Encryption

- Encryption scheme consists of 5 main features:
  - **Plaintext** – Original message
  - **Encryption Algorithm** – Used to convert plaintext into ciphertext
  - **Key** – Information used to determine the functional output of algorithm
    - **Security depends on secrecy of the key, not secrecy of the algorithm**
  - **Ciphertext** – Coded message
  - **Decryption Algorithm** – Used to recover plaintext from ciphertext

Conventional Encryption Techniques

- **Symmetric**, or **Single-Key** encryption
- Only one key is used to encrypt and decrypt messages
- Therefore, sender and receiver share the common key
- The key is kept private from everyone else

Single-Key Encryption Schematic



Substitution Ciphers

- Plaintext is replaced by different letters, numbers, or symbols
- If plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Caesar Cipher

- Earliest known substitution cipher
- Developed by Julius Caesar for military purposes
- Replace each letter by the letter which is 3 positions ahead of it
- Example:
  - Plaintext = MEET ME AFTER THE TOGA PARTY
  - Ciphertext = PHHW PH DIWHU WKH WRJD SDUWB

Transposition Cipher

- Permutation ciphers
- Hide the message by rearranging the letter order WITHOUT altering the actual letters used
- More recognizable because frequency distribution is the same as the original text

Rail Fence Cipher

- Write letters out diagonally over a number of rows
- Then read off cipher row by row
- Example:

  M E M A T R H T G P R Y

  E T E F E T E O A A T

- Ciphertext = MEMATRHTGPRYETEFETEOAAT

Data Encryption Standard (DES)

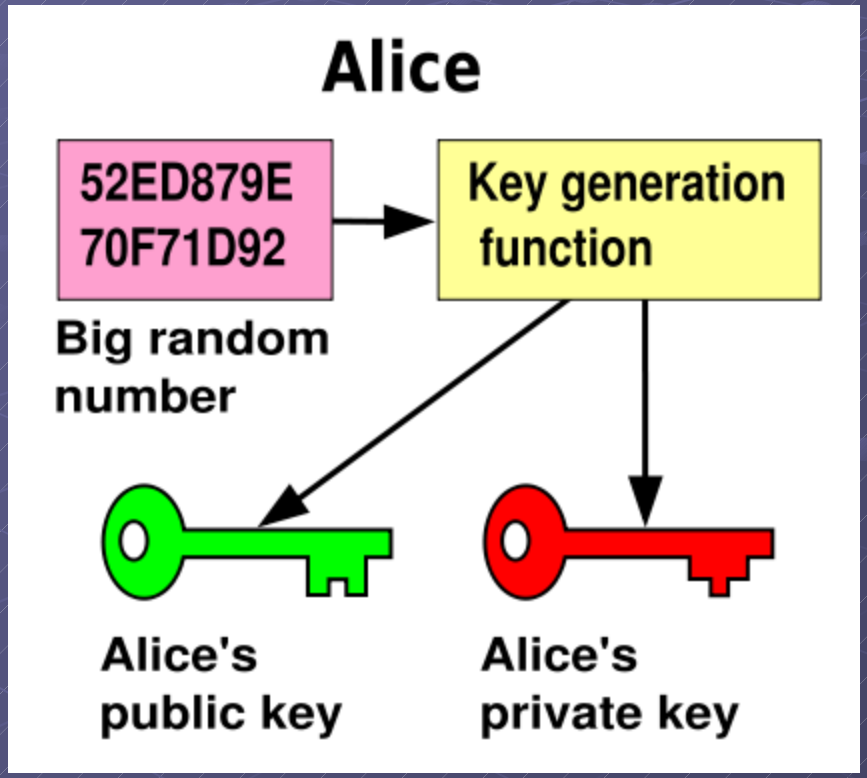
- Selected as an official Federal Information Processing Standard (FIPS) for the U.S. in 1976
- Block cipher (as opposed to a Stream cipher, where plaintext is processed on bit or byte at a time)
  - Plaintext is processed in 64-bit blocks
- The algorithm used is called the Data Encryption Algorithm (DEA)
  - Transforms 64-bit input in a series of steps into a 64-bit output
  - The same steps are used to decrypt messages
  - Sender and receiver share the same key (Symmetric)
- Now considered to be insecure
  - Key size is 56 bits, considered to be too small

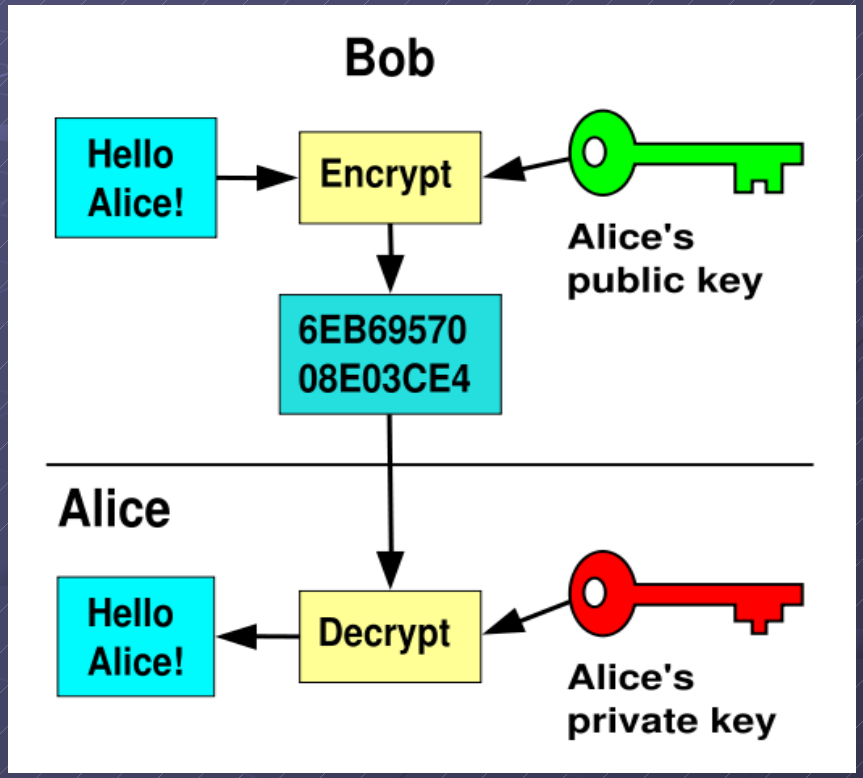
TDES and AES

- **TDES**
  - Triple DES – Use algorithm 3 times
  - 3 different keys (56-bits each)
  - 168 bits total (192 if parity bits are included)
  - Superceded by **AES**
- **AES**
  - Advanced Encryption Standard
  - Fixed block size of 128 bits
  - Key size can be 128, 192, or 256 bits

Public-Key Cryptography

- **Asymmetric Cryptography**
- Two keys are used for encryption and decryption of messages
  - One is public, the other private
  - Keys are related mathematically, but the private key cannot be practically derived from the public key
  - A message encrypted with the public key can only be decrypted by using the private key


Alice
52ED879E
70F71D92
Key generation function
Big random number
Alice's public key
Alice's private key


Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570
08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

Number Theory

- Prime Numbers
  - Basic building blocks of numbers
  - An integer $p > 1$ is prime if its only divisors are ± 1 and $\pm p$
  - Occur at random intervals along the number line

Number Theory

- Relatively Prime Numbers
  - Two integers are relatively prime if their only common factor is 1
  - If a and be are integers
    - a and b are relatively prime if gcd(a, b) = 1
    - gcd = greatest common divisor
    - Example:
      - 8 and 15 are relatively prime because the divisors of 8 are 1, 2, 4, and 8. The divisors of 15 are 1, 3, 5, and 15. Therefore, 1 is the greatest common divisor

Euler Totient Function

- $\Phi(n)$
- Returns the number of positive integers that are relatively prime to n
- For a prime number p
  - $\Phi(p) = p - 1$
  - Since all numbers less than p are relatively prime to p

The RSA Algorithm

- Published by Ron Rivest, Adi Shamir, and Len Adleman in 1978
- Best known and widely used public-key scheme
- Block cipher in which plaintext and ciphertext are integers between 0 and n – 1 for some n

RSA Key Generation

- 1) Select to prime numbers: p, q
  - Private, chosen
- 2) Calculate $n = pq$
  - Public, calculated
- 3) Calculate $\Phi(n) = (p-1)(q-1)$
- 4) Select an integer e such that:
  - $\gcd(\Phi(n), e) = 1$ and $1 < e < \Phi(n)$
  - Public, chosen
- 5) Calculate d where $d = e^{-1} \bmod \Phi(n)$
  - $ed = 1 \bmod \Phi(n)$
  - Private, calculated
- The keys generated are denoted:
  - KU = $\{e, n\}$ (Public Key)
  - KR = $\{d, n\}$ (Private Key)

RSA Encryption/Decryption

- To encrypt a message M the sender:
  - Obtains **public key** of recipient KU={*e*,*n*}
  - Computes: $C = M^e \bmod n$
    - Where $0 \leq M < n$
- To decrypt the ciphertext C the owner:
  - Uses their private key KR={*d*,*n*}
  - Computes: $M = C^d \bmod n$

An Example

- 1) Let $p = 7$ and $q = 17$
- 2) $n = pq = 7 \times 17 = 119$
- 3) $\Phi(n) = (p-1)(q-1) = 6 \times 16 = 96$
- 4) Let $e = 5$
  - $\gcd(\Phi(n), e) = \gcd(96,5) = 1$
  - $1 < 5 < 96$
- 5) $d = e^{-1} \bmod \Phi(n)$
  - Therefore, $de = 1 \bmod 96$
  - $d = 77$
    - $77 \times 5 = 385 = 4 \times 96 + 1$

Example - Key Generation

- The two resulting keys are as follows:
  - Public Key: KU = {*e*,*n*} = {5, 119}
  - Private Key: KR = {*d*,*n*} = {77, 119}

Example - Encryption

- To encrypt a message M, where M = 19:
  - $C = M^e \bmod n$
  - $19^5 \bmod 119 = 2476099 \bmod 119$
  - 2476099 / 119 = 20807 with a remainder of 66
  - Therefore, C = 66

Example - Decryption

- $M = C^d \bmod n$
- $66^{77} \bmod 119 = (1.27 \times 10^{140}) \bmod 119$
- $(1.27 \times 10^{140}) / 119 = (1.06 \times 10^{138})$ with a remainder of 19
- Therefore, M = 19

Summary

- Valuable information is constantly being exchanged between users
- A means to protect this information during transmission is critical
- Methods of security that were developed years ago are still being used (DES, RSA)
- The need for more complex encryption/decryption methods may be needed as advances in technology continue to flourish

Resources

- http://en.wikipedia.org/wiki/Data_Encryption_Star
- http://en.wikipedia.org/wiki/Rsa
- http://www.redbooks.ibm.com/abstracts/sg246168.html
- Stallings, William. Cryptography and Internet Security: Principles and Practice, 2e. Upper Saddle River, NJ: Prentice-Hall, 1999
- Stallings, William. Network Security Essentials: Applications and Standards, 3e.