Cryptography: Public Key Encryption

12-7-18

Journal

What types of online activities require information to be kept secret when it is transmitted?

How does cryptography allow for information to be kept secret when it is transmitted?

Objectives

•Students will understand the impact of the key distribution problem on secure communication.

•Students will understand that a carefully designed one-way mathematical function allows people to exchange keys or use public keys to solve the key distribution problem.

•Students will understand that digital certificates are used for authentication, and that these certificates rely on the trust model: the certificate authorities are being *trusted* to provide accurate information

CS Matters

Computer Encryption

- Encrypt Binary Sequences
- DES (Data Encryption Standard)
  - Adopted as the federal standard in the US in 1977
- AES (Advanced Encryption Standard)
  - Adopted in 2001
- Both are **symmetric key** algorithms.

Scenario

- Alice wants to send Li some secret information over the Internet.
- We know that she can encrypt the information before sending it, but how will Li know what key Alice used to encrypt the message?

Key Distribution Problem

- Delivery by Couriers
  - Expensive
  - Not necessarily reliable
  - Not practical for the average person

Key Distribution Problem

- Many people thought this problem could never be solved!
- Two “dreamers” teamed up to take on this problem and came up with two different solutions!
  - Martin Hellman
  - Whitfield Diffie

One-Way vs. Two-Way Functions

- Two-way functions are easy to use and easy to reverse.
  - Example: f(x) = 2x
    - Apply the function: f(5) = 2(5) = 10
    - Reverse the function: f(x) = 10, therefore 2x = 10, therefore x = 5

- One-way functions are easy to use but very difficult to reverse.

One-Way Functions

- Mixing Paint – video (2:25-???)
- Modulus → remainder %
  - Also called “clock arithmetic”

Hellman Key Exchange

- Activity:
  - You and a partner will establish a secret key while communicating publicly.
  - Your adversaries will eavesdrop on your communications to see if they can determine your secret key.

Was it really an original solution?

- http://cryptome.org/ukpk-alt.htm