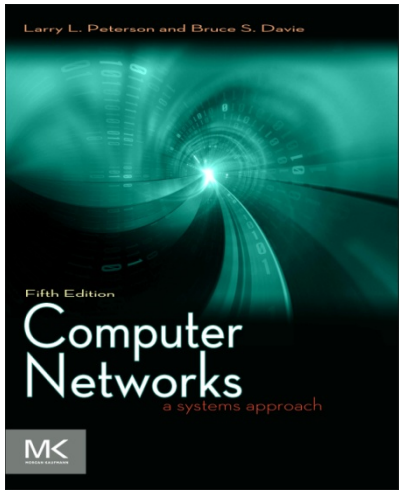


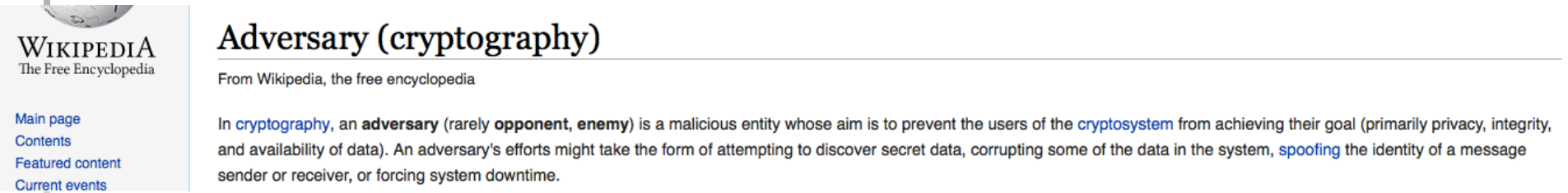
Chapter 8

Network Security

Problem

- Computer networks are shared resource
- The Internet is used by
  - Competing businesses
  - Not necessarily friendly governments,
  - Opportunistic criminals
- A network conversation or a distributed application may be compromised by an adversary.

Problem (Adversaries / Attackers)



WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events

Adversary (cryptography)

From Wikipedia, the free encyclopedia

In cryptography, an **adversary** (rarely **opponent**, **enemy**) is a malicious entity whose aim is to prevent the users of the cryptosystem from achieving their goal (primarily privacy, integrity, and availability of data). An adversary's efforts might take the form of attempting to discover secret data, corrupting some of the data in the system, spoofing the identity of a message sender or receiver, or forcing system downtime.

In cryptography, an **adversary** (rarely **opponent**, **enemy**) is a malicious entity whose aim is to prevent the users of the cryptosystem from achieving their goal (primarily privacy, integrity, and availability of data). An adversary's efforts might take the form of attempting to discover secret data, corrupting some of the data in the system, spoofing the identity of a message sender or receiver, or forcing system downtime.

Authentication

watched wikileak video about CIA

Problem (Adversaries / Attackers)

- Let's define these attacks in the context of:
  1. *Confidentiality*
  2. *Integrity*
  3. *Authentication*
  4. *Availability*
- Will also define other methods for exploiting end-systems vulnerabilities:
  1. *Worms*
  2. *Viruses*
  3. *Botnets*

Problem (Example Threat)

- Suppose you are a customer using a credit card to order an item from a website.
  - An adversary eavesdrops on your network communication
  - Can encrypt messages
    - A protocol that does so is said to provide *confidentiality*.
  - Concealing the quantity or destination of communication is called *traffic confidentiality*

Problem (Example Threat)

- Even with confidentiality there still remain threats for the website customer.
  - An adversary might still be able to change a few bits
    - Resulting in a valid order for, say, a completely different item or perhaps 1000 units of the item.
  - There are techniques to detect, if not prevent, such tampering.
    - A protocol that detects such message tampering provides *data integrity*.
  - The adversary could alternatively transmit an extra copy of your message in a *replay attack.*

Problem (Example Threat)

- Unknowingly being directed to a false website.
  - Can result from a DNS attack
  - Leads to translating a correct URL into an incorrect IP address—the address of a false website.
  - *Authentication* can be used.
    - *Authentication entails integrity*

Problem (Example Threat)

- The owner of the website can be attacked as well.
  - An *access control* issue
  - *Denial of Service (DOS)* attack
    - Ensuring a degree of access is called *availability*.

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.

Problem (Example Threat)

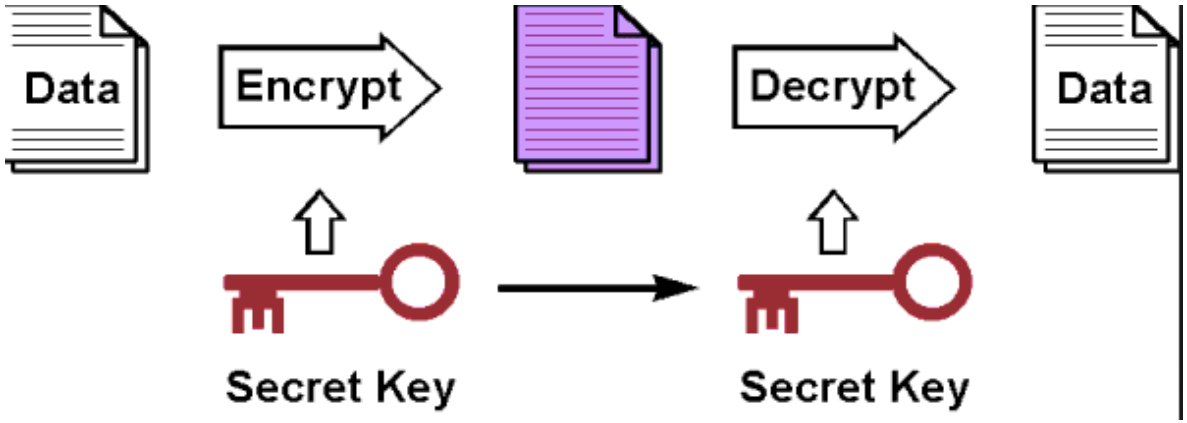
- Deployment of malicious code that exploits vulnerabilities in end-systems.
- *Worms*, have been known for several decades and continue to cause problems
- Their relatives, *viruses*, *which are spread by the* transmission of "infected" files.
- *Botnets*

A **botnet** is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks.

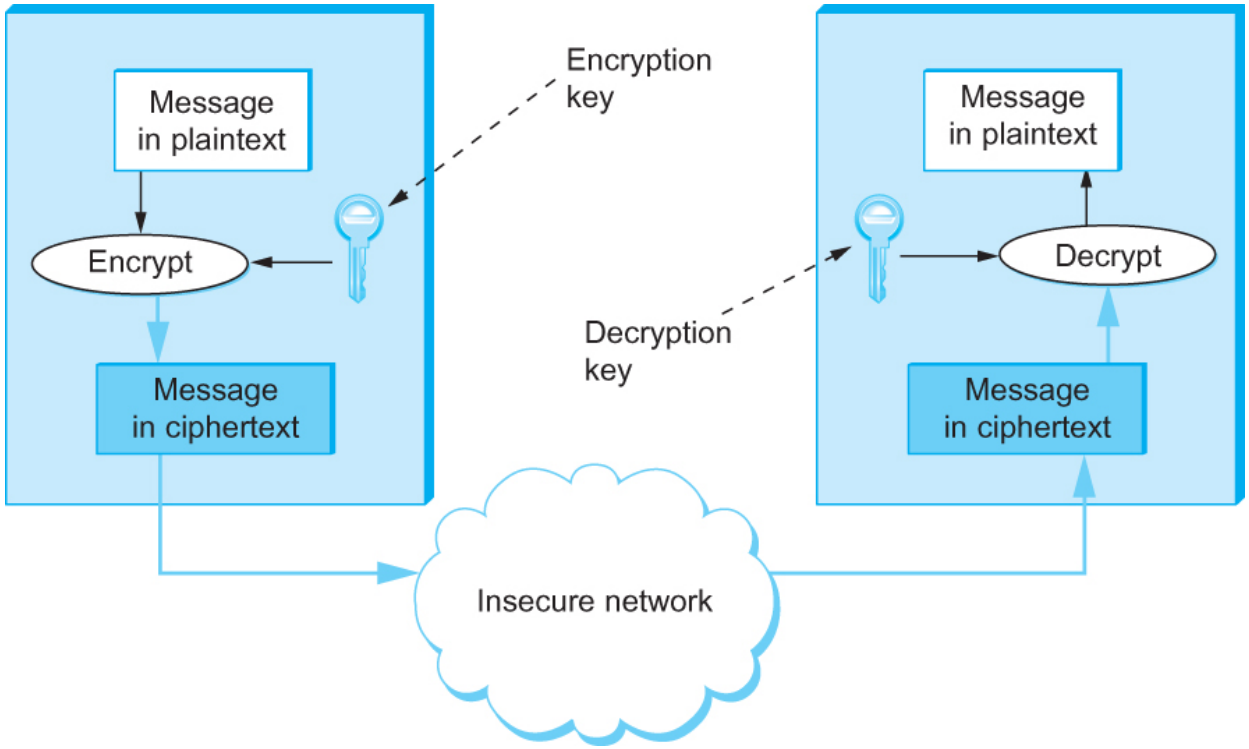
Botnet - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/**Botnet** Wikipedia

Cryptograhic Building Blocks

- We introduce the concepts of cryptography-based security step by step.
- The first step is the crypto-graphic algorithms
  - Ciphers (or codes)
- Cryptographic algorithms are parameterized by keys



Cryptograhic Building Blocks



Symmetric-key encryption and decryption

Cryptograhic Building Blocks

- Symmetric Key Ciphers
  - NIST has issued standards for a series of symmetric-key ciphers.
  - *Data Encryption Standard (DES) was the* first,
  - It has stood the test of time (so far)
    - However, brute force search has gotten faster.
  - DES's keys (56 independent bits) are now too small given current processor speeds.
    - With 56 bits we have $2^{56} = 7.21 \times 10^{16}$ keys to try
    - In fact, only half of those attempts (on average) are required, meaning 3.6×10^{16}

skipped

Cryptograhic Building Blocks

- Symmetric Key Ciphers
  - NIST also standardized the cipher *Triple DES (3DES), which leverages the cryptanalysis resistance* of DES while in effect increasing the key size.
  - A 3DES key has 168 (= 3 x 56) independent bits, and is used as three DES keys;
    1. DES-key1,
    2. DES-key2, and
    3. DES-key3.

skipped

Cryptograhic Building Blocks

- Symmetric Key Ciphers
  - 3DES Encryption of a block involves:
    1. DES-encrypting the block using DES-key1.
    2. Then DES-*decrypting the result using DES-key2.*
    3. *And finally* DES-encrypting that result using DES-key3.
  - 3DES Decryption involves:
    1. Decrypting using DES-key3.
    2. Then encrypting using DES-key2.
    3. And finally decrypting using DES-key1.

skipped

Cryptograhic Building Blocks

- Symmetric Key Ciphers
  - 3DES is being superseded by the *Advanced Encryption Standard (AES) standard* issued by NIST in 2001.
  - The cipher selected to become that standard was originally named Rijndael
    - Pronounced roughly like "Rhine dahl" based on the names of its inventors, Daemen and Rijmen.
  - AES supports key lengths of 128, 192, or 256 bits

skipped

Cryptograhic Building Blocks

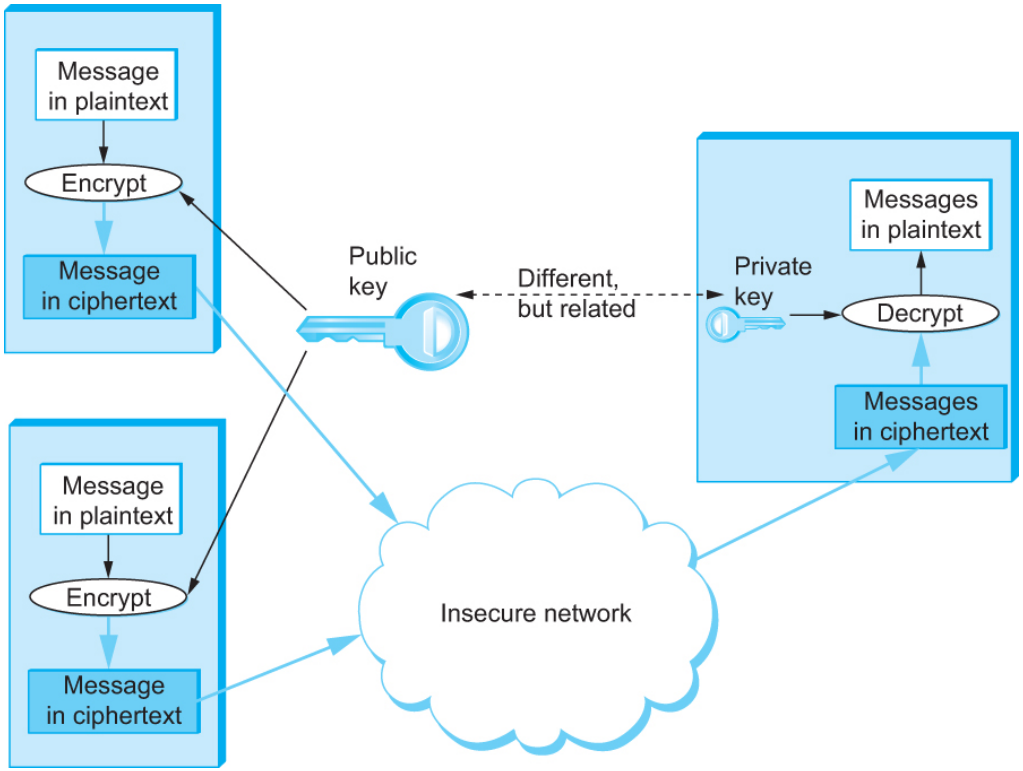
- Symmetric key encryption/decryption
  - Uses the same key for both encryption and decryption
- Asymmetric key (Public Key) encryption/ decryption
  - Uses a pair of related keys
    - One for encryption (public) and a different one for decryption (private).

Cryptograhic Building Blocks

- Public Key Ciphers **For data confidentiality**
  - The pair of keys is "owned" by just one participant.
  - The owner keeps the decryption key secret so that only the owner can decrypt messages; *private key.*
  - The owner makes *the* encryption key public, so that anyone can encrypt messages for the owner; *public key.*

Cryptograhic Building Blocks

- Public Key Ciphers



Public-key encryption

Use of asymmetric encryption to provide confidentiality for the message

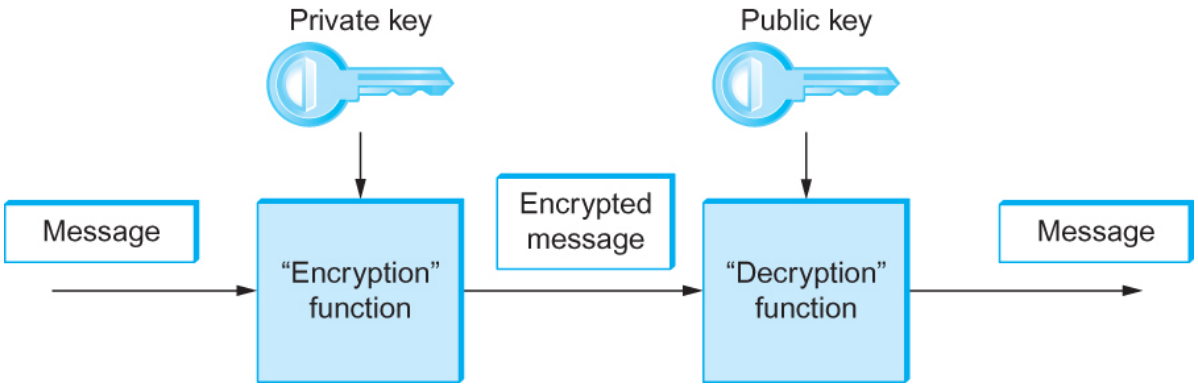
Cryptograhic Building Blocks

- Public Key Ciphers
  - The private key can be used (instead of public key) to encrypt messages (by the owner) so that they can only be decrypted using the public key.
  - This property clearly wouldn‘t be useful for ***confidentiality*** **bcoz everyone can know it**
    - Since anyone with the public key could decrypt such a message.
  - However, useful for ***authentication*** **Asymmetric Encryption used for authentication**
    - Since it tells the receiver of such a message that it could only have been created by the owner of the keys.

It could loose privacy when checking authentication who send this message from?

Cryptograhic Building Blocks

- Public Key Ciphers



Authentication using public keys

Cryptograhic Building Blocks

- Public Key Ciphers
  - The concept of public-key ciphers was first published in 1976 by Diffie and Hellman.
  - The best-known public-key cipher is RSA, named after its inventors: Rivest, Shamir, and Adleman.
    - RSA relies on the high computational cost of factoring large numbers.
  - Another public-key cipher is ElGamal.
    - It also relies on a mathematical problem and requires keys of at least 1024 bits.

the longer bits the stronger protection

Cryptograhic Building Blocks

- Summarizing the Symmetric versus Public Key Encryption
  - Symmetric method has better performance
  - Public key method has better security
- Using both can improve both security and performance

https://www.youtube.com/watch?v=ERp8420ucGs (0 to 7 mins)

Key Pre Distribution

- In the case of a symmetric-key cipher, how does a pair of participants obtain the key they share? (confidentiality of the key)
- In the case of a public-key cipher, how do participants know what public key belongs to a certain participant? (authentication of the key)
- The answer differs depending on whether the keys are short-lived *session keys* or *longer-lived pre-distributed keys*.

Key Pre Distribution

- A session key is a key used to secure a single, relatively short episode of communication: a session.
  - Each distinct session between a pair of participants uses a new session key, which is always a symmetric-key for speed.
  - The participants determine what session key to use by means of a protocol—a session key establishment protocol.
  - A session key establishment protocol needs its own security (so that, for example, an adversary cannot learn the new session key); that security is based on the longer-lived pre-distributed keys.

Key Pre Distribution

- There are several motivations for this division of labor between session keys and pre-distributed keys:
  1. Limiting the amount of time a key is used, results in
     - Less time for computationally intensive attacks,
     - Less ciphertext for cryptanalysis, and
     - Less information exposed should the key be broken.

Key Pre Distribution

- There are several motivations for this division of labor between session keys and pre-distributed keys:
  2. Pre-distribution of symmetric keys is problematic, too much overhead for a short session.
  3. Public key ciphers are generally superior for authentication and session key establishment
     - but too slow to use for encrypting the entire messages for confidentiality.

Key Pre Distribution

- Pre-Distribution of Public Keys
  - The algorithms to generate a matched pair of public and private keys are publicly known, and software that does it is widely available.
  - So if Alice wanted to use a public key cipher, she could generate her own pair of public and private keys, keep the private key hidden, and publicize the public key.
  - But how can she publicize her public key— assert that it belongs to her—in such a way that other participants can be sure it really belongs to her?

Key Pre Distribution

- Pre-Distribution of Public Keys
  - 2 keys system for communication
  - Public Key Infrastructure (PKI) is a complete scheme for certifying bindings between public keys and identities
  - A PKI starts with the ability to verify identities and bind them to keys out of band.
    - If Alice and Bob are individuals who know each other, then they could get together in the same room and Alice could give her public key to Bob directly, perhaps on a business card.
  - But what if they are two computers on the network?
    - Can use *public key certificate* or simply *certificates*
    - *Certificate Authorities* can be used to issue such certificates

Key Pre Distribution

- Pre-Distribution of Public Keys
  - X.509 standard specifies that a certificate must include:
    - The identity of the entity being certified
    - The public key of the entity being certified
    - The identity of the signer
    - The digital signature
    - A digital signature algorithm identifier
  - Certificate Authorities (CAs) can issue such certificates

Digital Certificate for authentication:
Condientiality: encrypts data using asymmetric keys

Key Pre Distribution

- Pre-Distribution of Public Keys
  - Certification Authorities can issue certificates
    - A *certification authority or certificate authority (CA) is an entity claimed (by someone)* to be trustworthy for verifying identities and issuing public key certificates.
    - There are commercial CAs, governmental CAs, and even free CAs.
    - To use a CA, you must know its own key.
    - Then you can believe any certificate signed by that new CA

https://www.youtube.com/watch?v=t0F7fe5Alwg (0 to 7 mins)

https://www.youtube.com/watch?v=LRMBZhdFjDI (0 to 15 mins)

Key Pre Distribution

- Pre-Distribution of Symmetric Keys
  - Diffie-Hellman Key Agreement
    - The Diffie-Hellman key agreement protocol establishes a session key without using any pre-distributed keys.
    - The messages exchanged between Alice and Bob can be read by anyone able to eavesdrop, and yet the eavesdropper won't know the session key that Alice and Bob end up with.
    - On the other hand, Diffie-Hellman doesn't authenticate the participants.
    - Since it is rarely useful to communicate securely without being sure whom you're communicating with, Diffie-Hellman is usually augmented in some way to provide authentication.

https://www.youtube.com/watch?v=YEBfamv-_do (0 to 8 mins)

Key Pre Distribution

- Pre-Distribution of Symmetric Keys
  - Diffie-Hellman Key Agreement Example
  - Both Alice and Bob know prime p = 29 and a large number g = 7

Alice's Private Key A = 5

Alice's Public Key = $g^A \bmod p$

$= 7^5 \bmod 29$

$= 16$

Pass 16 as public key to Bob ➔

Alice will use Bob's public key to generate the shared secret value:

$23^5 \bmod 29 = 6436343 \bmod 29$

$= 25$

Bob's Private Key B = 11

Bob's Public Key = $g^B \bmod p$

$= 7^{11} \bmod 29$

$= 23$

➔ Pass 23 as public key to Alice

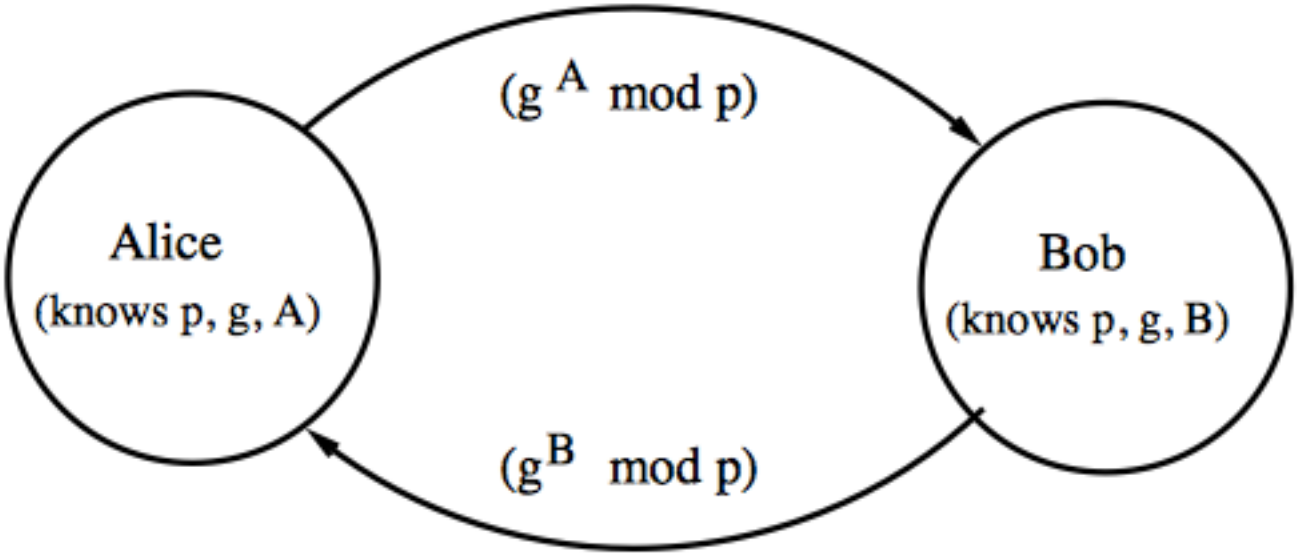
Bob will use Alice's public key to generate the shared secret value:

$16^{11} \bmod 29 = 2^{35} \bmod 29$

$= 25$

Key Pre Distribution

- Pre-Distribution of Symmetric Keys
  - Diffie-Hellman Key Agreement Example
  - Both Alice and Bob know prime p = 29 and a large number g = 7



https://www.youtube.com/watch?v=YEBfamv-_do

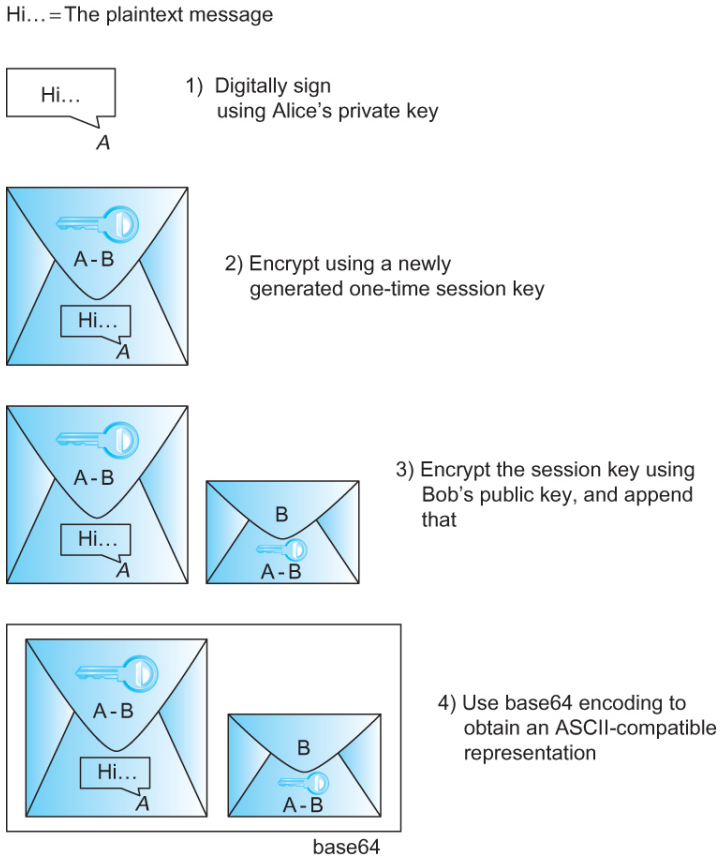
Example Systems

- Pretty Good Privacy (PGP)
  - Pretty Good Privacy (PGP) is a widely used approach to providing security for electronic mail. It provides authentication, confidentiality, data integrity, and nonrepudiation.
  - Originally devised by Phil Zimmerman, it has evolved into an IETF standard known as OpenPGP
  - PGP's confidentiality and receiver authentication depend on the receiver of an email message having a public key that is known to the sender.
  - To provide sender authentication and nonrepudiation, the sender must have a public key that is known by the receiver.
  - These public keys are pre-distributed using certificates and a web-of-trust PKI.
  - PGP supports RSA and DSS for public key certificates.

skipped

Example Systems

- Pretty Good Privacy (PGP)



skipped

PGP's steps to prepare a message for emailing from Alice to Bob

Firewalls

- A firewall is a system that typically sits at some point of connectivity between a site it protects and the rest of the network.
- It is usually implemented as an "appliance" or part of a router, although a "personal firewall" may be implemented on an end user machine.
- Firewall-based security depends on the firewall being the only connectivity to the site from outside;
  - There should be no way to bypass the firewall via other gateways, wireless connections, or dial-up connections.

Firewalls

- In effect, a firewall divides a network into a more-trusted zone internal to the firewall, and a less-trusted zone external to the firewall.
- This is useful if you do not want external users to access a particular host or service within your site.
- Firewalls may be used to create multiple *zones of trust, such as a hierarchy of* increasingly trusted zones.
- A common arrangement involves three zones of trust: the internal network; the *DMZ ("demilitarized zone");* and the rest of the Internet.

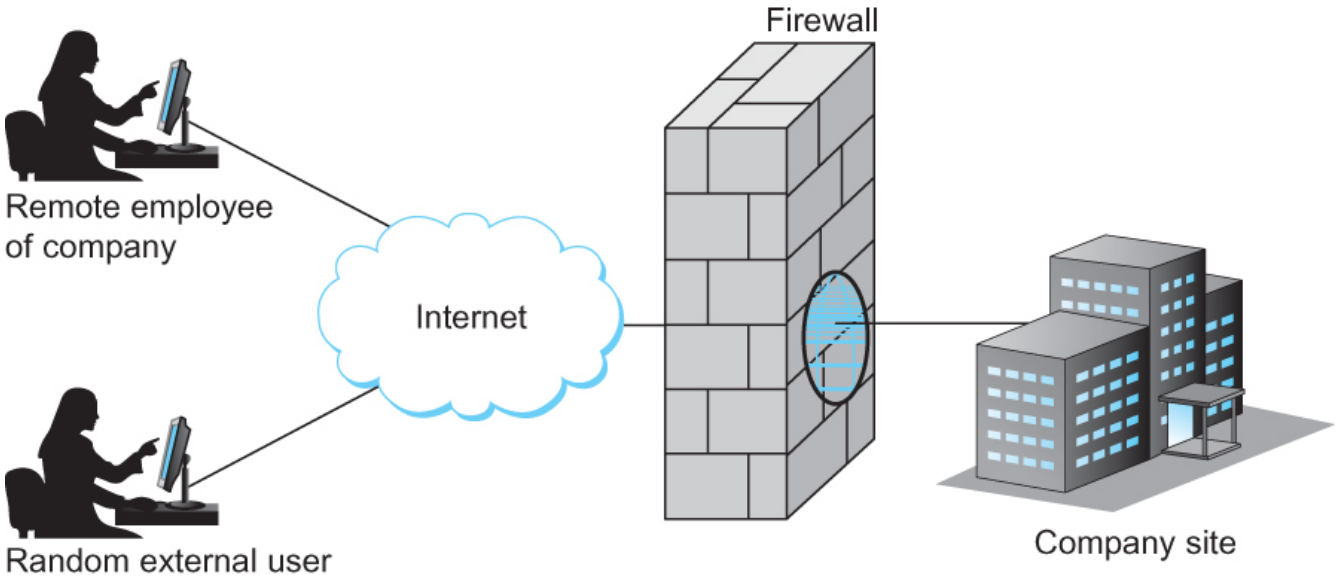
Firewalls

- Firewalls filter based on IP, TCP, and UDP information, among other things. ???
- They are configured with a table of addresses that characterize the packets they will, and will not, forward.
- By addresses, we mean more than just the destination's IP address, although that is one possibility.
- Generally, each entry in the table is a 4-tuple: It gives the IP address and TCP (or UDP) port number for both the source and destination.

4 tuples:
- Source IP address
- Source TCP (or UDP) port number
- Destination IP address
- Destination TCP(or UDP) port number

can do 2 things:
- allow
- deny

Firewalls



A firewall filters packets flowing between a site and the rest of the Internet

Summary

- We have discussed privacy and security issues in the network
- We have discussed different authentication protocols
- We have discussed different key distribution protocols
- We have discussed different cipher techniques
  - Classical (symmetric) and Public-Key