WIRELESS LAN SECURITY

02 – BASIC SECURITY MECHANICS AND MECHANISMS

02 – Basic Security Mechanics and Mechanisms

- Security Mechanics
- Security Mechanisms
- Authentication and Identity Protocols

Security Mechanics

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Access control
- Encryption
- Key management

Confidentiality

- **Definition**: The capability to send (and receive) data without divulging any part to unauthorized entities during the transmission of data.
- **Mechanisms**: Encryption—symmetric and asymmetric.

Integrity

- **Definition**: The capability to send (and receive) data such that unauthorized entities cannot change any part of the exchanged data without the sender/receiver detecting the change.
- If only integrity mechanics are in place, data can be changed, but the integrity will detect tampering.
- **Mechanisms**: Digital signatures using one-way hash functions.

Availability

- **Definition**: The capability to receive and send data.
- For example, if a system is under a DoS attack, it will not be able to receive or send data.
- **Mechanisms**: Availability mechanisms are mostly defense mechanisms that detect various forms of DoS attacks and guard against them.

Authentication

- **Definition**: Authentication establishes the identity of the sender or receiver of information.
- Any integrity check or confidential information is often meaningless if the identity of the sending or receiving party is not properly established.
- **Mechanisms**: Multiple levels and protocols such as 802.1x, RADIUS, PAP/CHAP, MS-CHAP, and so on.

Authorization

- **Definition**: Authorization is tightly coupled with authentication in most network resource access requirements. Authorization establishes what you are allowed to do after you have identified yourself. (It is also called access control, capabilities, and permissions)
- **Mechanisms**: Multiple levels and protocols.

Access control

- **Definition**: The capability to control access of entities to resources based on various properties: attributes, authentication, policies, and so on.
- **Mechanisms**: At the access point (AP) based on authentication or knowledge of the WEP key.

Encryption

- **Definition**: The capability to transform data (or plain text) into meaningless bytes (cipher text) based on some algorithm.
- Decryption is the act of turning the meaningless bytes to meaningful data again.
- **Mechanisms**: The wireless domain employs mechanisms such as WEP, TKIP, and CCMP.

Key management

- **Definition**: A key is a digital code that can be used to encrypt, decrypt, and sign information. Some keys are kept private, and others are shared and must be distributed in a secure manner.
- Key management refers to the process of distributing keys for the processes previously mentioned (for example, changing keys, not signing information).
- **Mechanisms**: The challenge in the wireless area is the key distribution—secure and scaleable in an automated fashion.

02 – Basic Security Mechanics and Mechanisms

- Security Mechanics
- Security Mechanisms
- Authentication and Identity Protocols

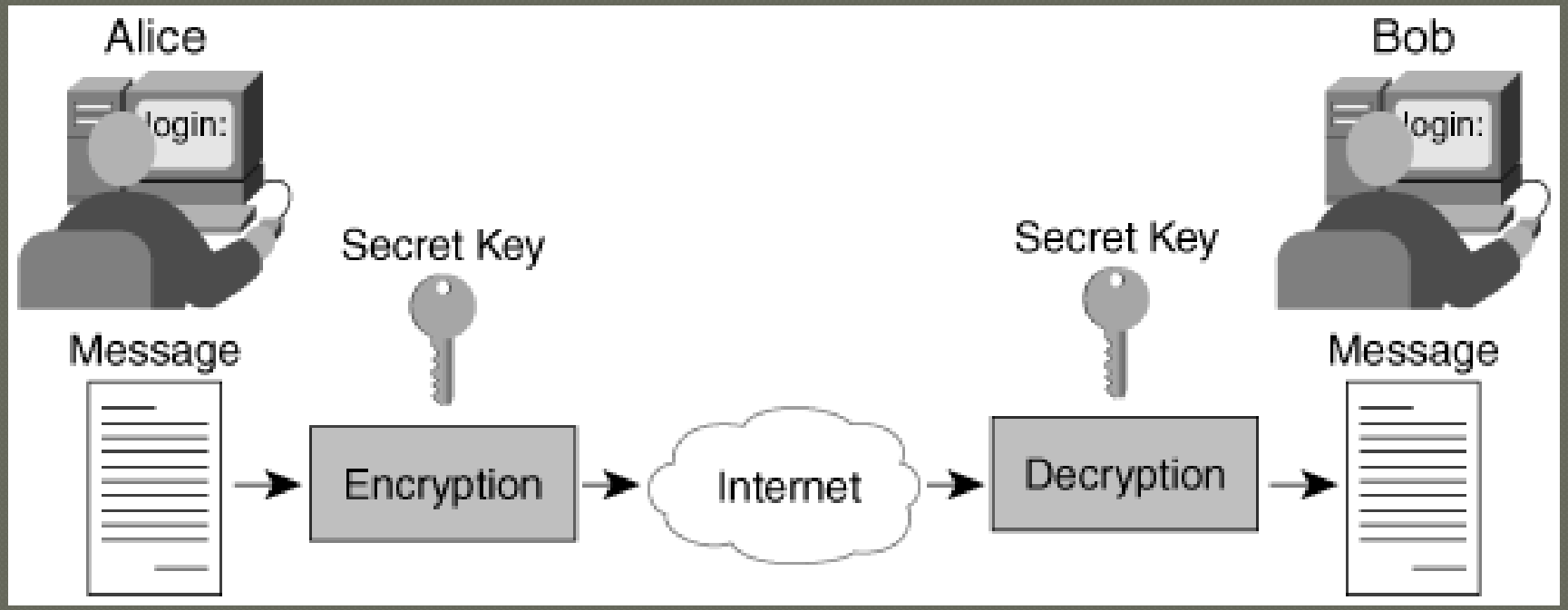
Confidentiality Mechanisms

- Confidentiality is achieved using data encryption.
- Encryption can be done using either the symmetric key paradigm or the asymmetric key paradigm.

Symmetric Key Encryption

- Symmetric key encryption - secret key encryption - uses a common key and the same cryptographic algorithm to scramble and unscramble a message.
- Symmetric key encryption and decryption are mathematically inexpensive compared to asymmetric key; therefore, they have a major performance advantage.

Symmetric Key Encryption



- Both Alice and Bob have to agree on the same cryptographic algorithm and common key—the secret key.

Symmetric Key Encryption Categories

- Block ciphers— Operate on 64-bit message blocks. Even though most of the block ciphers operate on a 64-bit block, it is not an absolute requirement.
- Stream ciphers— Operate on a stream of data, which basically means they operate on a byte at a time.

Chaining Mechanics in Block Cipher

- Larger messages are broken up into 64-bit blocks and somehow chain them together.
- Four common chaining mechanisms (modes), and each mode defines a method of combining the plain text, the secret key, and the cipher text to generate the stream of cipher text that is actually transmitted to the:
  - Electronic codebook (ECB)
  - Cipher block chaining (CBC)
  - Cipher feedback (CFB)
  - Output feedback (OFB)

Electronic Codebook (ECB)

- The ECB chaining mechanism encodes each 64-bit block independently but uses the same key.
- The result is that the same plain text will always result in the same cipher text.

Cipher Block Chaining (CBC)

- In CBC, the current block is XORed with the previous block.
- This still leaves the first block vulnerable, and for that, the CBC uses an initialization vector (IV) - an encrypted block of random data used as the first 64-bit block to begin the chaining process.

Cipher Feedback (CFB) Output Feedback (OFB)

- The CFB mode uses the cipher text of the preceding block rather than the plain text.
- The OFB mode is similar to the CFB, but the XORed block is generated randomly and is therefore independent of the preceding plain text.

Symmetric Key Encryption Algorithms

- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)
- 3DES (read "triple DES")
- Rivest Cipher 4 (RC4)
- International Data Encryption Algorithm (IDEA)

Data Encryption Standard (DES)

- most widely used encryption scheme today
- operates on 64-bit message blocks
- uses 64-bit keys, of which 56 bits are chosen randomly. The remaining 8 bits are parity bits (one for each 7-bit block of the 56-bit random value)
- Generally, DES operates in either CBC mode or CFB mode.

3DES (Triple DES)

- an alternative to DES
- takes a 64-bit block of data and performs the encrypt, decrypt, and encrypt operations
- can use one, two, or three different keys
- is defined only in ECB mode

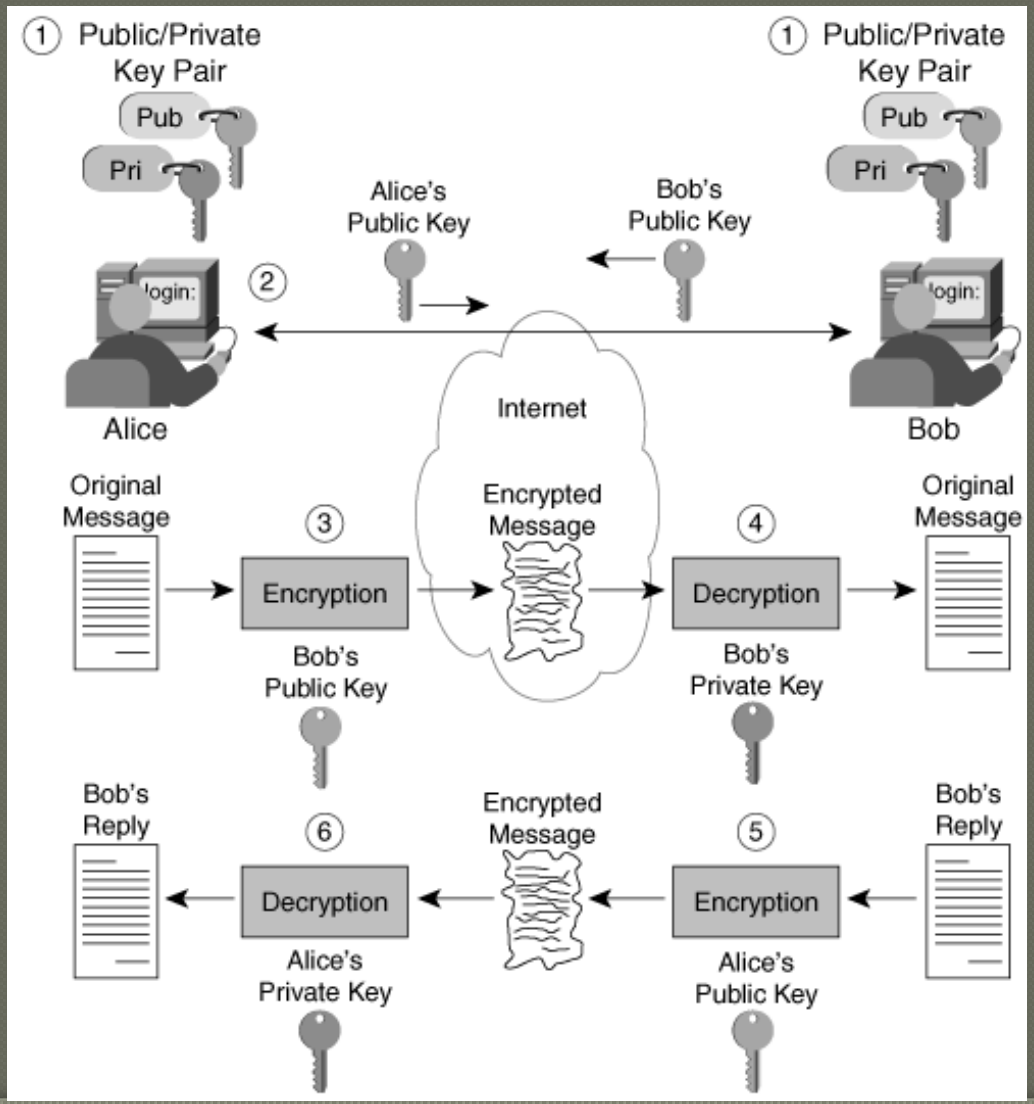
Asymmetric Encryption

- often referred to as Public Key Encryption.
- can use either the same algorithm or different but complementary algorithms to scramble and unscramble data
- Two different but related key values are required: a public key and a private key.
- If plain text is encrypted using the public key, it can only be decrypted using the private key (and vice versa).

Common Uses of Public Key Algorithms

- Data integrity
- Data confidentiality
- Sender non-repudiation
- Sender authentication

Ensuring Data Integrity and Confidentiality



Sender Authentication and Nonrepudiation