Chapter 8 Network Security

- Security threats
  - An adversary could eavesdrop on your network communication
    - It is possible to encrypt messages so as to prevent an adversary from understanding the message contents. A protocol that does so is said to provide confidentiality.
  - An adversary might be able to change your message
    - There are techniques to detect such tampering. A protocol that detects such message tampering provides data integrity.
  - An adversary could transmit an extra copy of your message in a replay attack.
    - A protocol that detects replays provides originality.
  - An adversary could impersonate someone else
    - A protocol that ensures that you really are talking to whom you think you’re talking is said to provide authentication.

- Principles of Ciphers
  - Encryption transforms a message in such a way that it becomes unintelligible to any party that does not have the secret of how to reverse the transformation
  - The sender applies an encryption function to the original plaintext message, resulting in a ciphertext message that is sent over the network
  - The receiver applies a secret decryption function to recover the original plaintext.
The transformation represented by an encryption function and its corresponding decryption function is called a *cipher*.

Encryption & decryption functions are parameterized by a *key*
- The functions are public, the key is secret

The basic requirement for an encryption algorithm is that it turns plaintext into ciphertext in such a way that only the intended recipient—the holder of the decryption key—can recover the plaintext.

Most ciphers are *block ciphers*: they take as input a plaintext block of a certain fixed size, typically 64 to 128 bits.

Using a block cipher to encrypt each block independently has the weakness that a given plaintext block will always result in the same ciphertext block.
- This makes it much easier for a cryptanalyst to break the cipher.

Block ciphers are always augmented to make the ciphertext for a block vary depending on context.

A common way to augment a block cipher is *cipher block chaining (CBC)*, in which each plaintext block is XORed with the previous block’s ciphertext before being encrypted.
- The result is that each block’s ciphertext depends in part on the preceding blocks, i.e. on its context.
- The first plaintext block is XORed with a random number called an initialization vector (IV)

- **Symmetric Key Ciphers**
  - Both participants in a communication share the same key
    - The shared key must be known only to the participants
The U.S. National Institute of Standards and Technology (NIST) has issued standards for a series of symmetric-key ciphers.

- **Data Encryption Standard (DES)** was the first
  - 64-bit block size, 56-bit key
  - No cryptanalytic attack better than brute force search has been discovered. However, 56-bit keys are now too small given current processor speeds.

- NIST also standardized the cipher **Triple DES (3DES)**, which applies DES three times to each data block.
  - Uses 3 DES keys
  - Encryption of a block is performed by first encrypting the block using key1, then decrypting the result using key2, and finally encrypting that result using key3.
  - Decryption involves decrypting using key3, then encrypting using key2, then decrypting using key1.

- 3DES is being superseded by the **Advanced Encryption Standard (AES)** issued by NIST in 2001.
  - AES supports key lengths of 128, 192, or 256 bits, and the block length is 128 bits.

- **Public Key Ciphers**
  - A participant owns a pair of keys, one for encryption and one for decryption
  - The owner keeps the decryption key secret so that only the owner can decrypt messages; that key is called the **private key**.
  - The owner makes the encryption key public, so that anyone can encrypt messages for the owner; that key is called the **public key**.
Any participant can get the public key and send an encrypted message to the owner of the keys, and only the owner has the private key necessary to decrypt it.

An important additional property of public-key ciphers is that the private decryption key can be used with the encryption algorithm to encrypt messages so that they can only be decrypted using the public encryption key.

- This property is useful for authentication since it tells the receiver of such a message that it could only have been created by the owner of the keys.

The best-known public-key cipher is RSA

- RSA relies on the high computational cost of factoring large numbers, and requires keys of at least 1024 bits.

Another public-key cipher is ElGamal.

- Like RSA, it relies on a mathematical problem, the discrete logarithm problem, for which no efficient solution has been found, and requires keys of at least 1024 bits.

Public-key ciphers are several orders of magnitude slower than symmetric-key ciphers. Symmetric-key ciphers are used for the vast majority of encryption, while public-key ciphers are used in authentication and session key establishment.

- Authenticators

An authenticator is a value, to be included in a transmitted message, that can be used to verify simultaneously the authenticity and the data integrity of a message.
One kind of authenticator combines encryption and a cryptographic hash function.

- A cryptographic hash function is a function that outputs sufficient redundant information about a message to expose any tampering.
  - Cryptographic hash algorithms are treated as public knowledge
- The value it outputs is called a message digest and is appended to the message.
  - All the message digests produced by a given hash have the same number of bits
- An authenticator can be created by encrypting the message digest
- The receiver computes a digest of the plaintext part of the message and compares that to the decrypted message digest
  - If they are equal, the receiver would conclude that the message is indeed from its alleged sender and has not been tempered with
- There will be different input messages that produce the same message digest, like collisions in a hash table.
  - The hash function must have the one-way property: it must be computationally infeasible for an adversary to find any plaintext message that has the same digest as the original plaintext message
- Common cryptographic hash algorithms
  - Message Digest 5 (MD5): 128-bit digest
  - Secure Hash Algorithm 1 (SHA-1): 160-bit digest
- A digest encrypted with a public key algorithm using the private key is called a *digital signature* because it provides nonrepudiation like a written signature.
  - Another kind of authenticator uses a hash-like function that takes a secret value (known to only the sender and the receiver) as a parameter.
    - Such a function outputs an authenticator called a *message authentication code (MAC)*.
    - The sender appends the MAC to her plaintext message.
    - The receiver recomputes the MAC using the plaintext and the secret value, and compares that recomputed MAC to the received MAC.
  - A common variation on MACs is to apply a cryptographic hash (e.g., MD5) to the concatenation of the plaintext message and the secret value
    - The resulting digest is called a *hashed message authentication code (HMAC)*
    - The HMAC is appended to the plaintext message.
    - Only a receiver who knows the secret value can compute the correct HMAC to compare with the received HMAC.