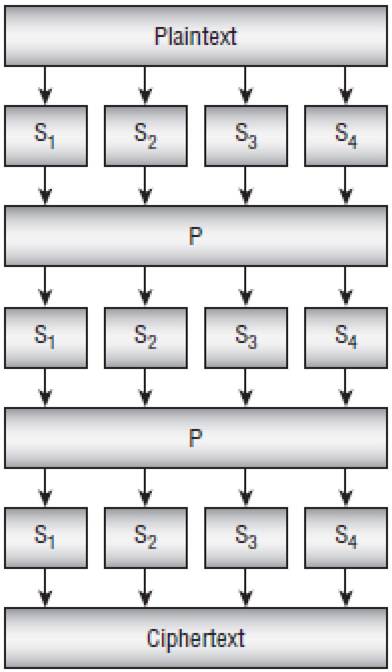
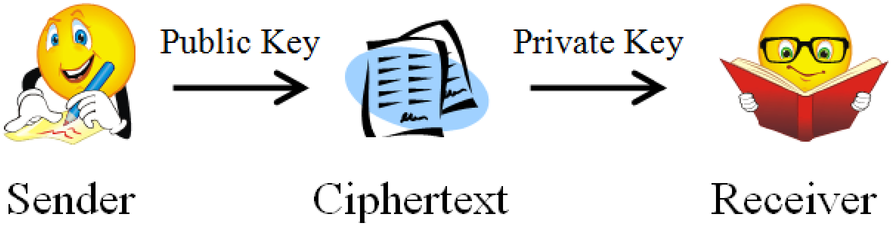
Modern Cryptography





Agenda

- Block Ciphers
- Public-Key Encryption
- Other Uses for Cryptography
- Summary
- Exercises

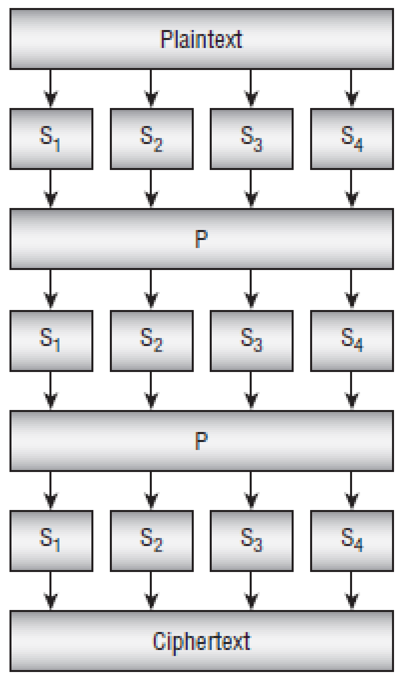
Block Ciphers

- The message is broken into blocks that are encrypted separately
- Allows easy streaming
- Allows efficient memory management

- Substitution-Permutation Networks

Substitution-Permutation Networks

- S-box: Combines part of a block with part of the key
- P-box: Rearranges the bits in the entire block



AES

- The Advanced Encryption Standard (AES) uses a substitution-permutation
- It uses a block size of 128 bits and a key size of 128, 192, or 256 bits, depending on the level of security you want
- # Rounds:
  - 10 rounds for 128-bit keys
  - 12 rounds for 192-bit keys
  - 14 rounds for 256-bit keys

Feistel Ciphers

- Named after cryptographer Horst Feistel

1. Split the plaintext into two halves, L_0 and R_0
2. Repeat:
   a. Set L_i+1 = R_i
   b. Set R_i+1 = $L_i \oplus F(R_i, K_i)$
3. Ciphertext is L_{i+1} together with R_{i+1}

K_i is the key for round i

F is some function

Decrypting Feistel Ciphers

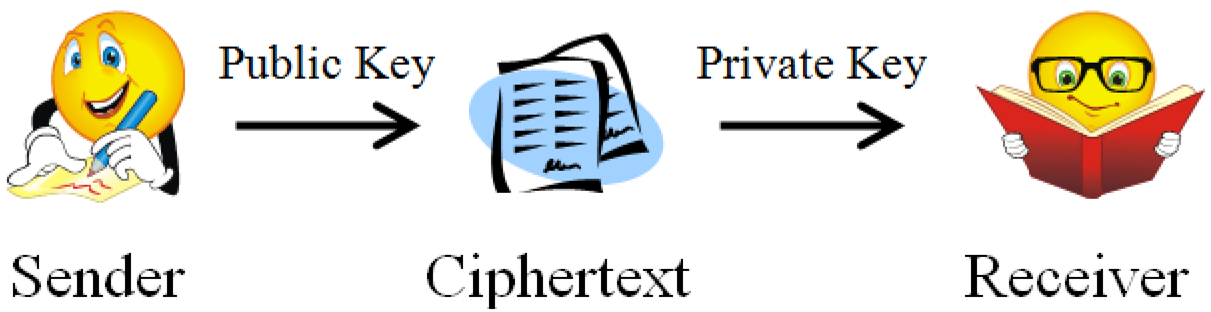
1. Split the ciphertext into halves, L_{i+1} and R_{i+1}
2. Repeat:
   a. Set $R_i = L_{i+1}$
   b. Set $L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$

DES

- The Data Encryption Standard (DES) is a Feistel cipher
- No longer considered secure enough, largely due to its relatively short 56-bit key
- A variation of this method called Triple DES simply applies DES three times to each block
- Triple DES is believed to be secure in practice, although most highly secure applications now use AES instead

Public-Key Encryption

- The sender uses the public key (known to everyone) to encrypt messages
- The receiver uses the private key (known only to the receiver) to decrypt messages



RSA

- Uses the fact that multiplying two numbers is easy but factoring large numbers is hard

Generating Keys

1. Pick two large prime numbers p and q
2. Compute $n = p \times q$. Release n as the public key modulus.
3. Compute $\phi(n)$, where ϕ is Euler's totient function (more about this later). Pick integer e where $1 \le e \le \phi(n)$ and e and $\phi(n)$ are relatively prime. Release n as the public key exponent.
4. Find d, the multiplicative inverse of e modulo $\phi(n)$. In other words, $e \times d \equiv 1 \bmod \phi(n)$. The value d is the private key.

Encrypting and Decrypting

- The public key consists of the values n and e

- To encrypt message M, the sender uses the formula $C = M^e \bmod n$
- To decrypt a message, the receiver simply calculates $C^d \bmod n$

Euler’s Totient Function

- $\phi(n)$ gives the number of positive integers less than n that are relatively prime to n
- Example: $\phi(12) = 4$ because 1, 5, 7, and 11 are relatively prime to 12

Euler's Totient Function (continued)

- A prime number is relatively prime to every number less than itself so $\phi(p) = p - 1$
- If p and q are relatively prime,

  $$\phi(p \times q) = \phi(p) \times \phi(p)$$

- If p and q are both primes, they are relatively prime, so in step 3 it is easy to compute:

  $$\phi(n) = \phi(p \times q) = \phi(p) \times \phi(q) = (p - 1) \times (q - 1)$$

Euler's Totient Function Example

- Suppose p = 3 and q = 5
- $\phi(15) = \phi(3) \times \phi(5)$
  $= (3 - 1) \times (5 - 1)$
  $= 2 \times 4$
  $= 8$
- The positive integers smaller than 15 that are relatively prime to 15 are:
  1, 2, 4, 7, 8, 11, 13, and 14

Multiplicative Inverses

- Method 1:
  - Compute:

    $(1 \times d) \bmod \phi(n)$

    $(2 \times d) \bmod \phi(n)$

    $(3 \times d) \bmod \phi(n)$

    ...

    until you find a value that makes the result 1
- Method 2:
  - Use an extended GCD algorithm

    (See http://en.wikipedia.org/wiki/Extended_Euclidean_algorithm)

RSA Example – Finding Keys

1. Pick two large prime numbers p and q.

   Let $p = 17$ and $q = 29$

2. Compute the public key modulus $n = p \times q$

   $n = 17 \times 29 = 493$

3. Compute $\phi(n)$ where ϕ is Euler's totient function

   $\phi(n) = (p - 1) \times (q - 1) = 16 \times 28 = 448$

RSA Example – Finding Keys (continued)

4. Pick an integer e where $1 \le e \le \phi(n)$ and e and $\phi(n)$ are relatively prime

   Need $1 \le e \le 448$, relatively prime to 448

   $448 = 2^6 \times 7$ so no factors of 2 or 7

   Let $e = 3 \times 5 \times 11 = 165$

5. Find d, the multiplicative inverse of e modulo $\phi(n)$. In other words, $d \times 165 \equiv 1 \bmod 448$.

   $d = 429$

RSA Example – Encryption

- Public exponent $e = 165$
- Public modulus $n = 493$
- Secret key $d = 429$

- Encrypt the message $M = 321$
- $C = M^e \bmod n = 321^{165} \bmod 493 = 359$

RSA Example – Decryption

- Public exponent $e = 165$
- Public modulus $n = 493$
- Secret key $d = 429$

- Decrypt the message $C = 359$
- $M = C^d \bmod n = 359^{429} \bmod 493 = 321$

Other Uses for Cryptography

- Hashing
- Digital signatures
- Document signing

Summary

- Block Ciphers
  - Substitution-Permutation Networks (AES)
  - Feistel Ciphers (DES)
- Public-Key Encryption
  - RSA
- Other Uses for Cryptography

Exercises

- Chapter 16 Exercise 15.
- Read *Essential Algorithms, 2e* Chapter 17 pages 543 – 560. (All of Chapter 17.)