Elementary Cryptography

Jun Li
lijun@cs.uoregon.edu

Cryptosystem

- Plaintext $P = <p_1, p_2, \ldots, p_n>$.
- Ciphertext $C = <c_1, c_2, \ldots, c_m>$.
- $C = E(P)$
- $P = D(C)$
- A cryptosystem satisfies: $P = D(E(P))$.

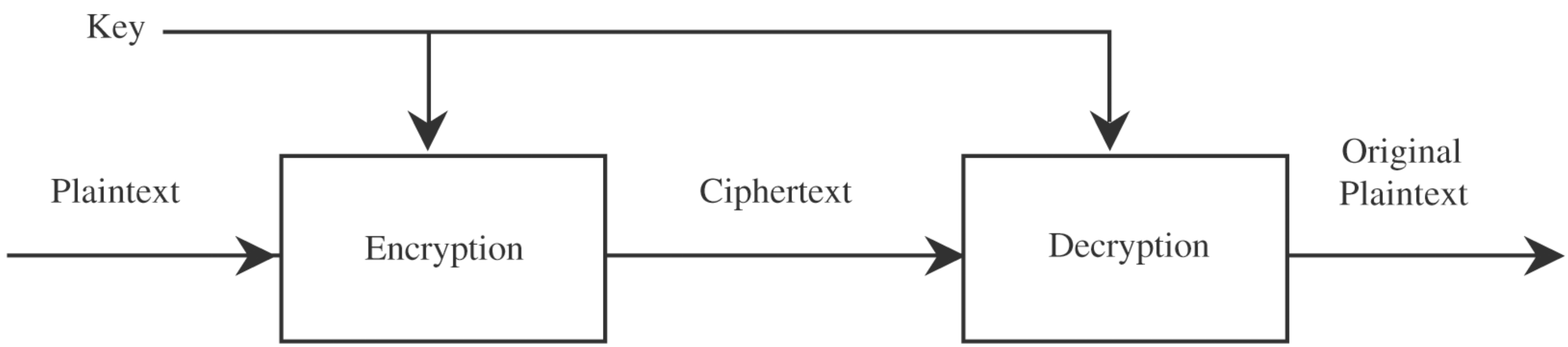
Symmetric and Asymmetric Encryption

- Encryption and decryption algorithms usually need a **key**:

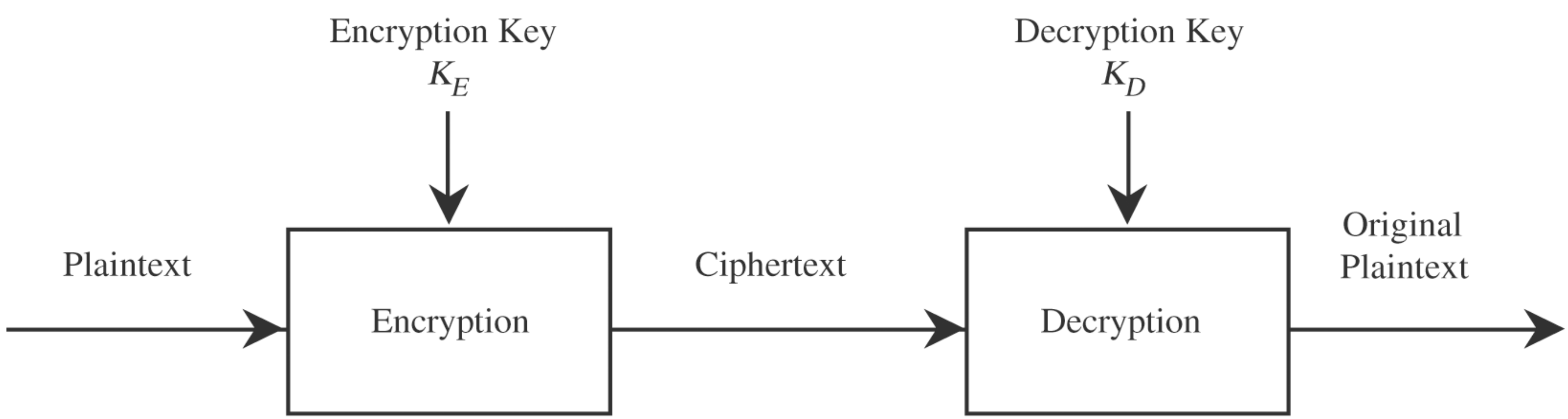
  $C = E\,(K_E, P)$ and $P = D\,(K_D, C)$

  Thus $P = D\,(K_D, E\,(K_E, P))$

- If $K_E = K_D$, then **symmetric** encryption
- Otherwise, **asymmetric** encryption



(a) Symmetric Cryptosystem



(b) Asymmetric Cryptosystem $(K_E \neq K_D)$

Cryptography, Cryptanalysis, Cryptology

- Cryptography: using encryption to hide text
- Cryptanalysis: trying to find hidden text
- Cryptology: includes cryptography and cryptanalysis

Cryptography: Confusion and Diffusion

- Confusion: hard to determine the relationship between plaintext, key, and ciphertext.
  - E.g., hard to know what happens to the ciphertext if changing one character in plaintext
- Diffusion: Spread the information from the plaintext over the entire ciphertext
  - A change in plaintext affects many parts of ciphertext

Substitution Cipher: Exchanging one letter with another

- Caecar Cipher: $c_i = E\,(p_i) = p_i{+}3$
- But such a cipher is vulnerable to cryptanalysis
- How to break Caecar cipher?

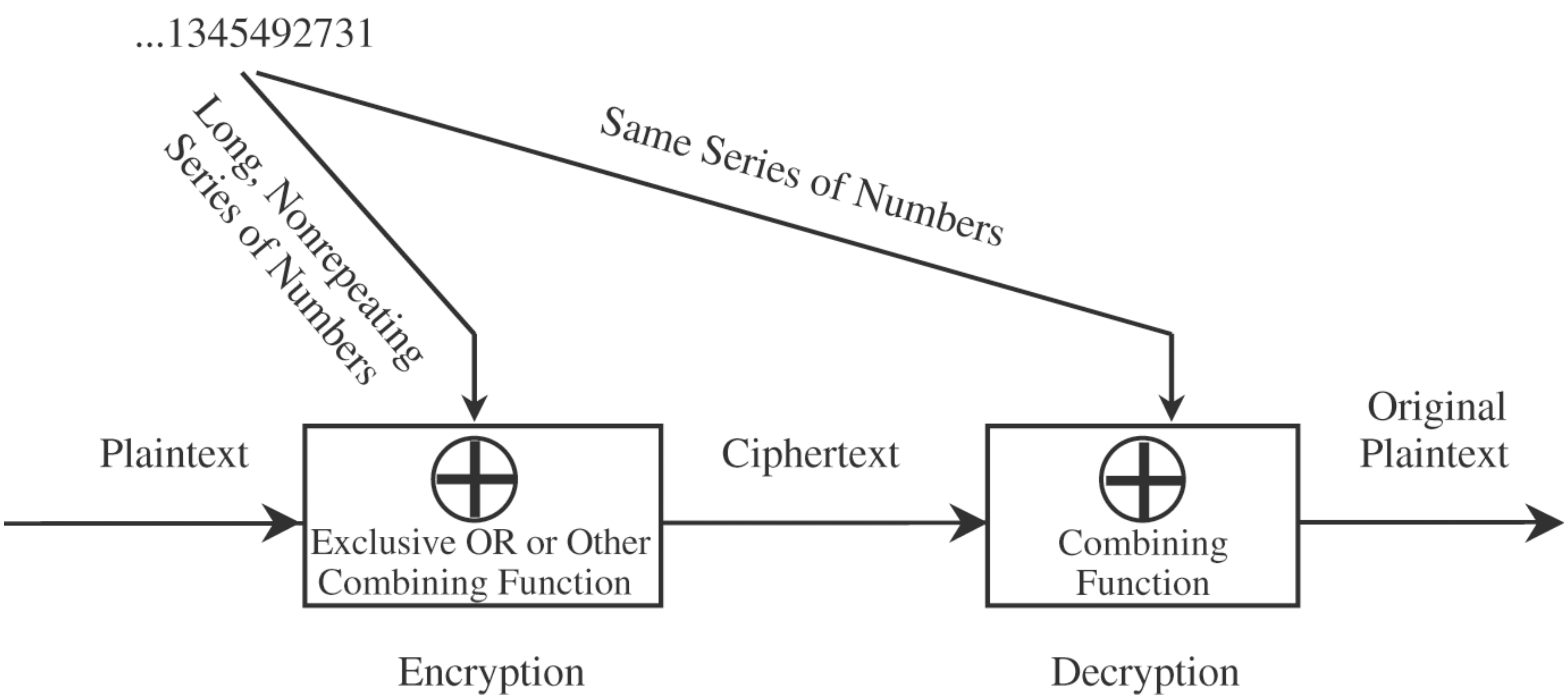
One-Time Pads

- Large, non-repeating keys written on sheets of paper glued into a pad
- For every p_i, find k_i from the pad
- $c_i = (p_i + k_i) \bmod 26$ (Vigenere tableau)

- Two Problems:
  - Absolute Synchronization
  - The need for an unlimited number of keys

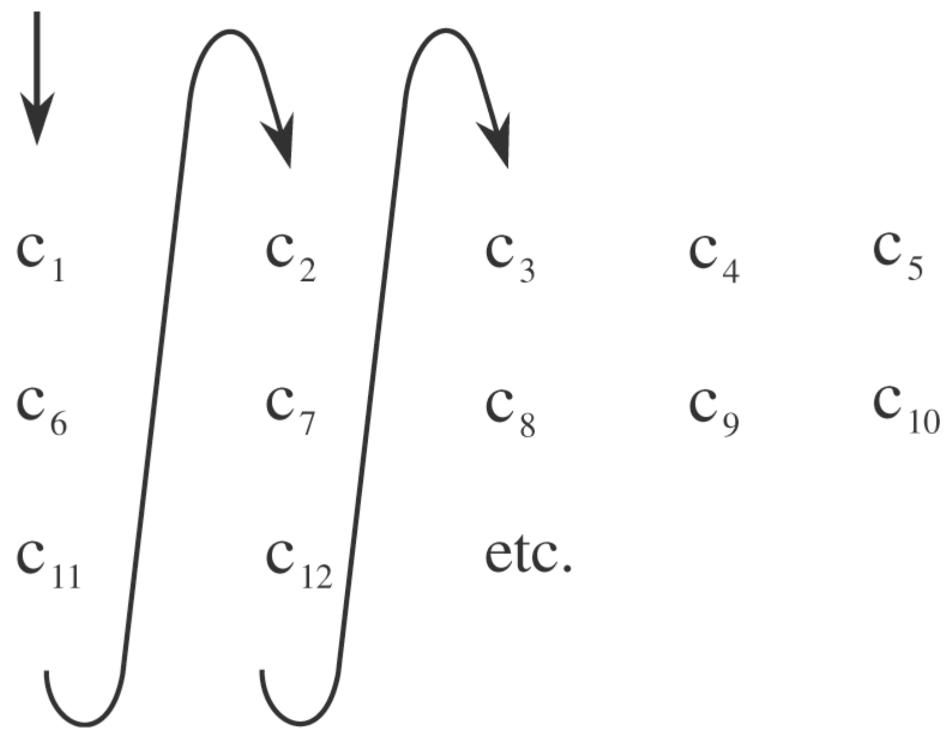
Vernam Cipher

- A type of one-time pad by Vernam.



Transposition/Permutation: Rearrange letters of plaintext

- **Columnar transposition**
- Cannot produce output until having the entire input
  - Why?



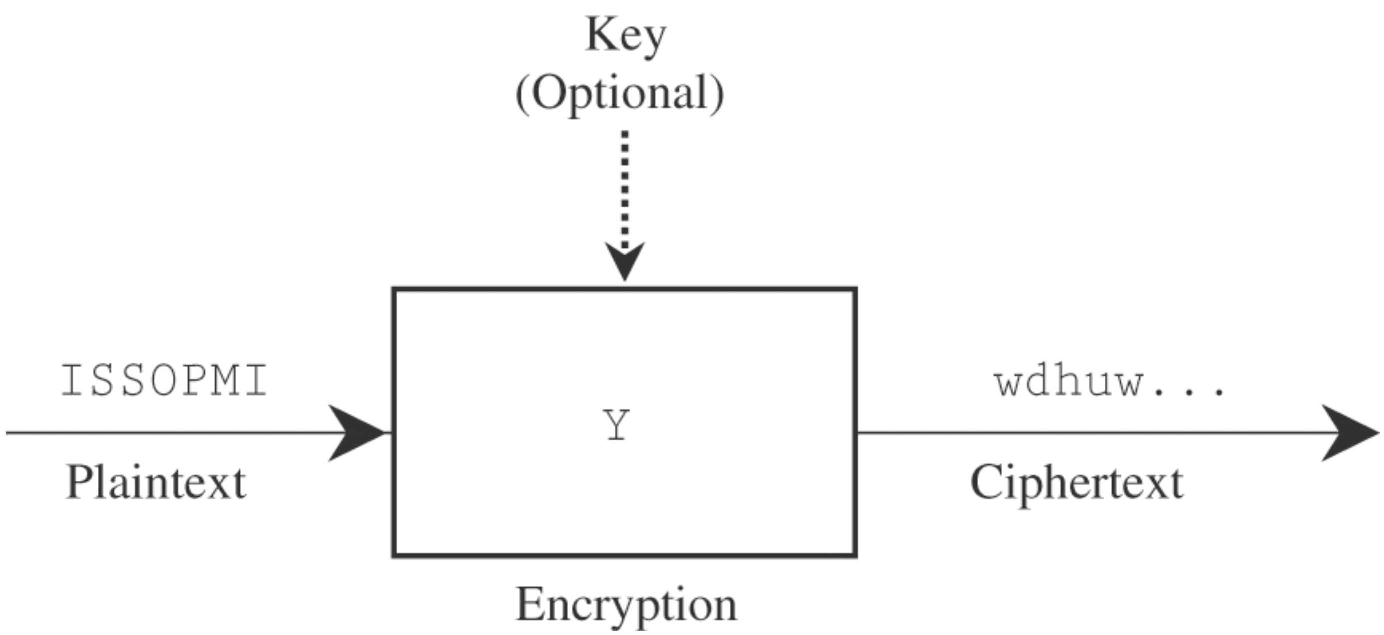
Product Cipher

- Combine multiple ciphers
  - E.g., a substitution cipher and a transposition cipher

- $C=E_2(E_1(P, k_1), k_2)$

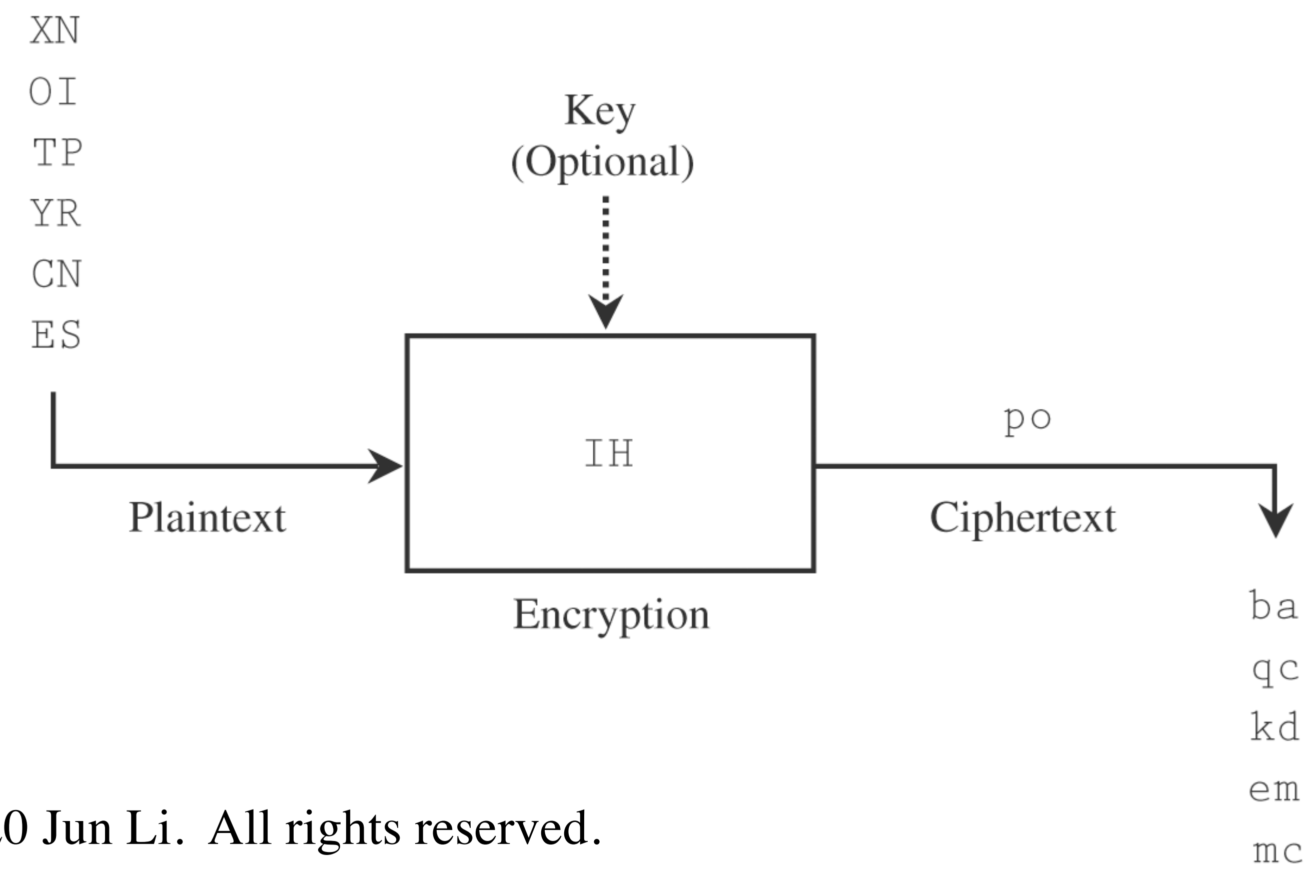
Stream and Block Ciphers

- **Stream Cipher**: Convert one symbol of plaintext *immediately* into a symbol of ciphertext.



Stream and Block Ciphers

- **Block Cipher**: Encrypt a *group* of plaintext symbols as *one block*.



DES, AES, RSA
Encryption Algorithms

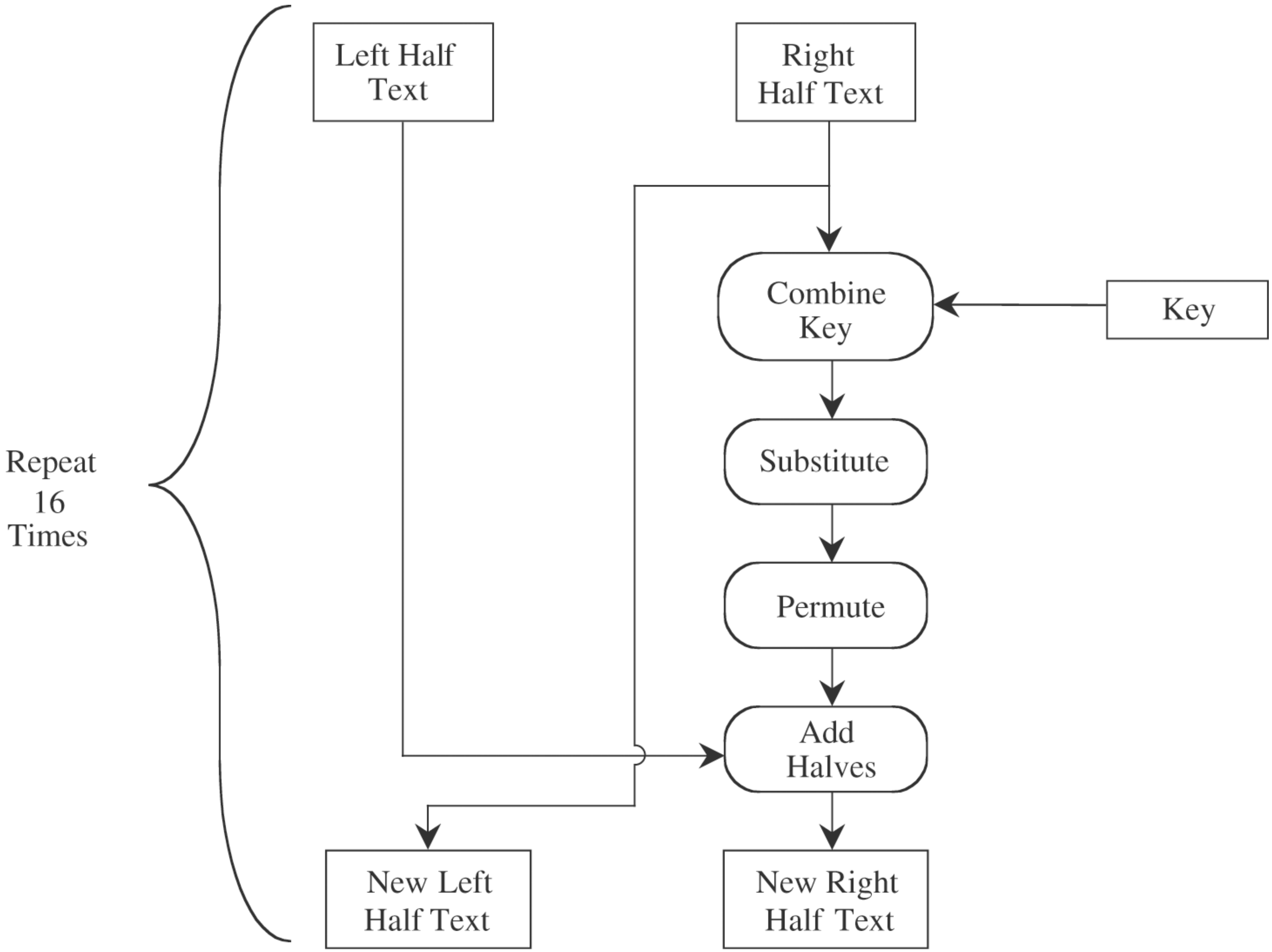
DES Design Criteria

- In 1972, US National Bureau of Standards (NBS) called for proposal and specified criteria
- High-level of security
- Specified and easy to understand
- Publishable
- Available to all users
- Adaptable to diverse applications
- Economical to implement
- Efficient to use
- Able to be validated
- Exportable

Overview of DES

- Repeated application of both substitution and transposition
- Confusion and diffusion
- Block cipher (64 bits)
- Key is 64 bits (incl. 8 bits for checking)
- Only standard arithmetic and logical operations are used
- Implementable in both SW and HW

Operation of DES



Security of DES

- Differential cryptanalysis
  - By Biham and Shmir, 1990
  - Any change of DES algorithm weakens its strength
  - Seems DES design is optimal
- 56-key is too short
  - Diffie and Hellman, 1977, argues 2^56 keys can be tested later
  - 1997, 3,500 machines in 4 months inferred a DES key
  - 1998, “DES cracker” machine, $100,000.

Double and Triple DES

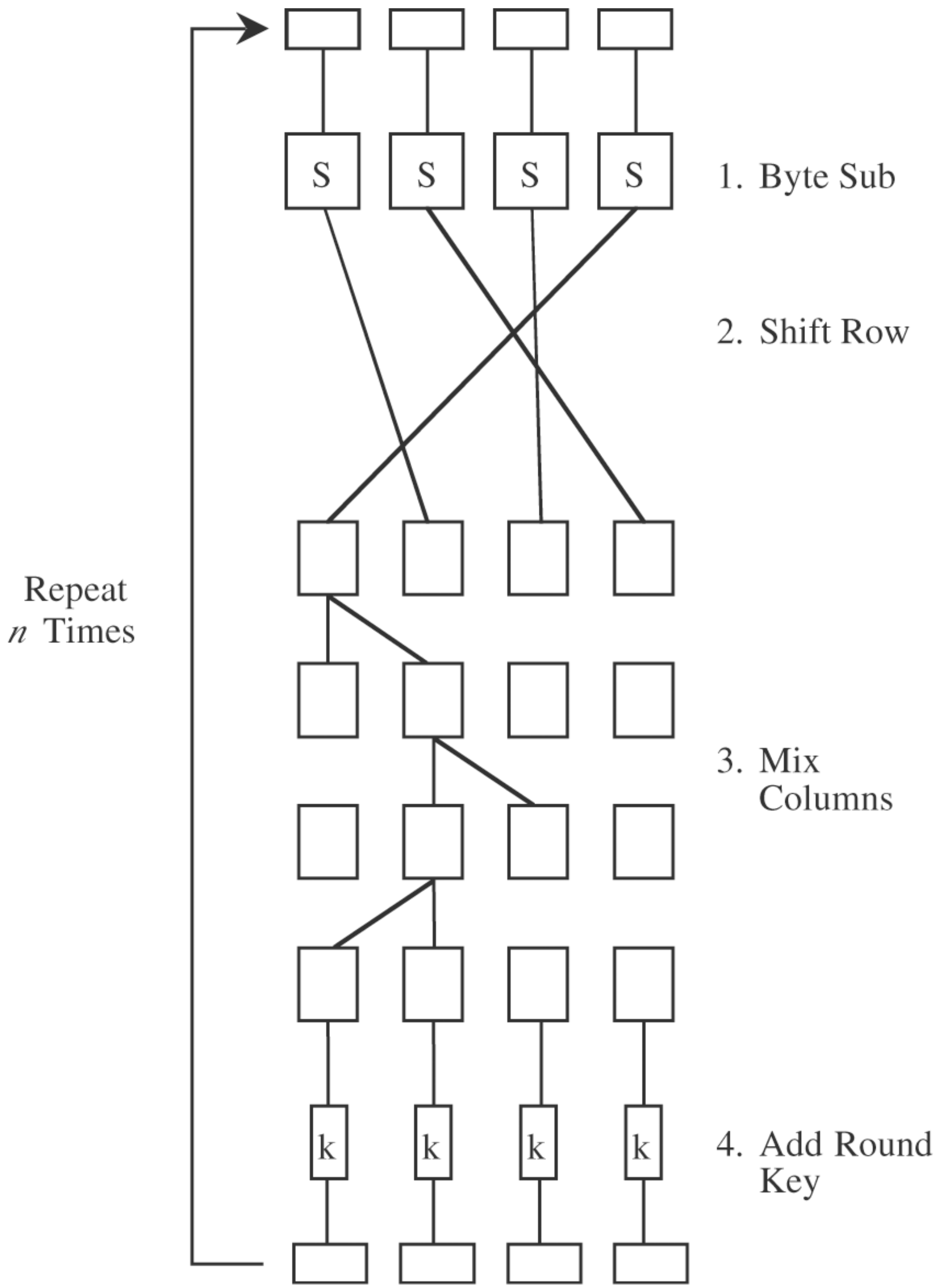
- Double DES: C= $DES(k_2, DES(k_1, m))$
  - Are two locks harder than one?
  - No. [Merkle and Hellman '81]
- Triple DES: C = DES $(k_3, DES(k_2, DES(k_1, m)))$
  - Strength = 112-bit key
- Two-key triple DES: $k_3=k_1$
  - Strength = 80-bit key

AES: Advanced Encryption Standard

- Call for AES 1997:
  - Unclassified
  - Publicly disclosed
  - Royalty-free for use worldwide
  - Symmetric block cipher (block=128 bits)
  - Key size = 128, 192, 256 bits
- One chosen based on algorithm, cost, efficiency, and ease of implementation
  - Rijndael [RINE dahl] by Two Dutch cryptographers

Rijndael

- Operations used:
  - Substitution, transportation, shift, XOR, addition
  - With 10, 12, 14 rounds (cycles) for keys of 128, 192, 256 bits
- Each round:
  - Byte substitution: substitute each byte in the 128-bit block using a substitution box
  - Shift row: transposition. 128-bit block = 4x4 bytes in a matrix. Shift row n left circular (n-1) bytes.
  - Mix column: for each column, multiply every element by a polynomial (done by shift and XOR)
  - Add subkey (derived from the encryption key)


S
S
S
S
1. Byte Sub
2. Shift Row
Repeat
n Times
3. Mix
Columns
k
k
k
k
4. Add Round
Key

RSA: Rivest-Shamir-Adelman Encryption

- 1978
- Based on number theory:
  - The problem of factoring large numbers is not known or believed to be NP-complete
  - The fastest known algorithm is exponential in time
- Encryption: $C = P^e \; mod \; n$
- Decryption: $P = C^d \; mod \; n$
- They are mutual inverses and commutative
  - $P = C^d \; mod \; n = (P^e)^d \; mod \; n \; = (P^d)^e \; mod \; n$
- $D(E(P)) = E(D(P) = P$

Key Choice (n, e, d)

- Encryption key: (e, n)
- Decryption key: (d, n)
- $n = p * q$, where p and q are large prime numbers
  - $n \sim 200$ decimal digits, inhibits factoring n to infer p and q
- e is relatively prime to $(p-1)*(q-1)$
  - E.g., e is a prime larger than both $(p-1)$ and $(q-1)$
- Select d such that $e*d = 1$ mod $(p-1)*(q-1)$

Example

- $p = 5, q = 3, n=15.$ $(p-1)*(q-1)=8$
- Choose $e=11$ and $d=3$.
- $P=2$
- $C=P^e \bmod n = 2^{11} \bmod 15 = 2048 \bmod 15 = 8$
- $P=C^d \bmod n = 8^3 \bmod 15 = 2$