Advanced Network Security

Amir Mahdi Sadeghzadeh, Ph.D.

Outline

- What is network security?
- Principles of cryptography
- Message integrity, authentication
- Securing e-mail
- Securing TCP connections: TLS
- Network layer security: IPsec

What is Security?

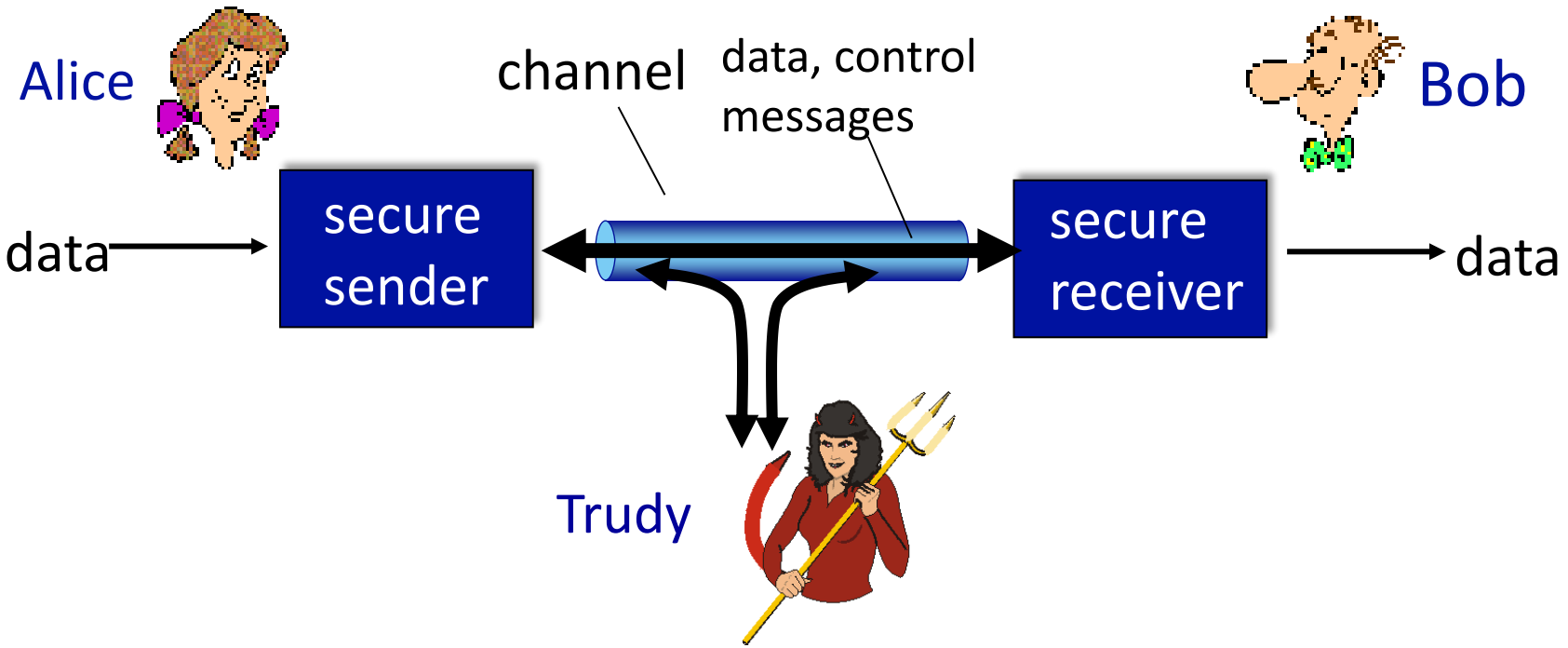
- Confidentiality
- Integrity
- Availability

More Definitions

- Vulnerability (آسیب‌پذیری): An error or weakness in the design, implementation, or operation of a system
- Attack (حمله): A means of exploiting some vulnerability in a system
- Threat (تهدید): An adversary that is motivated and capable of exploiting a vulnerability

Friends and enemies: Alice, Bob, Trudy

- Well-known in network security world
- Bob, Alice (Azam, Babak) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



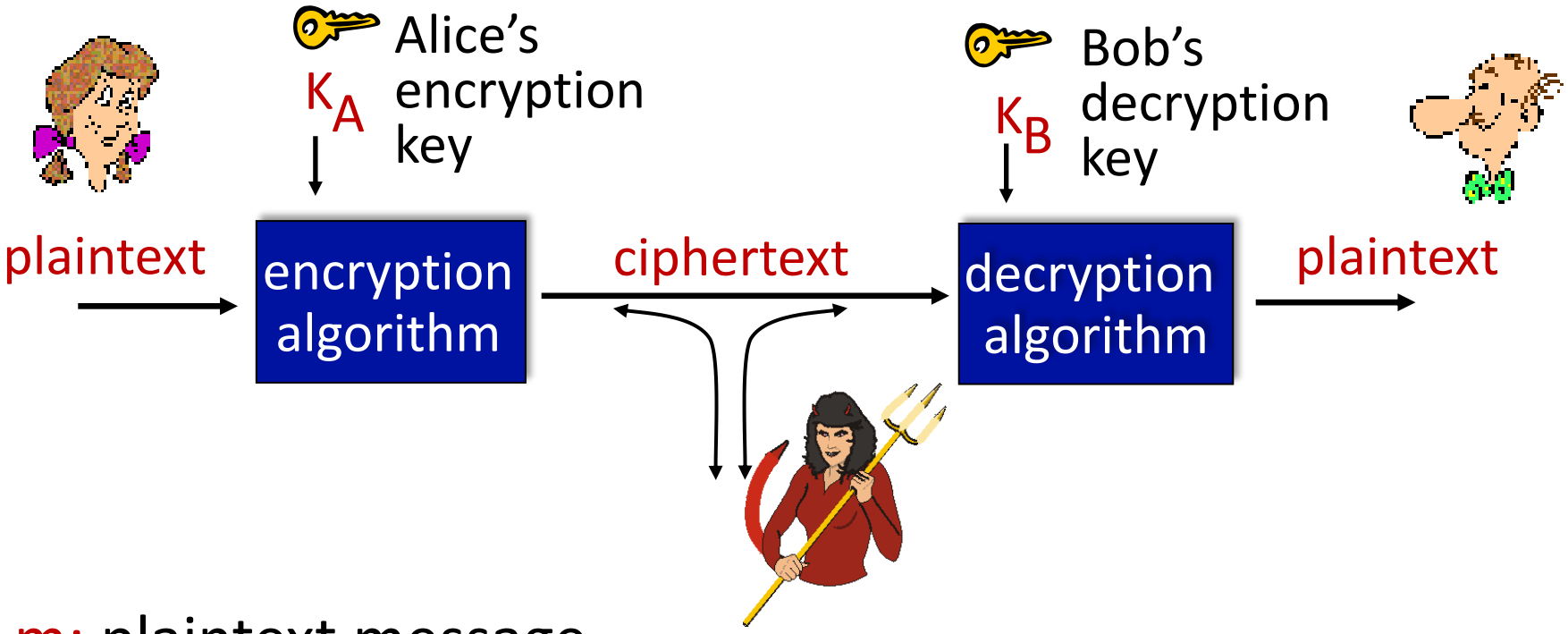
Network Vulnerabilities

- Each layer has it's own vulnerabilities
  - Link layer example: ARP-spoofing
  - Network layer example: IP address forgery
  - TCP example: Sequence number guessing attack
  - Application example: email-borne worms

Outline

- What is network security?
- Principles of cryptography
- Message integrity, authentication
- Securing e-mail
- Securing TCP connections: TLS
- Network layer security: IPsec

The language of cryptography



m: plaintext message

$K_A(m)$: ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

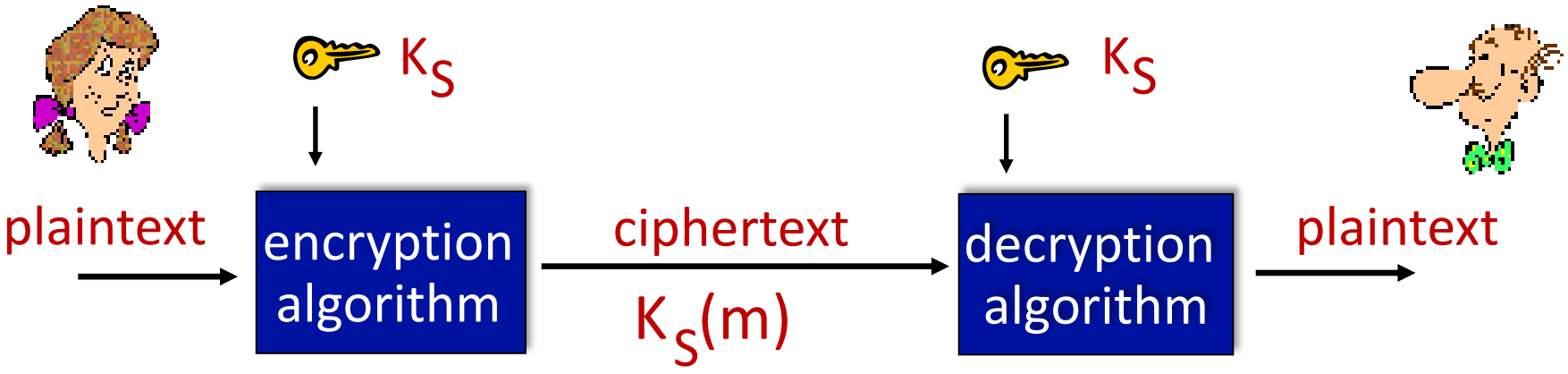
Kerckhoffs's principle

- Auguste Kerckhoffs was a professor in Paris. In early 1883, Kerckhoffs' article, La Cryptographie Militaire states six design rules for military ciphers.
  1. The system must be practically, if not mathematically, indecipherable;
  2. **It should not require secrecy, and it should not be a problem if it falls into enemy hands;**
  3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
  4. It must be applicable to telegraph communications;
  5. It must be portable, and should not require several persons to handle or operate;
  6. Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.

Breaking an encryption scheme

- cipher-text only attack:
  Trudy has ciphertext she can analyze
- known-plaintext attack:
  Trudy has plaintext corresponding to ciphertext
- chosen-plaintext attack:
  Trudy can get ciphertext for chosen plaintext
- two approaches:
  - brute force: search through all keys
  - statistical analysis

Symmetric key cryptography



symmetric key crypto: Bob and Alice share same (symmetric) key: K

- *e.g.,* key is knowing substitution pattern in mono alphabetic substitution cipher

Q: how do Bob and Alice agree on key value?

Simple encryption scheme

substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

e.g.: Plaintext: bob. i hear you. alice

ciphertext: nkn. s acmo wky. mgsbc

Encryption key: mapping from set of 26 letters to set of 26 letters

A more sophisticated encryption approach

- n substitution ciphers, $M_1,M_2,\ldots,M_n$
- cycling pattern:
  - e.g., n=4: M_1,M_3,M_4,M_3,M_2; M_1,M_3,M_4,M_3,M_2; ..
- for each new plaintext symbol, use subsequent substitution pattern in cyclic pattern
  - dog: d from M_1, o from M_3, g from M_4

Encryption key: n substitution ciphers, and cyclic pattern

- key need not be just n-bit pattern

Confusion and Diffusion

- In cryptography, confusion and diffusion are two properties of the operation of a secure cipher
  - identified by Claude Shannon in his 1945 classified report *A Mathematical Theory of Cryptography*.

Confusion

- Confusion refers to making the relationship between the **key** and the **ciphertext** as complex and involved as possible.
  - The property of confusion hides the relationship between the ciphertext and the key.
- How It's Achieved:
  - Non-linearity: Using non-linear mathematical functions to introduce complexity.
  - Substitution: Substituting bits or blocks of data based on the key.
- Example: S-boxes in the Advanced Encryption Standard (AES) provide confusion.

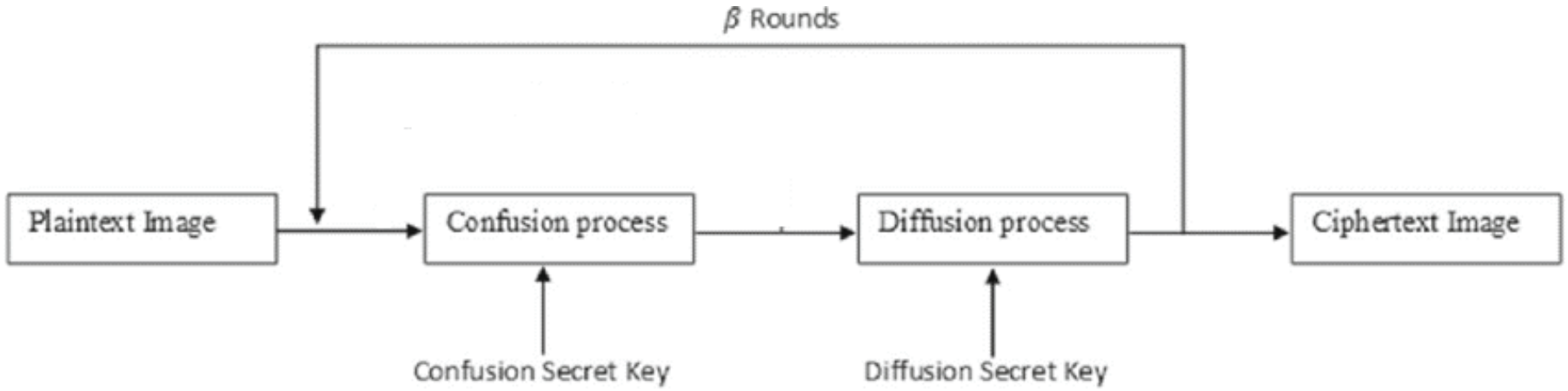
Diffusion

- Diffusion refers to the property that the **redundancy in the statistics** of the plaintext is **dissipated in the statistics of the ciphertext**.
  - In other words, the non-uniformity in the distribution of the individual letters (and pairs of neighbouring letters) in the plaintext should be redistributed into the non-uniformity in the distribution of much larger structures of the ciphertext, which is much harder to detect.
  - In a cipher with good diffusion, if one bit of the plaintext is changed, then the ciphertext should change completely, in an unpredictable or pseudorandom manner.

Diffusion

- How It's Achieved:
  - Permutation: Rearranging bits or blocks of data.
  - Mixing: Applying mathematical operations that mix data.
  - Generally speaking, Linear operation.
- Example: Permutation layers in block ciphers contribute to diffusion.

Encryption Scheme



https://www.researchgate.net/publication/284001953_A_secure_image_encryption_scheme_based_on_chaotic_maps_and_affine_transformation/

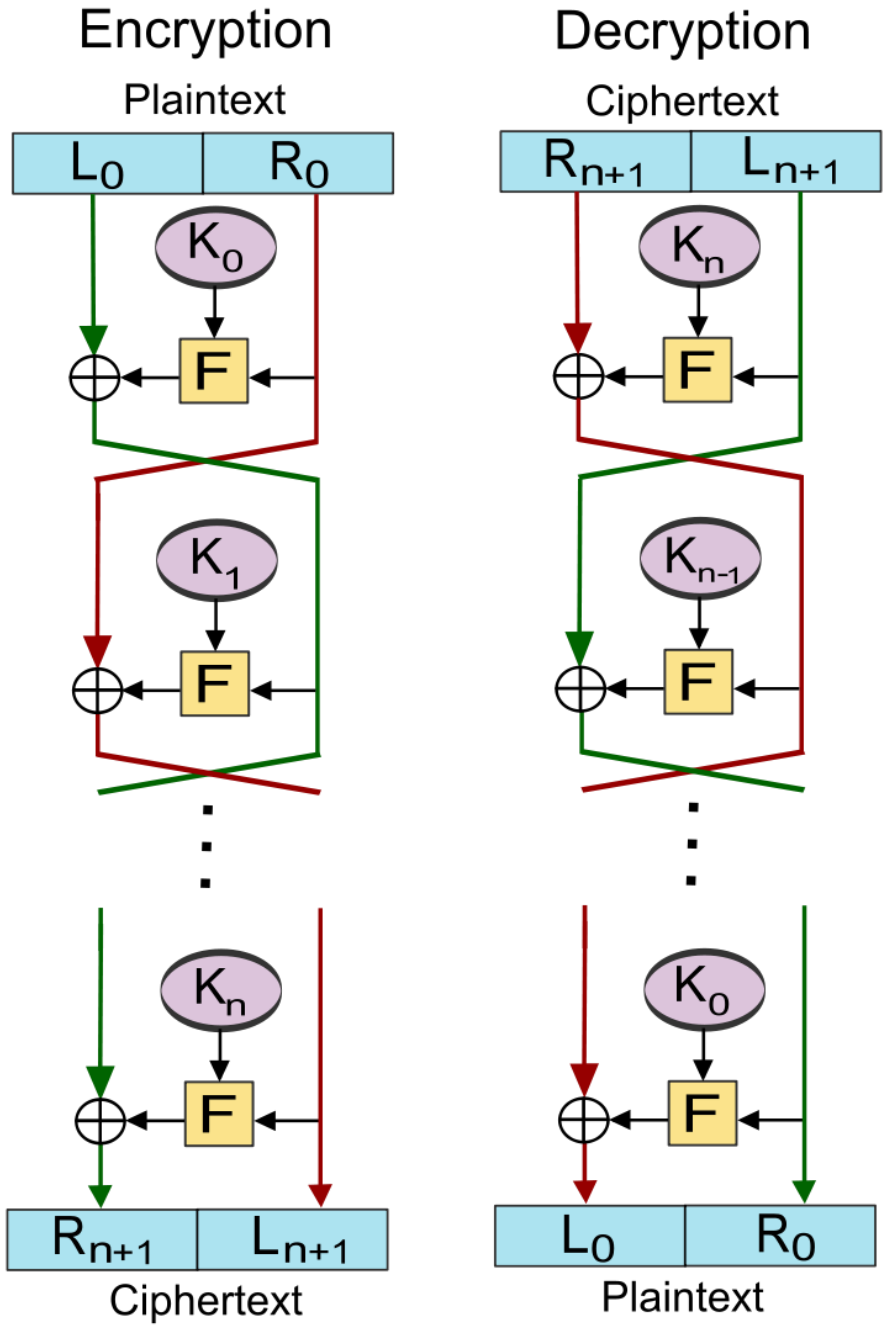
Symmetric key crypto: DES

DES: Data Encryption Standard

- US encryption standard [NIST 1993]
- 56-bit symmetric key, 64-bit plaintext input
- DES has 16 rounds
- how secure is DES?
  - DES Challenge: 56-bit-key-encrypted phrase decrypted (brute force) in less than a day
  - no known good analytic attack
- making DES more secure:
  - 3DES: encrypt 3 times with 3 different keys

Feistel Cipher (DES)

- Feistel Cipher Operations
  - F Function: the right half of the block (R) undergoes a non-linear transformation (F function) using a round-specific subkey.
  - XOR Operation: The output of the F function is XORed with the left half of the block (L).
  - Swap: The left and right halves are swapped, becoming the new L and R for the next round.



Wikipedia

Feistel Function F

The Feistel (F) function [edit]

The F-function, depicted in Figure 2, operates on half a block (32 bits) at a time and consists of four stages:

1. *Expansion*: the 32-bit half-block is expanded to 48 bits using the *expansion permutation*, denoted *E* in the diagram, by duplicating half of the bits. The output consists of eight 6-bit (8 × 6 = 48 bits) pieces, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side.
2. *Key mixing*: the result is combined with a *subkey* using an XOR operation. Sixteen 48-bit subkeys—one for each round—are derived from the main key using the *key schedule* (described below).
3. *Substitution*: after mixing in the subkey, the block is divided into eight 6-bit pieces before processing by the *S-boxes*, or *substitution boxes*. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The S-boxes provide the core of the security of DES—without them, the cipher would be linear, and trivially breakable.
4. *Permutation*: finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the *P-box*. This is designed so that, after permutation, the bits from the output of each S-box in this round are spread across four different S-boxes in the next round.

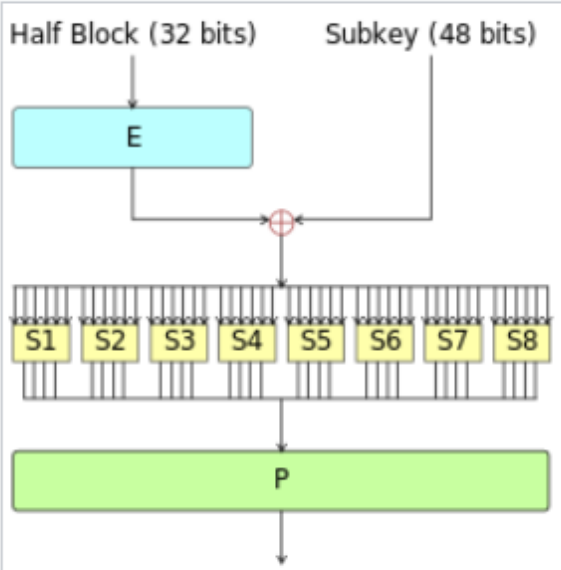


Figure 2—The Feistel function (F-function) of DES

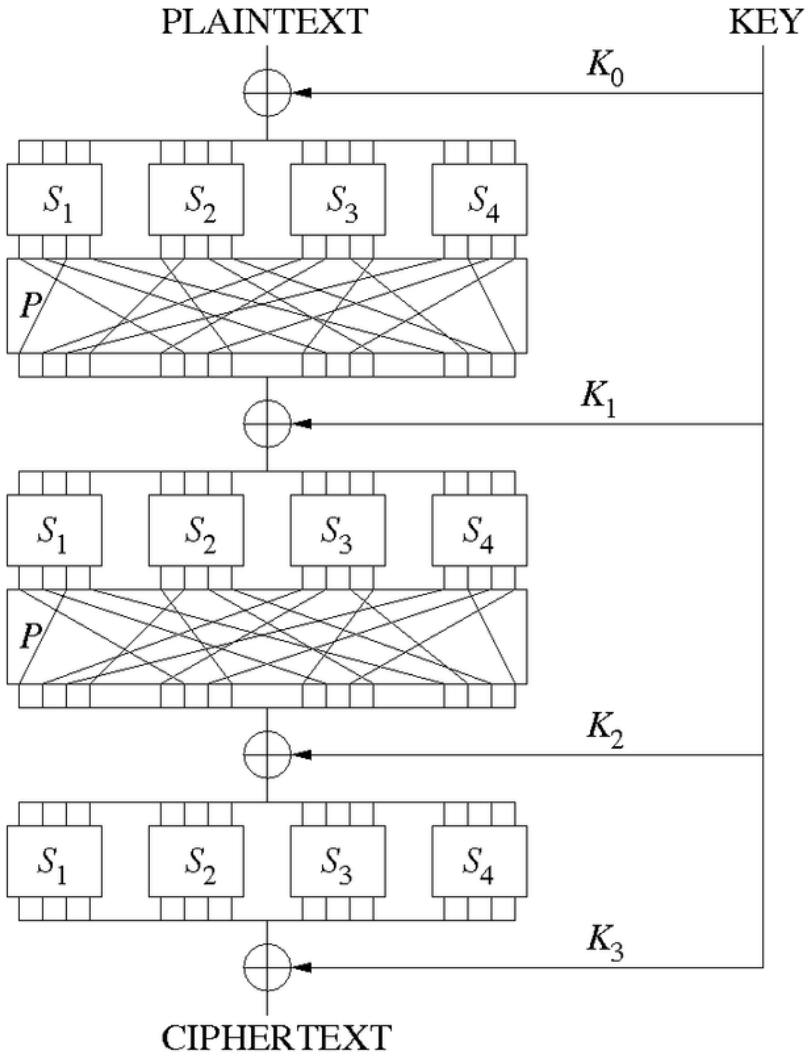
Wikipedia

AES: Advanced Encryption Standard

- symmetric-key NIST standard, replaced DES (Nov 2001)
- processes data in 128 bit blocks
- 128, 192, or 256 bit keys
  - 10 rounds for 128-bit keys.
  - 12 rounds for 192-bit keys.
  - 14 rounds for 256-bit keys.
- brute force decryption taking 1 sec on DES, takes 149 trillion years for AES

Substitution-Permutation Network (AES)

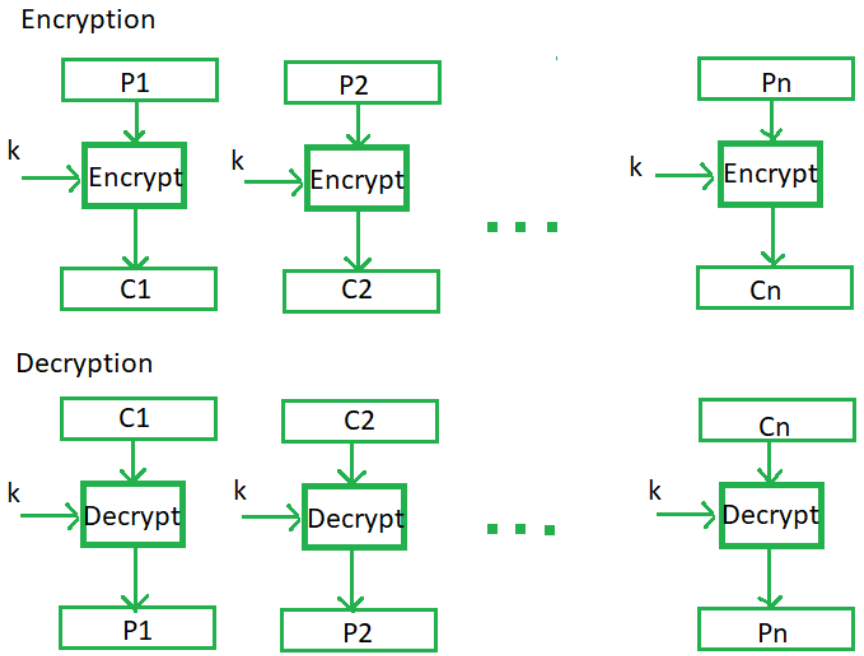
- SPN Cipher Operations
  - Substitution (S-Box): each block undergoes a nonlinear substitution operation, often involving lookup tables (S-boxes).
  - Permutation (P-Box): The permutation layer rearranges the bits within each block, introducing confusion and diffusion.
  - Key Mixing: The key is combined with the block at various points in the structure.



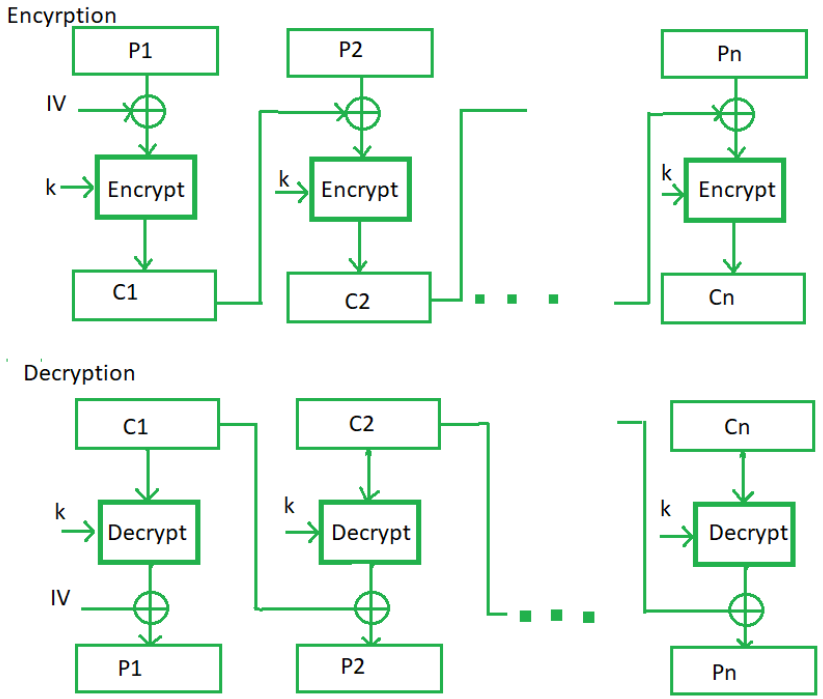
Wikipedia

Block Cipher modes of Operation

- Electronic Code Book (ECB)



- Cipher Block Chaining (CBC)



https://www.geeksforgeeks.org/block-cipher-modes-of-operation/

Public Key Cryptography

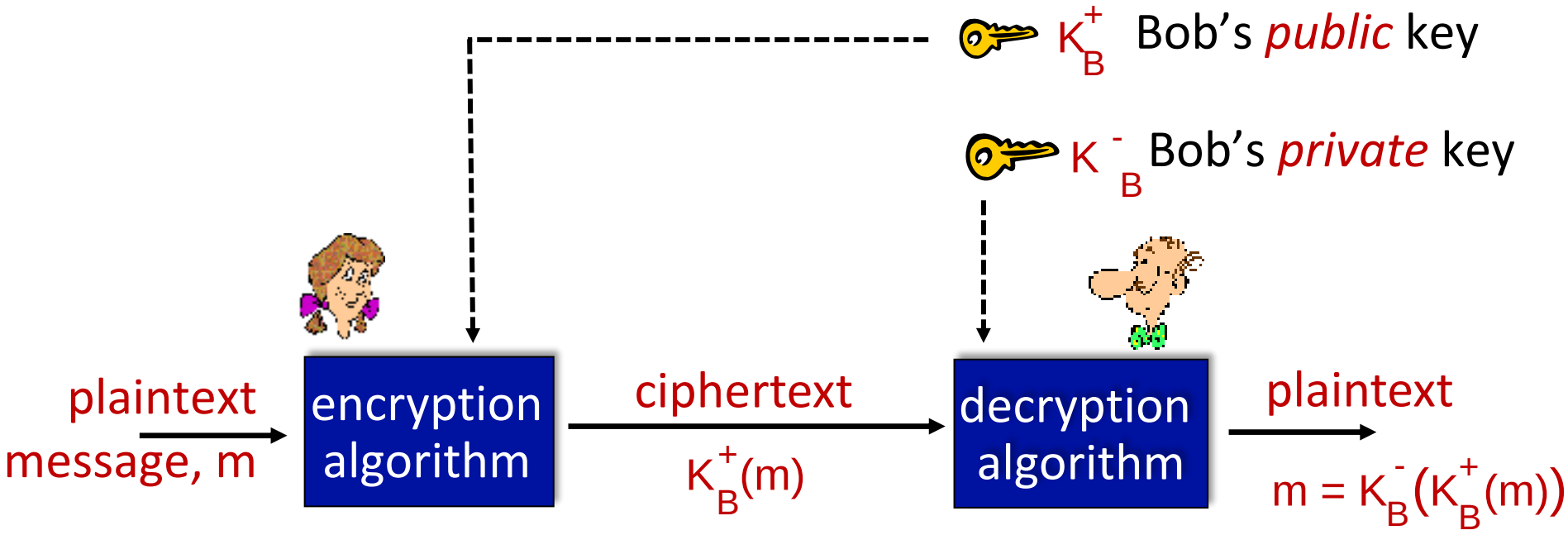
symmetric key crypto:

- requires sender, receiver know shared secret key
- Q: how to agree on key in first place (particularly if never “met”)?
- Message integrity, authentication?

public key crypto

- *radically* different approach [Diffie-Hellman76, RSA78]
- sender, receiver do *not* share secret key
- *public* encryption key known to *all*
- *private* decryption key known only to receiver

Public Key Cryptography



Public key cryptography revolutionized 2000-year-old (previously only symmetric key) cryptography!

- similar ideas emerged at roughly same time, independently in US and UK (classified)

Public key encryption algorithms

requirements:

1. need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that

$$K_B^-(K_B^+(m)) = m$$

2. given public key K_B^+, it should be impossible to compute private key K_B^-

RSA: Rivest, Shamir, Adelson algorithm

One-Way Functions for Public-Key Cryptography

- One-way Function
  - One-way functions are easy to compute but it is very difficult to compute their inverse functions.
    - Thus, having data x it is easy to calculate f(x) but, on the other hand, knowing the value of f(x) it is quite difficult to calculate the value of x.
  - Modular exponentiation is a common example of a one-way function in RSA cryptography.
    - Computing $c = m^e \ mod \ n$ is easy, but finding m given c, e, and n is computationally difficult.

One-Way Functions for Public-Key Cryptography

- Trapdoor one-way function
  - Trapdoor one-way functions are types of one-way functions that contain a kind of "back door" (trapdoor).
    - As in the case of ordinary one-way functions it is easy to compute their values for given data but it is very difficult to compute their inverse functions.
      - However, if one has some **additional secret information**, he can easily compute the inverse function as well.
      - Example: in RSA, d is the trapdoor.

Euler's phi function

- Euler's phi function $\phi(n)$ counts the positive integers up to a given integer n that are relatively prime to n.
  - In other words, it is the number of integers k in the range 1 ≤ k ≤ n for which the greatest common divisor gcd(n, k) is equal to 1.

$$\varphi(n) = p_1^{k_1-1}(p_1-1)\,p_2^{k_2-1}(p_2-1)\cdots p_r^{k_r-1}(p_r-1),$$

where $n = p_1^{k_1}\,p_2^{k_2}\cdots p_r^{k_r}$ is the prime factorization of n (that is, $p_1, p_2, \ldots, p_r$ are distinct prime numbers).

Wikipedia

Euler’s theorem

- Fermat's little theorem
  - For any prime number p, and for any number n, 0 < n < p,

  $n^{p-1} \equiv 1 \bmod p$.

- Euler’s theorem generalizes Fermat’s theorem to the case where the modulus is not prime.
  - if p is a positive integer and n, p are coprime (n <p), then $n^{\phi(p)} \equiv 1 \bmod p$ where ϕ(p) is the Euler's phi function .

  - $5^{\phi(12)} mod\ 12 = 5^4\ mod\ 12 = 625\ mod\ 12 = 1$

Prerequisite: modular arithmetic

- x mod n = remainder of x when divide by n
- facts:

  $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$
  $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$
  $[(a \bmod n) * (b \bmod n)] \bmod n = (a*b) \bmod n$
- thus

  $(a \bmod n)^d \bmod n = a^d \bmod n$
- example: x=14, n=10, d=2:

  $(x \bmod n)^d \bmod n = 4^2 \bmod 10 = 6$

  $x^d = 14^2 = 196 \quad x^d \bmod 10 = 6$

RSA: getting ready

- message: just a bit pattern
- bit pattern can be uniquely represented by an integer number
- thus, encrypting a message is equivalent to encrypting a number

example:

- m= 10010001. This message is uniquely represented by the decimal number 145.
- to encrypt m, we encrypt the corresponding number, which gives a new number (the ciphertext).

RSA: Creating public/private key pair

1. choose two large prime numbers *p, q.* (e.g., 1024 bits each)

2. compute *n = pq,* $\phi(n) =$ *z = (p-1)(q-1)*

3. choose *e (*with *e<z)* that has no common factors with z (*e, z* are "relatively prime"). The number e is usually 65537 (0x010001).

4. choose *d* such that *ed-1* is exactly divisible by *z*. (in other words: *ed* mod *z = 1*).

5. *public* key is *(n,e).* *private* key is *(n,d).*

K_B^+ K_B^-

RSA: encryption, decryption

0. given (n,e) and (n,d) as computed above

1. to encrypt message m ($<n$), compute
   $c = m^e \bmod n$

2. to decrypt received bit pattern, c, compute
   $m = c^d \bmod n$

$$m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$$

Why does RSA work?

- must show that $c^d \bmod n = m$, where $c = m^e \bmod n$
- thus,

$c^d \bmod n = (m^e \bmod n)^d \bmod n$

$= m^{ed} \bmod n$

$= m^{az+1} \bmod n$

$= m^{az} \,.\, m^1 \bmod n$

$= (m^{az} \bmod n.\ m \bmod n) \bmod n$

$= ((m^z)^a \bmod n.\ m) \bmod n$

$= ((m^z \bmod n)^a \bmod n.\ m) \bmod n$ #Euler's theorem

$= (1^a \bmod n.\ m) \bmod n = 1.m \bmod n = m$

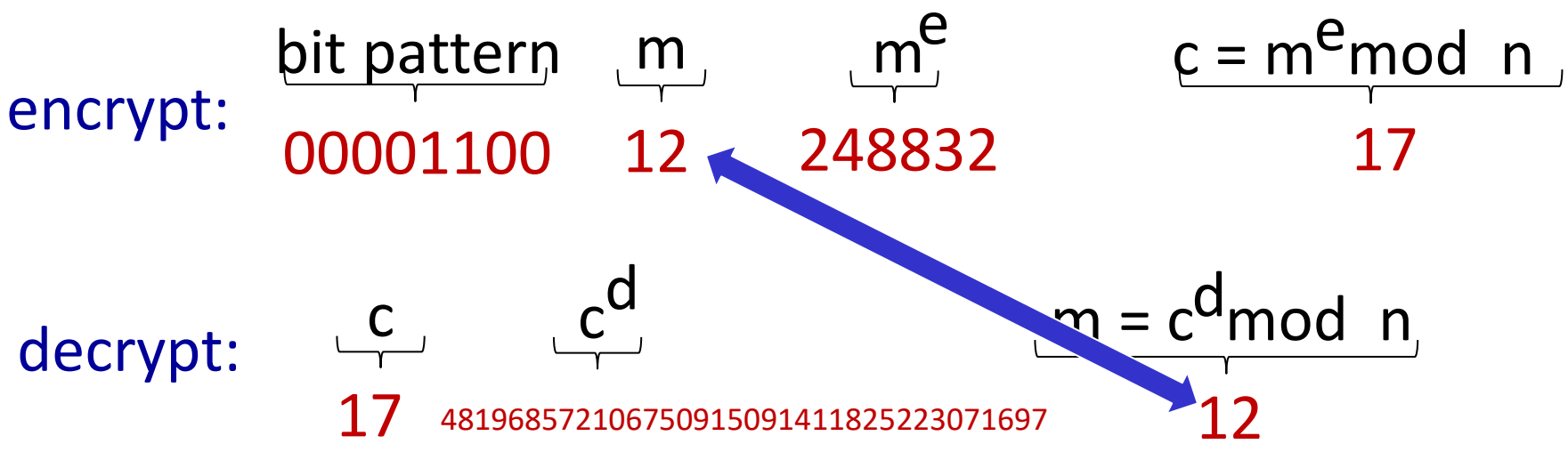
RSA example:

Bob chooses *p=5, q=7*. Then *n=35, z=24*.

e=5 (so *e, z* relatively prime).

d=29 (so *ed-1* exactly divisible by z).

encrypting 8-bit messages.



RSA: another important property

The following property will be *very* useful later:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{use public key first, followed by private key}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{use private key first, followed by public key}}$$

result is the same!

Why $K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$?

follows directly from modular arithmetic:

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$
$$= m^{de} \bmod n$$
$$= (m^d \bmod n)^e \bmod n$$

Why is RSA secure?

- suppose you know Bob's public key (n,e). How hard is it to determine d?
- essentially need to find factors of n without knowing the two factors p and q
  - fact: factoring a big number is hard

Prime-counting function

- The prime-counting function $\pi(x)$ is the function counting the number of prime numbers less than or equal to some real number x.
  - It was conjectured in the end of the 18th century by Gauss and by Legendre to be approximately

$$\pi(x) \approx \frac{x}{\ln x}$$

Input

$$\frac{2^{1024}}{\log(2^{1024})}$$

Decimal approximation

$$2.532737276080075837450112514401885703366568528844967434378 8\ldots \times 10^{305}$$

Input

$$2^{128}$$

Result

340 282 366 920 938 463 463 374 607 431 768 211 456

Scientific notation

$$3.40282366920938463463374607431768211456 \times 10^{38}$$

RSA in practice: session keys

- exponentiation in RSA is computationally intensive
- DES is at least 100 times faster than RSA
- use public key crypto to establish secure connection, then establish second key – symmetric session key – for encrypting data

session key, K_S

- Bob and Alice use RSA to exchange a symmetric session key K_S
- once both have K_S, they use symmetric key cryptography

References

- Kurose, James F., and Keith W. Ross. "Computer networking: A top-down approach edition." Addision Wesley (2007), chapter 8.
- Paar, Christof, and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.
- ChatGPT, OpenAI.