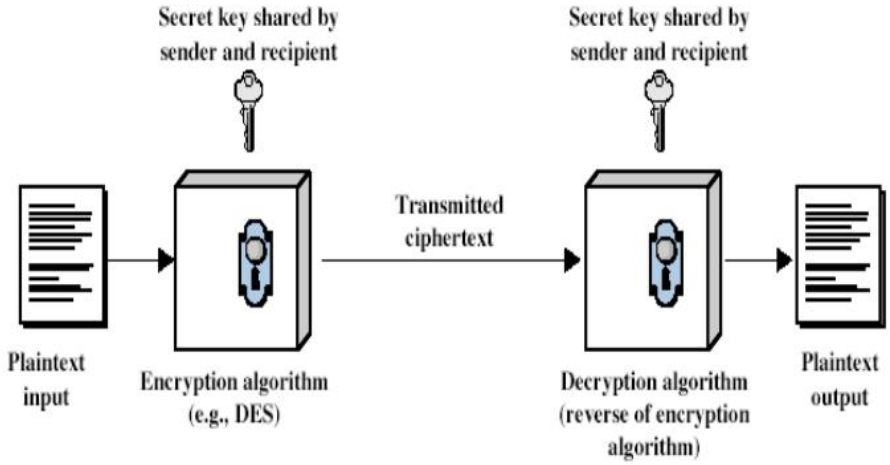
Chapter 1

Encryption or cryptography the name means secret writing.

Terminologies

- **Plaintext**
  the original message.
- **Ciphertext**
  the coded message.
- **Cipher**
  algorithm for transforming plaintext to ciphertext.
- **Key**
  info used in cipher known only to sender/receiver.
- **Encipher (Encrypt)**
  converting plaintext to ciphertext.
- **Decipher (Decrypt)**
  recovering ciphertext from plaintext.
- **Cryptography**
  study of encryption principles/methods.
- **Cryptanalysis (Codebreaking)**
  the study of principles/ methods of deciphering ciphertext without knowing key.
- **Cryptology**
  the field of both cryptography and cryptanalysis.

Symmetric Cipher Model

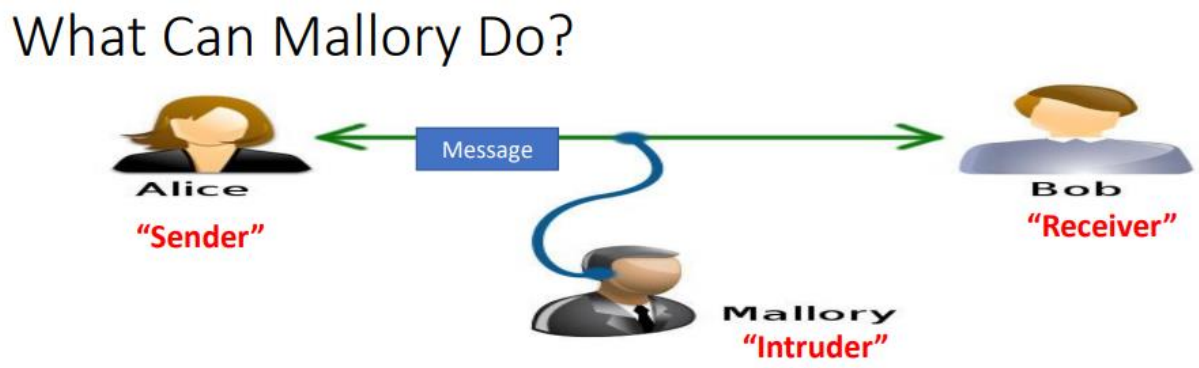


Requirements of symmetric encryption

- a strong encryption algorithm.
- a secret key known only to sender / receiver. $Y = E_K(X)$ $X = D_K(Y)$
- Assume the encryption algorithm is known.
- Implies a secure channel to distribute key.

Classification of Cryptography

1. **Number of keys used.**
   - Hash functions: no key
   - Secret key cryptography: one key (Symmetric encryption)
   - Public key cryptography: two keys - public, private (Asymmetric encryption)
2. **Type of encryption operations used.**
   - substitution
   - transposition
   - product
3. **Way in which plaintext is processed.**
   - block
   - stream



***Block* it**, by preventing its reaching Bob, thereby affecting the **availability** of the message

• ***Intercept* it**, by reading or listening to the message, thereby affecting the **confidentiality** of the message

• ***Modify* it**, by seizing the message and changing it in some way, affecting the message's **integrity**

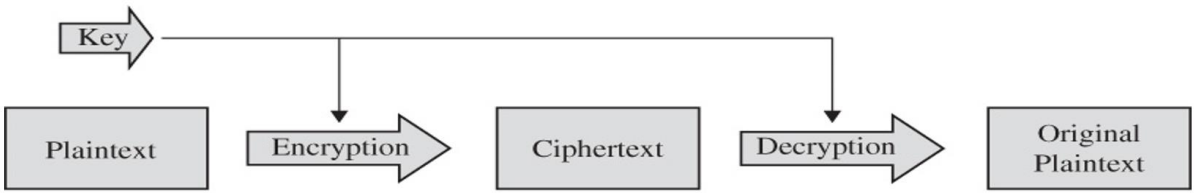
• ***Fabricate*** an authentic-looking message, arranging for it to be delivered as if it came from *Alice*, thereby also affecting the **integrity** of the message

Security Properties

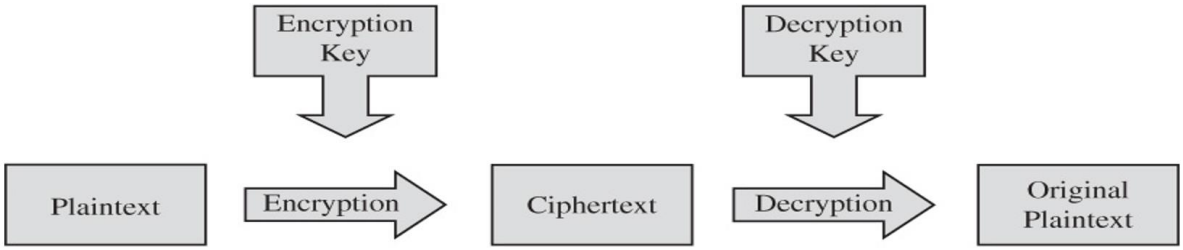
- **Availability**
  the ability of a system to ensure that an asset can be used by any authorized parties.
- **Integrity**
  the ability of a system to ensure that an asset is modified only by authorized parties.
- **Confidentiality**
  the ability of a system to ensure that an asset is viewed only by authorized parties.

Types of Encryption Keys

1. **Symmetric encryption**: one key encrypts and decrypts.
   Private/secret/single key cryptography



2. **Asymmetric encryption**: one key encrypts, a different key decrypts.
   Public Key cryptography



Cryptanalysis Attack

Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the Plaintext or even some symbol plaintext--ciphertext pairs.

Note// This type of attack exploits the characteristics of algorithm to attempt to deduce a specific plaintext or deduce the key being used.

Brute-Force Attack

The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plain text is obtained.

Note//On average half of all possible keys must be tried to achieve success.

Cryptographic Primitives

Cryptography involves two basic techniques: **substitution (replacing)** and **transposition (shuffling).**

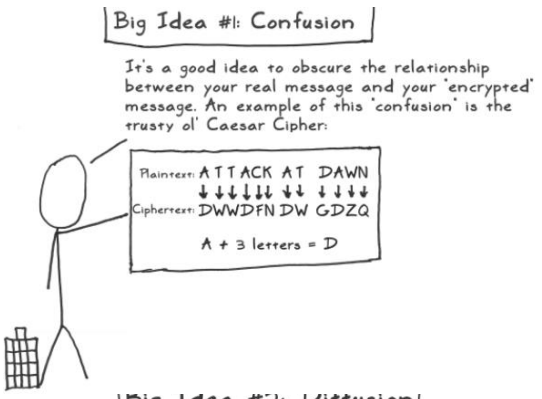
1. **Substitution**
   one set of bits is exchanged for another.
   If the encryption works on alphabetic letters, each letter can be replaced by another.
2. **Transposition**
   involves rearranging the order of the ciphertext to break any repeating patterns in the underlying plaintext.

Note// Many cryptographic algorithms involve both substitution and transposition.

Confusion

refers to making the relationship between the ciphertext and the key as complex as possible.

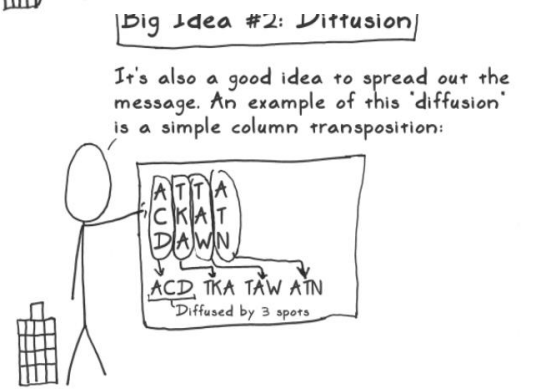
Substitution achieves **confusion**.



Diffusion

refers to dissipating the statistical structure of plaintext over the bulk of ciphertext.

Transposition achieves **diffusion**.



Caesar Cipher (Substitution)

Each letter is translated to the letter a fixed number of places after it in the alphabet.

Earliest known substitution cipher by Julius Caesar

Note// Caesar used a shift of 3.

- Mathematically each letter is given a number:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Then have Caesar cipher as:
  $c = E(k, p) = (p + k) \bmod (26)$
  $p = D(k, c) = (c - k) \bmod (26)$

Example:

Plaintext: meet me after the toga party

Cyphertext: PHHW PH DIWHU WKH WRJD SDUWB

Hill Cipher (Substitution)

The Hill cipher is a polygraphic substitution cipher where a group of plaintext letters is converted into a group of ciphertext letters.

Hill used matrices and matrix multiplication to mix up the plaintext.

Invented by Lester S. Hill in 1929, the Hill cipher is a polygraphic **substitution** cipher based on **linear algebra.**

The analysis of this algorithm requires a branch of mathematics known as **number theory**

size of the key matrix is (n × n), where n is number of plaintext letters in a group.

- Example:
  - Plaintext = JULY ➔ group into 2 letters ➔ JU & LY
  - Key matrix will be 2 x 2 = $\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$
- The plaintext letters a–z are assigned with decimal values from the range of 0–25.

A	B	C	.	.	Y	Z
0	1	2	.	.	24	25

Hill Cipher: Encryption and Decryption

C = **p** x **K** mod 26

C: represents a group of ciphertext letters

p: represents a group of plaintext letters

K: is a key matrix

Example:

Encryption

P = JULY

J = 9 , U = 20, L = 11, Y = 24.

K = $\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$ used for encryption

$$(9, 20) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99 + 60, 72 + 140) = (3, 4)$$

$$(11, 24) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (121 + 72, 88 + 168) = (11, 22).$$

C = DELW

Decryption

C = DELW

D = 3, E = 4, L = 11, W = 22.

K^{-1} = $\begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$ used for decryption

$$(3, 4) \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (9, 20)$$

$$(11, 22) \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (11, 24).$$

P = JULY

Note// Hill Cipher could be easily broken using cryptanalysis techniques

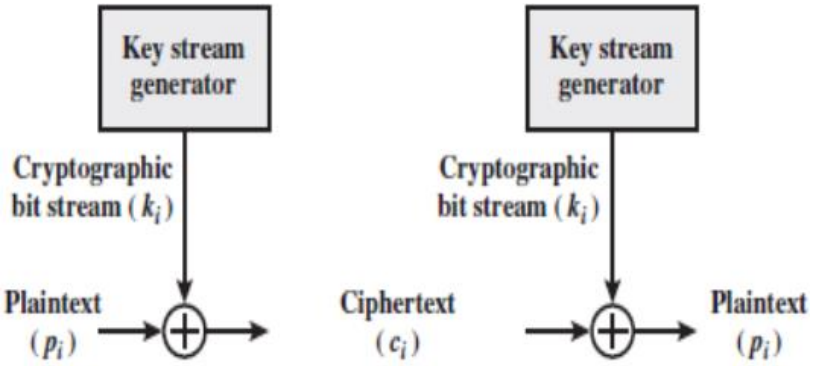
Vernam Cipher (Substitution)

we take a key to encrypt the plain text whose length should be **equal** to the length of the plain text.

P length = K length

Vernam Cipher was invented by an AT&T engineer Gilbert Vernam in 1918

Originally proposed using a very long but eventually repeating key



One-Time Pad (Substitution)

a system in which a randomly generated private key is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key.

truly random key as long as the message is used.
It is **unbreakable** since ciphertext bears no statistical relationship to the plaintext
Can only use the key **once**

- Suppose Alice wishes to send the message "HELLO" to Bob.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption					
Message->	H	E	L	L	O
	7	4	11	11	14
KEY->	X	M	C	K	L
	23	12	2	10	11
	30	16	13	21	25
	4(30-26)	16	13	21	25
CIPHERTEXT	E	Q	N	V	Z

Decryption					
CIPHERTEXT	E	Q	N	V	Z
	4	16	13	21	25
KEY->	X	M	C	K	L
	23	12	2	10	11
SUBTRACTION	-19	4	11	11	14
	-19+26=7	4	11	11	14
PLAINTEXTEXT	H	E	L	L	O

Columnar Transpositions

is a rearrangement of the characters of the plaintext into columns.

- **Plaintext** = written in rows of **n columns** and arranged in one row after another

C_1 C_2 C_3 C_4 C_5
C_6 C_7 C_8 C_9 C_{10}
C_{11} C_{12} C_{13} C_{14} C_{15}

- **Ciphertext** = read the columns one by one

$= C_1C_6C_{11}C_2C_7C_{12}C_3C_8C_{13}C_4C_9C_{14}C_5C_{10}C_{15}$

Transposition Techniques

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key to the algorithm. For example,

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Steganography

is the technique of hiding secret data within a non-secret file or message in order to avoid detection.

Various techniques used are:

1. **Character Marking**: Selected letters are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
2. **Invisible Ink**: A number of substances can be used for writing but secure trace until some other chemical is applied to the paper.
3. **Pin Punctures**: Small pin punctures on the pictures are ordinarily not visible unless the paper is held up in front of a light.
4. **Typewriter correction ribbon**: Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Shannon's Characteristics of "Good" Ciphers

1. The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
2. The set of keys and the enciphering algorithm should be free from complexity.
3. The implementation of the process should be as simple as possible.
4. Errors in ciphering should not propagate and cause corruption of further information in the message.
5. The size of the enciphered text should be no larger than the text of the original message.

Properties of "Trustworthy" Encryption Systems

1. It is based on sound mathematics. Good cryptographic algorithms are not just invented; they are derived from solid principles.
2. It has been analyzed by competent experts and found to be sound.
3. It has stood the "test of time."

Chapter 2

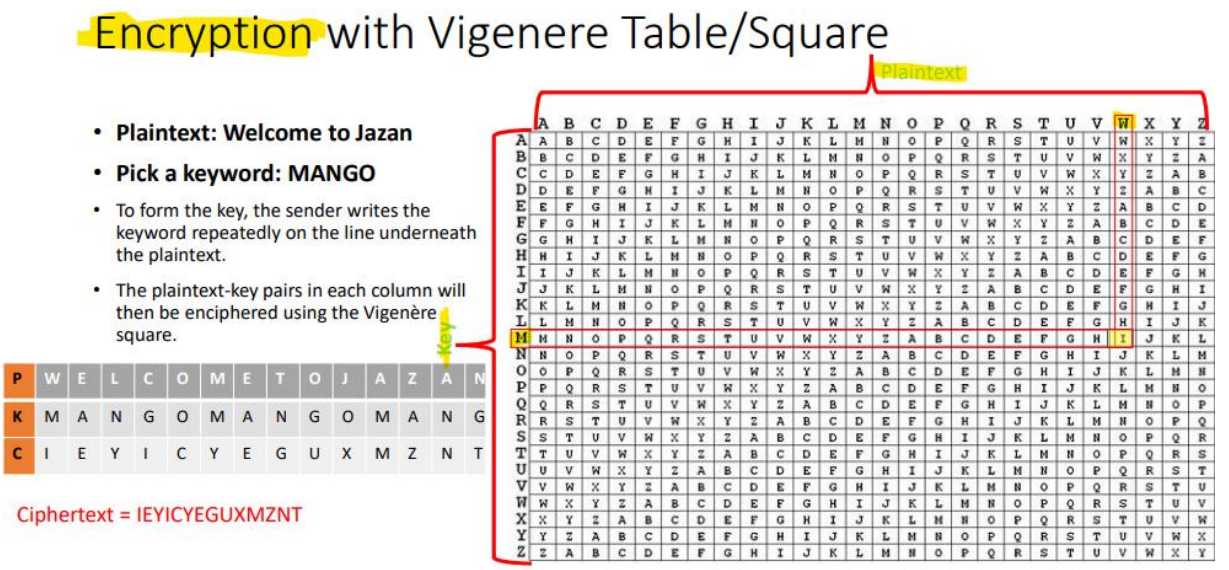
Vigenère Cipher

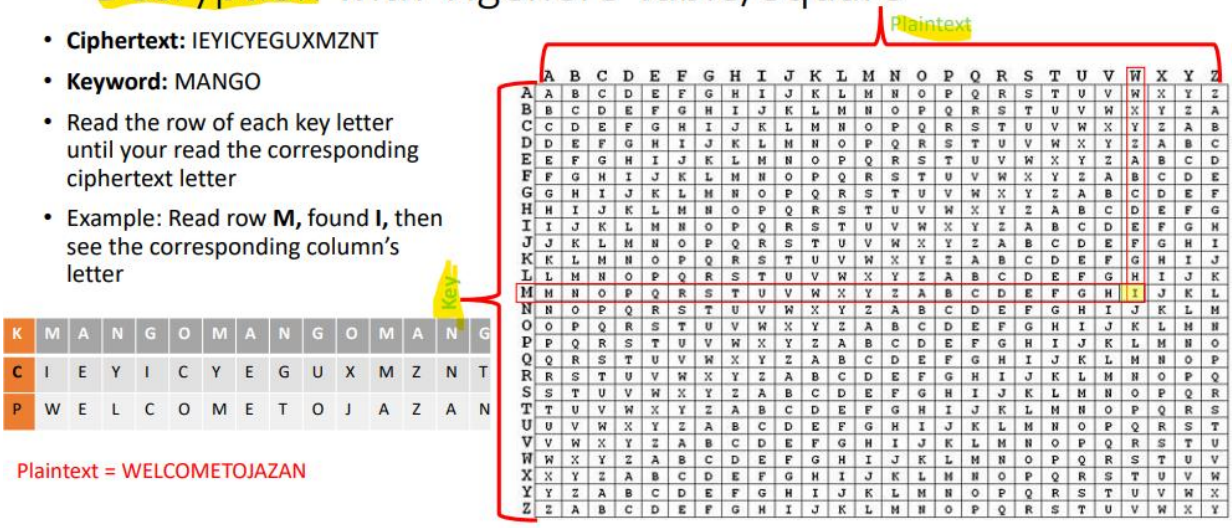
a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword.

The Vigenère cipher is an example of a **polyalphabetic substitution cipher**.

Blaise de Vigenère developed what is now called the Vigenère cipher in 1585.

Note// A **polyalphabetic substitution** cipher is similar to a **monoalphabetic substitution** except that the cipher alphabet is changed periodically while enciphering the message.





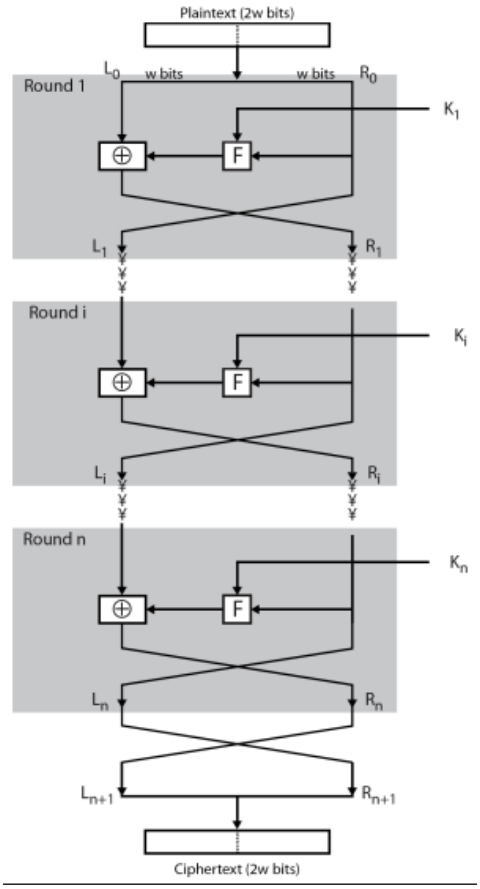
Feistel Cipher Structure

Feistel cipher implements Shannon's S-P network concept.

based on invertible product cipher

Process through multiple rounds which

- partitions input block into two halves.
- perform a substitution on left data half.
- based on round function of right half & subkey.
- then have permutation swapping halves.



Data Encryption Standard (DES)

DES is a careful and complex combination of two fundamental building blocks of encryption: **substitution** and **transposition**.

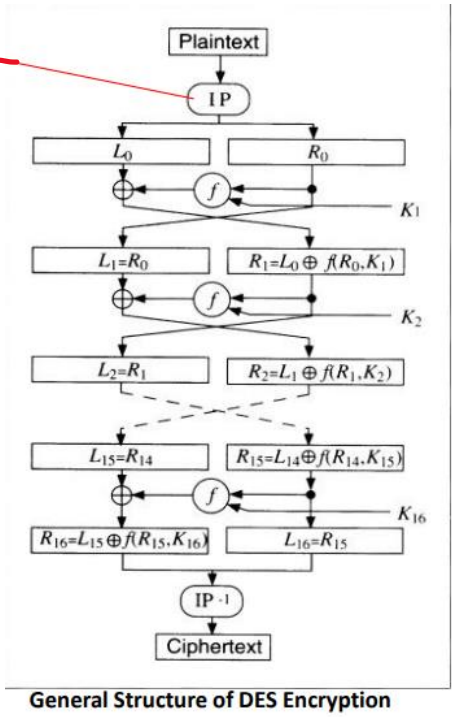
Note// The key is **64-bit** key 8 × 8 including **1 bit for parity**, so the actual key **56-bit.**

Note// The algorithm derives its strength from repeated application of these two techniques, one on top of the other, for a total of **16 rounds**.

Note// The DES algorithm was developed in the 1970s by IBM for the U.S. National Institute of Standards and Technology (NIST)

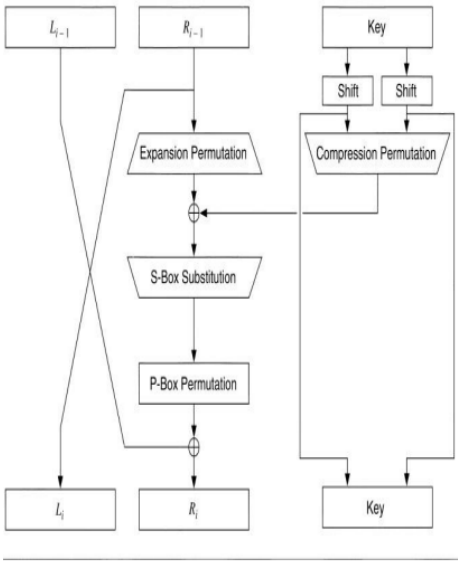
DES Algorithm

- DES operates on a **64-bit block of plaintext**.
- After an **initial permutation (IP)**, the block is broken into a right half and a left half, each 32 bits long.
- Then there are 16 rounds of identical operations, called Function f, in which the data are combined with the key.
- After the sixteenth round, the right and left halves are joined, and a final permutation (the inverse of the initial permutation) finishes off the algorithm.



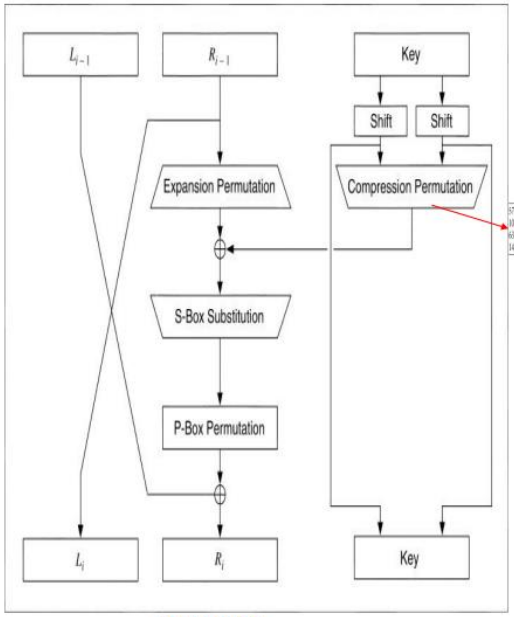
General Structure of DES Encryption

DES Round

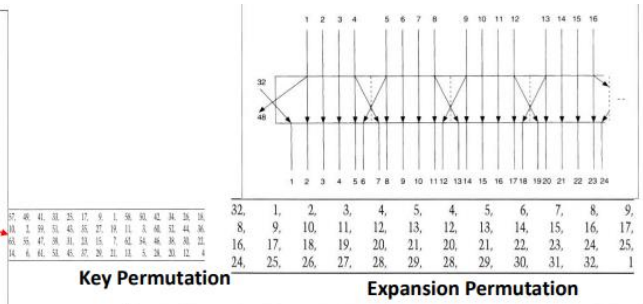


One Round of DES

- In each round, the key bits are shifted, and then 48 bits are selected from the 56 bits of the key.
- The right half of the data is expanded to 48 bits by an expansion permutation.
- It is then combined with 48 bits of a shifted and permuted key via an XOR.
- Then it's sent through **8 S-boxes** to produce 32 new bits.
- The bits are permuted again.
- These four operations make up **Function f.**
- The output of Function f is then combined with the left half via another XOR.
- The result of these operations becomes the new right half; the old right half becomes the new left half.
- These operations are repeated 16 times, making **16 rounds of DES**.

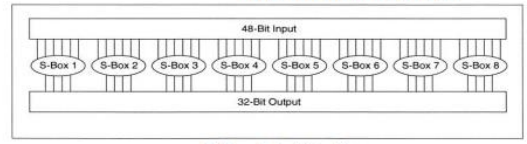


DES Round

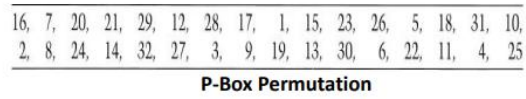


Key Permutation

Expansion Permutation



S-Box Substitution



P-Box Permutation

DES Decryption

- With DES it is possible to use the same function to encrypt or decrypt a block.
- The only difference is that the keys must be used in the reverse order.
- If the **encryption** keys for each round are **K1 , K2 , K3 , . . . , K16**, then the **decryption** keys are **K16, K15, K14, . . . , K1** .

DES Security

- DES **56-bit key** is **not long enough**.
- DES algorithm design is **fixed to a 56-bit key**.
- Some researchers were able to **brute-force the key in a few hours**.

Short-Term Solutions:

- **Double DES**: Take two keys, k1 and k2 , and perform two encryptions, one on top of the other: E(k2 , E(k1 ,m)).
- **Triple DES**: you encrypt with one key, then with the second, and finally with a third. This process gives a strength roughly equivalent to a **112-bit key**.

Advanced Encryption Standard (AES)

After a public competition and review, NIST selected an algorithm named Rijndael as the new advanced encryption system.

Now known as Advanced Encryption Standard (AES)
AES is likely to be the commercial-grade symmetric algorithm of choice for years, if not decades.

AES Overview

AES is a fast algorithm that can easily be implemented on simple processors.

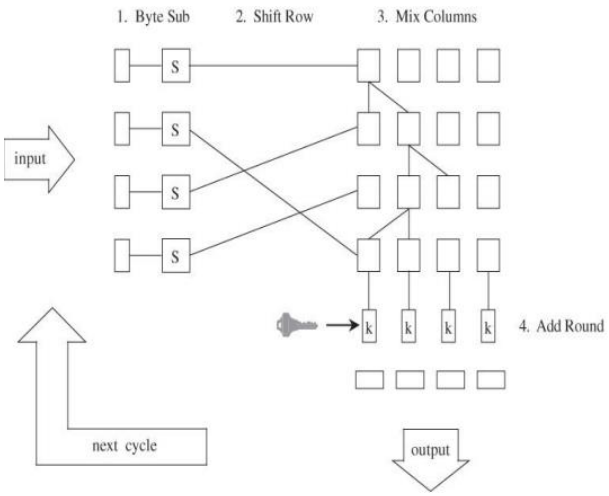
Although it has a strong mathematical foundation, it primarily uses substitution, transposition, the shift, exclusive OR, and addition operations. Like DES, AES uses repeat cycles.

There are **10, 12, or 14 cycles** for **keys of 128, 192, and 256 bits**, respectively.

Each round consists of **four extremely fast steps** that substitute and scramble bits.
Bits from the key are frequently combined with intermediate result bits, so key bits are also well diffused throughout the result.

The Four Steps

1. **Byte substitution**.
   This step uses a substitution substituting each byte of a 128-bit block according to a substitution table. This is a straight diffusion operation.
2. **Shift row**.
   Certain bits are shifted to other positions. This is a straight confusion operation.
3. **Mix column**.
   This step involves shifting left and XORing bits with themselves. These operations implement both confusion and diffusion.
4. **Add subkey**.
   A portion of the key unique to this cycle is XORed with the cycle result. This operation delivers confusion and incorporates the key.



DES vs. AES

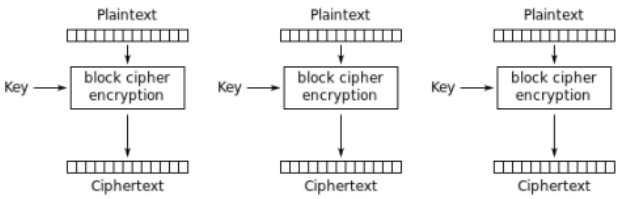
	DES	AES
Date designed	1976	1999
Block size	64 bits	128 bits
Key length	56 bits (effective length); up to 112 bits with multiple keys	128, 192, 256 (and possibly more) bits
Operations	16 rounds	10, 12, 14 (depending on key length); can be increased
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but open public comments and criticisms invited
Source	IBM, enhanced by NSA	Independent Dutch cryptographers

Block cipher Mode of operations

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed j bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

Problem!

- You may have noticed a weakness in description of the DES & AES.
- They use the same process for each 64-bit block.
- That means that any identical data blocks encrypted with the same key will have the same output.
- This mode of operation is called **Electronic Code Book (ECB).**

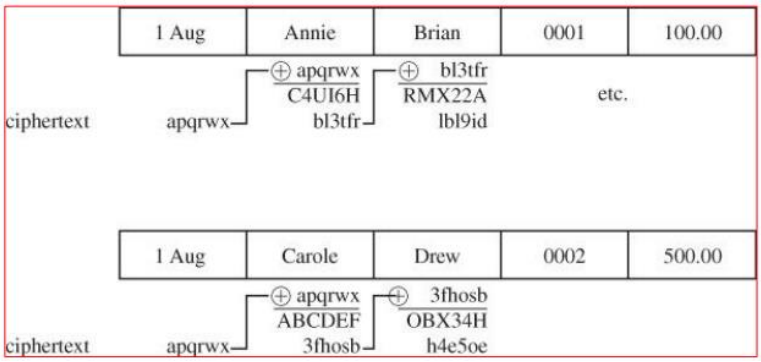


Electronic Codebook (ECB) mode encryption

Chaining

The solution for the previous problem is called **chaining**.

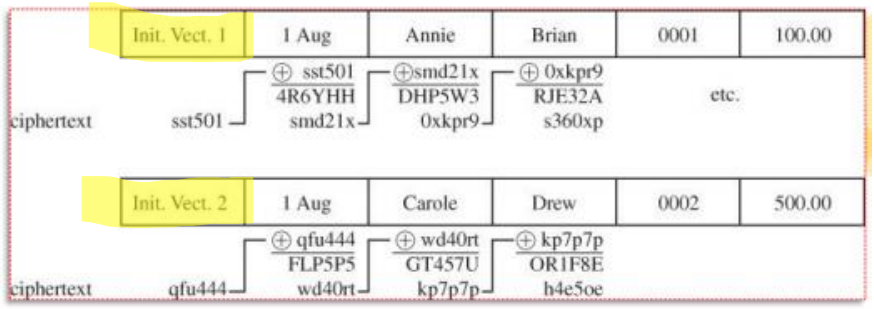
a process used to encrypt and decrypt large plaintext inputs by creating a cryptographic chain wherein each ciphertext block is dependent on the last.

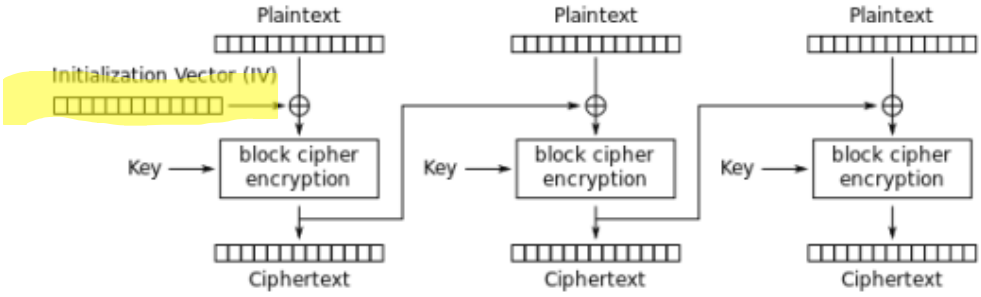


Initialization Vector (IV)

To start the encryption of a data stream, you first create one extra block containing any value.

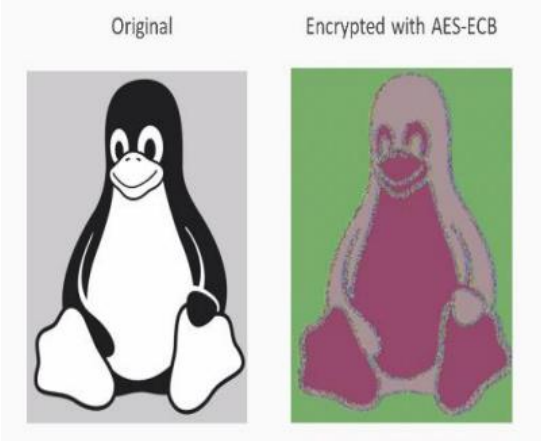
Then, you apply chained encryption, starting with the first block (the random number)

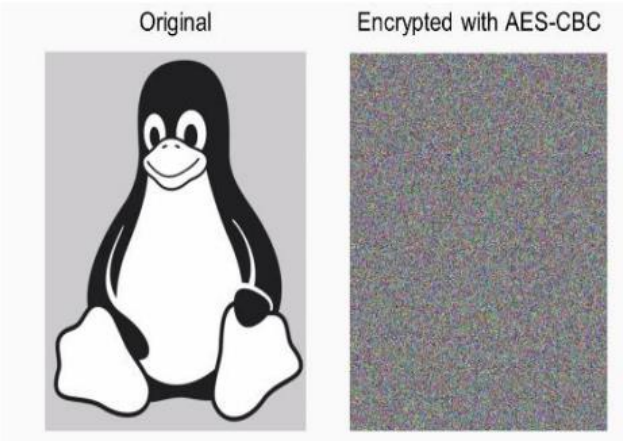




Cipher Block Chaining (CBC) mode encryption

With and Without Chaining

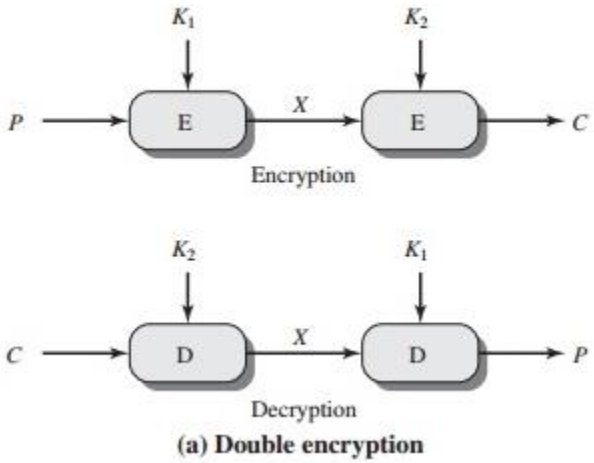




Chapter 3

Double-DES

is a encryption technique which uses two instance of DES on same plain text.



(a) Double encryption

Enc

$$C = E(K_2, E(K_1, P))$$

Dec

$$P = D(K_1, D(K_2, C))$$

Triple-DES with Two-Keys

is a encryption technique which uses three instance of DES on same plain text.

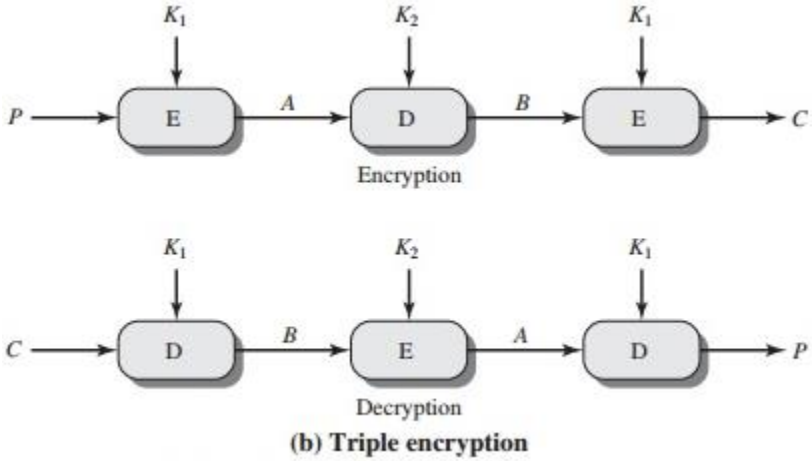
The function follows an encrypt-decrypt-encrypt (EDE) sequence

Enc

$$C = E(K_1, D(K_2, E(K_1, P)))$$

Dec

$$P = D(K_1, E(K_2, D(K_1, C)))$$



(b) Triple encryption

Multiple Encryption

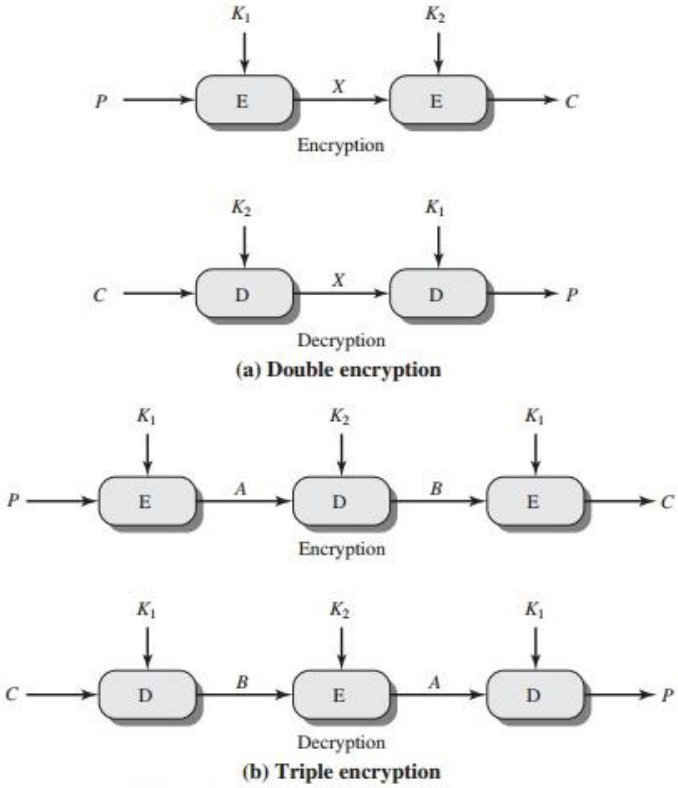


Figure 6.1 Multiple Encryption

The Use of Random Numbers

A number of network security algorithms and protocols based on cryptography make use of random binary numbers:

- Key distribution and reciprocal authentication schemes
- Session key generation
- Generation of keys for the RSA public-key encryption algorithm
- Generation of a bit stream for symmetric stream encryption

These applications give rise to two distinct and not necessarily compatible requirements for a sequence of random numbers: randomness and unpredictability.

- ## Randomness
  The generation of a sequence of allegedly random numbers being random in some well-defined statistical sense has been a concern

  two criteria are used to validate that a sequence of numbers is random
  - **Uniform distribution**: The distribution of bits in the sequence should be uniform; that is, the frequency of occurrence of ones and zeros should be approximately equal.
  - **Independence**: No one subsequence in the sequence can be inferred from the others.

- ## Unpredictability
  The requirement is not just that the sequence of numbers be statistically random, but that the successive members of the sequence are unpredictable.

TRNGs, PRNGs, and PRFs

Cryptographic applications typically make use of algorithmic techniques for random number generation.

If the algorithm is good, the resulting sequences will pass many tests of randomness and are referred to as **pseudorandom numbers.**

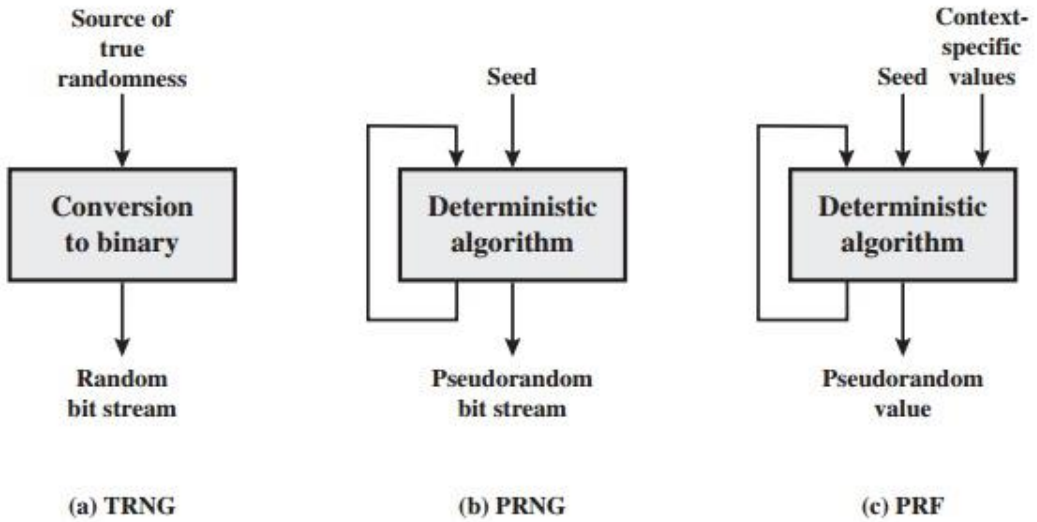


Figure 7.1 Random and Pseudorandom Number Generators

Stream Ciphers

A typical stream cipher encrypts plaintext one byte at a time. is combined one byte at a time with the plaintext stream using the bit- wise exclusive-OR (XOR) operation.

```
  11001100  plaintext
⊕ 01101100  key stream
  10100000  ciphertext
```

Decryption requires the use of the same pseudorandom sequence.

```
  10100000  ciphertext
⊕ 01101100  key stream
  11001100  plaintext
```

Note// although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time.

Stream Cipher Structure

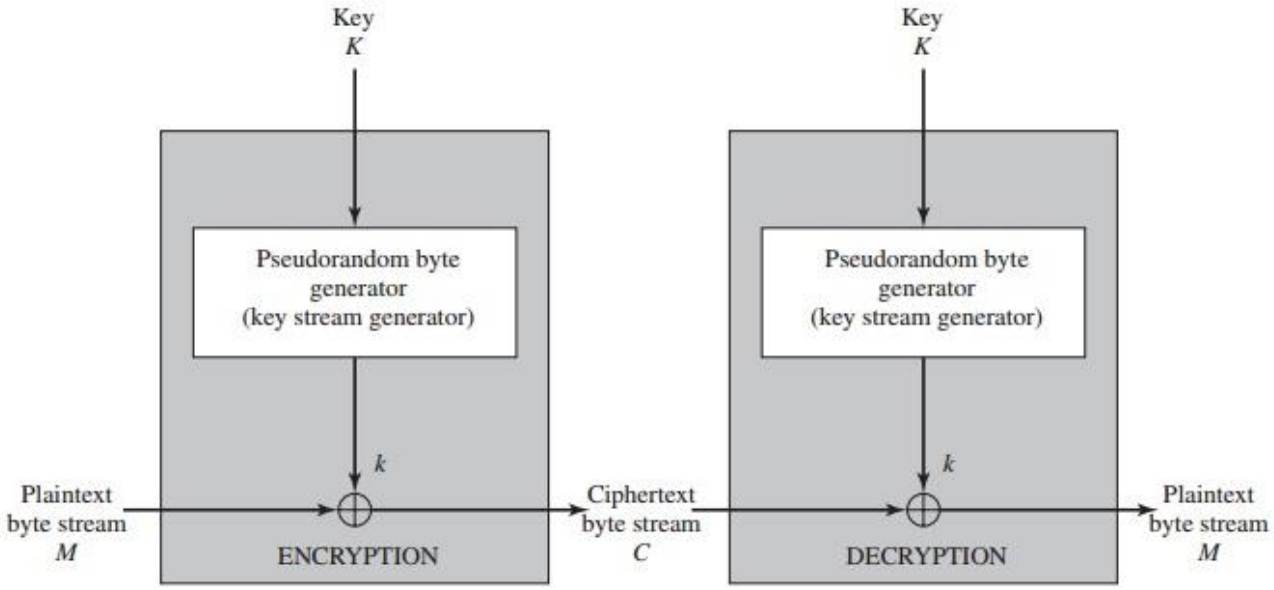


Figure 7.5 Stream Cipher Diagram

Stream Cipher Properties

- some design considerations are:
  - long period with no repetitions
  - statistically random
  - depends on large enough key
  - Large linear complexity
- properly designed, can be as secure as a block cipher with same size key
- but usually simpler & faster

RC4

RC4 is a stream cipher It is a variable key-size stream cipher with byte-oriented operations.

Note// RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA Security.

Note// It is a variable key-size stream cipher with byte-oriented operations.

widely used (web SSL/TLS, wireless WEP) .

key forms random permutation of all 8-bit values .

uses that permutation to scramble input info processed a byte at a time.

RC4 Key Schedule

- starts with an array S of numbers: 0..255 .
- use key to well and truly shuffle .
- S forms internal state of the cipher.

```
for i = 0 to 255 do
    S[i] = i
    T[i] = K[i mod keylen])
j = 0
for i = 0 to 255 do
    j = (j + S[i] + T[i]) (mod 256)
    swap (S[i], S[j])
```

RC4 Encryption

- encryption continues shuffling array values
- sum of shuffled pair selects "stream key" value from permutation
- XOR S[t] with next byte of message to en/decrypt

```
i = j = 0
for each message byte M_i
    i = (i + 1) (mod 256)
    j = (j + S[i]) (mod 256)
    swap(S[i], S[j])
    t = (S[i] + S[j]) (mod 256)
    C_i = M_i XOR S[t]
```

RC4 Security

- claimed secure against known attacks.
    - have some analyses, non-practical.
- result is very non-linear.
- since RC4 is a stream cipher, must **never reuse a key.**
- have a concern with WEP, but due to key handling rather than RC4 itself.

Chapter 4

Private-Key vs Public-Key

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if the key is kept secret. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and a related algorithm for decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if one of the keys is kept secret. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

RSA Algorithm

ماتتلخص ارجع للسلايدات ولا دور لك مقطع

Note// The Rivest–Shamir–Adelman (RSA) cryptosystem is a public key system introduced in 1978.

Note// Cryptanalysts have subjected RSA to extensive cryptanalysis, but they have found no serious flaws.

A plaintext message P is encrypted to ciphertext C by:

C = P e mod n

The plaintext is recovered by:

P = C d mod n

Key Generation by Alice

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

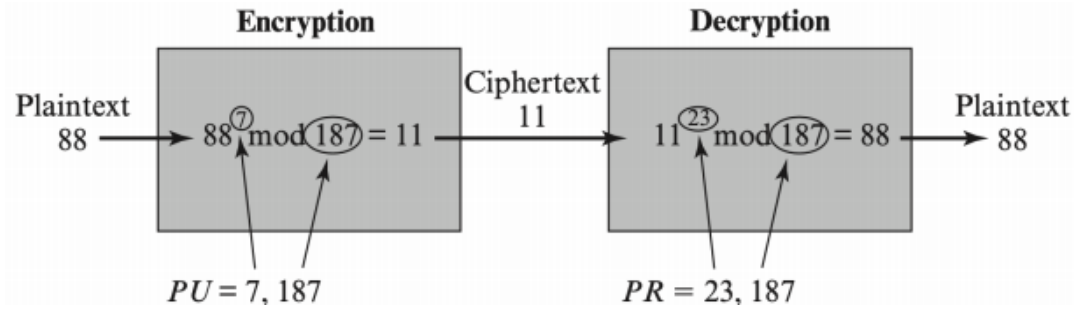
Encryption by Bob with Alice's Public Key

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Example



Key generation: https://www.youtube.com/watch?v=oOcTVTpUsPQ

Encryption & decryption: https://www.youtube.com/watch?v=4zahvcJ9glg

	Secret Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Key size (bits)	Depends on the algorithm; 56–112 (DES), 128–256 (AES)	Unlimited; typically no less than 256; 1000 to 2000 currently considered desirable for most uses
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse. Secrecy and integrity of data, from single characters to blocks of data, messages and files	Key exchange, authentication, signing
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow, typically by a factor of up to 10,000 times slower than symmetric algorithms

Elliptic Curve Cryptography (ECC)

sites that conduct large numbers of secure transactions. A competing system challenges RSA: elliptic curve cryptography (ECC).

ECC focuses on pairs of public and private keys for decryption and encryption of web traffic.

Note// Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA.

As we have seen, the key length for secure RSA use has increased over recent years, and this has put a heavier processing load on applications using RSA.

The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.

Note// An **elliptic curve** is defined by an equation in two variables with coefficients

For cryptography, the variables and coefficients are restricted to elements in a finite field, which results in the definition of a finite abelian group.

cubic equations for elliptic curves take the following form, known as a **Weierstrass equation**:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

where a, b, c, d, e are real numbers and x and y take on values in the real numbers.

For our purpose, it is sufficient to limit ourselves to equations of the form

$$y^2 = x^3 + ax + b$$

Such equations are said to be cubic, or of degree 3, because the highest exponent they contain is a 3.

Chapter 5

Diffie-Hellman Key Exchange

The purpose of the algorithm is to enable two users to securely exchange a Key that can then be used for subsequent symmetric encryption of messages.

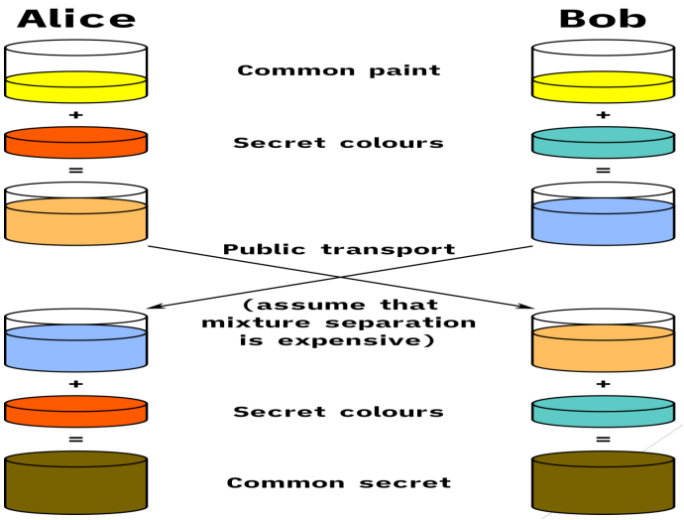
The Algorithm itself is limited to the exchange of secret values.

Note// The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography and is generally referred to as Diffie-Hellman key exchange.

Note// Several commercial products employ this key exchange technique.

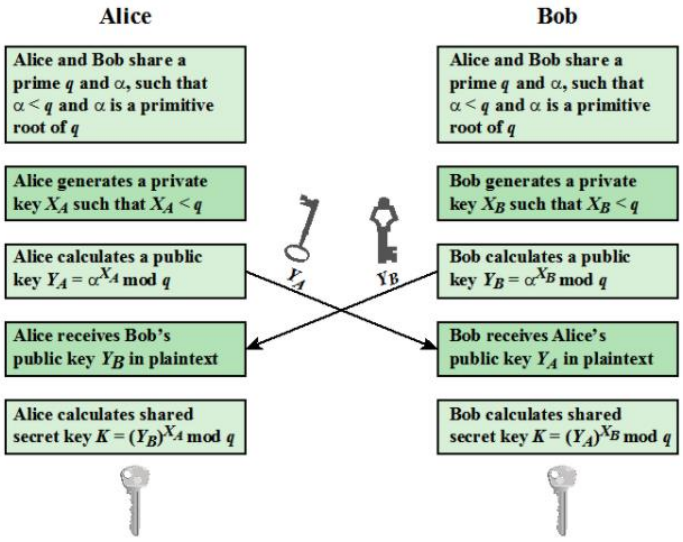
How it works

1. Alice and Bob agree on a common color.
2. Each one selects a secret color.
3. Each one mixes the secret color with the common color.
4. They exchange the new colors.
5. Each one add the secret color to the received color.
6. Each side gets the same color (common secret).



There are two publicly known numbers:

- a prime number q and an integer a.
- a is a primitive root of q.
- Suppose the users A and B wish to create a shared key.



ارجع للسلايدات ولا دور لك مقطع

Diffie-Hellman Key Exchange

Alice

Bob and Alice know and have the following :
$p = 23$ *(a prime number)* $g = 11$ *(a generator)*

Bob

Alice	Bob
Alice chooses a secret random number a = 6	Bob chooses a secret random number b = 5
Alice computes : $A = g^a \bmod p$ $A = 11^6 \bmod 23 = 9$	Bob computes : $B = g^b \bmod p$ $B = 11^5 \bmod 23 = 5$
Alice receives B = 5 from Bob	**Bob receives A = 9 from Alice**
Secret Key = $K = B^a \bmod p$	Secret Key = $K = A^b \bmod p$
$K = 5^6 \bmod 23 = \boxed{8}$	$K = 9^5 \bmod 23 = \boxed{8}$

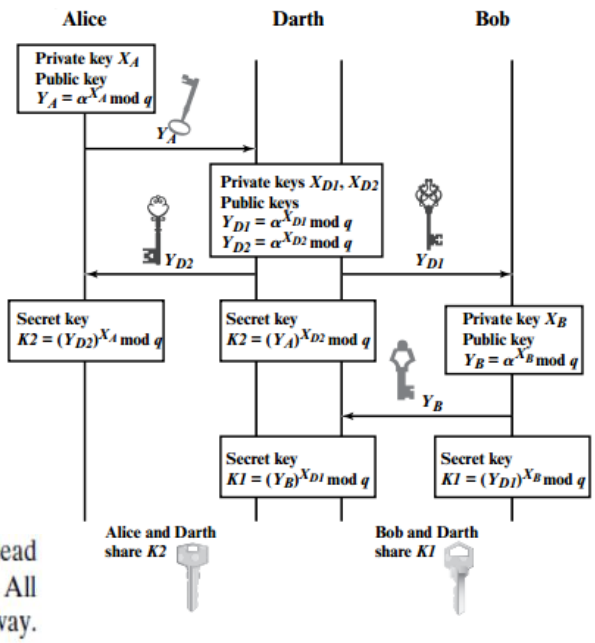
The common secret key is : 8

N.B. We could also have written : $K = g^{ab} \bmod$

Man-in-the-middle attack on DH

Diffie-Hellman is insecure against man in the middle attack.

1. Darth prepares for the attack by generating two random private keys X_{D1} X_{D2} and then computing the corresponding public keys Y_{D1} and Y_{D2}.
2. Alice transmits Y_A to Bob.
3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calcu $K2 = (Y_A)^{X_{D2}} \bmod q$.
4. Bob receives Y_{D1} and calculates $K1 = (Y_{D1})^{X_B} \bmod q$.
5. Bob transmits Y_B to Alice.
6. Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calcu $K1 = (Y_B)^{X_{D1}} \bmod q$.
7. Alice receives Y_{D2} and calculates $K2 = (Y_{D2})^{X_A} \bmod q$.



At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key $K1$ and Alice and Darth share secret key $K2$. All future communication between Bob and Alice is compromised in the following way.

1. Alice sends an encrypted message M: E($K2$, M).
2. Darth intercepts the encrypted message and decrypts it to recover M.
3. Darth sends Bob $E(K1, M)$ or E($K1$, M'), where M' is any message. In the first case, Darth simply wants to eavesdrop on the communication without altering it. In the second case, Darth wants to modify the message going to Bob.

The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates;

ElGamal Cryptographic System

ارجع للسلايدات ولا دور لك مقطع

In 1984, T. Elgamal announced a public-key scheme based on discrete logarithms,closely related to the Diffie-Hellman technique [ELGA84, ELGA85].

Note// The Elgamal cryptosystem is used in some form in a number of standards including the digital signature standard (DSS).

cryptography algorithm that uses the public and private key concepts to secure communication between two systems.

As with Diffie-Hellman, the global elements of Elgamal are a prime number q and a, which is a primitive root of q. User A generates a private/public key pair as follows:

Global Public Elements	
q	prime number
α	$\alpha < q$ and α a primitive root of q

Key Generation by Alice	
Select private X_A	$X_A < q-1$
Calculate Y_A	$Y_A = \alpha^{XA} \bmod q$
Public key	$PU = \{q, \alpha, Y_A\}$
Private key	X_A

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Ciphertext:	(C_1, C_2)

Decryption by Alice with Alice's Private Key	
Ciphertext:	(C_1, C_2)
Calculate K	$K = (C_1)^{XA} \bmod q$
Plaintext:	$M = (C_2 K^{-1}) \bmod q$

Figure 10.3 The ElGamal Cryptosystem

Message Digest

Wax seals

Wax seals used for protecting letters so that if a seal is broken, we can know that a letter has been exposed.

Cryptography can be used to seal a file so that any change becomes clear.

One technique for providing the "seal" is to compute a function, sometimes called a **hash** or **checksum** or **message digest** of the file.

One-Way Hash Functions

Hash or message digest functions are ways to detect possible changes to a block of data.

Note// These functions signal unintentional changes as well as intentional (malicious) ones.

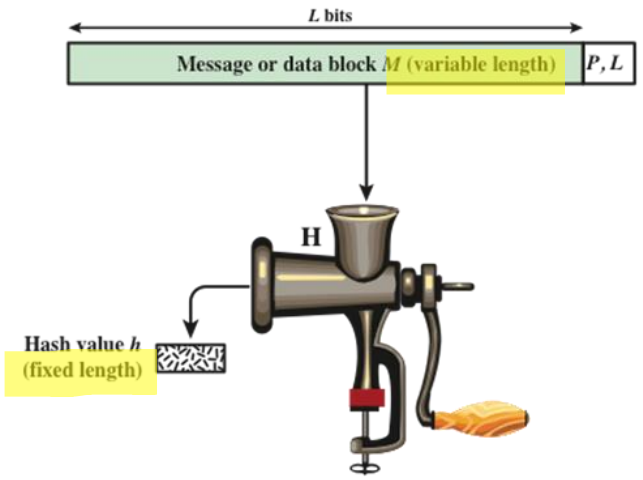
One-way hash functions are a cryptographic construct with multiple **uses**.

- Used in conjunction with public-key algorithms for both encryption and digital signatures.
- Used in integrity checking.
- Used in authentication.
- Used in communications protocols.

Note// Much more than encryption algorithms, **one-way hash functions** are the **workhorses of modern cryptography.**

Requirements for Hash Functions

1. **They are one-way.**
   They convert input to a digest, but it is infeasible to start with a digest value and infer an input that could have produced that digest.
2. **They do not have obvious collisions.**
   It is infeasible to find a pair of different plaintexts that produce the same digest.



P, L = padding plus length field

Figure 11.1 Cryptographic Hash Function; $h = H(M)$

Message Authentication using Hash Functions

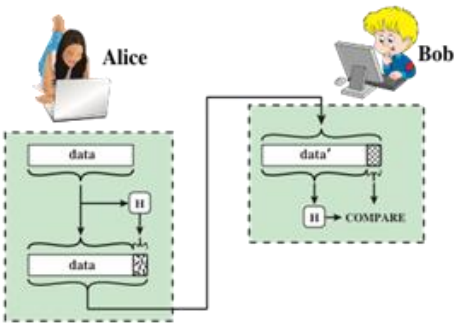
Figure a:

Alice sends two things

1. Data
2. Hash value of the data

Bob receives the data and hash value

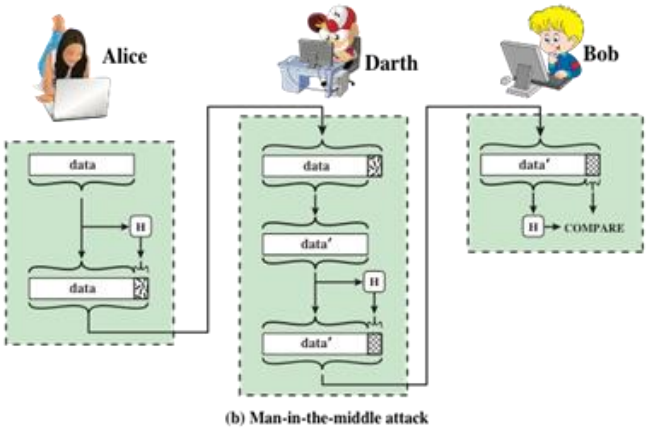
1. Then he calculates the hash value of data and compares the two values
2. If the calculated hash is equal to the received one, then Bob assumes the data is accurate



(a) Use of hash function to check data integrity

Figure B:

- Darth interrupts Alice's message
- Modifies it and creates another hash value
- Sends it to Bob



(b) Man-in-the-middle attack

Figure 11.2 Attack Against Hash Function

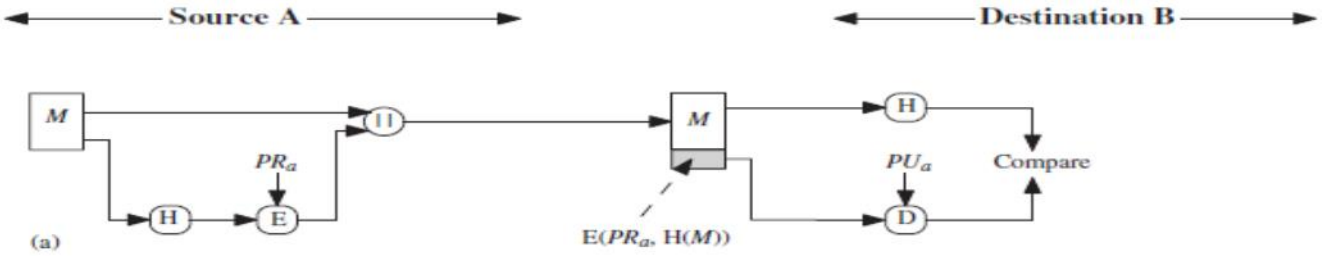
Digital Signatures

Like its counterpart on paper, a digital signature is a way by which a person or organization can affix a bit pattern to a file such that it implies confirmation, pertains to that file only, cannot be forged, and demonstrates authenticity.

Note// The most powerful technique to demonstrate authenticity is a digital signature.

We want a way by which one party can sign something and, as on paper, have the signature remain valid for days, months, years—indefinitely.

simplified fashion, how a hash code is used to provide a digital signature



The hash code is encrypted, using public-key encryption with the sender's private key.

If confidentiality as well as a digital signature is desired, then the message plus the private-key-encrypted hash code can be encrypted using a symmetric secret key.