Ahsanullah University of Science and Technology (AUST)
Department of Computer Science and Engineering

LABORATORY MANUAL

Course No.: CSE 4174
Course Title: Cyber Security Lab

For the students of 4th Year, 1st semester of
B.Sc. in Computer Science and Engineering program

Table of Contents

Cryptography

Terminologies

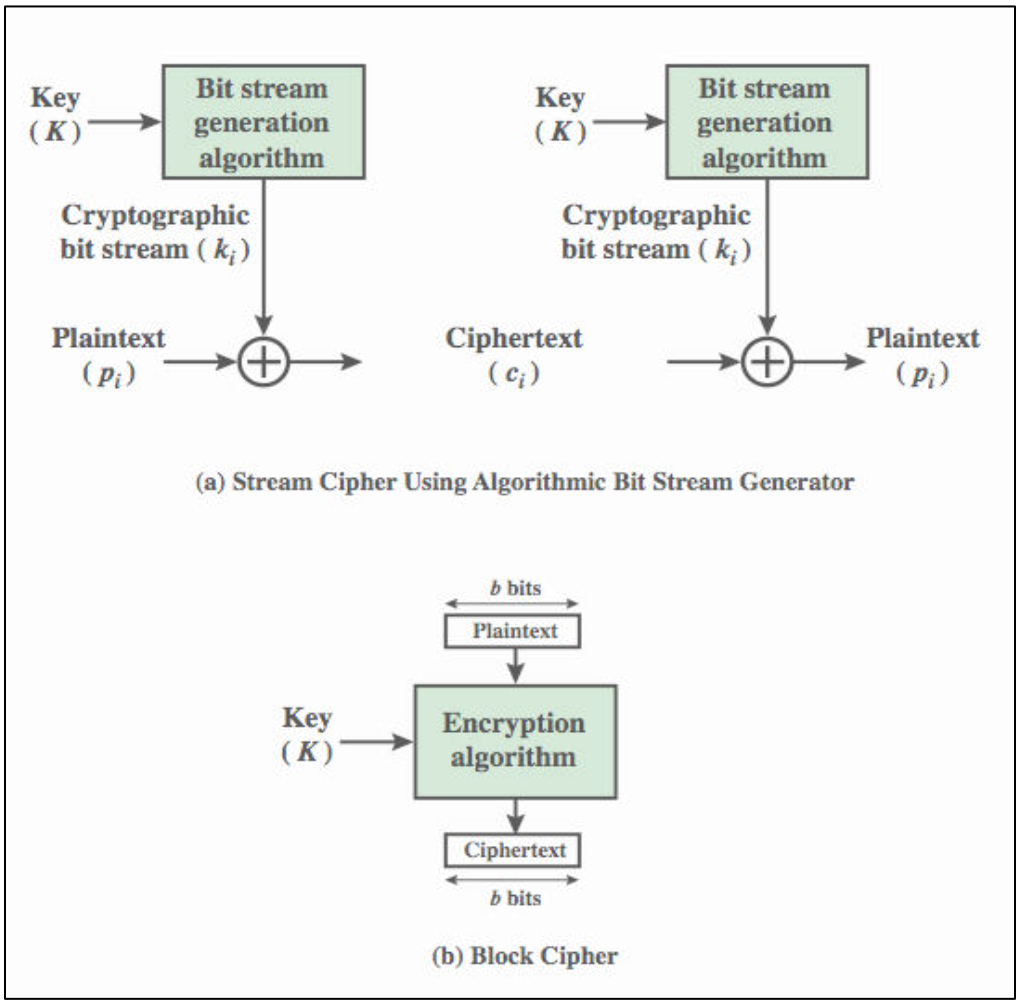
- Plaintext - original message
- Ciphertext - coded message
- Cipher - algorithm for transforming plaintext to ciphertext
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to ciphertext
- Decipher (decrypt) - recovering ciphertext from plaintext
- Cryptography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

Different Cryptographic Systems

Cryptographic system can be characterized by:

- **Type of encryption operations used**
  - **Substitution**: Substitution cipher is a data encryption scheme in which units of the plaintext (generally single letters or pairs of letters of ordinary text) are replaced with other symbols or groups of symbols.
  - **Transposition**: Transposition cipher is a simple data encryption scheme in which plaintext characters are shifted in some regular pattern to form ciphertext.
  - **Product**: Product cipher is the data encryption scheme in which the ciphertext produced by encrypting a plaintext document is subjected to further encryption. By combining two or more simple transposition ciphers or substitution ciphers, a more secure encryption may result.
- **Number of keys used**
  - **Single-key/ Private key/ Symmetric key**: In the Private key approach, the same key is used for encryption and decryption.
  - **Two-key/ Public key/ Asymmetric key**: In a Public key approach, two keys are used; one key is used for encryption and another key is used for decryption. One key (public key) is used to encrypt the plain text to convert it into cipher text and another key (private key) is used by the receiver to decrypt the cipher text to read the message.
- **Way in which plaintext is processed**
  - **Block**: A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length. Typically, a block size of 64 or 128 bits is used.

- **Stream**: A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.



Symmetric Encryption

Symmetric encryption is also known as conventional/ private-key/ single-key encryption. Here, sender and receiver share a common key. All classical encryption algorithms are private-key approach. This was only type prior to invention of public-key in 1970's and by far most widely used.

There are two requirements for secure use of symmetric encryption:

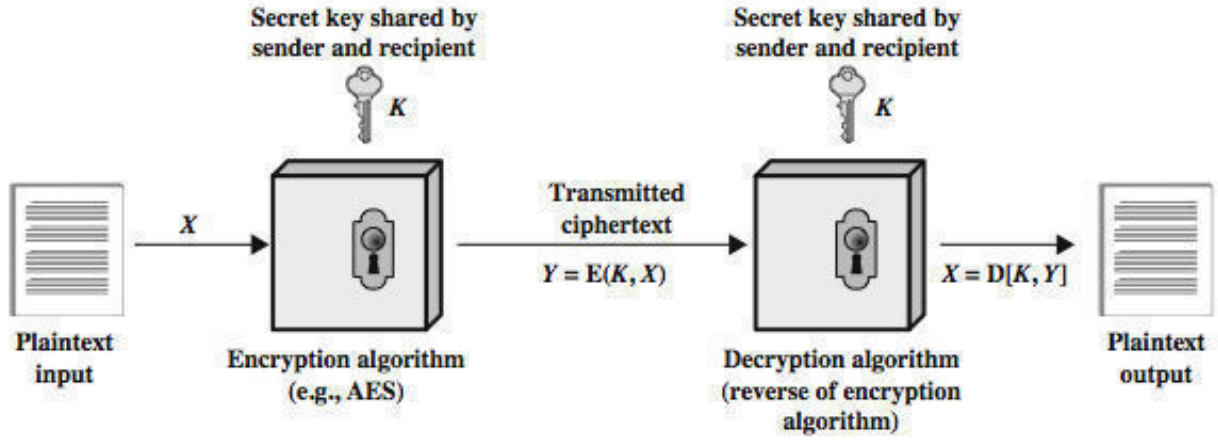
- a strong encryption algorithm
- a secret key known only to sender / receiver

Mathematically,

$Y = E(K, X)$

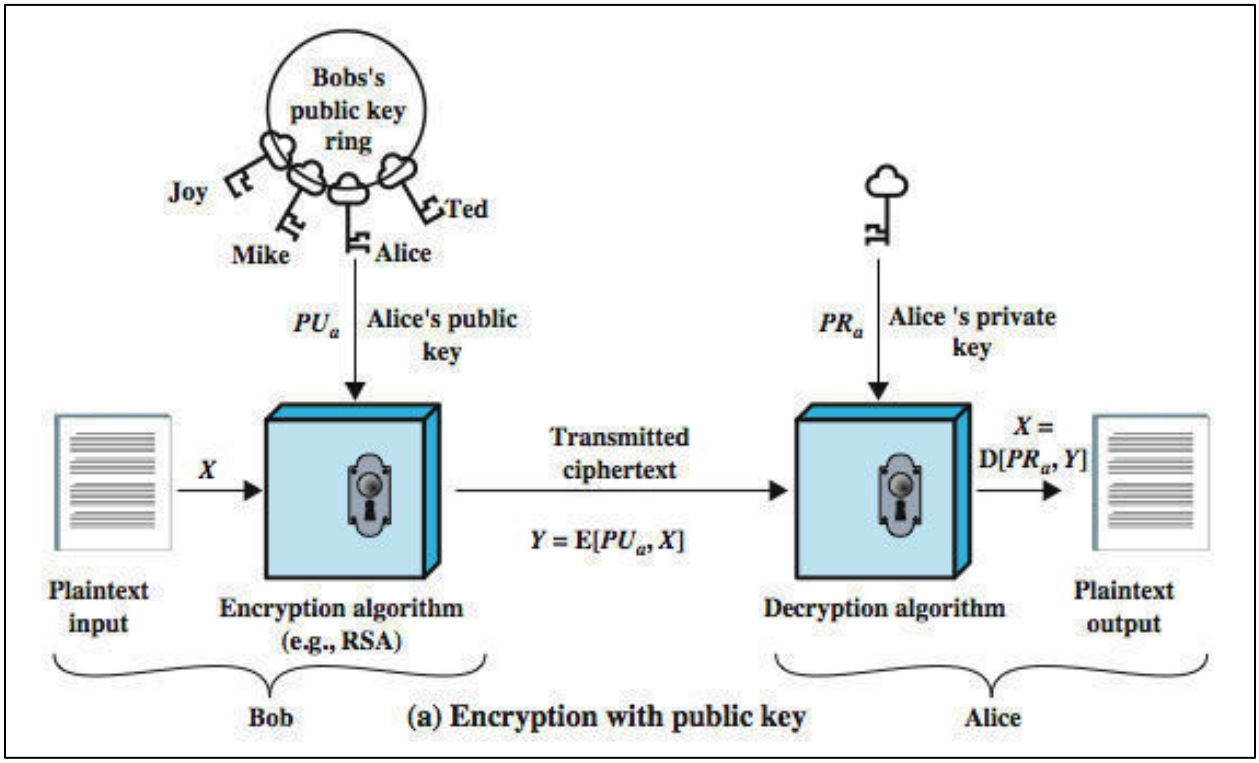
$X = D(K, Y)$

assuming encryption algorithm is known and implying a secure channel to distribute key.



Public Key Cryptography

Traditional **private/secret/single key** cryptography uses **one** key that is shared by both sender and receiver. If this key is disclosed, communications are compromised. Public key cryptography uses **two** keys – a public & a private key. It uses clever application of number theoretic concepts to function. The approach complements **rather than** replaces private key cryptography.



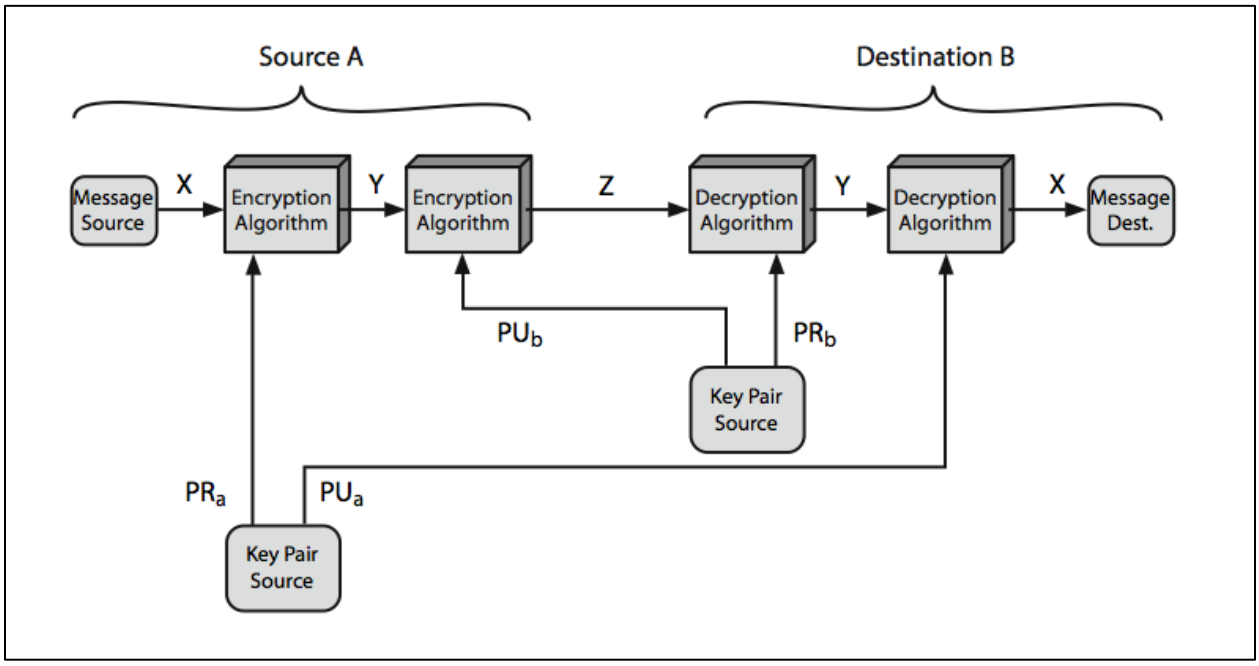
Public key cryptography was developed to address two key issues:

- **key distribution** – how to have secure communications in general without having to trust a KDC with your key
- **digital signatures** – how to verify a message comes intact from the claimed sender

Public-key/two-key/asymmetric cryptography involves the use of **two** keys:

- a **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
- a related **private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures**

It is **asymmetric** because those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures.



Feistel Cipher Structure

Most **symmetric block** encryption algorithms in current use are based on a structure referred to as a Feistel block cipher. A block cipher operates on a plaintext block of n bits to produce a ciphertext block of n bits.

Feistel's method (developed in 1973) is a practical application of Claude Shannon's proposal in 1945 to alternate **confusion** and **diffusion** functions in the product cipher. It is worth It is worth commenting that modern symmetric cipher is based on Feistel's structure which in turn is developed on Claude Shannon's suggestions. Thus, today's wide used symmetric encryption is dated back to more than half a century. In particular, Feistel proposed the use of a cipher that alternates substitutions and permutations. The terms **diffusion** and **confusion** were introduced by Claude Shannon to capture the two basic building blocks for

any cryptographic system. Shannon's concern was to thwart cryptanalysis based on statistical analysis. Every block cipher involves a transformation of a block of plaintext into a block of ciphertext, where the transformation depends on the key. **The mechanism of diffusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible** in order to thwart attempts to deduce the key. **Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key** as complex as possible, again to thwart attempts to discover the key. So successful are diffusion and confusion in capturing the essence of the desired attributes of a block cipher that they have become the cornerstone of modern block cipher design.

The exact realization of a Feistel network depends on the choice of the following parameters and design features:

- **block size** - increasing size improves security, but slows cipher
- **key size** - increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- **number of rounds** - increasing number improves security, but slows cipher
- **subkey generation algorithm** - greater complexity can make analysis harder, but slows cipher
- **round function** - greater complexity can make analysis harder, but slows cipher
- **fast software en/decryption** - more recent concern for practical use
- **ease of analysis** - for easier validation & testing of strength

Cryptanalysis

Cryptanalysis is a process of finding vulnerabilities in cryptographic algorithms and using these weaknesses to decipher the ciphertext without knowing the secret key (instance deduction). Sometimes the weakness is not in the cryptographic algorithm itself, but rather in how it is applied that makes cryptanalysis successful. There are two general approaches, they are Cryptanalytic Attack and Brute Force Attack.

Cryptanalytic Attack

- ✓ **Cypher Text Only Attack**: In cryptography, a ciphertext-only attack (COA) or known ciphertext attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts. The attack is completely successful if the corresponding plaintexts can be deduced, or even better, the key. The ability to obtain any information at all about the underlying plaintext is still considered a success
- ✓ **Known Plaintext Attack**: The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the plaintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further

secret information such as secret keys and code books. The term "crib" originated at Bletchley Park, the British World War II decryption operation.

- ✓ **Chosen Plaintext Attack**: A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key.

Brute Force Attack

Brute force attack is to simply try every key. It is the most basic attack, proportional to key size.

Unconditional and Computational Security

- **Unconditional security**: No matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext.
- **Computational security**: Given limited computing resources (e.g., time needed for calculations is greater than age of universe), the cipher cannot be broken.

Symmetric Key Cryptography

Classical Substitution Cipher

Here, letters of plaintext are replaced by other letters or by numbers or symbols, or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Ceasar Cipher

It is the earliest known substitution cipher. The approach was first used in military affairs. Here, each letter is replaced by 3rd letter on. An example can be:

Plain text: meet me after the toga party
Cipher text: PHHW PH DIWHU WKH WRJD SDUWB

So, Caesar cipher can be represented as

$c = E(k, p) = (p + k) \bmod (26)$
$p = D(k, c) = (c - k) \bmod (26)$

Mono Alphabetic Substitution

In Mono-alphabetic Substitution, each of the symbols in the plaintext, say, the 26 letters for simplicity, map onto some other letter. For example,

Plaintext: 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
Ciphertext: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

The general system of symbol for symbol substitution is called a mono alphabetic substitution. 'attack' would be transformed into the cipher text 'QZZQEA'.

Poly Alphabetic Substitution

A poly-alphabetic cipher is any cipher based on substitution, using several substitution alphabets. In polyalphabetic substitution ciphers, the plaintext letters are enciphered differently based upon their installation in the text. Rather than being a one-to-one correspondence, there is a one-to-many relationship between each letter and its substitutes. For example, 'a' can be enciphered as 'd' in the starting of the text, but as 'n' at the middle.

Transposition Cipher

In classical **transposition** or **permutation** ciphers, the message is hidden by rearranging the letter order without altering the actual letters used.

Rail Fence Cipher

Message letters are written out diagonally over a number of rows and then the cipher is read off row by row. For example,

Plain text: meet me after the toga party

m	e	m	a	t	r	h	t	g	p	r	y
	e	t	e	f	e	t	e	o	a	a	t

Cipher text: MEMATRHTGPRYETEFETEOAAT

Row Transposition Cipher

It is a more complex transposition approach where letters of message are written out in rows over a specified number of columns and then the columns are reordered according to some key before reading off the rows.

Key: 41532
Plain text: the simplest possible transpositions

1	2	3	4	5
t	h	e	s	i
m	p	l	e	s
t	p	o	s	s
i	b	l	e	t
r	a	n	s	p
o	s	i	t	i
o	n	s	x	x

4	1	5	3	2
s	t	i	e	h
e	m	s	l	p
s	t	s	o	p
e	i	t	l	b
s	r	p	n	a
t	o	i	i	s
x	o	x	s	n

Cipher Text: s t i e h e m s l p s t s o p e i t l b s r p n a t o i i s x o x s n

Columnar Transposition Cipher

In Columnar transposition cipher, each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.

Plain text: meet me after the party
Keyword: HACK Order of alphabets in HACK: 3124

H	**A**	**C**	**K**
3	**1**	**2**	**4**
m	e	e	t
m	e	a	f
t	e	r	t
h	e	p	a
r	t	y	x

Cipher text: e e e e t e a r p y m m t h r t f t a x

Product Cipher

Ciphers using only substitutions or transpositions are not secure because of language characteristics. Hence, using several ciphers can be considered in succession to make harder.

- two substitutions make a more complex substitution
- two transpositions make more complex transposition
- but a substitution followed by a transposition makes a new much harder cipher

Steganography

Stenography is an alternative to encryption that hides existence of message. The technique involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected; for example, hiding in LSB in graphic image or sound file.

Data Encryption Standard (DES)

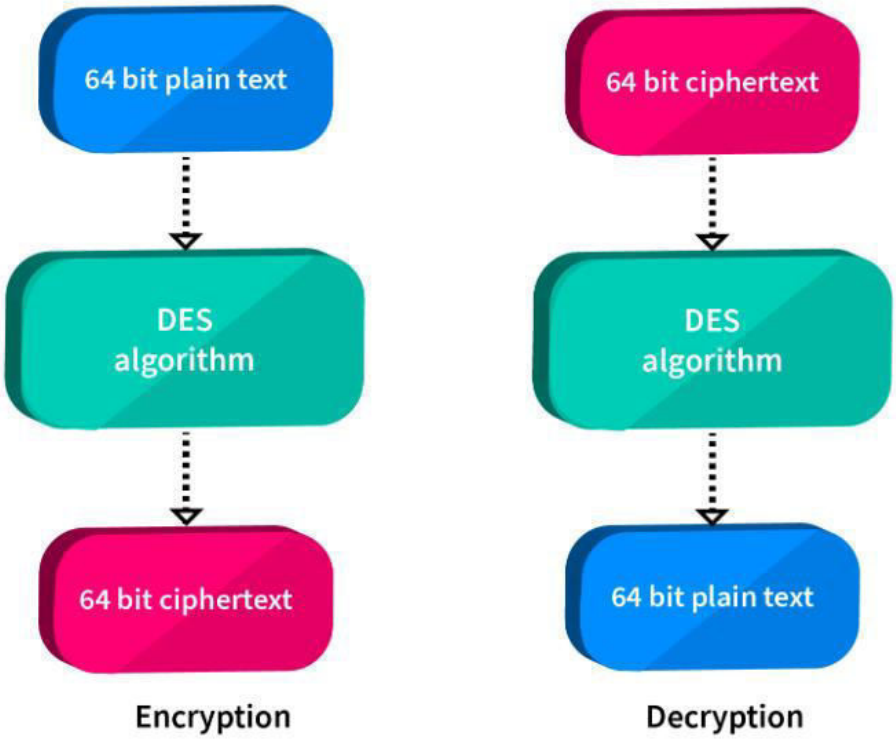
DES was Adopted by NIST in 1977. It is based on a cipher (Lucifer) developed earlier by IBM for Lloyd's of London for cash transfer. DES uses the Feistel cipher structure with 16 rounds of processing. DES uses a 56-bit encryption key. The key size was apparently dictated by the memory and processing constraints imposed by a single-chip implementation of the algorithm for DES. The key itself is specified with 8 bytes, but one bit of each byte is used as a parity check.

DES encryption was broken in 1999 by Electronics Frontiers Foundation (EFF, www.eff.org). This resulted in NIST issuing a new directive that year that required organizations to use Triple DES, that is, three consecutive applications of DES. Later, NIST initiated the development of new standards for data encryption. The result is Advanced Encryption Standard (AES).

Triple DES continues to enjoy wide usage in commercial applications even today. What is specific to DES is the implementation of the F function in the algorithm and how the round keys are derived from the main encryption key.

Data Encryption Standard (DES)

DES is the most widely used private key block cipher. It was adopted in 1977 by the National Bureau of Standards as Federal Information Processing Standard 46 (FIPS PUB 46). DES encrypts data in 64-bit blocks using a 56-bit key. The DES enjoys widespread use. It has also been the subject of much controversy its security.



DES Encryption Overview

The overall scheme for DES encryption is illustrated in the following figure, which takes as input 64-bits of data and of key.

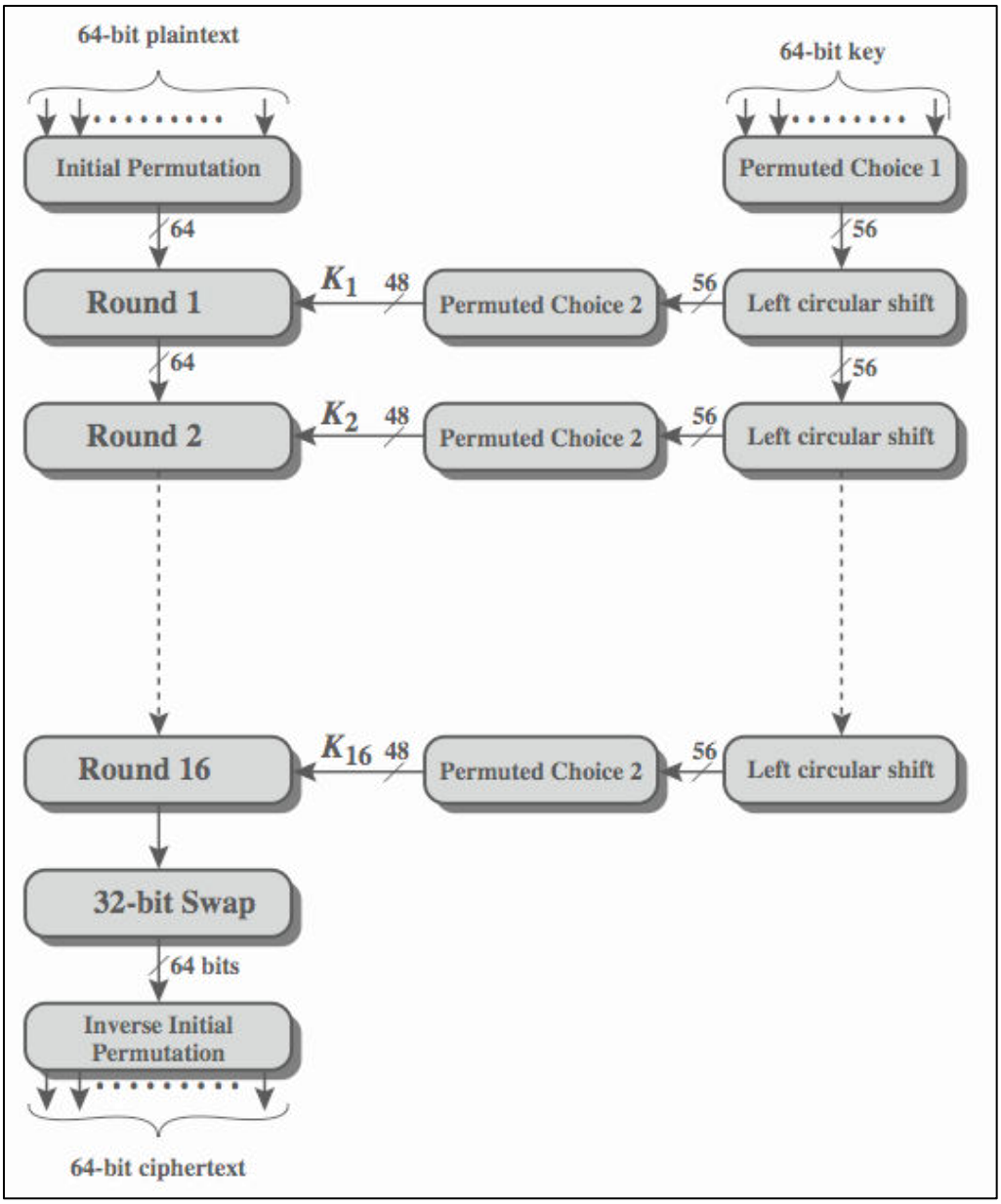
The left side shows the basic process for enciphering a 64-bit data block which consists of:

- an initial permutation (IP) which shuffles the 64-bit input block
- 16 rounds of a complex key dependent round function involving substitutions & permutations
- a final permutation, being the inverse of IP

The right side shows the handling of the 56-bit key and consists of:

- an initial permutation of the key (PC1) which selects 56-bits out of the 64-bits input, in two 28-bit halves
- 16 stages to generate the 48-bit subkeys using a left circular shift and a permutation of the two 28-bit halves

Initial Permutation (IP) is first step of the data computation. IP reorders the input data bits.



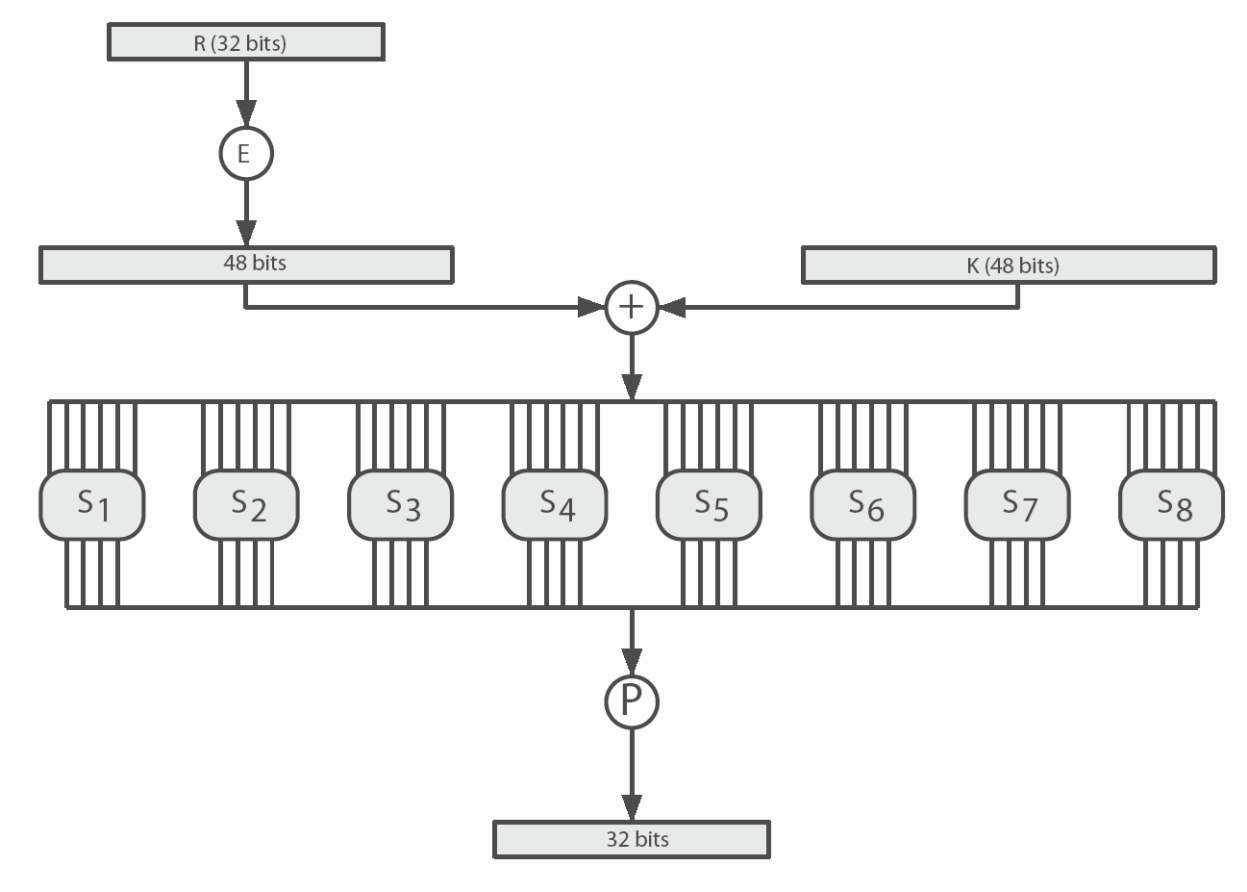
The DES Key Schedule generates the subkeys needed for each data encryption round. A 64-bit key is used as input to the algorithm. It is first processed by Permuted Choice One. The resulting 56-bit key is then treated as two 28-bit quantities C & D. In each round, these are separately processed through a circular left shift (rotation) of 1 or 2 bits. These shifted values serve as input to the next round of the key schedule. They also serve as input to Permuted Choice Two, which produces a 48-bit output that serves as input to the round function F.

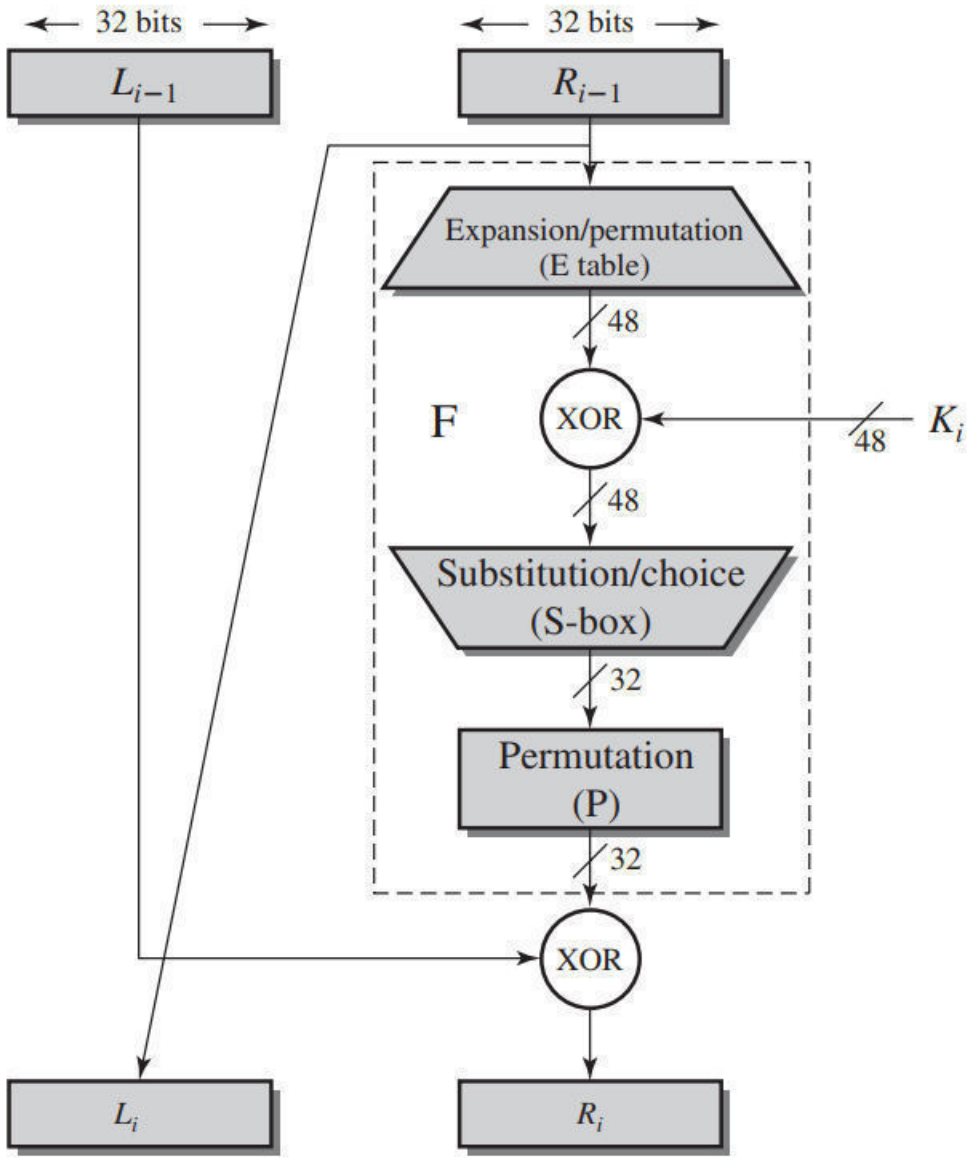
DES Round function uses two 32-bit L & R halves.

$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus \mathrm{F}(R_{i-1}, K_i)$

F takes 32-bit R half and 48-bit subkey:

- expands R to 48-bits using E
- adds to subkey using XOR
- passes through 8 S-boxes to get 32-bit result
- finally permutes using 32-bit P





DES Decryption Overview

DES decryption uses the same algorithm as encryption except that the subkeys are used in reverse order (Sub key 16 to Sub key 01).

Avalanche Effect

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched. DES exhibits a strong avalanche effect.

Suppose the original plain text is 02468aceeca86420 and the original key is 0f1571c947d9e859 and the altered plaintext is 12468aceeca86420 and the altered key is 1f1571c947d9e859.

Round		δ
	02468aceeca86420 12468aceeca86420	1
1	3cf03c0fbad22845 3cf03c0fbad32845	1
2	bad2284599e9b723 bad3284539a9b7a3	5
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18
4	0bae3b9e42415649 171cb8b3ccaca55e	34
5	4241564918b3fa41 ccaca55ed16c3653	37
6	18b3fa419616fe23 d16c3653cf402c68	33
7	9616fe2367117cf2 cf402c682b2cefbc	32
8	67117cf2c11bfc09 2b2cefbc99f91153	33

Round		δ
9	c11bfc09887fbc6c 99f911532eed7d94	32
10	887fbc6c600f7e8b 2eed7d94d0f23094	34
11	600f7e8bf596506e d0f23094455da9c4	37
12	f596506e738538b8 455da9c47f6e3cf3	31
13	738538b8c6a62c4e 7f6e3cf34bc1a8d9	29
14	c6a62c4e56b0bd75 4bc1a8d91e07d409	33
15	56b0bd7575e8fd8f 1e07d4091ce2e6dc	31
16	75e8fd8f25896490 1ce2e6dc365e5f59	32
IP^{-1}	da02ce3a89ecac3b 057cde97d7683f2a	32

Avalanche Effect in DES due to Change in Plaintext

The table above shows that, after just three rounds, 18 bits differ between the two blocks. On completion, the two ciphertexts differ in 32-bit positions.

Round		δ
	02468aceeca86420 02468aceeca86420	0
1	3cf03c0fbad22845 3cf03c0f9ad628c5	3
2	bad2284599e9b723 9ad628c59939136b	11
3	99e9b7230bae3b9e 9939136b768067b7	25
4	0bae3b9e42415649 768067b75a8807c5	29
5	4241564918b3fa41 5a8807c5488dbe94	26
6	18b3fa419616fe23 488dbe94aba7fe53	26
7	9616fe2367117cf2 aba7fe53177d21e4	27
8	67117cf2c11bfc09 177d21e4548f1de4	32

Round		δ
9	c11bfc09887fbc6c 548f1de471f64dfd	34
10	887fbc6c600f7e8b 71f64dfd4279876c	36
11	600f7e8bf596506e 4279876c399fdc0d	32
12	f596506e738538b8 399fdc0d6d208dbb	28
13	738538b8c6a62c4e 6d208dbbb9bdeeaa	33
14	c6a62c4e56b0bd75 b9bdeeaad2c3a56f	30
15	56b0bd7575e8fd8f d2c3a56f2765c1fb	33
16	75e8fd8f25896490 2765c1fb01263dc4	30
IP^{-1}	da02ce3a89ecac3b ee92b50606b62b0b	30

Avalanche Effect in DES due to Change in Key

The results show that about half of the bits in the ciphertext differ and that the avalanche effect is pronounced after just a few rounds due to change in key.

Triple DES

It has been demonstrated through exhaustive key search attacks that DES can be broken. AES is a new cipher alternative to DES. Prior to AES, multiple encryption approach was used with DES implementations. Triple-DES is the most chosen form.

In Triple-DES, 3 encryptions are done. It can be done with 2 keys with E-D-E sequence. It is evident that encrypt operation & decrypt operation are equivalent in security.

$$C = E_{K1}(D_{K2}(E_{K1}(P)))$$

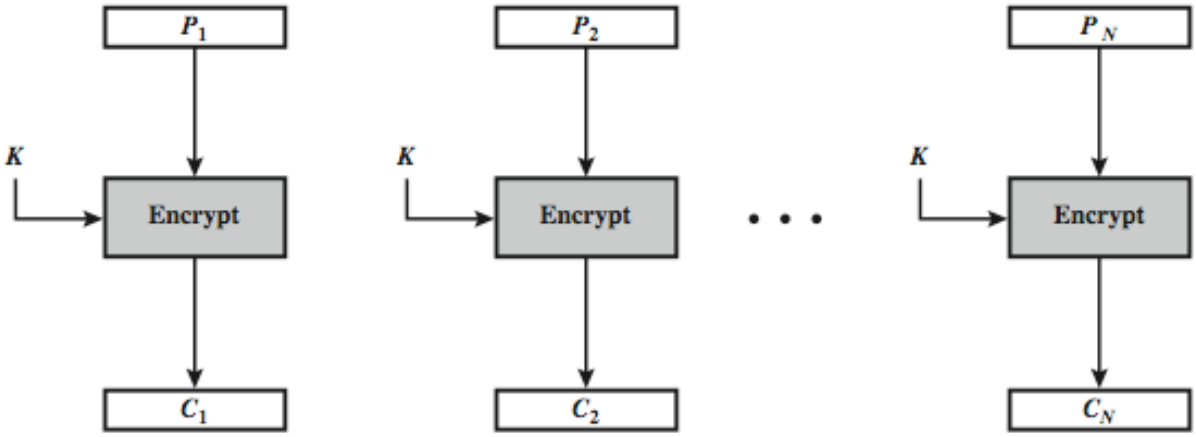
Although are no practical attacks on two-key Triple-DES, there have been several proposed impractical attacks which might become basis of future attacks. Henceforth, Triple-DES with Three-Keys can be used to avoid these possible attacks.

$$C = E_{K3}(D_{K2}(E_{K1}(P)))$$

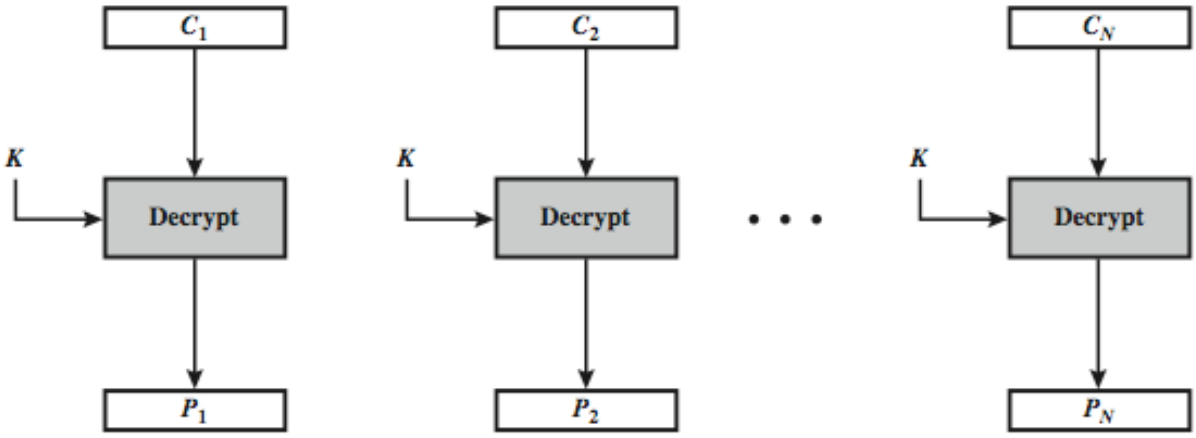
Modes of DES

DES has several **block** and **stream** modes to cover a wide variety of applications. Some of the modes are discussed below.

Electronic Code Book (ECB) Mode



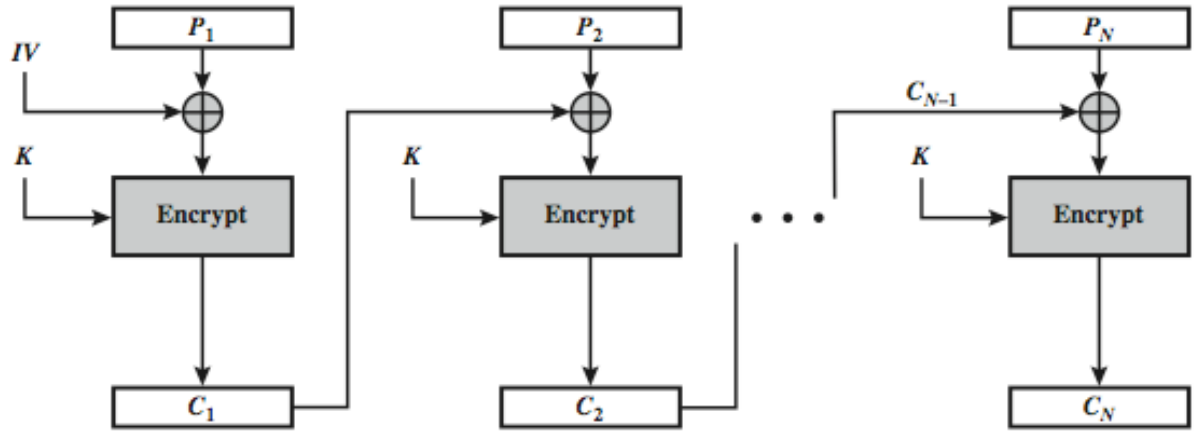
(a) Encryption



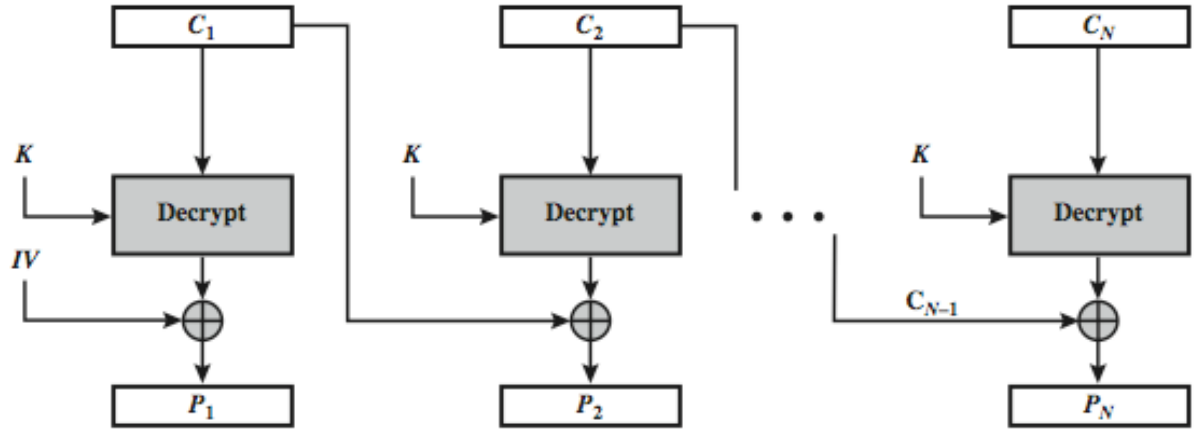
(b) Decryption

In EBC mode, message is broken into independent blocks which are encrypted. Here, each block is a value which is substituted, like a codebook, hence the name. In this mode, each block is encoded independently of the other blocks. It can be said $C_i = E_K(P_i)$

Cipher Block Chaining (CBC) Mode



(a) Encryption

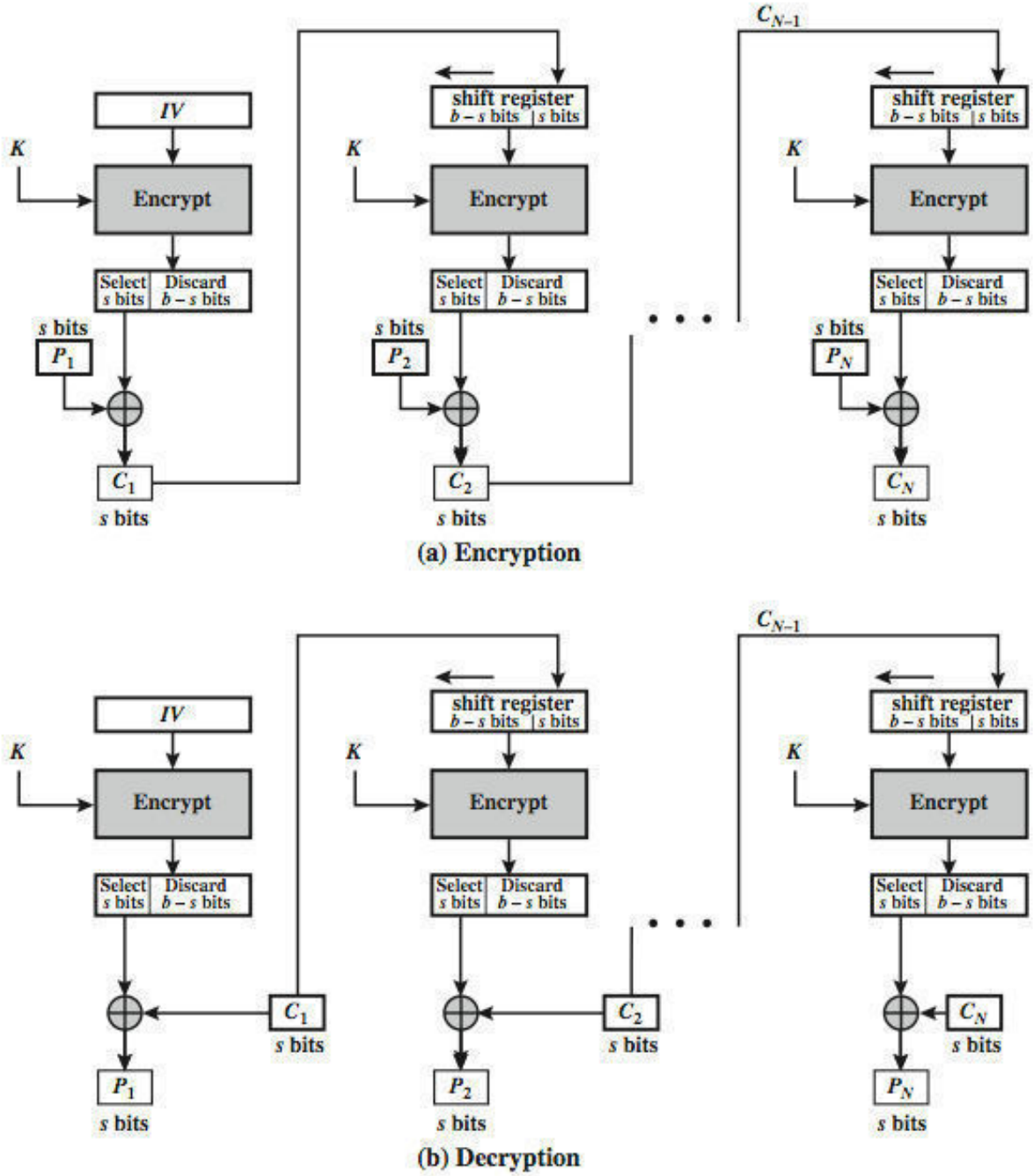


(b) Decryption

In CBC mode, message is broken into blocks and linked together in encryption operation. Each previous cipher block is chained with current plaintext block, hence name. The process uses Initial Vector (IV) to start process. IV must be known to the sender and the receiver.

- $C_i = E_K(P_i \text{ XOR } C_{i-1})$
- $C_{-1} = IV$

Cipher Feed Back (CFB) Mode

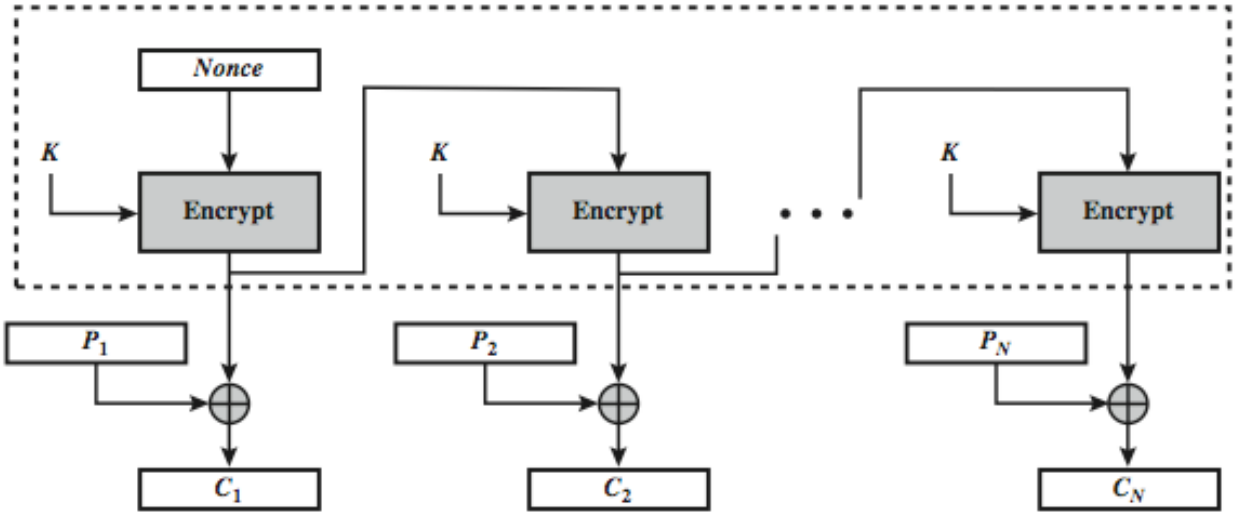


s-bit Cipher Feed Back (CFB-s)

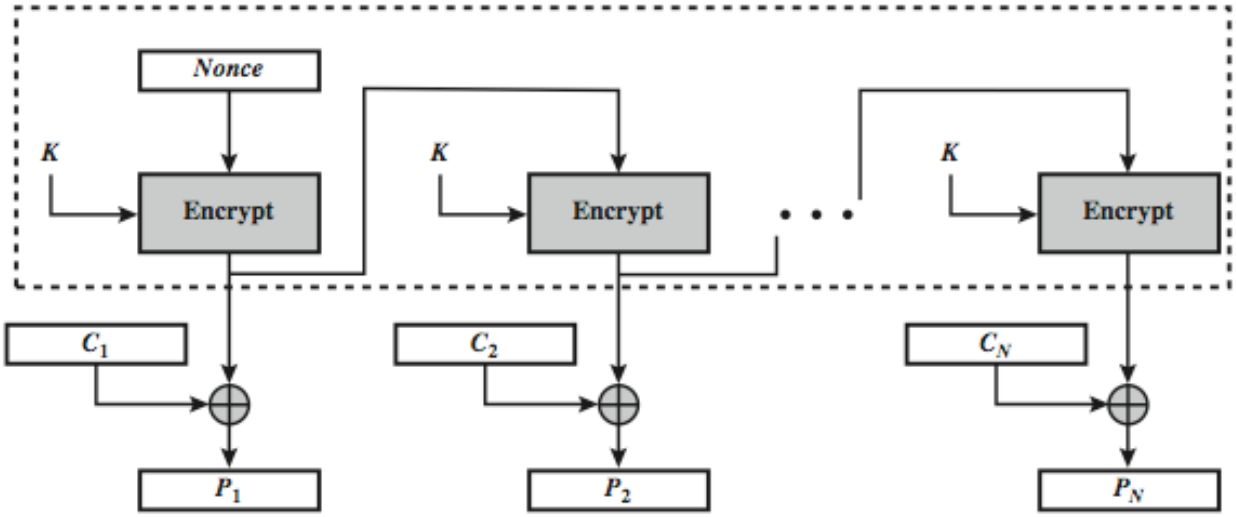
Here, message is treated as a stream of bits and added to the output of the block cipher. The result is feedback for the next stage, hence the name. Standard allows any number of bit (1,8, 64 or 128 etc.) to be feedback, denoted CFB-1, CFB-8, CFB-64, CFB-128 etc.

- $C_i = P_i$ XOR $E_K(C_{i-1})$
- C_{-1} = IV

Output Feed Back (OFB) Mode



(a) Encryption



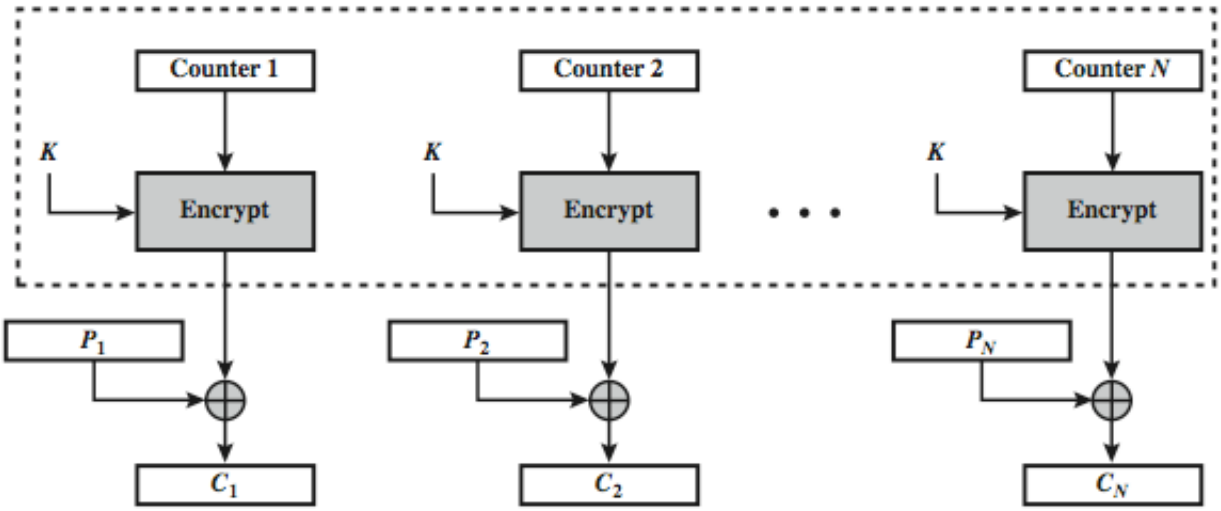
(b) Decryption

Here, Output of cipher is added to message. Output is then feedback (hence name). Feedback is independent of message and can be computed in advance.

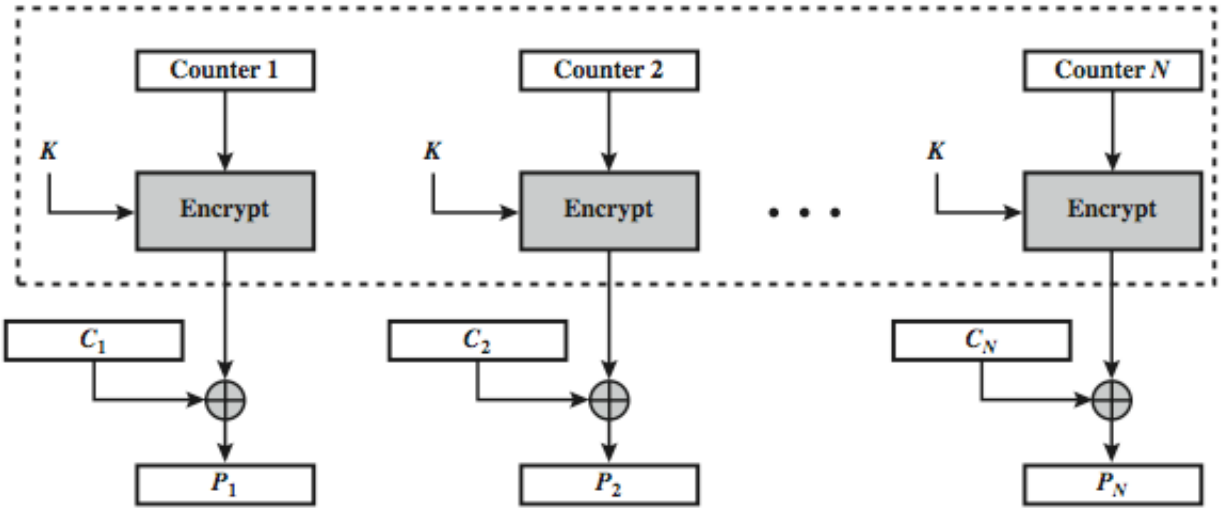
- $O_i = E_K(O_{i-1})$
- $C_i = P_i$ XOR O_i
- $O_{-1} = IV$

IV and nonce are often used interchangeably. However, a careful definition does differentiate between these two concepts. For our purposes, an IV is a nonce with an additional requirement: it must be selected in a nonpredictable way. That is, the IV can't be sequential; it must be random.

Counter (CTR) Mode



(a) Encryption



(b) Decryption

CTR is similar to OFB but encrypts counter value rather than any feedback value. It must have a different key & counter value for every plaintext block.

- $O_i = E_K(i)$
- $C_i = P_i$ XOR O_i

Rivest Shamir Adleman (RSA)

RSA was proposed by Rivest, Shamir & Adleman of MIT in 1977. It is a widely used public-key scheme. The algorithm uses number theory and modular arithmetic along with large integers. It is very a very secure approach due to cost of factoring large numbers.

RSA Encryption/ Decryption

- For encrypting a message M the sender:
  - obtains public key of recipient PU={e,n}
  - computes: $C = M^e \bmod n$, where $0 \le M < n$
- To decrypt the ciphertext C the owner:
  - uses their private key PR={d,n}
  - computes: $M = C^d \bmod n$
- It should be noted that the message M must be smaller than the modulus n

RSA Key Set up

Each user generates a public/private key pair by

- selecting two large primes at random: p, q
- computing their system modulus n = p . q
  - note, $\phi(n)=(p-1)(q-1)$
- selecting at random the encryption key e
  - where $1<e<\phi(n)$, $\gcd(e, \phi(n))=1$
- solving the following equation to find decryption key d
  - $e \cdot d=1 \bmod \phi(n)$ and $0 \le d \le n$
  - By Euler's theorem, $e \cdot d = 1 + k \cdot \phi(n)$ for some k

The public encryption key is PU={e,n} which is published and the private decryption key is PR={d,n} which is kept secret.

RSA Example

- **Key Setup**
  - At first, p and q are selected; p=17 & q=11
  - Then, n is calculated. $n = p \times q = 17 \times 11 = 187$
  - $\phi(n)$ is calculate. $\phi(n)=(p-1) \times (q-1) = 16 \times 10 = 160$
  - e is selected so that gcd(e,160) = 1; e=7
  - d is determined. $d \times e = 1 \bmod 160$ & $0 \le d \le 187$. d=23 as, $23 \times 7 = 161 = 10 \times 160 + 1$
  - Public key PU= {7,187} is published.
  - Private key PR= {23,187} is kept secret.
- **Encryption/Decryption**
  Sample RSA encryption/decryption is:
  - Given message M = 88 (nb. 88<187)
  - Encryption: $C = 88^7 \bmod 187 = 11$
    - Exploiting the properties of modular arithmetic, following can be done:
      $88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$
  - Decryption: $M = 11^{23} \bmod 187 = 88$

RSA Example with text

p = 73, q = 151
n = 11023
ø(n) = 10800
e = 11
d = 5891

Text = How are you?

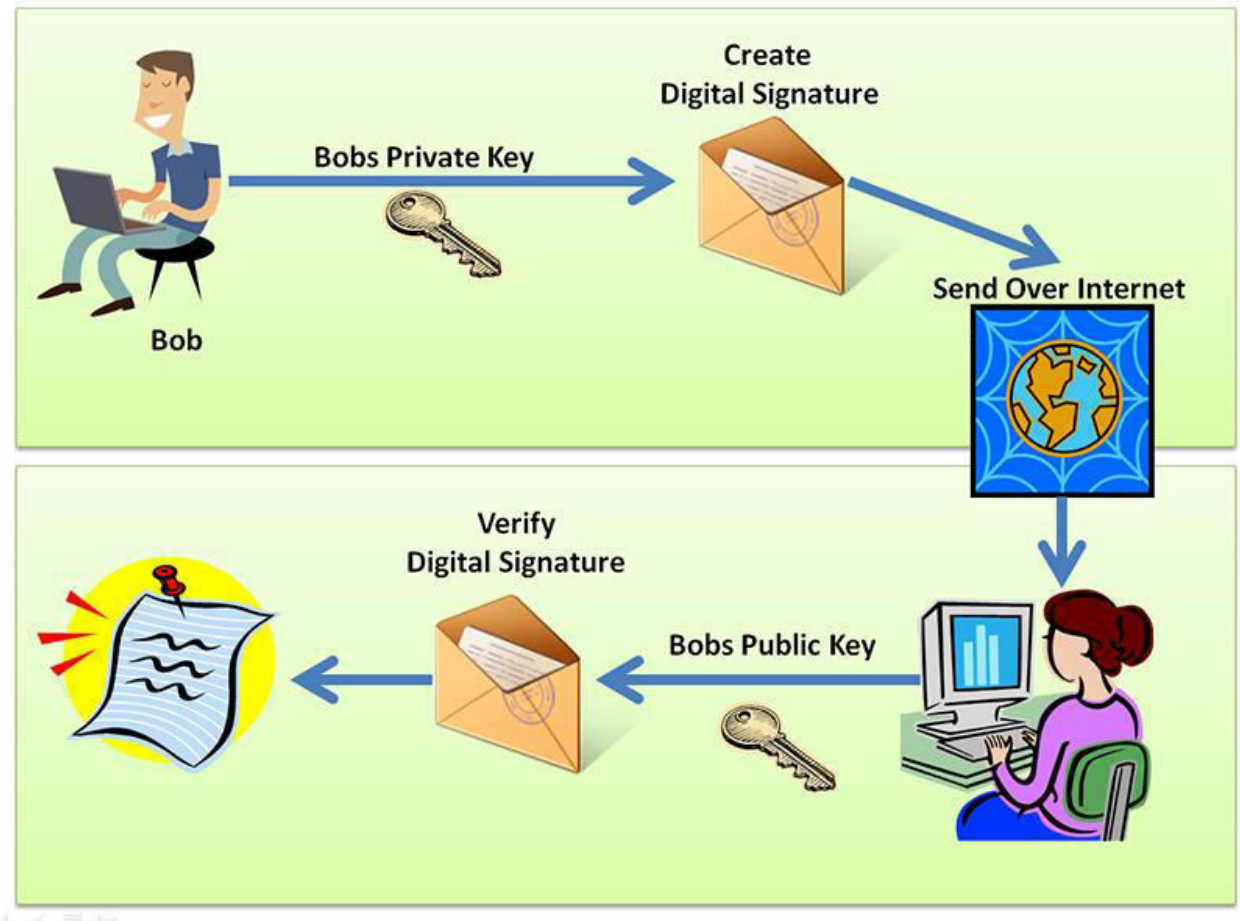
H=	33	a=	00	y=	24
o=	14	r=	17	o=	14
w=	22	e=	04	u=	20
_	62	_	62	?=	66

$M_1 = 3314$ $M_2 = 2262$ $M_3 = 0017$
$M_4 = 0462$ $M_5 = 2414$ $M_6 = 2066$

$C_1 = 3314^{11} \bmod 11023 = 10260$
$C_2 = 2262^{11} \bmod 11023 = 9489$
$C_3 = 17^{11} \bmod 11023 = 1782$
$C_4 = 462^{11} \bmod 11023 = 727$
$C_5 = 2414^{11} \bmod 11023 = 10032$
$C_6 = 2006^{11} \bmod 11023 = 2253$

$M_1 = 10260^{5891} \bmod 11023 = 3314$
$M_2 = 9489^{5891} \bmod 11023 = 2262$
$M_3 = 1782^{5891} \bmod 11023 = 0017$
$M_4 = 727^{5891} \bmod 11023 = 0462$
$M_5 = 10032^{5891} \bmod 11023 = 2414$
$M_6 = 2253^{5891} \bmod 11023 = 2006$

Basics of Digital Signatures

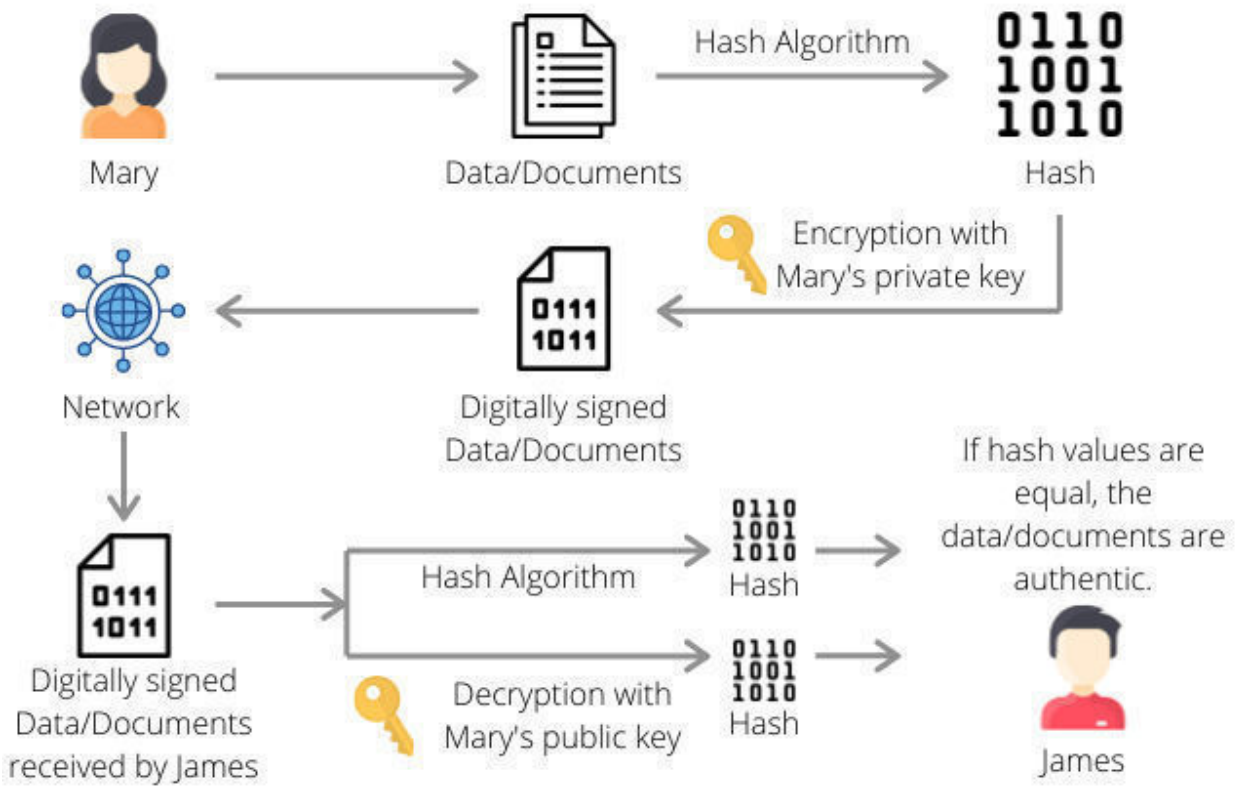


Digital Signature is a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate. **In case of digital signature**, message is encrypted with the private key and decrypted with the public key.

A digital signature is a mathematical method for confirming the veracity and consistency of a digital message, document, or piece of software. It gives much more intrinsic security than a handwritten signature or stamped seal, yet it is the digital version of them. The issue of tampering and impersonation in digital communications is addressed by a digital signature.

Public key cryptography, commonly referred to as asymmetric cryptography, is the foundation of digital signatures. Two keys are generated, one private and one public, using a public key algorithm like RSA. This results in a pair of keys that are mathematically connected. Public key cryptography's two mutually authenticating cryptographic keys are how digital signatures function. The person who generates the digital signature uses a private key to encrypt the data associated with the signature for encryption and decryption. With the signer's public key, that data can only be decrypted. The signature or the document

may be flawed if the recipient is unable to open the file using the signer's public key. Digital signatures are verified in this way.



To create a digital signature, signing software is used to provide a one-way hash of the electronic data to be signed.

A hash is a fixed-length string of letters and numbers generated by an algorithm. The digital signature creator's private key is used to encrypt the hash. The encrypted hash, along with other information, such as the hashing algorithm, is the digital signature.

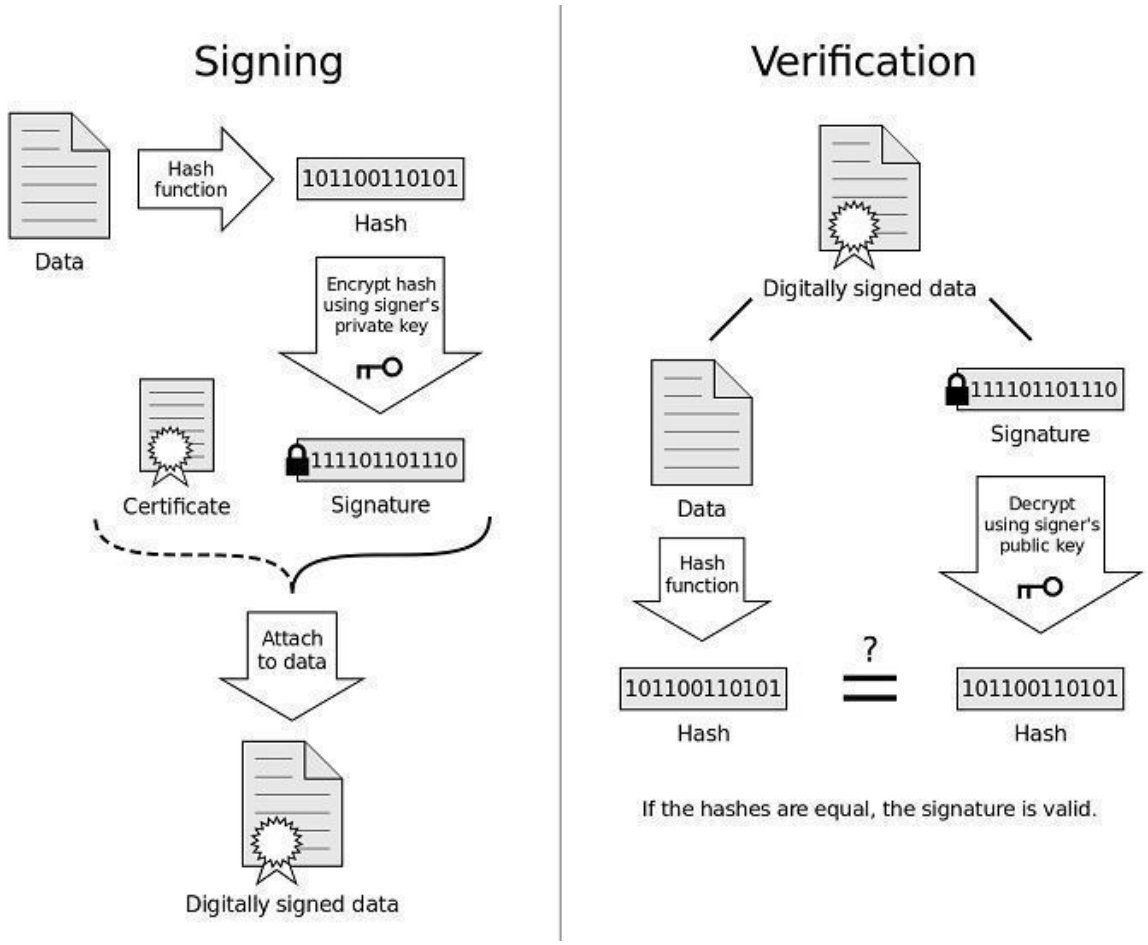
The reason for **encrypting the hash instead of the entire message** or document is because a hash function can convert an arbitrary input into a fixed-length value, which is usually much shorter. This saves time, as hashing is much faster than signing.

The value of a hash is unique to the hashed data. Any change in the data, even a modification to a single character, results in a different value. This attribute enables others to use the signer's public key to decrypt the hash to validate the integrity of the data.

If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. But, if the two hashes don't match, the data has either been tampered with in some way and is compromised or the signature was created with a

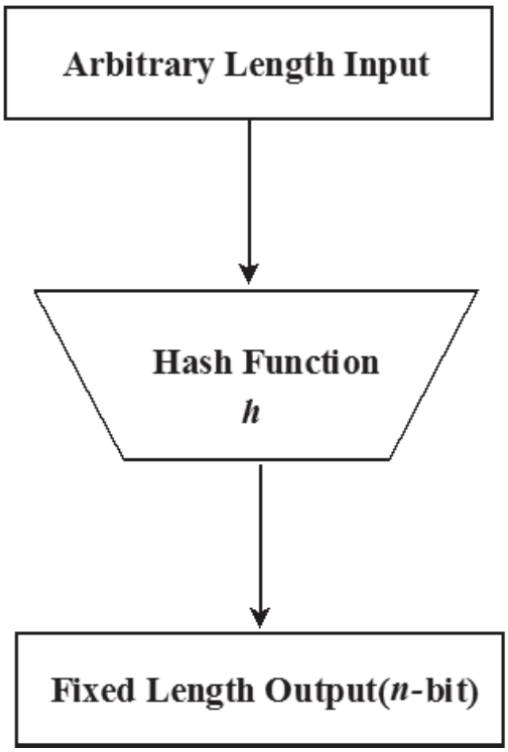
private key that doesn't correspond to the public key presented by the signer. This signals an issue with authentication.

Digital certificates, also called public key certificates, are used to verify that the public key belongs to the issuer. Digital certificates contain the public key, information about its owner, expiration dates and the digital signature of the certificate's issuer. Digital certificates are issued by trusted third-party certificate authorities (CAs). The party sending the document and the person signing it must agree to use a given CA.



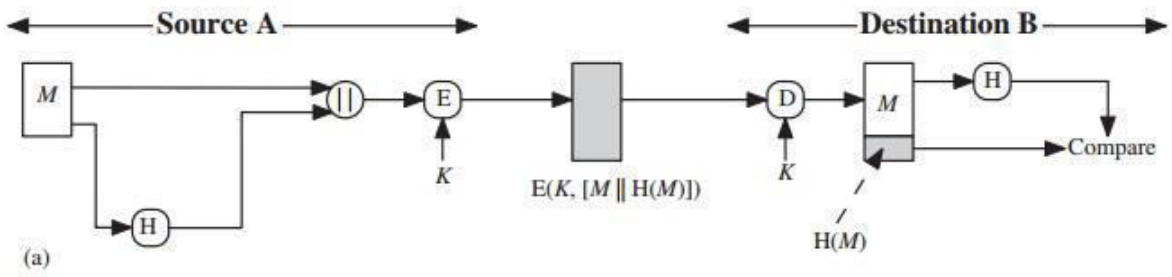
Basics of Cryptographic Hash Function

A hash function maps a variable-length message into a fixed-length hash value, or message digest. A hash function H accepts a variable-length block of data as input and produces a fixed-size hash value h = H(M). The kind of hash function needed for security applications is referred to as a cryptographic hash function.

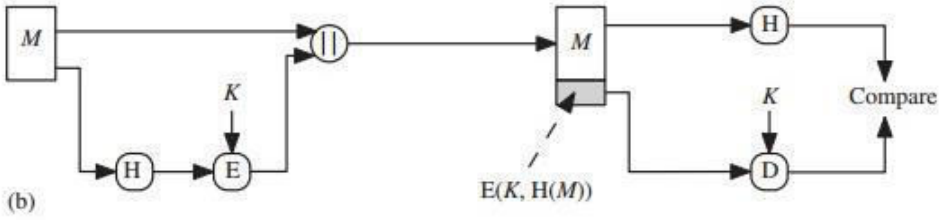


Cryptographic Hash Function and Message Authentication

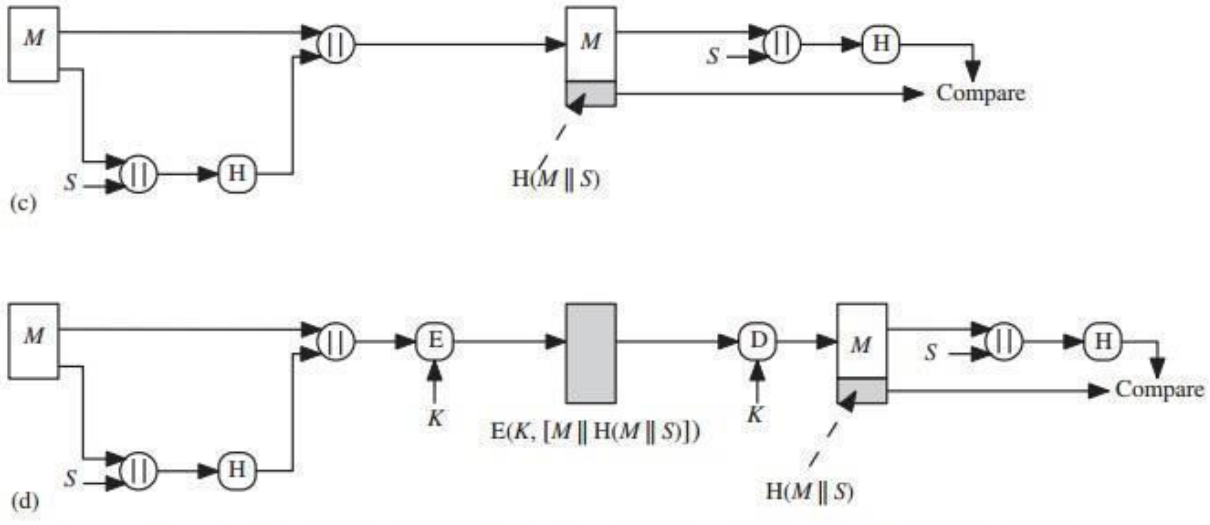
Hash functions are often used to determine whether or not data has changed. Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent. When a hash function is used to provide message authentication, the hash function value is often referred to as a message digest.



In the case of figure (a): The message plus concatenated hash code is encrypted using symmetric encryption. Because only A and B share the secret key, the message must have come from A and has not been altered. The hash code provides the structure or redundancy required to achieve authentication. Because encryption is applied to the entire message plus hash code, confidentiality is also provided.



In the case of figure (b): Only the hash code is encrypted, using symmetric encryption. This reduces the processing burden for those applications that do not require confidentiality.

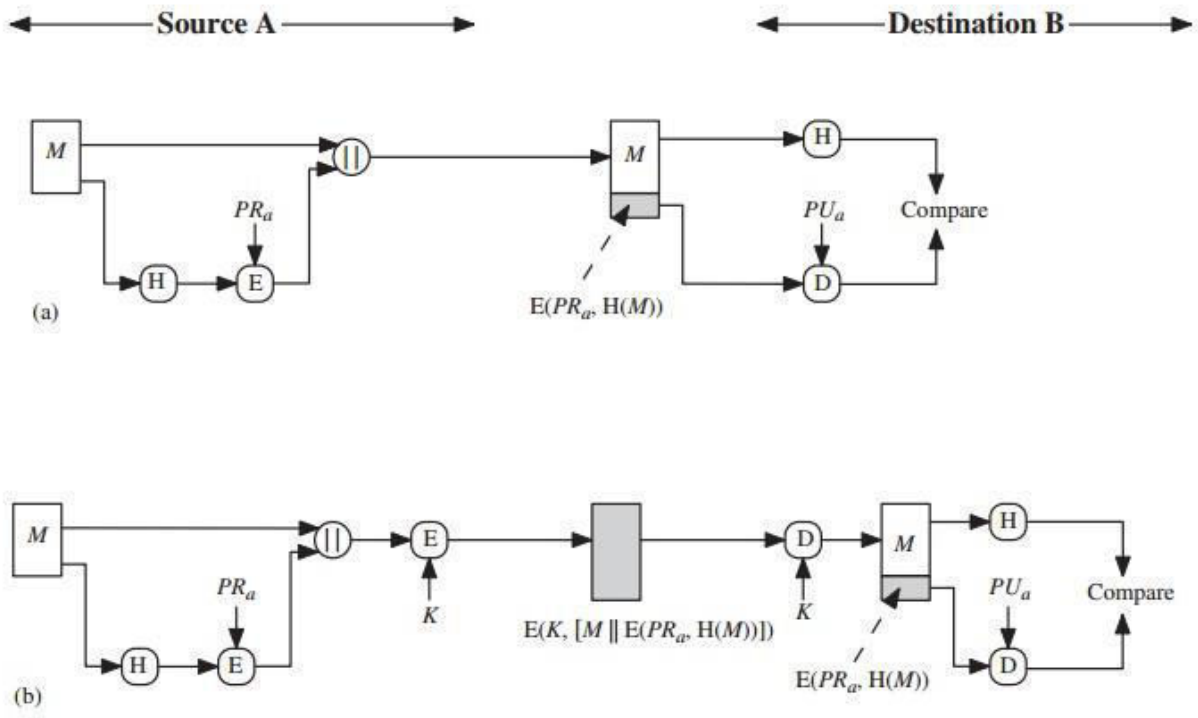


In the case of figure (c): It is possible to use a hash function but no encryption for message authentication. The technique assumes that the two communicating parties share a common secret value S. A computes the hash value over the concatenation of M and S and appends the resulting hash value to. Because B possesses the knowledge of S, it can recompute the hash value to verify. Since the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message.

In the case of figure (d): Confidentiality can be added to the approach of (c) by encrypting the entire message plus the hash code.

Cryptographic Hash Function and Digital Signature

In the case of the digital signature, the hash value of a message is encrypted with a user's private key. Anyone who knows the user's public key can verify the integrity of the message that is associated with the digital signature. In this case, an attacker who wishes to alter the message would need to know the user's private key.



In case of (a): The hash code is encrypted, with the sender's private key. It also provides a digital signature, because only the sender could have produced the encrypted hash code. In fact, this is the essence of the digital signature technique.

In case of (b): If confidentiality as well as a digital signature is desired, then the message as well as the private-key encrypted hash code can be encrypted using a symmetric secret key.