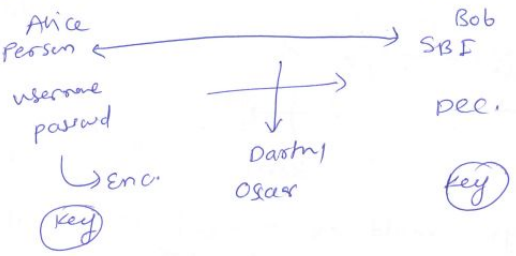
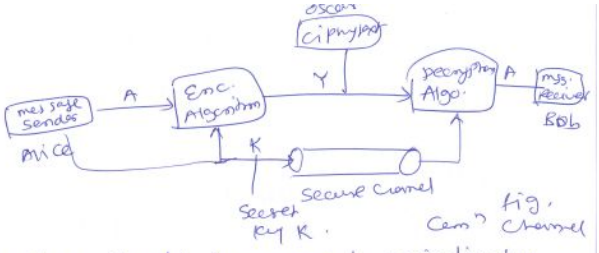
CNS

- Secure comn over unsecure channel.



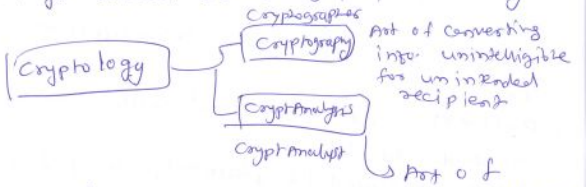
Cipher text → o/p after Encryption

- plain text :- the info. that alice wants to send to Bob.
- Alice encrypts the plain text, using the predetermined key, and send the resulting cypher text to Bob over the public channel.
- Darth cannot determine what the plain text was.
- Bob knows the decryption key, he can decrypt the cipher text & get the plain text



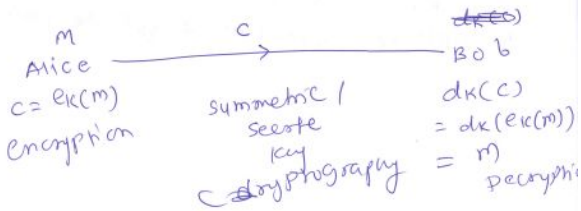
Comm. fig. Channel

- Keys should be changed periodically.



Types of cryptography

- Symetric (secret-key)
- Assymetric (public key)



Cryptosystem

- It is a five tuple (P, C, K, E, D)

Plaintext Space (P) : Set of all possible plain texts.

Ciphertext Space (C) :- Set of all possible ciphers texts.

Key space (K) :- Set of all possible keys.

E :- Set of all possible encryption Rules

D :- Set of all possible decryption Rules

- For each $k \in K$, there is an encryption rule $e_k \in E$ and a corresponding decryption rule $d_k \in D$ such that, $d_k(e_k(x)) = x$ for every plaintext $x \in P$.

$E \Rightarrow \quad P \times K \rightarrow C \Rightarrow d_k(m) = c$

$D = \quad C \times K \rightarrow P \quad d_k(c) = m$

- For every $k \in K$, $\exists$ a $e_k \in E$ and $d_k \in D$ such that

$$d_k(e_k(m)) = m \quad \forall m \in P$$

Classical cryptosystem

Shift cipher

$P = Z_{26} = \{0, 1, 2 \dots 25\}$

$C = Z_{26}$

$K = Z_{26}$

$K = 3$

$y = (x + K) \bmod 26 \quad x \in P$

$x = (y - K) \bmod 26 \quad y \in C$

A	B			Z
0	1	–	–	25

Key K = 11

SGGSITDEPT

0	1	2	3	4	5	6	7	8	9	10
A	B	C	D	E	F	G	H	I	J	K

11	12	13	14	15	16	17	18	19	20	21
L	M	N	O	P	Q	R	S	T	U	V

22	23	24	25
W	X	Y	Z

S ⇒ 18 , G ⇒ 6 , I ⇒ 8 , T ⇒ 19 ,

D ⇒ 3 , E ⇒ 4 , P ⇒ 15 ,

S	G	G	S	I	T	D	E	P	T
18	6	6	18	8	19	3	4	15	19

C D R R D T E O P A E

$$
\begin{array}{lllllll}
\text{p} & \longrightarrow & 15 & \longrightarrow & 15+3 \equiv 18 \pmod{26} & \longrightarrow & \text{S} \\
\text{i} & \longrightarrow & 8 & \longrightarrow & 8+3 \equiv 11 \pmod{26} & \longrightarrow & \text{L} \\
\text{z} & \longrightarrow & 25 & \longrightarrow & 25+3 \equiv 2 \pmod{26} & \longrightarrow & \text{C} \\
\text{z} & \longrightarrow & 25 & \longrightarrow & 25+3 \equiv 2 \pmod{26} & \longrightarrow & \text{C} \\
\text{a} & \longrightarrow & 0 & \longrightarrow & 0+3 \equiv 3 \pmod{26} & \longrightarrow & \text{D}
\end{array}
$$

Information Technology⇒ Tyqzcxletzy Epnsyzwzrj

key 11

$C = (p+11) \bmod 26$

$m = (c+11) \bmod 26$

modulo Addition & subtraction

18	6	6	18	8	19	3	4	15	19
S	G	G	S	I	T	D	E	P	T

Caesar cipher $\Rightarrow K = 3$

- Oscar is getting cipher text.
- The attacker has to perform 26 possibilities of keys. ; when he gets meaningful text he stops. ; $K = 0, 1, 2, \ldots 25$
- Shift cipher is not secure

Substitution cipher

- $P = C =$ set of Eng. Alphabets $\Rightarrow A$

$= \{A, B, \ldots Z\}$

$P = \{a, b, \ldots z\}$

$C = \{A, B, \ldots Z\}$

$\phi : A \to A$

$K =$ set of all possible permutations of 26 alphabetic characters — permutation

- For each permutation $\phi \in K$

$e_\phi(x) = \phi(x)$ for $x \in P$

$d_\phi(y) = \phi^{-1}(y)$ for $y \in C$ where ϕ^{-1} is the inverse permutation

Example

Encryption

a	b	c	d	e	f	g	h	i	j
X	N	Y	A	H	P	O	G	Z	Q

k	l	m	n	o	p	q	r	s	t
W	B	T	S	F	L	R	C	V	M

u	v	w	x	y	z
U	E	K	J	D	I

Decryption ϕ^{-1}

A	B	C	D	E	F	G	H
d	l	r	y	v	o	h	e

I	J	K	L	M	N	O	P
z	x	w	p	t	b	g	f

Q	R	S	T	U	V	W
j	q	n	m	u	s	k

X	Y	Z
a	c	i

Plaintext alphabet: 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 alphabet: 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

- N → D
- A → Q
- N → D
- D → R
- E → T
- D → R

So, "NANDED" becomes "DQDRTR".

Encryption

sggsit

VOOVZM Ciphertext

sggsit plaintext

$P = C = \{a, b, c, \dots z\} = A$

$K = \{\phi \mid \phi \text{ is a permutation of } A\}$

$|K| = 26! \Rightarrow 4 \times 10^{26} \approx 2^{88}$ 2) for getting plaintext

- For a key of an alphabet with 26 characters First letter $\Rightarrow$ 26 characters, second have 25 characters ... last one get 1

$(26 \times 25 \times 24 \dots 1) \approx 2^{88}$

$\log_2(26!) \Rightarrow x$

$26! = 2^x$

$\log(26) + \log(25) + \log(24) - + \log_2(1)$

Frequency Analysis

- For english alphabets e is most frequent alphabet (Example of mis)

Polyalphabetic cipher

Example Vigenere cipher ; let m be a +ve integer

$P = (Z_{26})^m = C = K$

$K = (K_1, K_2 \dots K_m) \in Z_{26}^m \Rightarrow Z_{26} \times Z_{26} \times \dots Z_{26}$

$x = (x_1, x_2 \dots, x_m)$

$e_K(x) = (x_1+k_1, x_2+k_2 + \dots x_m+k_m) = y_0$

$= (y_1, y_2 \dots y_m)$

$d_K(y) = (y_1-k_1, y_2-k_2, \dots y_m-k_m)$

Example

$Z_{26} = \{0, 1, 2, \dots 25\}$

A B C Z

$m = 6$ $K = CIPHER$

$= (2, 8, 15, 7, 4, 17)$

- Plaintext : "thiscryptosystem is not secure"
- Encryption : add module 26

19	7	8	18	2	17	24	15	19	14	18	24	18	19	4	12
2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7
21	15	23	25	6	8	0	23	8	21	22	15	20	1	19	19

8	18	13	14	19	18	4	2	20	17	4
4	17	2	8	15	7	4	17	2	8	15
12	9	15	22	8	25	8	19	22	25	19

Ciphertext

V P X Z G I A X I V W P U B T T M J P W I Z I T W Z T

plaintext is mapped to other characters in cipher text.

- cryptanalysis depends on key.

Transposition / Permutation cipher (Rail fence)

meet me after the party is over

m	e	m	a	t	r	h	p	r	y	s	v	r
e	t	e	f	e	t	e	a	t	i	o	e	

ciphertext m e m a t r h p r y s v r e t e f e t e

a

- m is a +ve integer
- $P = C = (Z_{26})^m$
- $K = \{ \Pi : \{1, 2, \ldots m\} \to \{1, 2, 3 \ldots m\}$
- $K = \Pi \in K$, $e_\Pi(x) = (x_{\Pi(1)}, x_{\Pi(2)} \ldots x_{\Pi(m)})$

  $y = (y_1 \quad y_2 \ldots y_m)$

  $d_K(y) = \{y_{\Pi^{-1}(1)}, y_{\Pi^{-1}(2)}, \ldots y_{\Pi^{-1}(m)}\}$

  Π^{-1} is the inverse permutation of Π

ex. $m = 6$

key is following permutation Π

Swapping →

x	1	2	3	4	5	6
$\Pi(x)$	3	5	1	6	4	2

Inverse permutation

x	1	2	3	4	5	6
$\Pi^{-1}(x)$	3	6	1	5	2	4

Permutation Pattern : (3, 1, 4, 6, 2, 5)
PLain Text: A C T I V E
Cipher Text: T A I E C V

Permutation Pattern: (3, 1, 4, 6, 2, 5)
Inverse Permutation Pattern: (2, 5, 1, 3, 6, 4)

Let's consider a permutation σ given by:
$\sigma = (3, 1, 4, 6, 2, 5)$

This means:

- $\sigma(1) = 3$
- $\sigma(2) = 1$
- $\sigma(3) = 4$
- $\sigma(4) = 6$
- $\sigma(5) = 2$
- $\sigma(6) = 5$

To find the inverse permutation σ^{-1}, we need to determine which element maps to each position:

- Since $\sigma(1) = 3$, $\sigma^{-1}(3) = 1$
- Since $\sigma(2) = 1$, $\sigma^{-1}(1) = 2$
- Since $\sigma(3) = 4$, $\sigma^{-1}(4) = 3$
- Since $\sigma(4) = 6$, $\sigma^{-1}(6) = 4$
- Since $\sigma(5) = 2$, $\sigma^{-1}(2) = 5$
- Since $\sigma(6) = 5$, $\sigma^{-1}(5) = 6$

Thus, the inverse permutation σ^{-1} is:
$\sigma^{-1} = (2, 5, 1, 3, 6, 4)$

Plaintext :- "defendthehillstopatsunset"

defend | thehil | ltopat | sunset

Rearrange according to π

fnddee | eithlh | oltept | nestsu

ciphertext : "FNDDEEEITLHHOALTPTNESTSU"

decryption can be done using π⁻¹

	1	2	3	4	5	6
π	3	5	1	6	4	2

$x_1 x_2 x_3 x_4 x_5 x_6$
defend

$x_{\pi(1)} x_{\pi(2)} x_{\pi(3)} x_{\pi(4)} x_{\pi(5)} x_{\pi(6)}$
$x_3 x_5 x_1 x_6 x_4 x_2$
f n d d e e

playfair cipher

Shift cipher, substitution cipher

$26! \approx 2^{88}$ ⇒ monoalphabetic cipher

26

polyalphabetic ← vigenere

Transposition / Permutation

Rules of Playfair Cipher

- If the letters are in the **same row**, replace each with the letter immediately **to its right** (wrapping around to the beginning of the row if necessary).
- If the letters are in the **same column**, replace each with the letter immediately **below it** (wrapping around to the top of the column if necessary).
- If the letters **form a rectangle**, replace each with the letter on the **same row but in the column of the other letter** of the pair.

Playfair Cipher

“Why, don’t you?”

WH YD ON TY OU
YI EA ES VK EZ

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

Cryptographic algorithms and protocols

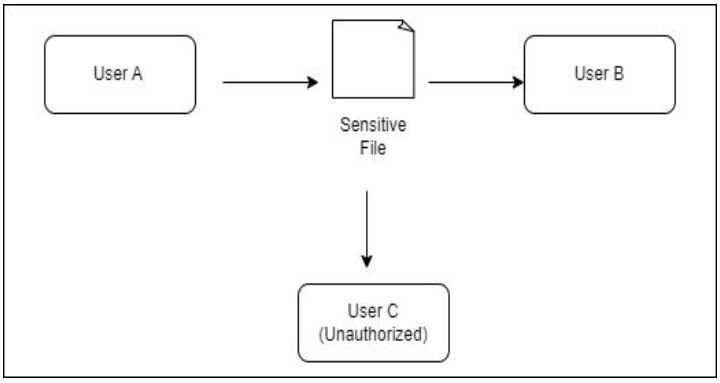
- **Symmetric encryption**: Uses the same key for both encryption and decryption. The key must be kept secret, and both parties must have access to the same key.
- **Asymmetric encryption**: Uses a pair of keys: a public key for encryption and a private key for decryption. The public key can be shared openly, while the private key is kept secret.
- **Data integrity algorithms**: Used to protect blocks of data, such as messages, from alteration.
- **Authentication protocols**: These are schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities.

Network and Internet security

- The field of network and Internet security consists of measures to **deter, prevent, detect, and correct security violations** that involve the transmission of information.

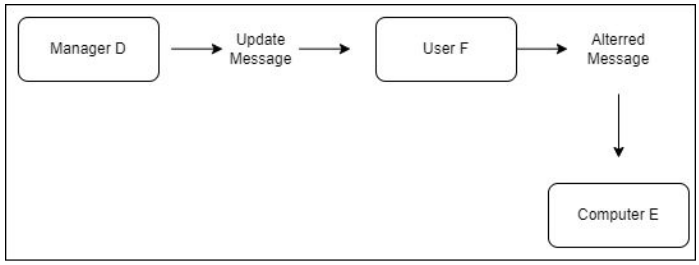
1. Unauthorized Monitoring

User A transmits a file with sensitive information to User B. User C intercepts the transmission.



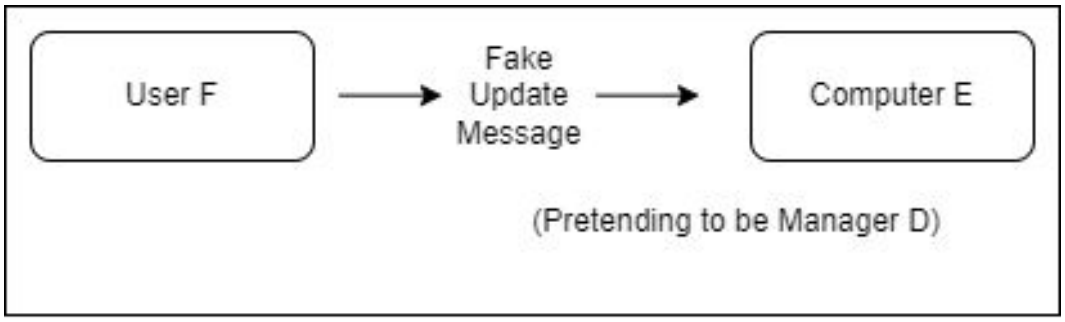
2. Message Interception and Alteration

- Network Manager D sends an update message to Computer E. User F intercepts and alters the message before forwarding it.



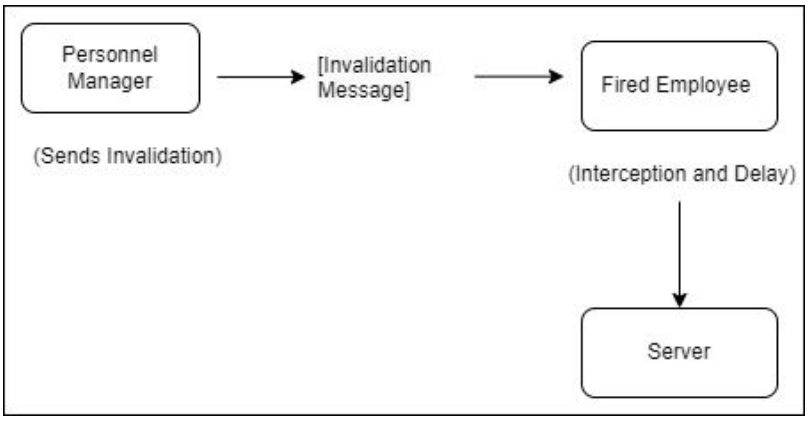
3. Message Fabrication

- User F fabricates a message pretending to be from Network Manager D and sends it to Computer E.



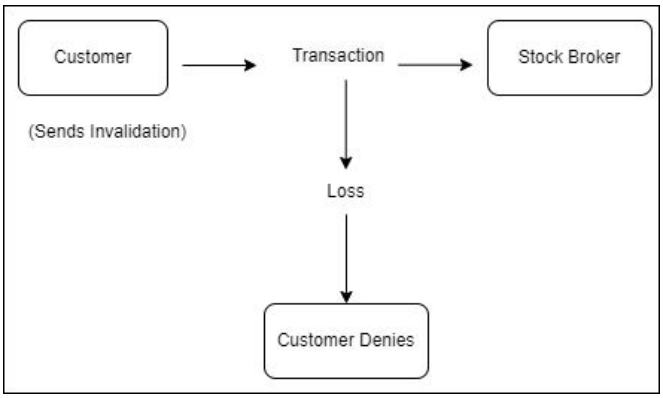
4. Message Delay

- A personnel manager sends an account invalidation(proving wrong) message to a server. The fired employee intercepts and delays the message to make a final access.

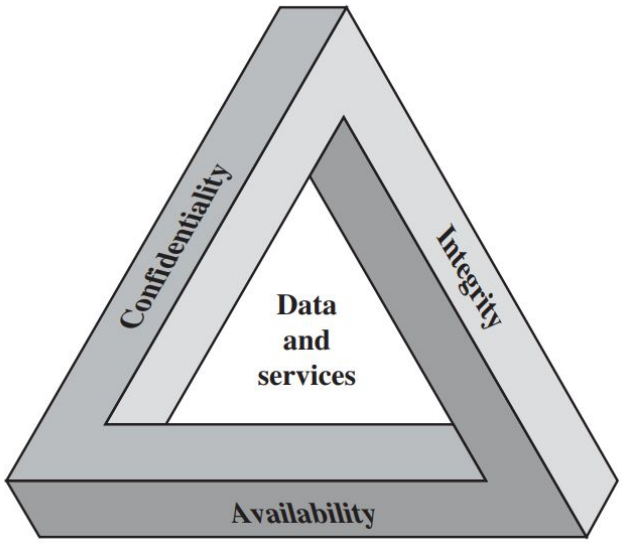


5. Message Denial

- A customer sends instructions to a stockbroker. Later, the customer denies sending the message after the investments lose value.



The Security Requirements Triad



- **Confidentiality**: Ensures that in**formation is accessible only to those authorized** to have access. A loss of confidentiality means unauthorized disclosure of information.
- **Integrity**: Protects information from being altered in an unauthorized way, ensuring non repudiation and authenticity. A loss of integrity refers to unauthorized modification or destruction of information.
- **Availability**: Ensures that information and **resources are accessible when needed.** A loss of availability means disruption of access to or use of information or an information system.

- **Authenticity** ensures that users and information **sources are genuine and verified**
- **Accountability** requires actions to be **traceable** to their origin to support security measures like nonrepudiation, deterrence, and forensic analysis.

Confidentiality:

- Example: Data is encrypted with passwords to protect customers' personal and financial information (for **example, account numbers, transaction details**) while it is transmitted on the internet.
- Importance: It is used to keep impostor away from any data that they cannot reach unless they have the Authority to entitle them to see or change it.

Integrity:

- Example: Checks on the **validity of the data are established** so that the transactions are accurate and free from fraud. Additionally, audit logs keep a record of all the transactions.
- Importance: It is supposed to verify the extent to which the information is accurate and unaltered, so the integrity of the data is authentic.

Availability:

- Example: The banking system **uses replicated servers and backup** systems to allow users to access their accounts and carry out the transactions every time in case of failure of a server.
- Importance: The reason why users can use the system is because of its constant reliability and availability during demand periods. It is also kind of responsible as it does not make finer decisions for transporting data.

Find the solution in terms of CIA Triad

- Once the student submitted their assignment online, a classmate intercepted and altered it after it had been sent to the teacher. As a result, the student received a lower grade because the assignment did not accurately reflect their original work.
- How to address this issue?

Solution

- Tool: Adobe Acrobat or another program where digital signatures are supported.

- How It Helps: **Digital signatures** can prove the **originality** and indestructibility of the document; thus, we are guaranteed that the document was not altered since the signature.

Find the solution in terms of CIA Triad

- Sensitive student data such as the grades and personal details is looked at by unwanted people, exposing details that should remain private.

Solution

- In a scenario like this, a student's private data, for example, these scores or details related to one's person, were accessible to those who did not have a right to do so through a breach in information.
- Solution: Apply role-based **access controls** (RBAC) to the school information systems.
- Set strong passwords, regularly change access permissions, and introduce multi factor authentication (MFA) for better safety.

Find the solution in terms of CIA Triad

- An academic institution is having online tests wherein the students answer by using computers. On the other hand, issues are concerned about such things as cheating and unauthorized access to exam materials.

Solution

- Solution: Ensure secure delivery of examination questions and materials against unauthorized access or tampering.
- Implement: Both **in-transit and at-rest encryption** of examination content, transfer through secure protocols like **HTTPS**. This functionality, however, remains with access limited only to those authorized.

The Challenges of Computer Security

- **Complexity in Security Requirements:** Some security services, like confidentiality, authentication, and integrity, are easy to conceive but **require complex mechanisms for their implementation**, often subtle reasoning.

- **Designing Under Attack**: The security mechanisms will be **designed under scrutiny of possible attacks** exploiting unexpected weaknesses and hence require a different way of problem-solving.

- **Counterintuitive Security Procedures**: Effective security measures often turn out to be **counterintuitive (does not happen in the way you would expect it to**) at first glance because **they must deal with elaborate threats** that are not immediately obvious from basic security requirements.

- **Complexity Beyond Algorithms:** Security mechanisms not only depend on algorithms, but also require secret information, typically connected with keys, besides communication protocols, which can give **complexity to their design and deployment.**

- **Battle of attacker and Defender**: Security is an ongoing battle between attackers who are continuously on the lookout for loopholes and defenders trying to shut them all
- **Perception about Security Investment**: Unless a security breach takes place, users and managers may not realize the benefits of a security investment and hence underestimate its importance.
- **Challenges of Monitoring**: Security needs to be monitored, and monitoring in today's fast and overloaded environments is challenging.
- **Security vs. Usability**: Effective security measures are often perceived as impediments to efficient and easy utilization of systems or information.

- **Security attack**: Any **action** that compromises the security of information owned by an organization.
- **Security mechanism**: A process (or a device incorporating such a process) that is designed to **detect, prevent, or recover** from a security attack.
- **Security service**: A processing or **communication serv**ice that enhances the security of the data processing systems and the **information transfers** of an organization.

Security Attacks

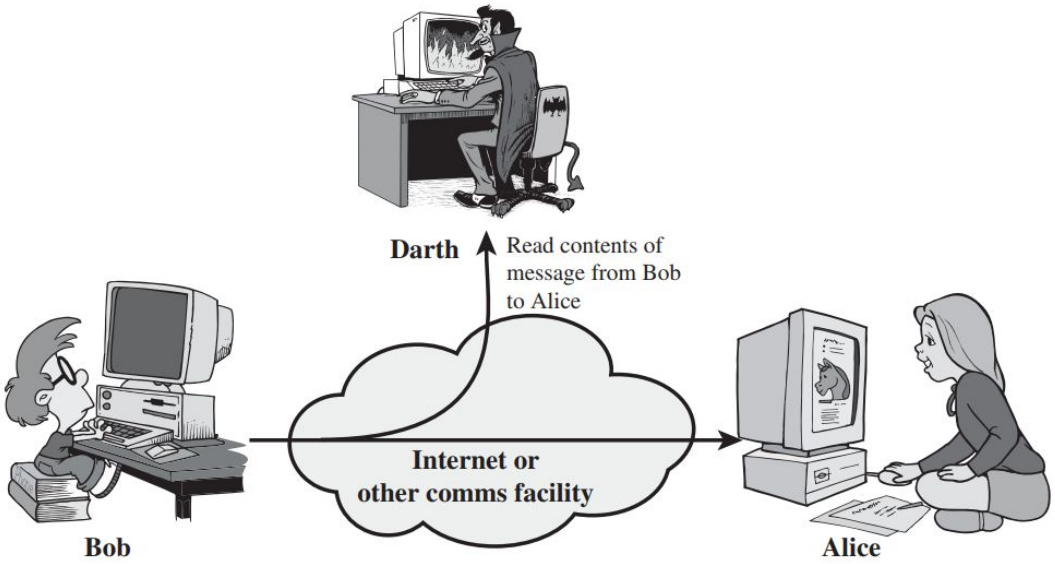
Passive Attacks:

The objective of passive attacks is to **intercept** information from the system without modification or effect on systems resources.

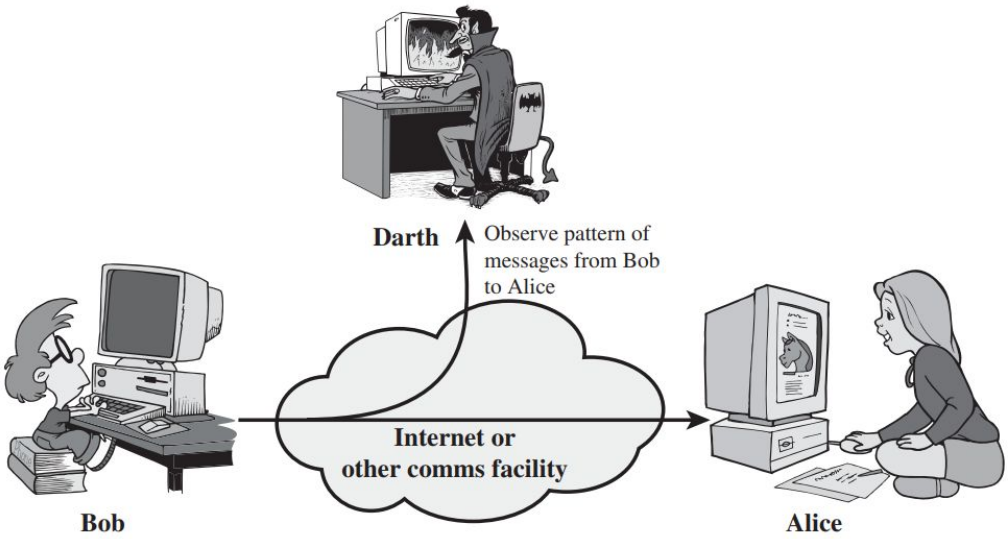
Active Attacks:

Active attacks involve **modification or manipulation** of system resources to **disturb their normal operation** or to gain unauthorized access.

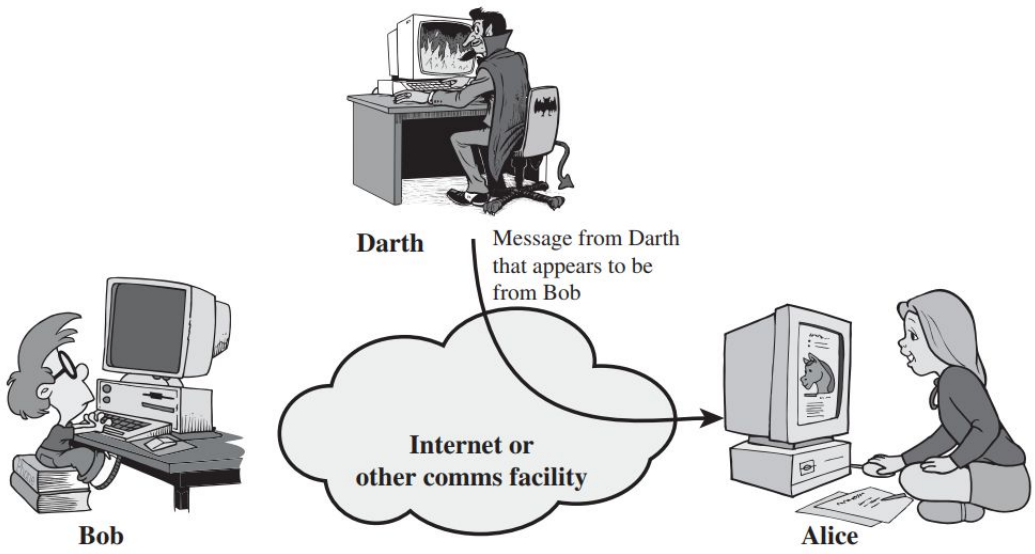
Release of message contents



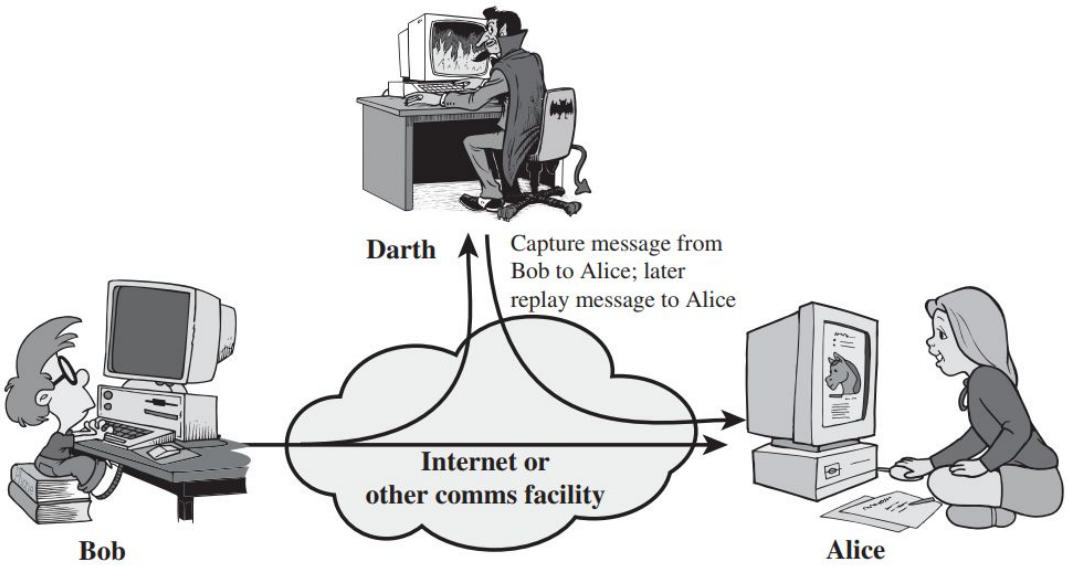
Traffic Analysis



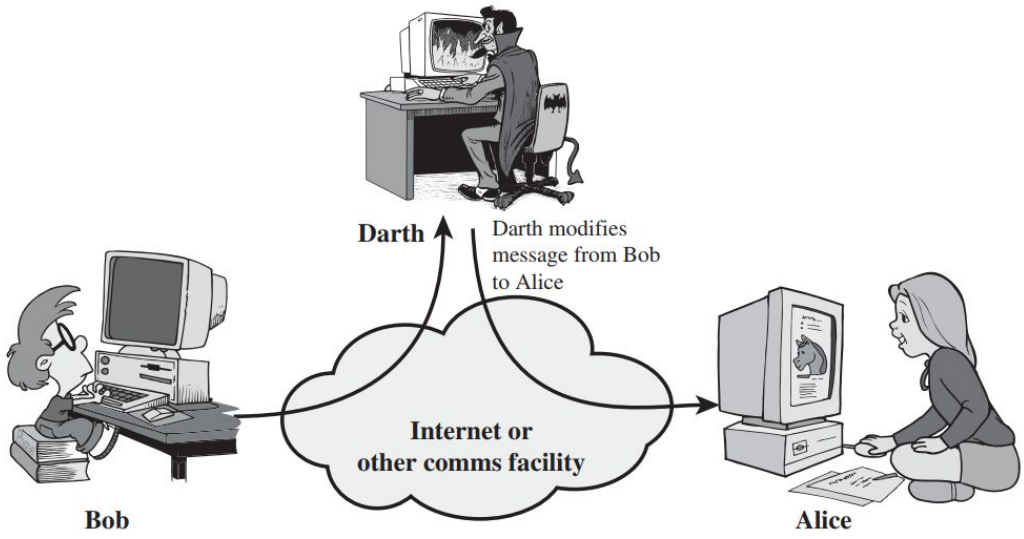
Masquerade


Darth
Message from Darth
that appears to be
from Bob
Internet or
other comms facility
Bob
Alice

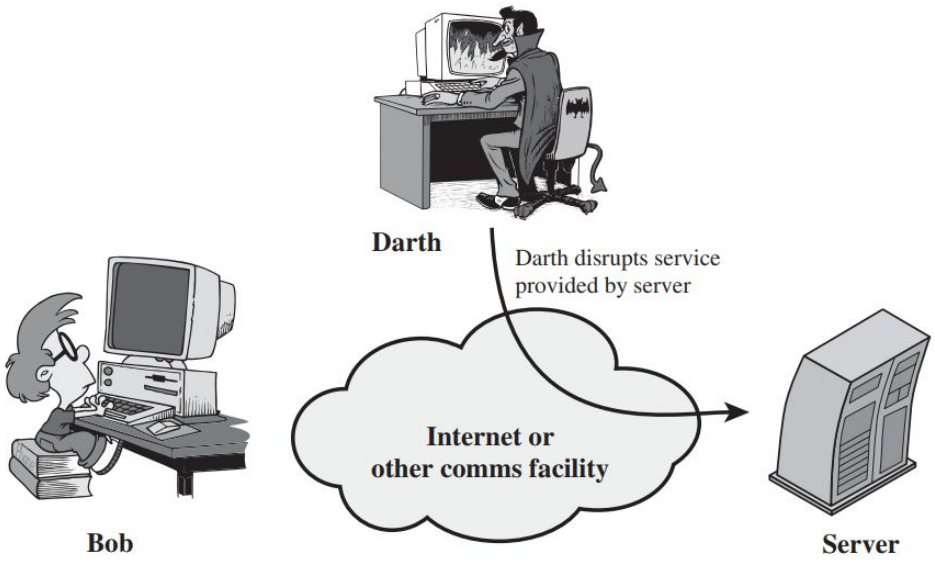
Replay


Darth
Capture message from
Bob to Alice; later
replay message to Alice
Internet or
other comms facility
Bob
Alice

Modification of messages



Denial of service



Security Services

- **Authentication**

Peer entity authentication **identifies the entities** involved in a communication relationship.

It ensures that communicating peer entities are those with whom the connection was established or to whom data are presently being sent.

It must be resistant to masquerade attacks and unauthorized replays to provide secure interaction between entity instances of the same protocol at different systems.

- **Data origin authentication** verifies the **source of a data unit, such as an email,** ensuring its authenticity without protecting against data **duplication** or **modification**.
- This service is essential for applications **like electronic mail**, where verifying the sender's identity is crucial despite the absence of prior interactions between the communicating parties.

Access Control

- The ability to limit and control the **access to host systems and applications.**
- Each entity trying to gain access must first be **identified, or authenticated**, so that access rights can be tailored to the individual.

Data Confidentiality

- It gives protection to the transmitted data from passive attacks.
- Protection from **eavesdropping** includes everything from full protection of all user data carried over a TCP connection to narrower protection of single messages or even protection of specific fields of messages.
- **Protection of traffic flow from analysis** means that no attacker would be able to observe source, destination, frequency, length, or any other characteristic of communication traffic.
- This type of protection provides confidentiality over the communications facility.

Data Integrity

- Integrity refers to the **validity and reliability** of data in a stream or individual messages.
- **Connection-oriented** integrity provides protection against duplication, modifications aimed at **message streams**.
- **Connectionless** integrity focuses on **source identification** at the level of single messages.
- **Recovery mechanisms** can provide sound detection and response to integrity violations through enabling **automated responses** that complement the practice of tighter security for associated data.

Nonrepudiation

- Nonrepudiation prevents either sender or receiver from **denying a transmitted message.**
- Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

Availability Service

- Availability, ensures systems and resources are **accessible and usable as intended**, responding to authorized requests.
- It addresses threats such as denial-of-service attacks, requiring effective resource management and security controls, including access control mechanisms, to maintain uninterrupted service delivery.

Security Mechanisms

Encipherment

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature

Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the **source and integrity** of the data unit and protect against forgery (e.g., by the recipient).

Access Control

A variety of mechanisms that enforce access rights to resources.

Data Integrity

A variety of mechanisms used to assure the integrity of a data unit or stream of data units. Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding

The insertion of bits into gaps in a data stream **to frustrate traffic analysis attempts.**

Routing Control

Enables selection of particular physically **secure routes for certain data** and allows routing changes, especially when a breach of security is suspected.

Notarization

The use of a trusted **third party to assure** certain properties of a data exchange.

Event Detection

Detection of security-relevant events.

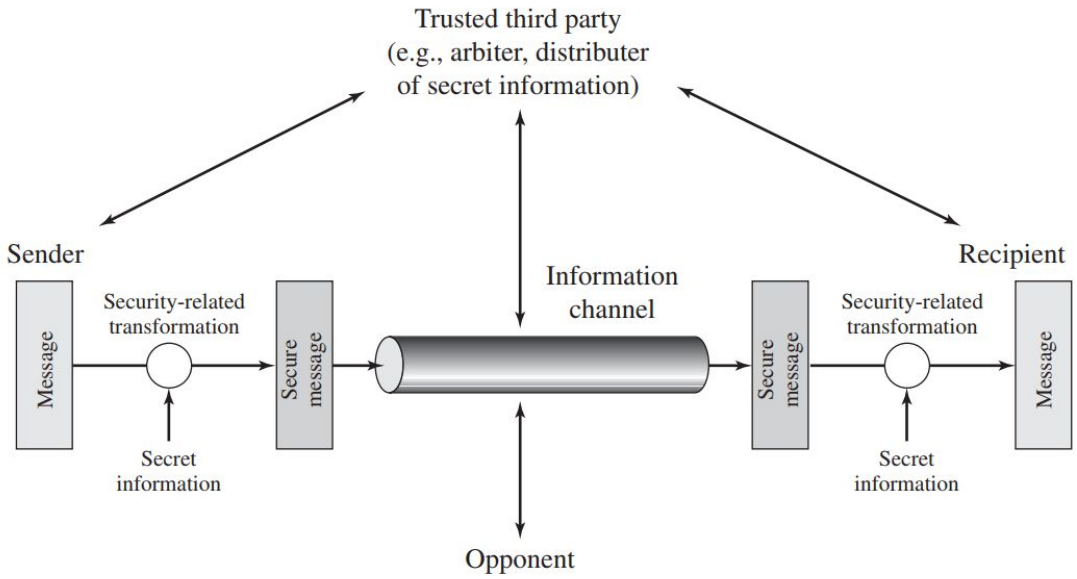
Security Audit Trail

Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

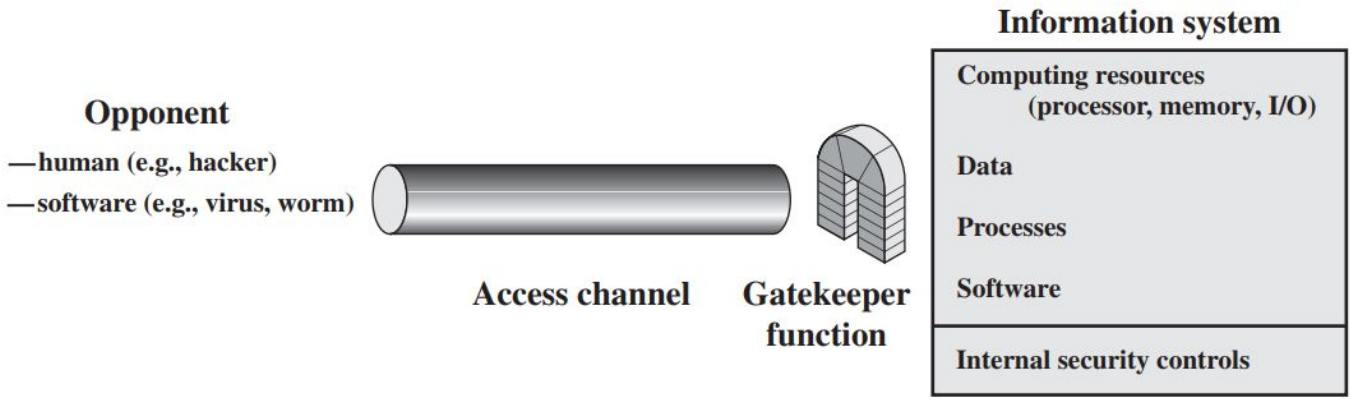
Security Recovery

Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

A model for Network Security



Network Access Security Model



Find the solution in terms of Security Mechanisms

- Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement.

Confidentiality

- Requirement: **The PIN and account information have to be kept secret to prevent a crime**, like identity theft, from being committed when there is unauthorized access to them.
- Importance: Very high. A certain risk of financial loss or user privacy exposure if the PIN or account details are disclosed to unauthorized people

Integrity

- Requirement: Integrity of data in transactions ensures accuracy and reliability. It also involves checking that **no modifications are done on the transaction itself** during its processing.
- Importance: Any compromise to transaction integrity may include cash being withdrawn or deposited incorrectly, resulting in financial disparities and a loss of confidence in the system.

Availability

- Requirement: The ATM system shall be **available to customers for use every time they need to perform** some transactions with not too much downtime.
- Importance: High. Customers rely on ATMs for quick access to their money. Downtime may inconvenience users, which can cause dissatisfaction; alternatively, it may force them to rely on less safe methods.

Problem

- Repeat above problem for a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller

Confidentiality

- Requirement: Details of the calls, such as caller numbers and call destination, are entitled to confidentiality against unauthorized access and eavesdropping.
- Importance: The unauthorized access to call details may reveal the user's privacy and can result in probable misapplication of the information.

Integrity

- Requirement: Call routing should ensure that calls are accurately routed to the dialed telephone number without alteration or manipulation.
- Importance: For even the slightest weakness in call integrity could create opportunities for misrouting or interception that would reduce communication reliability, leading to potential legal or security implications.

Availability

- The requirement is that the switching system is to be available to handle calls reliably and efficiently, with minimum time wasted on non-availability, to guarantee that connectivity remains uninterrupted.
- Importance: Continuity within telecommunications services is of central importance. Downtime could mean interference in communication services that impact businesses, emergency services, or simply personal communication requirements.

Symmetric Cipher Model

• **Plaintext**: This is the original intelligible message or data that is fed into the algorithm as input.

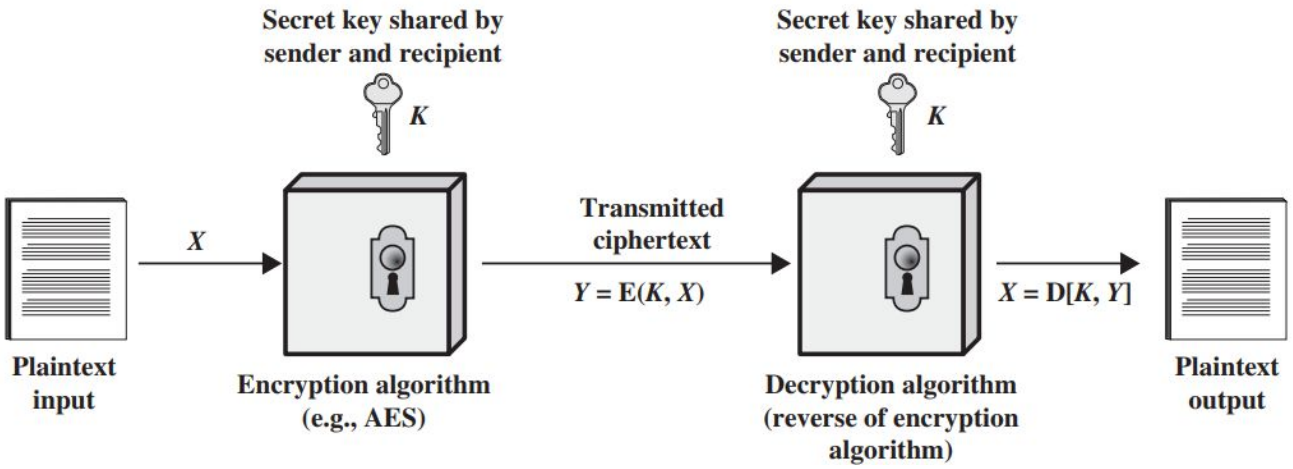
• **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on the plaintext.

• **Secret key**: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

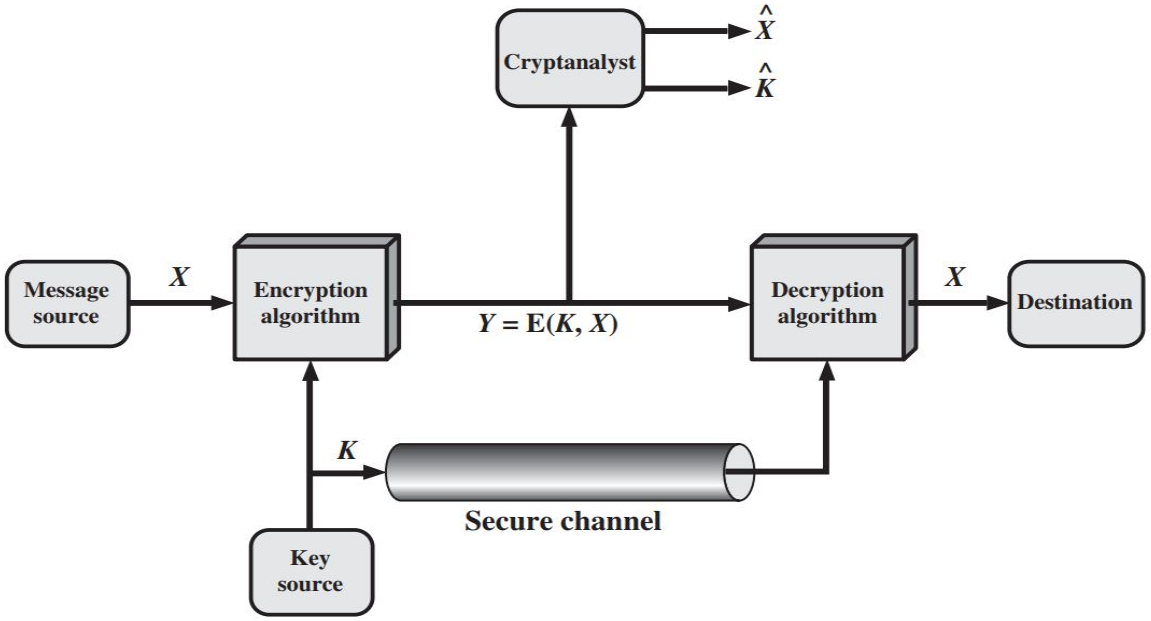
• **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

• **Decryption algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Simplified Model of Symmetric Encryption



Model of Symmetric Cryptosystem



Cryptography

1. Types of Operations in Encryption
Substitution and Columnar Transposition Cipher.

2. Number of Keys
Symmetric and Asymmetric Encryption.

3. The way in which the plaintext is processed
Block and Stream Ciphers.

Cryptanalysis and Brute-Force Attack

Cryptanalysis

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

Brute-force attack

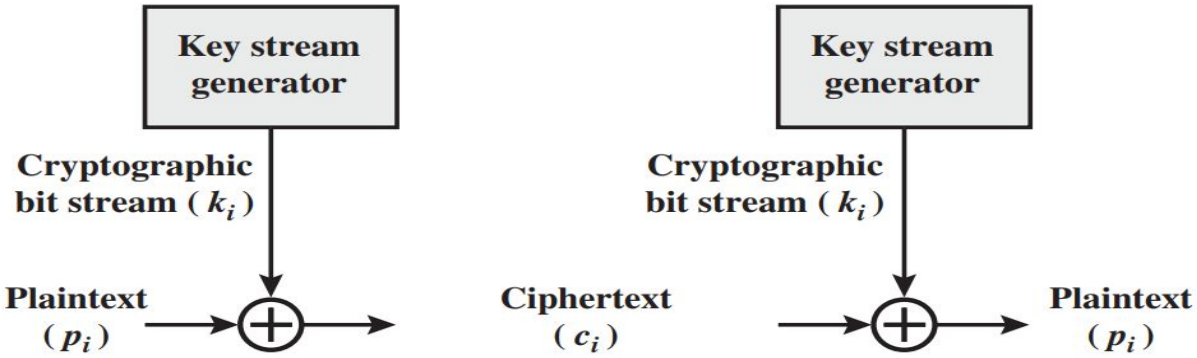
The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

Average Time Required for Exhaustive Key Search

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\mu s$ = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\mu s$ = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

Vernam Cipher

- Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key. Because of the properties of the XOR, decryption simply involves the same bitwise operation



Steganography

- Steganography is the practice of **concealing information within another message** or physical object to avoid detection.
- For example, the **sequence of first letters of each word of the overall message** spells out the hidden message.
- **Character marking**: Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
- **Invisible ink**: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

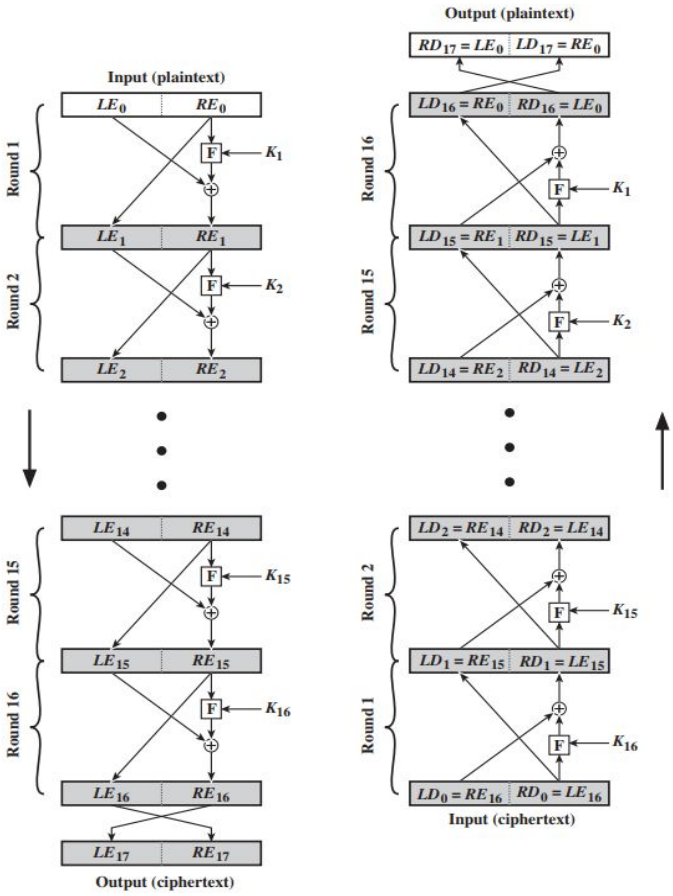
Example Digital watermarking

Block Cipher Principles

Stream Ciphers and Block Ciphers

- A stream cipher encrypts data one bit or byte at a time.
- A block cipher encrypts fixed-size blocks of plaintext to produce ciphertext blocks of equal length, typically 64 or 128 bits.

Feistal Cipher Structure



Encryption and Decryption Tables for Substitution Cipher

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

- If is sufficiently **large and an arbitrary reversible** substitution between plaintext and ciphertext is allowed, then the statistical characteristics of the source plaintext are masked to such an extent that this type of cryptanalysis is **infeasible**.

- A **product cipher**, which is the execution of **two or more simple ciphers in sequence** in such a way that the result or product is cryptographically stronger than any of the component ciphers.

- **Substitution**: Each plaintext element or group of elements is uniquely **replaced** by a corresponding ciphertext element or group of elements.
- **Permutation**: A sequence of plaintext elements is replaced by a **permutation of that sequence**.

- In **diffusion**, the statistical **structure of the plaintext is dissipated** into long-range statistics of the ciphertext.
- This is achieved by having each **plaintext** digit **affect** the value of **many ciphertext digits.**

- **Block Size:** Larger block sizes enhance security through **greater diffusion** but may slow down encryption/decryption. Traditionally, 64-bit blocks were common, but AES uses 128-bit blocks.
- **Key Size:** Larger key sizes improve security by **resisting brute-force** attacks and increasing confusion but may slow down processing. Key sizes of 128 bits or more are now standard, as 64-bit keys are considered inadequate.
- **Number of Rounds:** Multiple rounds of encryption enhance security. A typical block cipher uses around 16 rounds to ensure strong encryption.
- **Subkey Generation Algorithm**: More complex algorithms for generating subkeys increase the difficulty of cryptanalysis.
- **Round Function F:** Greater complexity in the round function improves resistance to cryptanalysis, enhancing overall security.

- The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of digital data.
- It operates on blocks of data, using a series of transformations to encrypt and decrypt information.
- The initial permutation (IP) is one of the key steps in the DES process, which rearranges the bits of the input data block before the main rounds of encryption begin.

Initial Permutation

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Initial Permutation

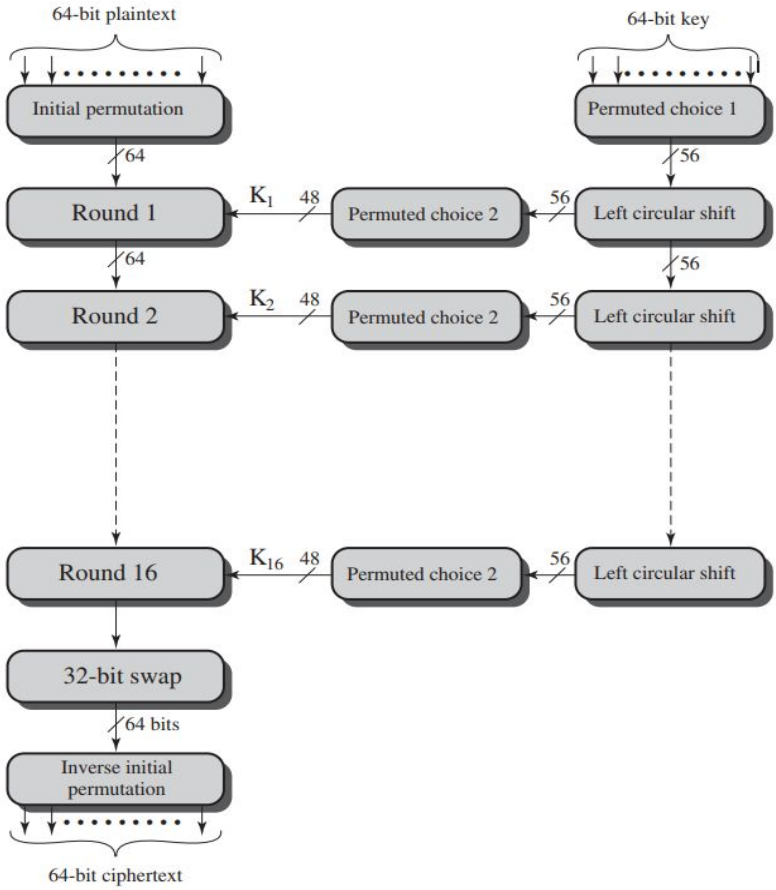
Position 58 in original (value 1) becomes position 1 in permuted block.
Position 50 in original (value 0) becomes position 2 in permuted block.
Position 42 in original (value 1) becomes position 3 in permuted block.
Position 34 in original (value 0) becomes position 4 in permuted block.
Position 26 in original (value 1) becomes position 5 in permuted block.
Position 18 in original (value 0) becomes position 6 in permuted block.

Inverse Initial Permutation

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

- Bit 1 in permuted block (position 40 in original)
- Bit 2 in permuted block (position 8 in original)
- Bit 3 in permuted block (position 48 in original)
- Bit 4 in permuted block (position 16 in original)
- Bit 5 in permuted block (position 56 in original)
- Bit 6 in permuted block (position 24 in original)

Data Encryption Standard

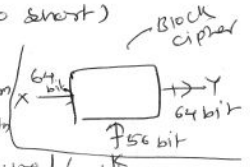


DES

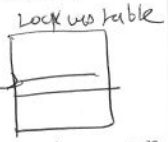
Cryptography
- Symmetric
  - Stream
  - Block cipher

- 1974 proposed by IBM, with i/p NSA
- 1977 – 1998 US standard
- Best studied ciphers in the world.
- Unsecure today (key too short)
- Two atomic operations

basic
The block cipher should perform



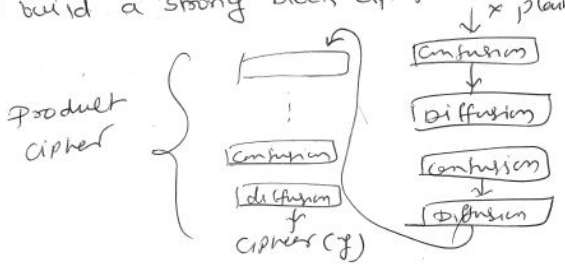
(i) Confusion :- Relationship between plain and ciphertext is obscured/hidden
e.g. Substitution Table



(ii) Diffusion :- The influence of each plaintext bit is spread over many ciphertext bits.
e.g. Permutation

like caesar cipher

- Combine Confusion and diffusion many times to build a strong block ciphes



Product ciphers

Most of today's block ciphers are product ciphers as they consist of rounds which are applied repeatedly to the data.

- Can reach excellent diffusion changing one bit of plaintext results on average in the change of o/p bits.

$x_1 \Rightarrow 0010\ 1011$
$x_2 \Rightarrow 0000\ 1011$ (↑ difference)

→ [Block Ciphers] →

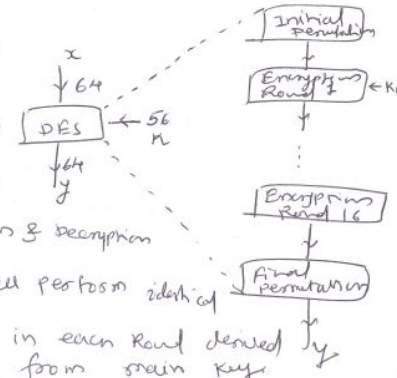
$y_1 = 1011\ 1001$
$y_2 = 0110\ 1100$ (many bits flip)

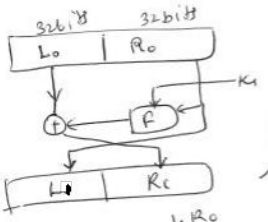
- Avalanche effect

Feistel Network

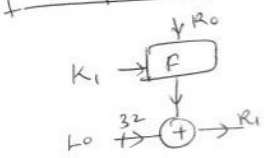
Many of today's ciphers are based on ~~ciphers~~ feistel n/w.

- Encrypts block of size 64 bit
- uses a key of size 56 bits
- Symmetric ciphers uses same encryption & decryption key.
- Uses 16 Rounds all perform identical operations
- Different sub key in each Round derived from main key.

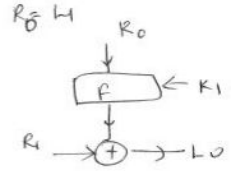




Read 1 (only) L_0 is encrypted using an XOR operation



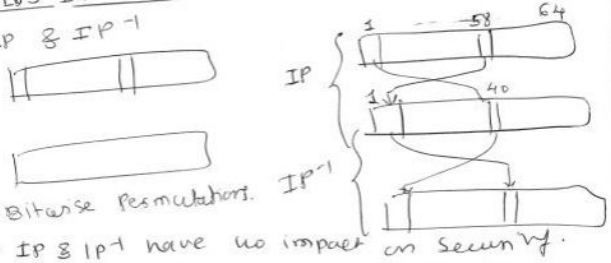
$R_0 = L_1$



$L_0 = R_1 \oplus f(R_0, K_1)$

DES internally

IP & IP^{-1}



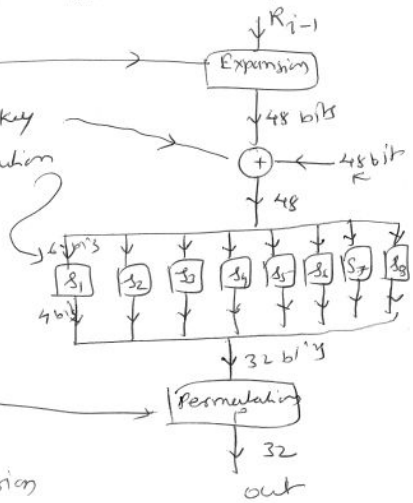
- Bitwise permutations.
- IP & IP-1 have no impact on security.
- Implementation was easier in HW context at that time.
- 8 bit registers were used (cheaper)

Details of F function

- F function i/p $\Rightarrow R_{i-1}$ and Round key K_i

4 steps

1. Expansion E
2. XOR with Round key
3. S Box Substitution
4. Permutation



5. DES

E-Box => Diffusion

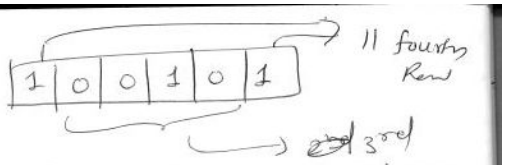
16 → once
16 → twice
$\Rightarrow$ 48 o/p bits.

S-Box Substitution

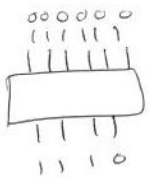
→ Eight substitution tables

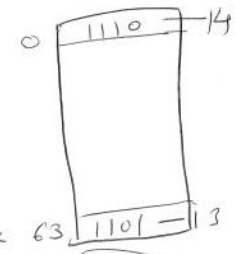
→ 6 bit i/p, 4 bit o/p

S_1	0	1	2	— —	15
0					
1					
2					
3					



S-Box provides confusion.

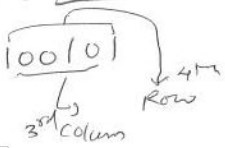




- Unusual decoding of S-Box tables.

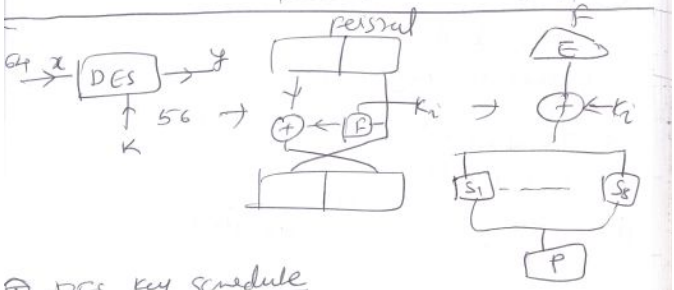
ex. $S_i \Rightarrow 37 \Rightarrow$ 1001 0

$\Rightarrow 08 \Rightarrow 1000$



- Depends on structure of S Boxes
- NSA already new cryptanalysis. they wanted to keep itself to them
- Design the own cipher & break it
- 1 bit flip ⇒ & see what happens at o/p.

- 1 bit flip ⇒ at least 2 bit flip



Ⅱ DES key schedule

- Split key into 28 bit halves C_0 and D_0
- In rounds i ⇒ 1, 2, 9, 16, the two halves are each rotated left by 1 bit
- In all other rounds where the two halves are each rotated by left by two bits
- In each round i permuted choice PC-2, selects a permuted subset of 48 bits of C_i and D_i as round key K_i i.e each K_i is a permutation of K
- To find no of Rotations ⇒ $4 \times 1 + 12 \times 2 = 28$

(a) PC-1 ⇒ Permuted Choice 1

→ Drops bits 8, 16, 24 - - - 64

→ Effective key length of DES 64-8=56 bits.

→ The dropped bits are reserved for parity bits.

(b) LS_i $i \Rightarrow 1$ to 16

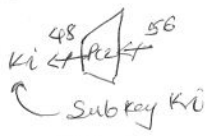
→ Left Swift (Left Rotate)

$$LS_i = \begin{cases} 1 \text{ position shift for Rounds } 1, 2, 9, 16 \\ 2 \text{ position shift for other Rounds} \end{cases}$$

$4 \cdot 1 + 12 \cdot 2 = 28$ (i.e. 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15)

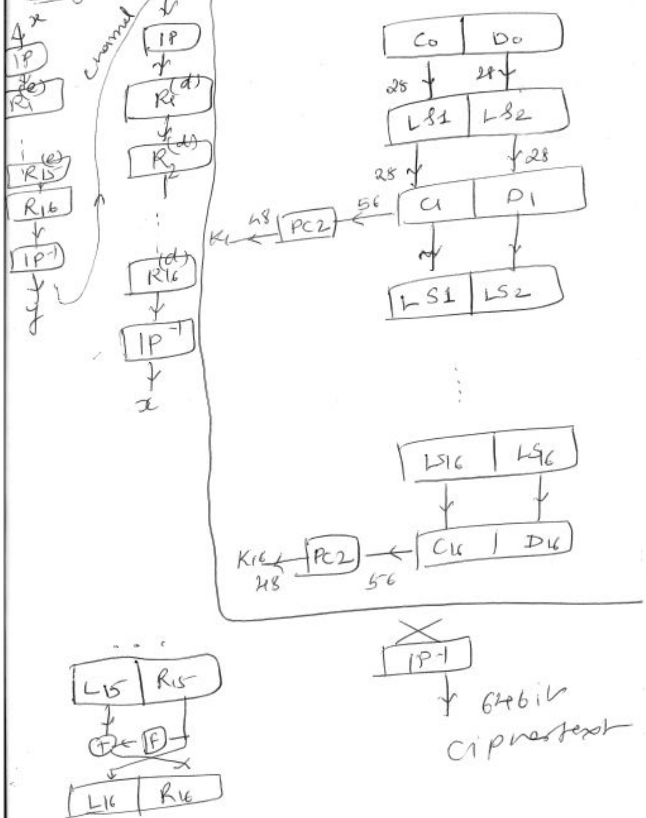
(c) PC-2 :- Permuted Choice 2

- 8 bits are dropped
- remaining 48 i/p bits are permuted.

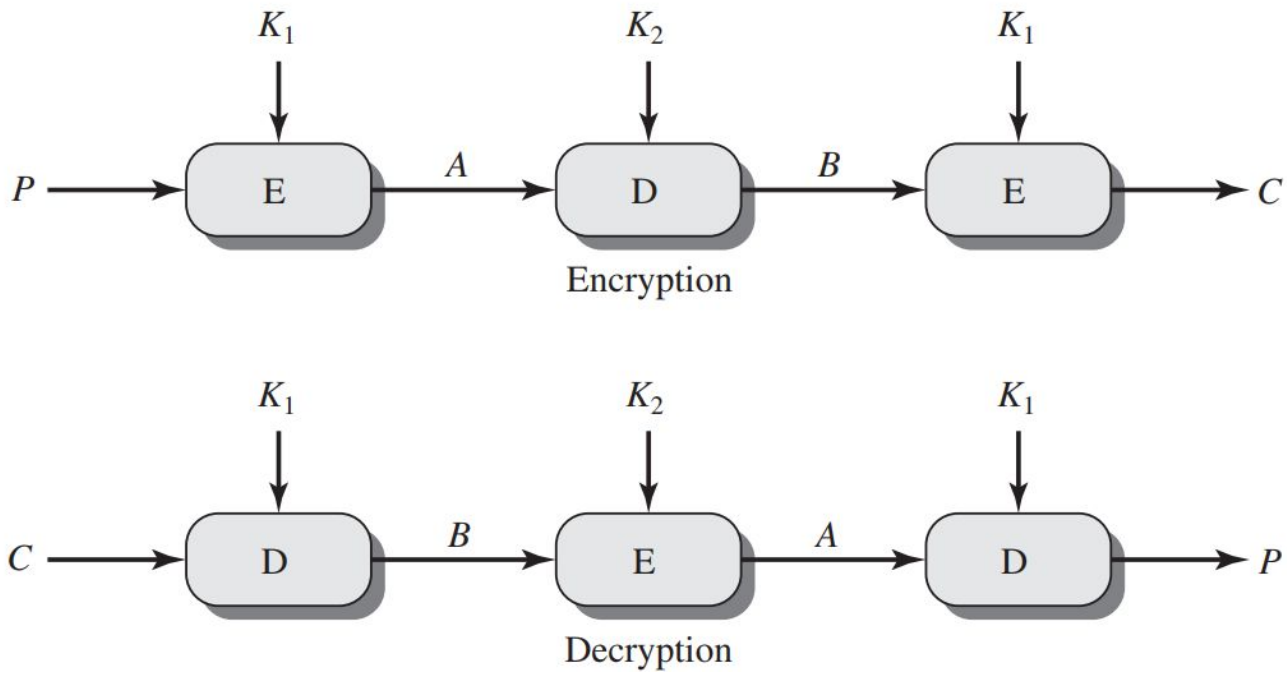


- Each key K1 to K16 is merely a permutation of the original 56 bit key.

Decryption


x
IP
R1
R15
R16
IP-1
y
channel
IP
R1(d)
R2(d)
R16(d)
IP-1
x
C0
D0
28
LS1
LS2
C1
D1
56
48
PC2
K1
LS1
LS2
LS16
C16
D16
PC2
K16
48
56
L15
R15
F
L16
R16
IP-1
64 bit
ciphertext

Triple DES Encryption



- **Encryption:** $C = E_{K1}(D_{K2}(E_{K1}(P)))$
- **Decryption:** $P = D_{K1}(E_{K2}(D_{K1}(C)))$

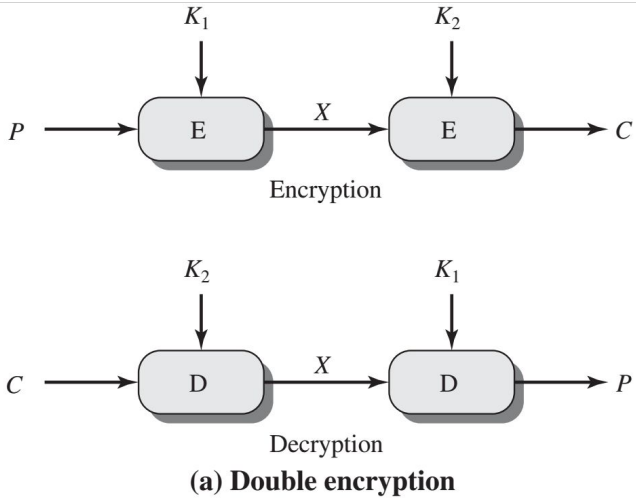
Double DES Encryption:

Double DES encrypts plaintext P using two keys, K1 and K2:

1. **First Encryption:**
   - Encrypt plaintext P with key K1 to get interme

     -diate ciphertext A:

2. **Second Encryption:**
   - Encrypt A with key K2 to get final ciphertext C:



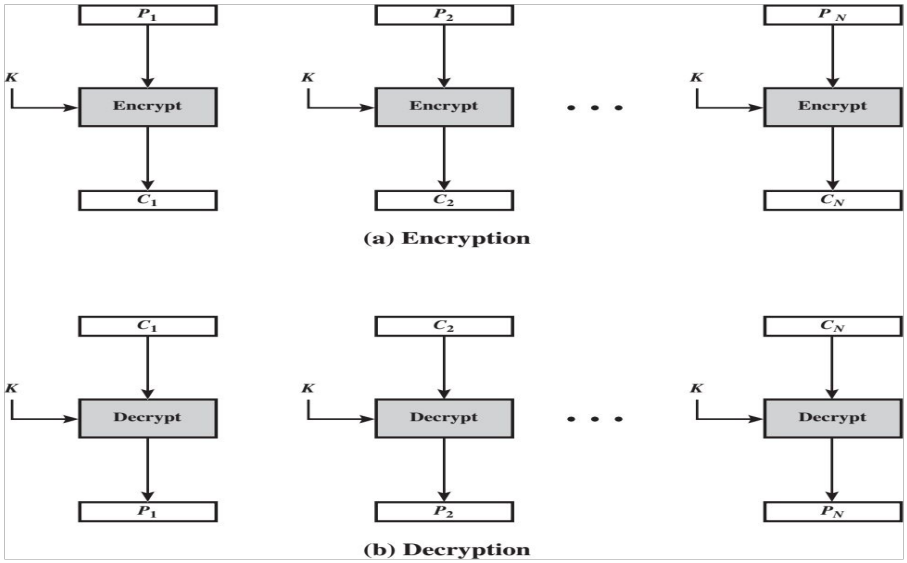
(a) Double encryption

Modes of Operation

A mode of operation is a technique for enhancing the effect of a cryptographic algorithm

Block ciphers encrypt data in fixed-size chunks. Modes of operation allow us to encrypt data that’s larger than a single block by splitting it into multiple blocks.

Electronic codebook Mode

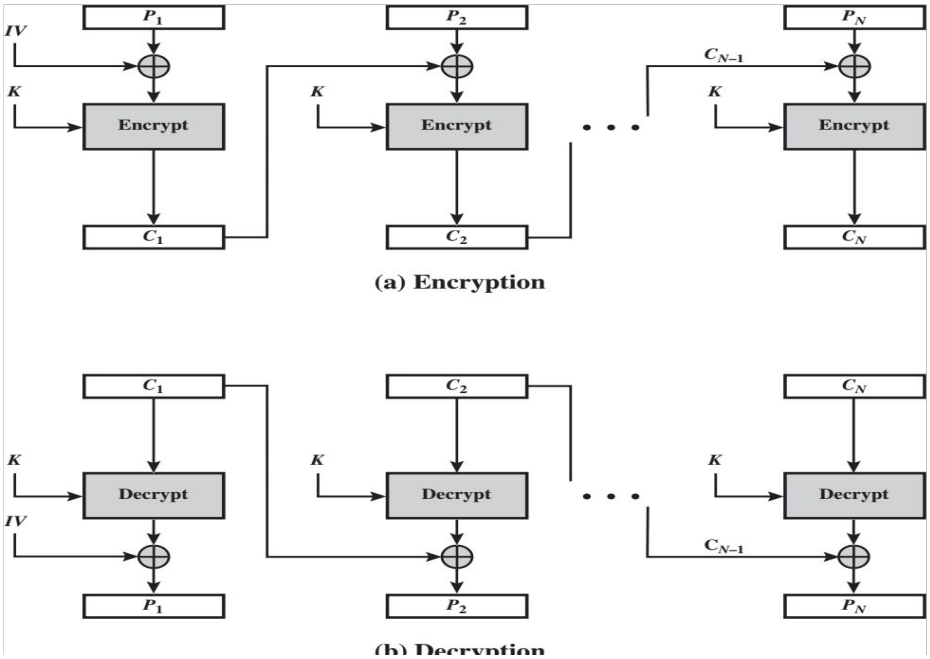


Disadvantage

Identical blocks produce identical results, which can expose patterns in the data.

The ECB method is ideal for a short amount of data, such as an encryption key.

Cipher Block Chaining



Disadvantages:

Sequential processing

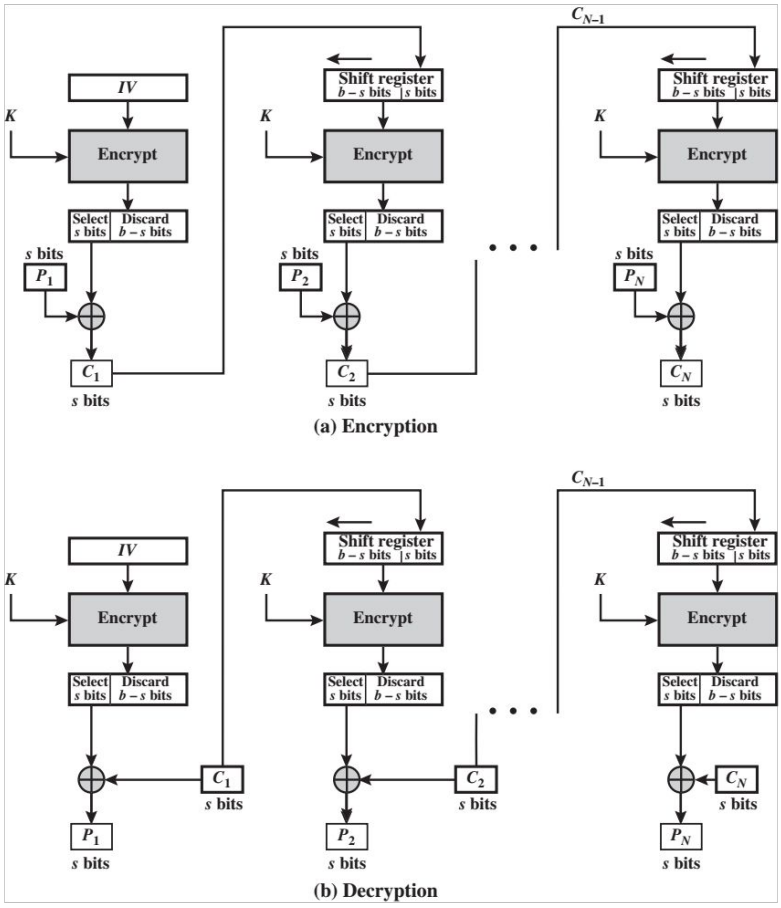
Error Propagation

It is possible to convert block cipher into steam cipher using cipher feedback mode, output feedback mode and counter mode

In stream cipher ciphertext is of same length as plaintext

CFM

Cipher Feedback Mode



it is assumed that the unit of transmission is bits; a common value is 8 bits .

b -bit shift register that is initially set to some initialization vector (IV)

The contents of the shift register are shifted left by s bits,

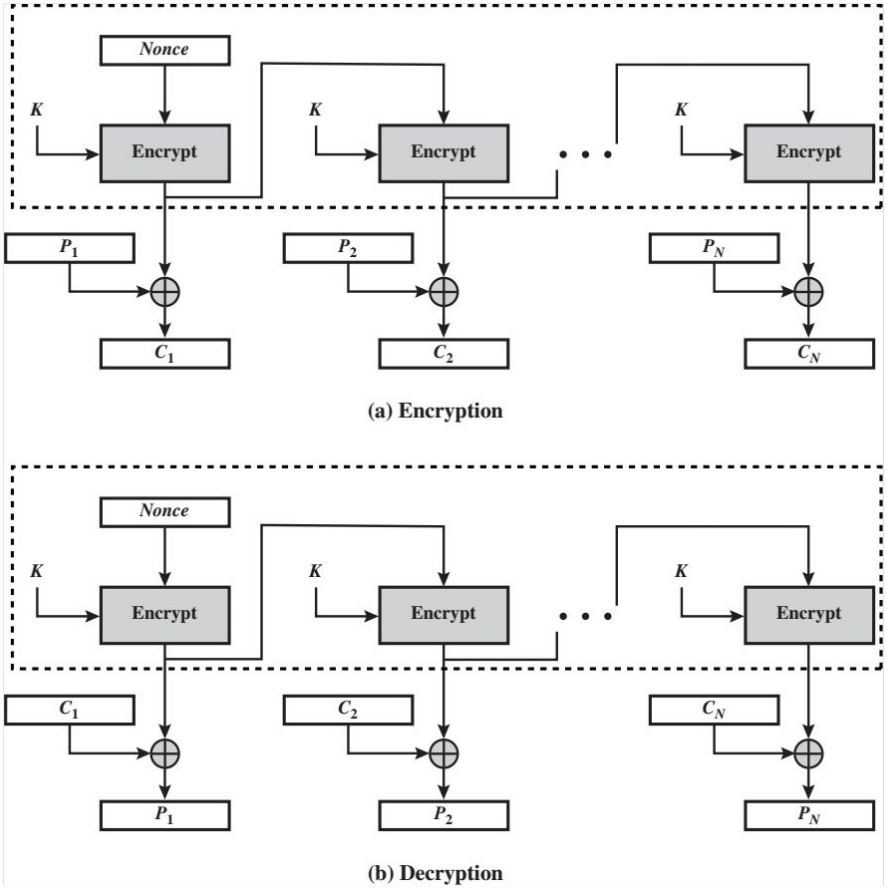
and C1 is placed in the rightmost (least significant)s bits of the shift register.

$$C_1 = P_1 \oplus \text{MSB}_s[\text{E}(K, \text{IV})]$$

$$P_1 = C_1 \oplus \text{MSB}_s[\text{E}(K, \text{IV})]$$

OFM

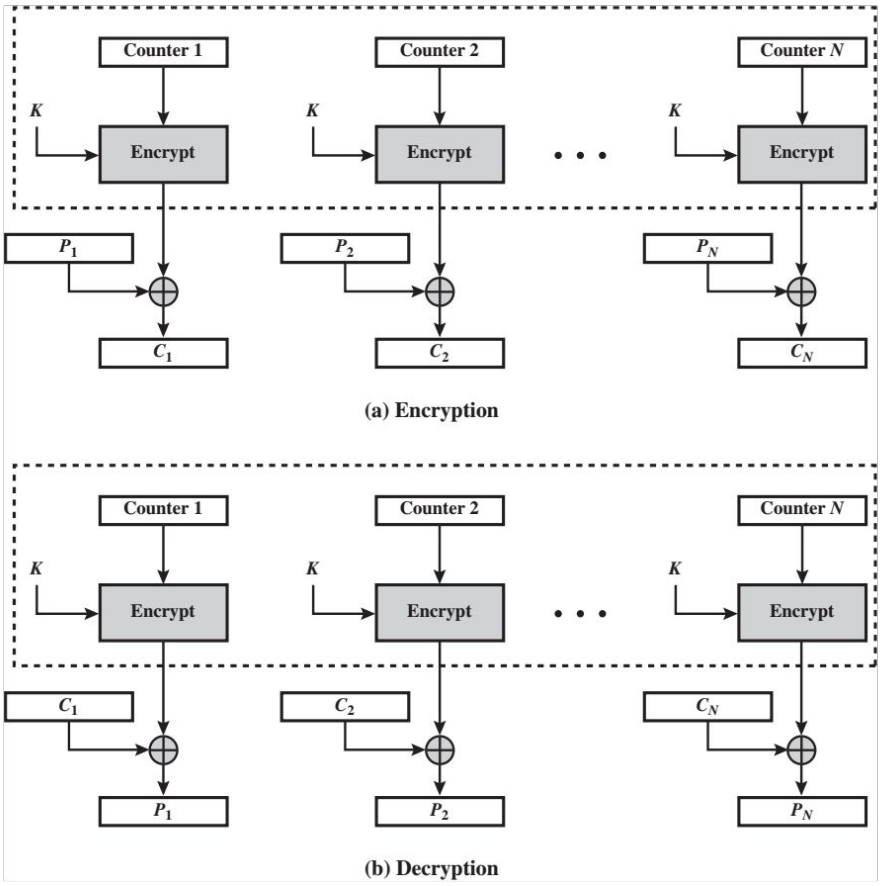
Output Feedback Mode



Difference is that the OFB mode operates on full blocks of plaintext and ciphertext, not on an -bit subset.

Output Feedback (OFB) mode has the key advantage of not propagating errors beyond the bit or block where they occur, ensuring that a single bit error affects only the corresponding bit in the plaintext.

Counter Mode



In CTR mode, a counter is used in conjunction with the IV. The counter is a value that starts at a specific number (usually 0) and is incremented for each subsequent block.

Blowfish

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time.

The algorithm follows feistal network and is divided into 2 main parts

1 Key Expansion

2 Encryption

Key expansion converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes.

Data encryption occurs via a 16-round Feistel network.

Each round consists of permutation, and substitution.

All operations are XORs and additions on 32-bit words.

Subkeys:

Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption.

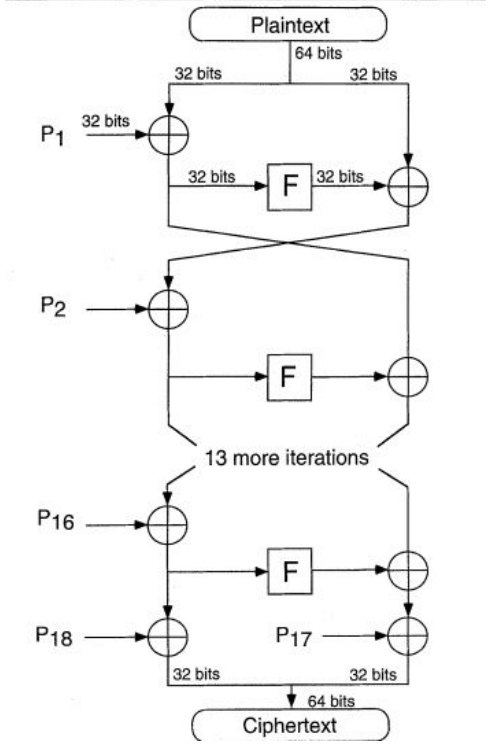
1 The P-array consists of 18 32-bit subkeys:

P1,P2,P3…,P18

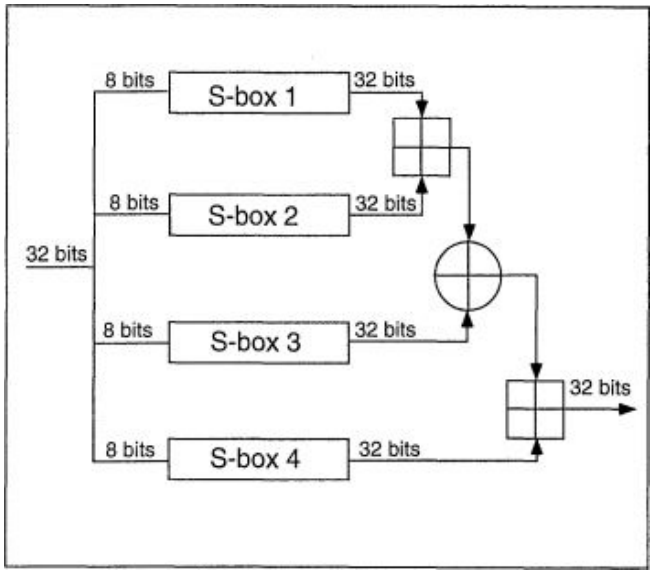
2 There are four 32-bit S-boxes with 256 entries each:

S1,0,.....S1,255

S4,0,.....S4,255


Plaintext
64 bits
32 bits
32 bits
P1
32 bits
32 bits
F
32 bits
P2
F
13 more iterations
P16
F
P18
P17
32 bits
32 bits
64 bits
Ciphertext

F function


8 bits
S-box 1
32 bits
8 bits
S-box 2
32 bits
32 bits
8 bits
S-box 3
32 bits
32 bits
8 bits
S-box 4
32 bits

IDEA

The IDEA cipher was designed by Xuejia Lai and James Massey in 1990 and initially named PES (Improved Proposed Encryption Standard).

Despite some progress made in cryptanalysis against reduced-round versions, IDEA remains one of the strong encryption algorithms.

It still has limited general acceptance as a DES successor because of patent license fees and cryptanalysis underway.

IDEA is a block cipher, working on 64-bit plaintext blocks, under a 128-bit key.

The scheme uses both confusion and diffusion and mixes operations from the different algebraic groups:

XOR,

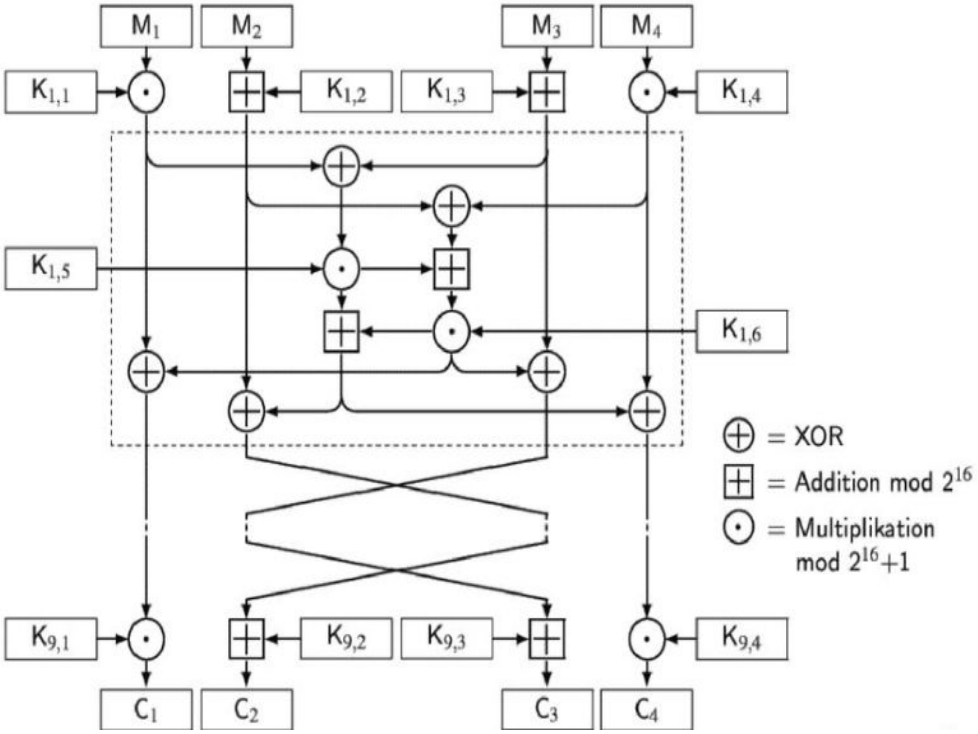
addition modulo 2^{16},

multiplication modulo $2^{16}+1$ (which is IDEA's S-box).

The operations work on 16-bit sub-blocks and are efficiently implemented both in hardware and software.

Thus even 16-bit processors can use this algorithm.

IDEA Block diagram



(1) Multiply M1 and the first subkey.
(2) Add M2 and the second subkey.
(3) Add M3 and the third subkey.
(4) Multiply M4 and the fourth subkey.
(5) XOR the results of steps (1) and (3).
(6) XOR the results of steps (2) and (4).
(7) Multiply the results of step (5) with the fifth subkey.
(8) Add the results of steps (6) and (7).
(9) Multiply the results of step (8) with the sixth subkey.
(10) Add the results of steps (7) and (9)

(11) XOR the results of steps (1) and (9).
(12) XOR the results of steps (3) and (9).
(13) XOR the results of steps (2) and (10).
(14) XOR the results of steps (4) and (10).

After the eighth round, there is a final output transformation:

(1) Multiply M1 and the first subkey.

(2) Add M2 and the second subkey.

(3) Add M3 and the third subkey.

(4) Multiply M4 and the fourth subkey.

Finally, the four sub-blocks are reattached to produce the ciphertext.

First, the 128-bit key is divided into eight 16-bit subkeys.

These are the first eight subkeys for the algorithm (the six for the first round, and the first two for the second round).

Then, the key is rotated 25 bits to the left and again divided into eight subkeys.

The first four are used in round 2; the last four are used in round 3.

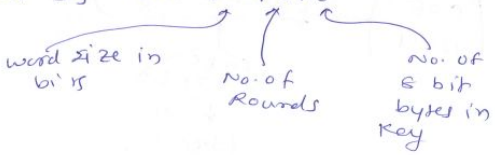
The key is rotated another 25 bits to the left for the next eight subkeys, and so on until the end of the algorithm

RC5

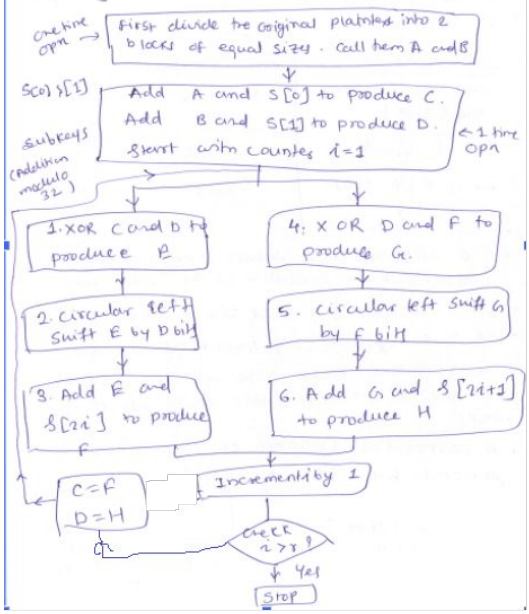
- Symmetric Block cipher developed by Ron Rivest
- It uses primitive operations i.e, Addition XOR, Shift
- It allows for variable numbers of rounds and a variable bit size key.
- It requires less memory.

Parameter	Allowed values
Word size (plaintext Block size)	16, 32, 64
No. of Rounds	0 - 255
No. of 8 bit bytes in the key	0 to 255

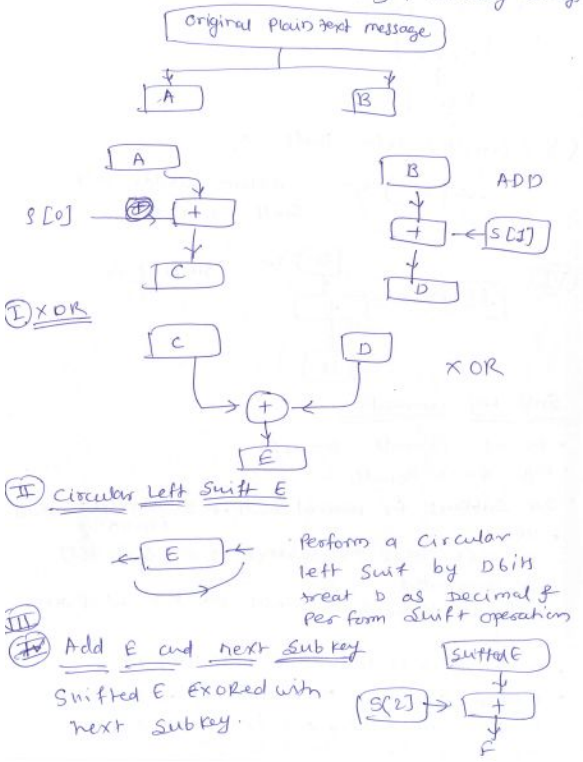
- once decided these values remain same throughout the execution of the algorithm
- word size = 16 ; Block size = 2 × word size
- RC-5 encrypts 2 word blocks at a time
- The plaintext block size can be 32, 64 or 128 bits since RC5 makes use of 2 word blocks.
- A particular instance of RC5 algorithm is denoted by RC5 w/r/b



- If we have RC5-32/16/16 means that we are using RC5 with a block size of 64 bits, 16 Rounds of encryption, and 16 bytes in key.



5) Each iteration we are making use of 2 subkeys (3)
• Each round Requires 2 subkeys, initially 2 keys



(I) XOR

(II) Circular Left Shift E

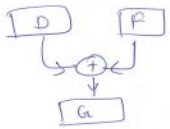
Perform a circular left shift by DBits treat D as Decimal & Perform shift operation

(III)

(IV) Add E and next subkey

Shifted E EXORed with next subkey.

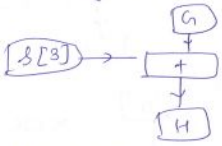
(IV) XOR D and F



(V) Circular left Shift G

Perform Circular left Shift by F Bits.

(VI)

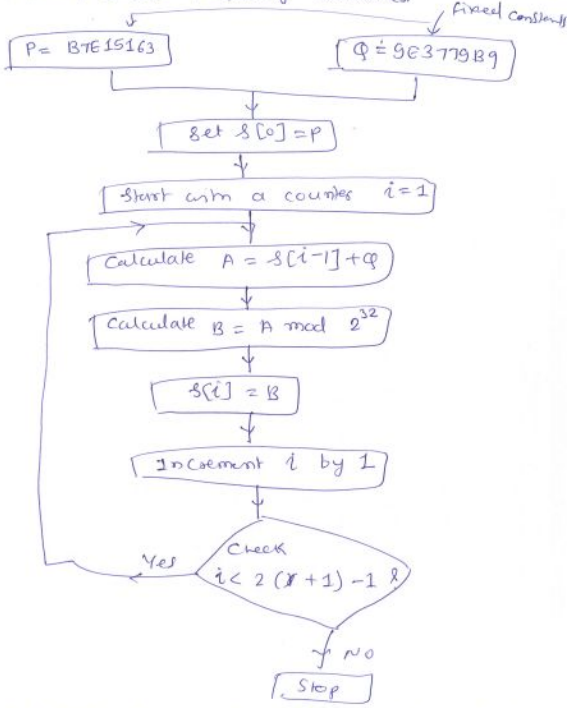


Shifted G.

Sub Key Generation

- No of Rounds 0 - 255
- e.g. R = 12 Rounds.
- 24 Subkeys for intenral Rounds + 2 subkeys required initially. = 26.
- In this steps the subkeys i.e. S[0], S[1]... are generated.
- In this step, 2 constemsts are P and Q are used.
- P = B7E15163 , Q = 9E3779B9
- Each sub key is calculated on the basis of previous subkey and the constent Q using addition modulo 2^{32}

- A and B are temporary variables.



- E and H are appended and it is the cipher text.

CAST Algorithm

Initials of the scientists who discovered it.

CAST algorithm uses a 64-bit block size and a 64-bit key.

The algorithm uses six S-boxes with an 8-bit input and a 32-bit output.

Construction of these S-boxes is implementation dependent and complicated.

To encrypt, first divide the plaintext block into a left half and a right half.

The algorithm has 8 rounds.

In each round the right half is combined with some key material using function f and then XORed with the left half to form the new right half.

The original right half (before the round) becomes the new left half.

After 8 rounds , the two halves are concatenated to form the ciphertext

F function

(1) Divide the 32-bit input into four 8-bit quarters: a, b, c, d.

(2) Divide the 16-bit subkey into two 8-bit halves: e, f.

(3) Process a through S-box 1, b through S-box 2, c through S-box 3, d through S-box 4, e through S-box 5, and f through S-box 6.

(4) XOR the six S-box outputs together to get the final 32-bit output.

The 16-bit subkey for each round is easily calculated from the 64-bit key. If k1,

k2,..., k8 are the 8 bytes of the key, then the subkeys for each round are:

Round 1: k1, k2
Round 2: k3, k4
Round 3: k5, k6
Round 4: k7, k8
Round 5: k4, k3
Round 6: k2, k1
Round 7: k8, k7
Round 8: k6, k5

There is no known way to break CAST other than brute force.

Abstract Algebra

- Let G be a set of elements. Set is distinct coll of well defined objects.
- e.g. set of natural numbers i.e. $\{1, 2, \ldots\}$
- G is a non empty set and $\cdot$ is binary operato

(i) closure :- $a \cdot b \in G \quad \forall \; a, b \in G$

(ii) Associativity: $a, b, c \in G$ then $a \cdot (b \cdot c) = (a \cdot b) \cdot$
$\forall \; a, b, c \in G.$

- If (i) & (ii) are satisfied, $(G, \cdot)$ is semigrou

(iii) Identity Element :- $\exists \; e \in G$ such th
$a \cdot e = a \;, \forall \; a \in G.$
$a \cdot e = e \cdot a = a$

- Then e is called identity element of G.

(iv) Inverse :- For a given element a ∃ an element b such that $a \cdot b = e$, $b = a^{-1}$

- $(G, \cdot)$ is call group if (i), (ii), (iii), (iv) are satisfied.
- E.g. $G = N$, $\cdot = +$, Is $(N, +)$ is a group.
  $m, n \in N$, (i) $m+n \in N$ (ii) $(m+n)+k = m+(n+k)$
  (iii) $n \in N$ $m+0 = m$ but $0 \notin N$, so it is not a group.
- $(I, +)$ is a group!, I set of integers
  - $e = 0$, $i+0, 0+i = i$ where $i \in I$
  - $i + (-i) = 0$, $i \in I$
- $(I, \cdot)$ is a group!
- Not a group due to inverse not available
- Q = set of Rational number
  $(Q, \cdot)$ is a group
  $(R, \cdot)$ is a group.
- If $(G, \cdot)$ is group, then order of group is $|G|$

Abelian Group

- $(G, \cdot)$ is a group and it must satisfy commutative property.

$$\forall\ a, b \in G,\ a \cdot b = b \cdot a$$

Cyclic Group

- Let $(G, \cdot)$ be a group

$a \cdot a = a^2$	$a+a = a^2$
$a \cdot a \cdot a = a^3$	$a+a+a = a^3$
$a \cdot a \cdots a = a^i$	$a+a \cdots a = a^i$

- Then $(G, \cdot)$ is called a cyclic group if $\exists a \in G$

$\{a, a^2, a^3 \cdots a^i \cdots\} = G$

$b \in G \quad b = a^k$

- a is called generator or primitive element of group.
- Exponential is repeated application of group operator.
- we might have a^3 and this would equal $a \cdot a \cdot a$
- so if the operation was addition then a^3 would in fact be $a+a+a$.
- Also we have $a^0 = e$ which for an additive group is 0
- Also $a^{-3} = (a^{-1})^3$
- A group is said to be cyclic if every element of the group G is power a^k (k is integer) of fixed element $a \in G$.

The element a is said to generate G or be generator of G.

- Cyclic group is always abelian

Ring

• $(Rg, +, \times)$, A Ring is a set with two binary operations addition and multiplication that satisfies following axioms.

(i) Abelian Group under addition ($A_1 \to A_5$) :- i.e. it satisfies all the axioms of Abelian group, with the operation of addition. The identity element is 0 and inverse is denoted by $-a$.

(ii) closure under multiplication (m_1): For any two elements $a, b, \in Rg$, if $c = a \cdot b$ then $c \in Rg$

(iii) Associativity of multiplication (m_2): For any elements $a, b, c \in Rg$, $(ab)c = a(bc)$

(iv) Distributive (m_3): For any elements $a, b, c \in Rg$, $a(b+c) = ab + ac$.

• It is said to be commutative ring if in addition the ring follows the axiom

(v) commutativity (m_4) :- For any $a, b \in Rg$, $ab = ba$

Integral Domain $(Rg, +, \cdot)$

(1) Commutative Ring (2) Multiplicative Identity (m_5) (v_1)

i.e. $\forall\ a \in Rg$, $a \cdot 1 = 1 \cdot a$

(vi) No zero Divisors (m_6): If $a, b \in Rg$ and $ab = 0$ then either $a = 0$ or $b = 0$. This means no non zero element can multiply with another non zero element to give - zero.

- A field $\{P, +, \times\}$ is a set with two binary operations addition and multiplication that satisfies the following axioms:

(1) Integral Domain ($A_1 - M_6$): It satisfies all of the axioms for an Integral Domain

(2) multiplicative Inverse (M_7) Each element in P (except 0) has an inverse i.e. $\forall_{a \neq 0 \in F} \exists a^{-1} \in P$,

$a \cdot a^{-1} = a^{-1} \cdot a = 1$

- $(R, +, \cdot)$ is a field
- $(R,+)$ is a abelian group
- $(R - \{0\}, \cdot)$ is a abelian group

$\forall a, b, c \in R \Rightarrow a(b+c) = ab + ac$

$|R| =$ infinity

Group
- (A1) closure under Addition
- (A2) Associativity under Addition
- (A3) Additive Identity
- (A4) Additive Inverse
- (A5) Commutativity of Addition
- (M1) closure under multiplication
- (M2) Associativity under multiplication
- (M3) Distributive law
- (M4) Commutativity under multiplication
- (M5) multiplicative Identity

(M6) No zero divisor

(M7) multiplicative Inverse

(A1) to (A4) ⇒ Group

(A1) to (A5) ⇒ Abelian Group

(A1) to (M3) ⇒ Ring

(A1) to (M4) ⇒ Commutative Ring

(A1) to (M2) ⇒ Integral domain

(A1) to (M7) ⇒ Field.

Prime Numbers

- A prime number is p is an integer greater than 1 with only two positive divisors 1 and itself.
- Therefore its entire set of divisors (i.e. its factors) consists of only 4 integers ±1 and ±p
- It can be seen that 1 is not a prime number
- Prime numbers are of utmost importance to certain cryptographic algorithms and most of the techniques used will not work without them
- Any positive integer I ≥ 2 is either a prime or can be expressed as the product of primes.
- This is known as the fundamental theorem of arithmetic.

- Let n and m be two integers
- $n = q \times m + r$ — Remainder
- If gcd of two numbers is 1 they are called as co prime
- $\gcd(a,b) = \gcd(a+kb, b)$

→ Set of common divisors of a, b

= set of common divisors of $a+kb, b$

→ Suppose c is common divisor of a and b

$a = xc$, $b = yc$

$a + kb = xc + kyc = (x+ky)c = \alpha c$

∵ c divides $x+kb$ and c divides b

→ Suppose c divides $a+kb$ and c divides b

$a + kb = xc$ and $b = yc$

$a = xc - kb = xc - kyc = (x-ky)c$

∵ c divides a and b

gcd(a,b) = gcd(a mod b, b)

Euclidean Algorithm

- Let a and b be any two integers

gcd(a,b) = gcd(a mod b, b)

gcd(24,32) = gcd(24, 32 mod 24)
= gcd(24, 8)
= gcd(8, 24 mod 8)
= gcd(8, 0)
⇒ 8

Euclid Algorithm

Input : a and b
output : gcd(a,b)

```
set b = |b|
while (b > 0) do
    set c = b
    set b = a mod b
    set a = c
```

- gcd(a,b)
If b = 0 return a
else return gcd(b, a mod b)

} Recursive

• Euclid's algorithm produced a sequence of remainders $r_0, r_1, r_2 \ldots$

$r_0 = a \bmod b$

$r_1 = b \bmod r_0$

$r_2 = r_0 \bmod r_1$

$\vdots$

till $r_n \neq 0$

$r_{n+1} = r_{n-1} \bmod r_n$

If $r_{n+1} = 0$ then

$r_n = \gcd(a, b)$

Modular Arithmetic (Congruence Relation)

- Let n be an integer
- Let I = set of integers.
- If $a \bmod n = b \bmod n$ then we say a and b are related, i.e.

$a \equiv b \pmod n$

i) **Reflexive** $\Rightarrow$ $a \equiv a \pmod n$

ii) **Symmetric** $\Rightarrow$

$a \equiv b \pmod n$

$\Rightarrow b \equiv a \pmod n$

iii) **Transitivity** $\Rightarrow$ $a \equiv b \pmod n$

$b \equiv c \pmod n$

$\Rightarrow a \equiv c \pmod n$

- If (i), (ii) & (iii) are satisfied then it is a equivance relation

$[0]$ = $\{n, 2n, 3n \ldots\}$
↑ Remainder
0

$[1]$ = $\{n+1, 2n+1, 3n+1, \ldots\}$

$Z_n = \{[0], [1], \ldots [n-1]\}$
↑ set of all equivalence classes.

- $Z_n = \{0,1,2,3,4,5\}$, $n=6$;- If you divide by 6 then remainder will be an element from set Z_n.
- $[r] + [s] = [r+s \bmod n]$
- $(Z_n, +)$ is a group

$Z_6 = \{0,1,2,3,4,5\}$

$(3+5) \bmod 6$

$= 2 \in Z_6$

Modular Inverse

- $(Z_n, +)$ is a cyclic group.

$n = 7$

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$a \in Z_7 - \{0\}$

- Any element in $Z_p - \{0\}$ is a primitive element
- $a + b \equiv 0 \pmod n$

  $b \equiv -a \pmod n$ → Additive Inverse
- Let n be an integer.

  $Z_n = \{0, 1, 2, \ldots n-1\}$

  $a, b \in Z_n$

  $a \times b = a.b \bmod n$

  $[a] \times [b] = [ab \bmod n]$

e.g. $n = 8$

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

If $a.b \equiv 1 \pmod n$

then $b \equiv a^{-1} \bmod n$

	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	
2	0	2	4	6	0	2	4	6	
3	0	3	6	1	4	7	2	5	
4	0	4	0	4	0	4	0	4	
5	0	5	2	7	4	1	6	3	
6	0	6	4	2	0	6	4	2	
7	0	7	6	5	4	3	2	1	

Arithmetic modulo 8

- Co prime

a, b, if gcd of (a, b) is 1

Z_n $a \in Z_n$

$ab \equiv 1 \pmod n$

$b \equiv a^{-1} \pmod n$

a and b are co prime i.e. $gcd(a, n)$

- Let n and a be two integers
- Then we say a has a inverse modulo n if and only if $\exists$ b such that

$a \cdot b \equiv 1 \pmod n$

$b = a^{-1} \pmod n$

- For this a must be coprime with n
e.g. (5, 8)
- Let p be a prime number

$Z_p = \{0, 1, 2, \dots p-1\}$

$Z_p^* = \{1, 2, 3, \dots p-1\} \Rightarrow Z_p - \{0\}$

$(Z_p^*, \times)$ for a multiplicative group i.e. cyclic group.

$(Z_p, +, \times)$ is a field

$Z_n^* = \{0 < a < n \mid \gcd(a, n) = 1\}$

$(Z_n^*, \times)$ is a cyclic group.

AES (Advanced Encryption Std.)

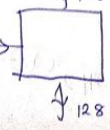
- DES algorithm was broken in 1998 using system that cost about $250,000.
- Triple DES turned out to be too slow for efficiency it has 3 times as many rounds as DES and is thus slower.
- NIST set up a contest in which anyone in the world could take part.
- The contest was announced on the 2nd Jan 1997 and the idea was to develop a new encryption algorithm that would be used for protecting sensitive, non-classified, US govt information.
- Five algorithms selected, i.e.
  ① MARS ② RC6 ③ Rijndael ④ Serpent ⑤ Twofish
- After all these investigation NIST finally chose Rijndael i.e. AES.

Named after two Belgian cryptographers

AES is a symmetric block cipher

It allows variety of key and block sizes

No. of Rounds	Key
10	128
12	192
14	256

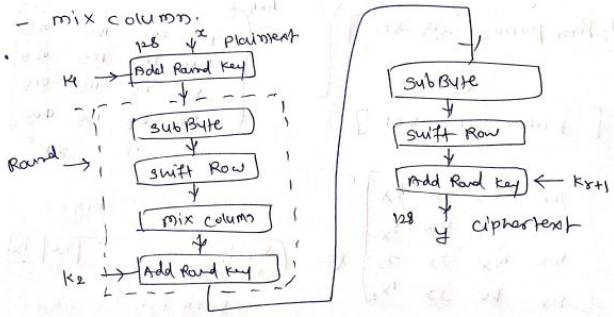


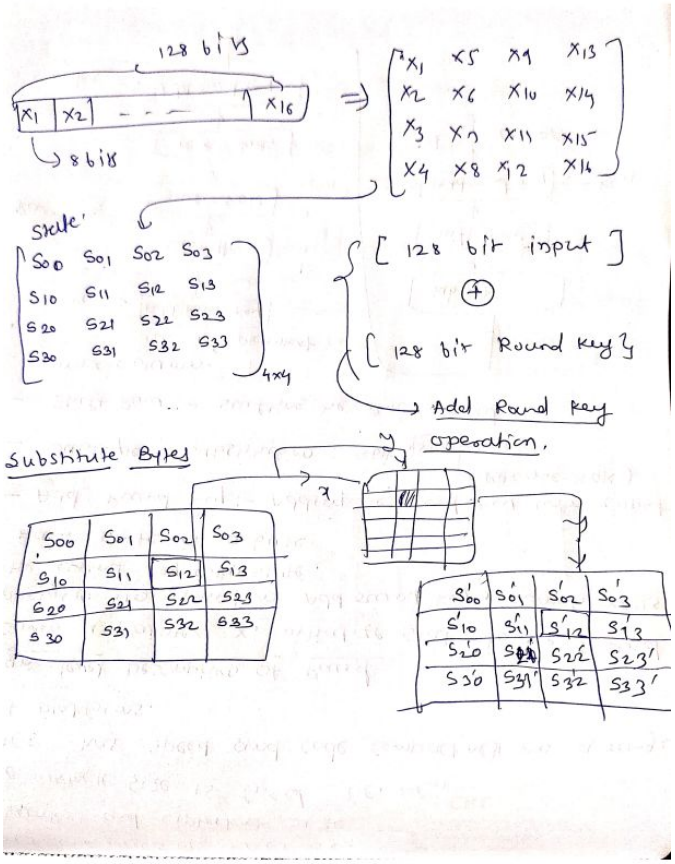
128 bit block.

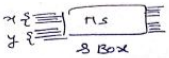
- AES-128, AES 192, AES-256.
- plaintext and ciphertext size i.e. Block size is fixed i.e. 128 bit
- AES has speed and code compactness on a range of platforms.

High level Description of Round

- Given a plaintext X, initialize state to be X and perform an operation Add round key, which XORs the round key with state.
- Each state is a byte
  - Add Round Key :- Adding the round key with input (Bitwise XOR)
  - SubByte :- Substitution ; 8bit → SBox → 8 bit
  - Shift Row :- Shifting the Row input.
  - mix column.

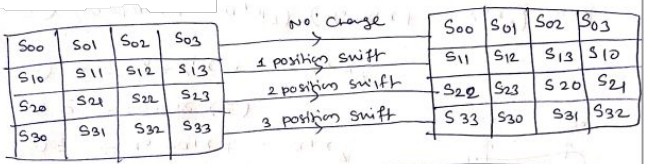



128 bits
X1 X2 - - - X16
8 bit
X1 X5 X9 X13
X2 X6 X10 X14
X3 X7 X11 X15
X4 X8 X12 X16
State
S00 S01 S02 S03
S10 S11 S12 S13
S20 S21 S22 S23
S30 S31 S32 S33
4x4
[128 bit input]
⊕
[128 bit Round key]
Add Round key
Substitute Bytes
x
y
operation.
S00 S01 S02 S03
S10 S11 S12 S13
S20 S21 S22 S23
S30 S31 S32 S33
S'00 S'01 S'02 S'03
S'10 S'11 S'12 S'13
S'20 S'21 S'22 S'23
S'30 S'31 S'32 S'33

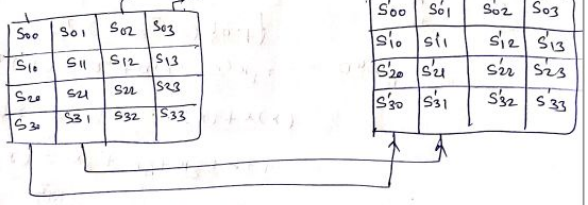


• Each state is replaced by other state byte by byte.

Shift Row



Mix Column



Euclidean Algorithm

- Goal given r_0, r_1 find $\gcd(r_0, r_1) = ?$

e.g. $r_0 = 27, r_1 = 21$

- The idea is to reduce the numbers.

$$\gcd(r_0, r_1) \equiv \gcd(r_0 \bmod r_1, r_1)$$
$$\equiv \gcd(r_1, r_0 \bmod r_1)$$

e.g. $\gcd(27, 21) \equiv \gcd(27 \bmod 21, 21)$
$$\equiv \gcd(6, 21)$$
$$\equiv \gcd(6, 3)$$
$$\equiv 3$$

$27 = 1 \cdot 21 + 6$
$21 = 3 \cdot 6 + 3$
$6 = 2 \cdot 3 + 0$

$\gcd(973, 301) = 3 \cdot 301 + 70$
$301 = 4 \cdot 70 + 21$
$70 = 3 \cdot 21 + 7$
$21 = 3 \cdot 7 + 0$

④ ⑦

Extended Euclidean Algorithm

- Given : r_0, r_1
  Goal : $\gcd(r_0, r_1) = \underbrace{s r_0 + t r_1}$ Compute these coefficients.

$gcd(r_0, r_1) \Rightarrow r_0 = q_1 r_1 + r_2, \; r_2 = s_2 r_0 + t_2 r_1$

$gcd(r_1, r_2) \Rightarrow r_1 = q_2 r_2 + r_3, \; r_3 = s_3 r_0 + t_3 r_1$

$\vdots \qquad\qquad \vdots$

$gcd(r_{l-2}, r_{l-1}) \Rightarrow r_{l-2} = q_{l-1} r_{l-1} + r_l,$

$r_l = s_l r_0 + t_l r_1$

$r_{l-1} = q_l r_l + \phi$ $\quad = \text{LCD}$

Euclidean Algorithm

Input :- Positive integers r_0 and r_1 with $r_0 > r_1$

output :- $gcd(r_0, r_1)$

Initialization :- $i = 1$

Algorithm

DO

$i = i + 1$

$r_i = r_{i-2} \bmod r_{i-1}$

WHILE $r_i \neq 0$

RETURN

$gcd(r_0, r_1) = r_{i-1}$

- we will compute sequence $x_0, x_1, x_2, \ldots$ and $y_0, y_1, y_2, \ldots$ such that $r_k = a x_k + b y_k$ where $r_0, r_1, r_2, \ldots$ are the sequence of remainders in Euclid Algorithm.

- $r_0 = a$, $r_1 = b$

$(x_0, y_0) = (1, 0)$

$(x_1, y_1) = (0, 1)$

$r_0 = a = a \cdot 1 + b \cdot 0 = a x_0 + b y_0$

$r_1 = b = a \cdot 0 + b \cdot 1 = a x_1 + b y_1$

- $i > 0$, set $q_{i+1} = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$ and

$r_{i+1} = r_{i-1} - r_i q_{i+1}$

- so r_{i+1} is the next remainder

- we set, $x_{i+1} = x_{i-1} - x_i q_{i+1}$

$y_{i+1} = y_{i-1} - y_i q_{i+1}$

- $r_k = a x_k + b y_k$, for all k

For $k = 0, 1$ it is true.

- we assume it is true for $k = i-1$ and $k = i$

$r_{i-1} = a x_{i-1} + b y_{i-1}$

$r_i = a x_i + b y_i$

$$r_{i+1} = r_{i-1} - r_i q_{i+1}$$

$$= a x_{i-1} + b y_{i-1} - (a x_i + b y_i) q_{i+1}$$

$$= \underbrace{a(x_{i-1} - x_i q_{i+1})}_{x_{i+1}} + \underbrace{b(y_{i-1} - y_i q_{i+1})}_{y_{i+1}}$$

$r_k = a x_k + b y_k$, $\forall k$

- Eventually $r_{n+1} = 0$ and $r_n = \gcd(a, b)$

$= a x_n + b y_n$

- Let b and m be two integers such that $\gcd(b, m) = 1$ i.e. $b \perp m$

$1 = bx + my$, for some integer x and y

$x = b^{-1} \bmod y$

Fermat's Little Theorem

- Let p be a prime, and a be an integer such that $a \perp p$ i.e. $\gcd(a, b) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}$$

$Z_p = \{0, 1, 2, \dots, p-1\}$

$Z_p^* = Z_p - \{0\} = R$ i.e. Reduced Residue System mod p

- Since p is a prime, then

$aR = \{ar \mid r \in R\}$

$aR = \{a, 2a, 3a \cdots, (p-1)a\}$

$aR = R \Rightarrow$ Claim

- Suppose, $na \equiv ma \pmod p$

$a \perp p$

$na\,a^{-1} \equiv maa^{-1} \pmod p$

$n \equiv m \pmod p$

- $a, 2a, 3a \cdots (p-1)a$ are congruent to $1, 2, \cdots p-1$ in some order

- $aR = R$.

$a \cdot 2a \cdot 3a \cdots (p-1)a = 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod$

$a^{p-1}(p-1)! \equiv (p-1)! \pmod p$

$(p-1)! = x \quad x \perp p$

$a^{p-1} x \cdot x^{-1} = x\,x^{-1} \pmod p$

$$a^{p-1} \equiv 1 \bmod p$$

Euler's Phi function

- Let n be an integer

$Z_n = \{0, 1, 2, \dots n-1\}$

$Z_n^* = \{0 < r < n \mid r \perp n\}$ $\Rightarrow \perp \Rightarrow$ Coprime

(Integer)

$|Z^*| = \phi(n)$

Z_n^*

$\phi(n)$ = No. of +ve integers < less than n and coprime to n.

- Let p be a prime then

$\phi(p) = p-1$

$Z_n^* = \{1, 2, \dots p-1\}$

- If $p = 7$, then $Z_7^* = \{1, 2, 3, 4, 5, 6\}$
- $n = 12$, $\phi(12) = ?$

$Z_{12}^* = \{1, 5, 7, 11\}$

$\phi(12) = |Z_{12}^*| = 4$

- Let n and m be two integers such that they are relatively prime ($n \perp m$) then

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$

• $n = 3,\ m = 4$

$\phi(3 \cdot 4) = \phi(12) = 4$

$\phi(3) = 2\ ,\ \phi(4) = 2$

$\phi(3 \cdot 4) = 2 \cdot 2 = 4$

Euler's Theorem

• Let n and a be two integers such that a & n ($\gcd(a, n) = 1$) then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

$n = p$ = prime

$$a^{\phi(p)} = a^{p-1} \equiv 1$$

• $\mathbb{Z}_n^* \{0 < r < n \mid r \perp n\} = R$ (Reduced Residue class mod n)

if $a \perp n$ then $aR = \{ar \mid r \in R\}$

• $aR = R$, ~~$x \equiv y \pmod{n}$~~

~~$x \equiv y \pmod{\phi(n)}$~~

$$a^{\phi(n)} \cdot \prod_{r \in R} r \equiv \prod_{r \in R} r \mod n$$

$$\prod_{r \in R} r \perp n = z$$

$$a^{\phi(n)} z \equiv z \pmod{n}$$

- $z = nr, r \in R \Rightarrow r \perp n$

  $nr \perp n$
  $r \in R$

  $a^{\phi(n)} \equiv 1 \pmod{n}$

- $n = 21, \phi(n) = \phi(21) = \phi(3 \cdot 7) = \phi(3)\phi(7)$

$\Rightarrow 2 \cdot 6 \Rightarrow 12$

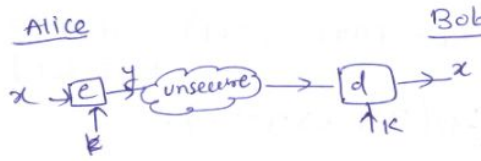
- $a = 5$

  $5^{12} \equiv 1 \pmod{21}$

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 encryption of messages.

Diffie Hellman Key Exchange



public parameters p, α

Alice

$a = K_{prA} \in \{2, 3, \dots p-2\}$

$A \equiv \alpha^a \bmod p = K_{pubA}$ —A→

Bob

$b = K_{prB} \in \{2, 3, \dots p-2\}$

$B \equiv \alpha^b \bmod p \equiv K_{pubB}$

←B—

$K_{AB} \equiv B^a \bmod p$

$K_{AB} \equiv A^b \bmod p$

Key Exchange

$y = AES_{K_{AB}}(x)$ —y→ $AES^{-1}_{K_{AB}}(y) = x$

Alice Computes :-

$$B^a = (\alpha^b)^a = \alpha^{ab} \bmod p$$

Bob Computes

$$A^b = (\alpha^a)^b = \alpha^{ab} \bmod p$$

Finite Groups

Group ≈ "Set of elements and 1 group operation".

- A group is a set of elements G together with an operation ∘ which combines two elements of a. A group has following properties.

① The group operation ∘ is closed. i.e.
$\forall\ a, b \in G$, it holds that $a \circ b = c \in G$.

② The group operation is associative. i.e.
$a \circ (b \circ c) = (a \circ b) \circ c \quad \forall\ a, b, c \in G$.

③ There is an element $1 \in G$ called the neutral element (or identity element) such that
$a \circ 1 = 1 \circ a = a \quad \forall\ a \in G$.

④ For each $a \in G$ there exists an element $a^{-1} \in G$ called the inverse of a, such that
$a \circ a^{-1} = a^{-1} \circ a = 1$

⑤ A group G is abelian (or commutative) if furthermore $a \circ b = b \circ a \quad \forall\ a, b \in G$.

- First 4 properties ⇒ Group.
  All 5 properties ⇒ Abelian Group.
- Is $(\mathbb{Z}_9, \times)$ a group?
  $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
  $\circ \Rightarrow \times \Rightarrow$ multiplication mod 9.
  Problem:- Inverses only exists for elements a:
  i.e $gcd(a, 9) = 1$

for 0, 3, 6 inverse property not satisfied ⑥

Def :- $\mathbb{Z}_9^*$ = {1, 2, 4, 5, 7, 8} is a multiplicative group.

- The set $\mathbb{Z}_n^*$ which consists of all integers $i = 0, 1, \ldots n-1$ for which $\gcd(i, n) = 1$ forms an abelian group under multiplicative modulo n. The identity element is $e = 1$.
- $\mathbb{Z}_p^*$, p is prime forms a multiplicative group.

$$\mathbb{Z}_p^* = \{1, 2 \ldots p-1\}$$

Cyclic Groups

- Finit Group :- A group $(G, \circ)$ is finite if it has a finite number of elements. we denote cardinality or order of the group G by $|G|$

e.g.

$|\mathbb{Z}_9^*| \Rightarrow 6$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

- what happens if we compute all powers of $a = 3$?

$a^1 = 3$, $a^2 = 9$, $a^3 = 27 \equiv 5$, $a^4 \equiv 4$, $a^5 = 1$

↳ $a^3 \cdot a = 5 \cdot 3$

$a^6 = a^5 \cdot a \equiv 1 \cdot 3$, $a^7 = a^6 \cdot a \equiv 3 \cdot 3 = 9$

- It forms a cycle of remainders

$3^{78122457 63} \bmod 11 = \overline{}$

↑ only 5 possibilities

cycle length is 5 here.

$Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$a^1 = 2$
$a^2 = 4$
$a^3 = 8$
$a^4 = 5$
$a^5 = 10$
$a^6 = 9$
$a^7 = 7$
$a^8 = 3$
$a^9 = 6$
$a^{10} = 1$
$a^{11} = 2$

2^i

$ord(2) = 10$

The order $ord(a)$ of an element a of a group $(G, \circ)$ is the smallest positive integer k such that

$$a^k = \underbrace{a \circ a \circ \dots \circ a}_{k \text{ times}} = 1$$

where 1 is the identity element of G.

- A group which contains an element α with maximum order $ord(\alpha) = |G|$ is said to be cyclic. Elements with maximum order are called primitive elements or generators.

e.g. $a = 2$ is a generator for set Z_{11}^*.

- Cyclic groups For every prime p $(Z_p^*, \cdot)$ is an abelian finite cycle group.

Properties of cyclic Group

Let $a \in G$, G is acyclic group.

(1) $a^{|G|} = 1$

(2) $ord(a)$ divides $|G|$

Property 1

Fermat's little theorem for Z_p^*

$$a^p \equiv a \bmod p$$

$$a^{p-1} \equiv 1 \bmod p$$

$$|\mathbb{Z}_p^*| = p-1$$

$$a^{p-1} = a^{|\mathbb{Z}_p^*|} = 1$$

Property 2

e.g.

$|\mathbb{Z}_{11}^*| = 10$

what are the possible elements orders in $\mathbb{Z}_{11}^*$?

possible cycle length $\in \{1, 2, 5, 10\}$

- cyclic groups can ~~make~~ can be used in discrete logarithm problems.

$\mathbb{Z}_{47}^*$, 5 is generator

- For this a must be coprime with n
e.g. (5, 8)
- Let p be a prime number

$Z_p = \{0, 1, 2, \dots p-1\}$

$Z_p^* = \{1, 2, 3, \dots p-1\} \Rightarrow Z_p - \{0\}$

$(Z_p^*, \times)$ for a multiplicative group i.e. cyclic group.

$(Z_p, +, \times)$ is a field

$Z_n^* = \{0 < a < n \mid \gcd(a, n) = 1\}$

$(Z_n^*, \times)$ is a cyclic group.

Extended Euclidean Algorithm

- Let n be an integer and a be an integer $a \perp n$ ($\gcd(a, n) = 1$), $\exists\, b$ such that

$a \equiv 1 \pmod n$, $b = a^{-1} \bmod n$

$\gcd(a, b)$ multiplicative inverse

$a = 41$, $b = 54$.

$\gcd(41, 54)$

$= \gcd(54, 54 \bmod 41)$

$= \gcd(41, 13)$

$\Rightarrow \gcd(13, 41 \bmod 13)$

$\Rightarrow \gcd(13, 2)$

$\Rightarrow \gcd(2, 13 \bmod 2)$

$= \gcd(2, 1)$

$\Rightarrow \underline{1}$

- $\gcd(a, b) = ax + by$, for some integer x and y
- e.g. $\gcd(41, 54) = 1 \Rightarrow 41x + 54y$

$54 = 1 \cdot 41 + 13$

$41 = 3 \cdot 13 + 2$

$13 = 6 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

gcd

$1 = 13 - 6 \cdot 2$

$= 13 - 6 \cdot (41 - 3 \cdot 13)$

$= 19 \cdot 13 - 6 \cdot 41$

$= 19 \cdot (54 - 1 \cdot 41) - 6 \cdot 41$

$= 19 \cdot 54 - 25 \cdot 41$

$= 54 \cdot (19) + 41 \cdot (-25)$

x y

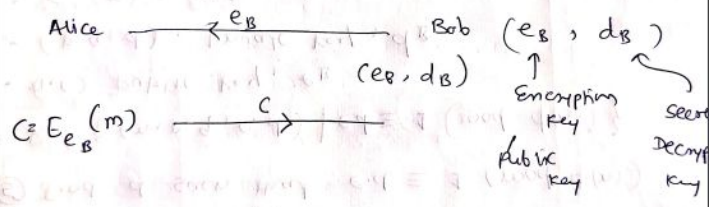
- The gcd of two integers a and b can be written as $ax + by$ for some integers x and y.

$\boxed{\gcd(a, b) = ax + by}$

RSA

→ 1997, by Rivest, Shamir and Adelman at MIT

→ Public Key



$D_{d_B}(C)$

$= D_{d_B}(e_{e_B}(m$

$= m$

RSA set up

① select two prime numbers p and q

② $n = pq$

③ $\phi(n) = (p-1)(q-1)$

④ Choose an integer e such that $\gcd(e, \phi(n))$

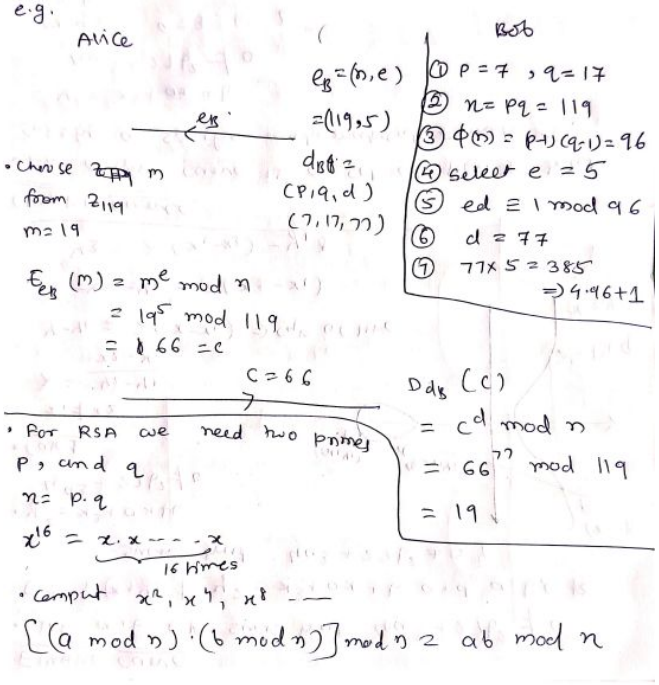
⑤ Find d such that $e \cdot d \equiv 1 \pmod{\phi(n)}$

- $K = \{(n, p, q, e, d) \mid ed \equiv 1 \pmod{\phi(n)}\}$
- (n, e) public key, e_B
- (p, q, d), private key, d_B
- $E_{e_B}(m) = m^{e_B} \bmod n = c$
- $m = c^{d_B} \bmod n = D_{d_B}(c)$
- $c^{d_B} \bmod n$
- $c^{d} \bmod n$
- $(me)^{d} \bmod n$
- $m^{ed} \bmod n$
- $ed = K\phi(n) + 1$
- $m^{K\phi(n)+1} \bmod n$
- $(m^{\phi(n)})^{K} \cdot m \bmod n$
- $(m^{\phi(n)} \bmod n)^{K} \cdot m \bmod n$

$\phi(n)$ ⇒ Euler's pw function

⇒ No. of integers $< n$ which are co prime to n

e.g.



• For RSA we need two primes p, and q

$n = p \cdot q$

$x^{16} = \underbrace{x \cdot x \cdots x}_{16 \text{ times}}$

• Compute $x^2, x^4, x^8 \cdots$

$[(a \bmod n) \cdot (b \bmod n)] \bmod n = ab \bmod n$

Elliptic curve

- An elliptic curve is a set of points that satisfy a specific mathematical equation.

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

$$4a^3 + 27b^2 \neq 0$$

(x, y) $\quad a = 3, b = 2$

$(2, 4)$

$$4^2 = 2^3 + 3 \cdot 2 + 2$$

$$16 = 16$$

- Elliptic curver over finite field
- Finite field example GF(5)

$y^2 = x^3 + ax + b \mod p$

$4a^3 + 27b^2 \mod p \neq 0$

- $Z_{11} = \{0, 1, 2 \text{ —— } 10\}$
- $y^2 \equiv x^3 + ax + b \mod p$

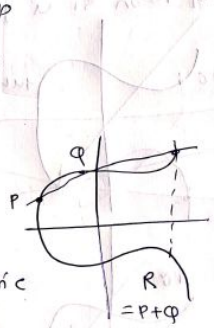
  $4a^3 + 27b^2 \mod p \neq 0$

$y^2 \mod p \equiv x^3 + ax + b \mod p$

$y^2 \mod 11 \equiv x^3 + x + 1 \mod 11$

$P + Q =$

Let the points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be in the elliptic group $E_p(a, b)$ and $Q \neq -P$



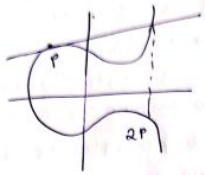
The rules for addition over Elliptic group $E_p(a, b)$ is

$$x_3 = \lambda^2 - x_1 - x_2 \mod p$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \mod p$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \mod p \quad , P \neq Q$$

- P+Q will also be on Ec , P ≠ Q
- P+P = 2P



- points 2P, 3P, 4P will be on EC
- If we have P and another point nP.
- Finding nP is difficult, if n is very la
- This concept is used EC cryptography
- P is called generator, and we find n.P
- Adding a point P with P

Let's consider the point P(x,y) in the EC group $E_p(a,b)$

The rules for addition of P with P over E

Elliptic group $E_p(a,b)$ is

$x_3 = (\lambda^2 - x) - x \bmod p$

$y_3 = \lambda(x - x_3) - y \bmod p$

$\lambda = \frac{3x^2 + a}{2y_1} \bmod p$

$x_3 = (\lambda^2 - x) - x \bmod p$

$y_3 = \lambda(x - x_3) - y \bmod p$

$\lambda = \frac{3x^2 + a}{2y_1} \bmod p$

- Adding point with itself
- $P(4,6)$ $E_{11}(1,1)$

$$\lambda = \frac{3x^2 + a}{2y} \bmod p$$

$$= \frac{3 \cdot 4^2 + 1}{2 \cdot 6} \bmod 11 = \frac{49}{12} \bmod 11 = 5$$

$x_3 = 6$, $y_3 = 6$

- $2P(6,6)$ $E_{11}(1,1)$

$y^2 \bmod 11 = x^3 + x + 1 \bmod 11$

- we have a set of points of EC. If we add two points. the resultant point will be in same set.
- Elliptic curve E is over finite field is a finite abelian group
- Considers points $P, Q \in E(P)$ then $P+Q \in E(P)$
- If we add a point with point at infinity the we get the point itself.
-

* It is an assymetric key cryptography.

Steps

① Encode a plain text message as a point on the curve
② Establish the public key and private key
③ Encrypt the message using the public key
④ Decrypt using the private key.

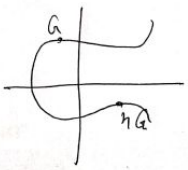
① Encode the plaintext message as a point on the curve.

- Lets consider the point to be the encodeded plain text message on the curve
- (4, 6) => plaintext message as a point on curve

② Establish the public key and the private key

- Choose a generator point $G \in E_p(a,b)$
- select a private key n
- Compute public key as $P_u = nG$
- n could be from $1 \leq n \leq 10$

③ Encrypt the message using the public key



$C = [(kG), (m + kP_u)]$

k is a random number

$kG \Rightarrow$ Adding G to itself k times

(4) Decrypt using the private key

- $m = C_2 - [nC_1]$

Chinese Remainder Theorem

- Let $n_1, \ldots, n_k$ be pairwise coprime (i.e. $gcd(n_i, n_j) = 1$ whenever $i \neq j$)
- Then the system of k equations

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\ldots$$
$$x \equiv a_k \pmod{n_k}$$

has a unique solution for x modulo N

- $x \equiv 2 \pmod 3$
  $x \equiv 3 \pmod 4$
  $x \equiv 1 \pmod 5$
- $x = a_1 N_1 C_1 + a_2 N_2 C_2 + \ldots a_k N_k C_k \pmod N$
- Formula to compute N

$N = n_1 * n_2 * \cdots * n_k$

$N_i = N/n_i$

- Lets use the formula to find x

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 4$

$x \equiv 1 \pmod 5$

- Check whether 3, 4, and 5 are coprime
- $a_1 = 2$, $a_2 = 3$, $a_3 = 1$;
- $n_1 = 3$, $n_2 = 4$, $n_3 = 5$
- $N = n_1 * n_2 * n_3 = 60$
- $N_1 = 20 = n_2 * n_3$

$N_2 = 15 = n_1 * n_3$

$N_3 = 12 = n_1 * n_2$

- $C_1, C_2, C_3 \Rightarrow$ multiplicative Inverse
- $N_1 = 20$, $N_2 = 15$, $N_3 = 12$

$N_1 \cdot C_1 = 1 \bmod n_1$

$N_1 C_1 \bmod n_1 = 1$

$20\, C_1 \bmod 3 = 1$

$20/3 = 2 \rightsquigarrow$

$2 \cdot c_1 \bmod 3 = 1$

$2 \cdot 2 \bmod 3 = 1$

$c_1 = 2$

- $N_2 \cdot c_2 = 1 \bmod m_2$

  $N_2\, c_2 \bmod m_2 = 1$

  $15\, c_2 \bmod 4 =$

  $15/4 = 3$

  $3 \cdot c_2 \bmod 4 = 1$

  $3 \cdot 3 \bmod 4 = 1$

  $c_2 = 3$

- $N_3\, c_3 = 1 \bmod m_3$

  $12\, c_3 \bmod 5 = 1$

  $12/5 = 2$

  $2 \cdot c_3 \bmod 5 = 1$

  $2 \cdot 3 \bmod 5 = 1$

  $c_3 = 3$

$x = (2 \times 20 \times 2 + 3 \times 15 \times 3 + 1 \times 12 \times 3) \bmod 60$

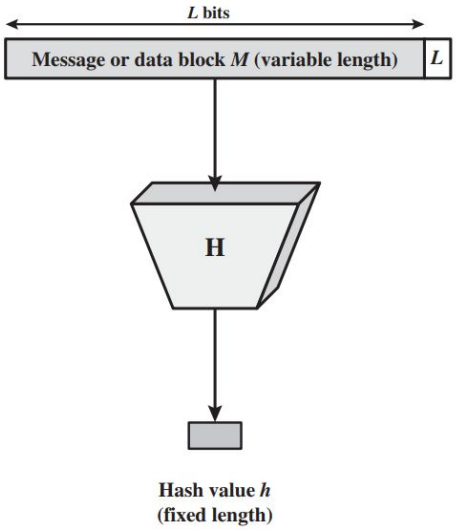
$x = 11$

Testing for Primality(Miller Rabin)

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

Cryptographic hash Functions

A hash function H accepts a variable-length block of data as input and produces a fixed-size hash value .

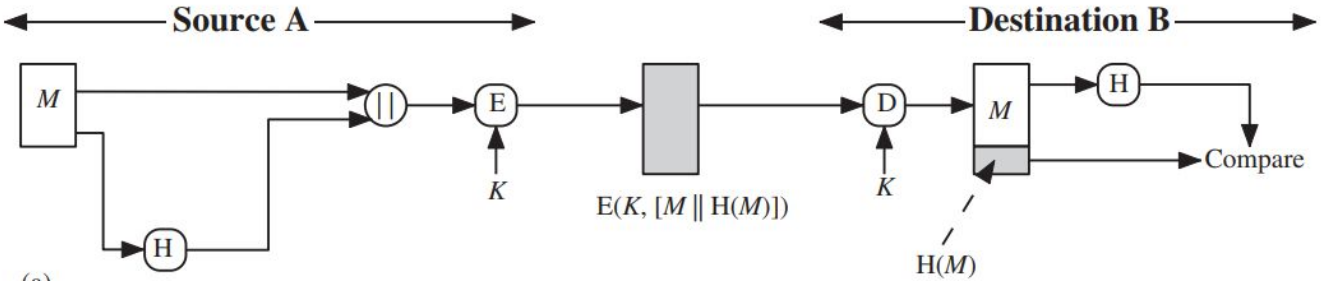


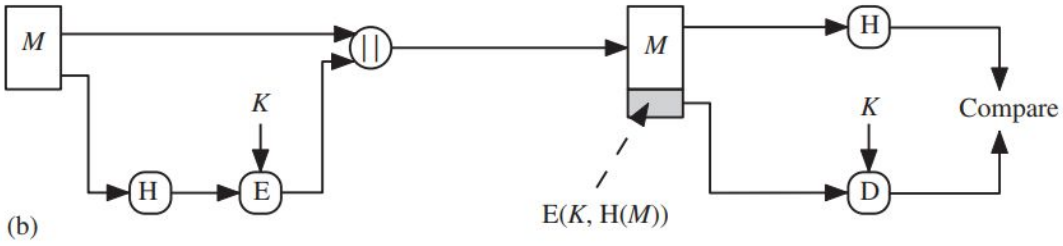
Message Authentication

Message authentication is a mechanism or service used to verify the integrity of a message.

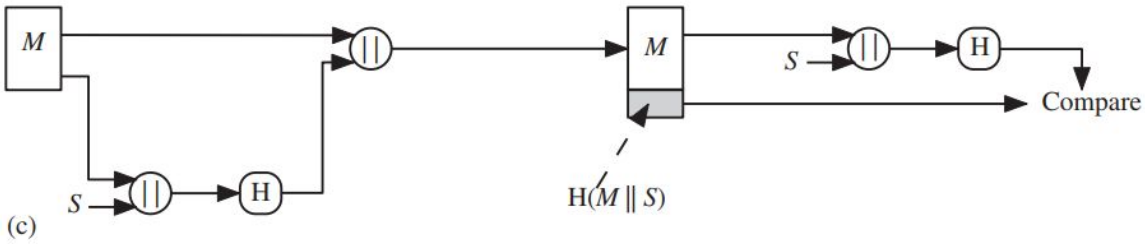
Message authentication assures that data received are exactly as sent

When a hash function is used to provide message authentication, the hash function value is often referred to as a message digest.

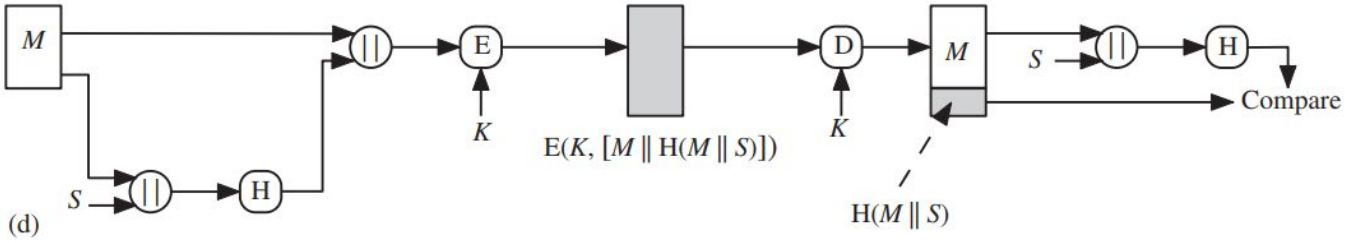

Source A
Destination B
M
||
E
K
H
E(K, [M || H(M)])
D
K
M
H
Compare
H(M)


M
||
K
H
E
M
H
K
Compare
D
E(K, H(M))

(b)



(c)



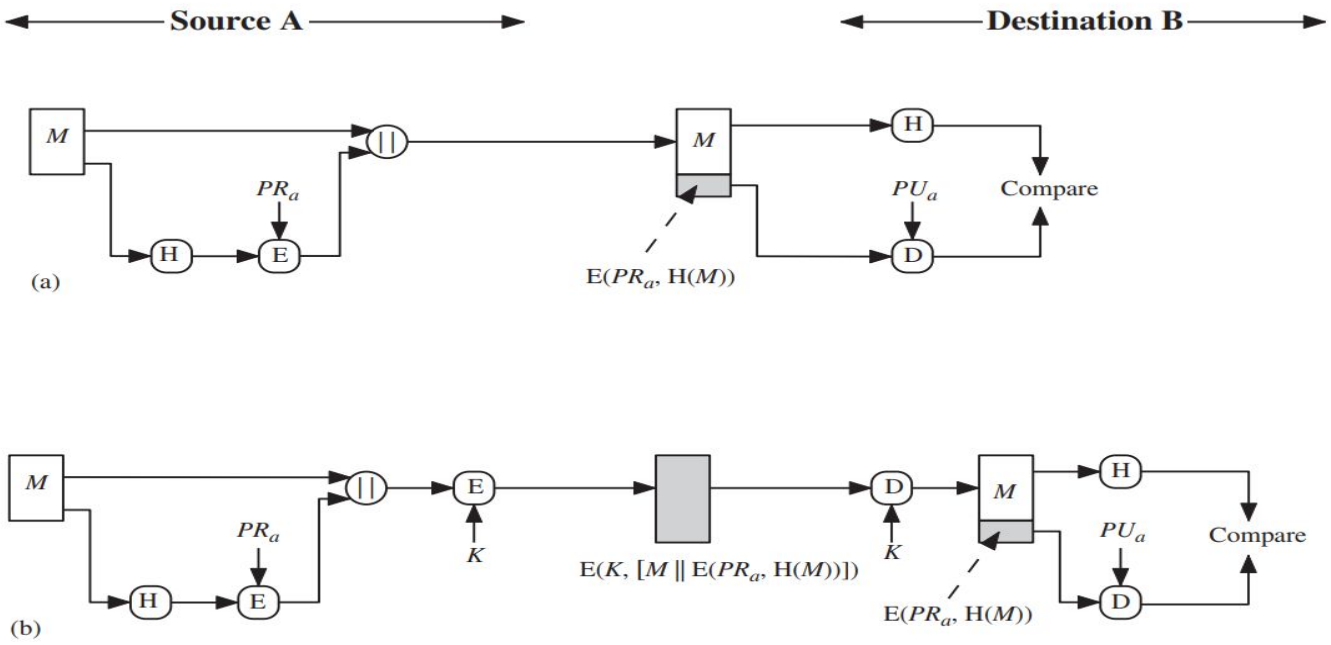
(d)

Digital Signatures

In the case of the digital signature, the hash value of a message is encrypted with a user's private key.

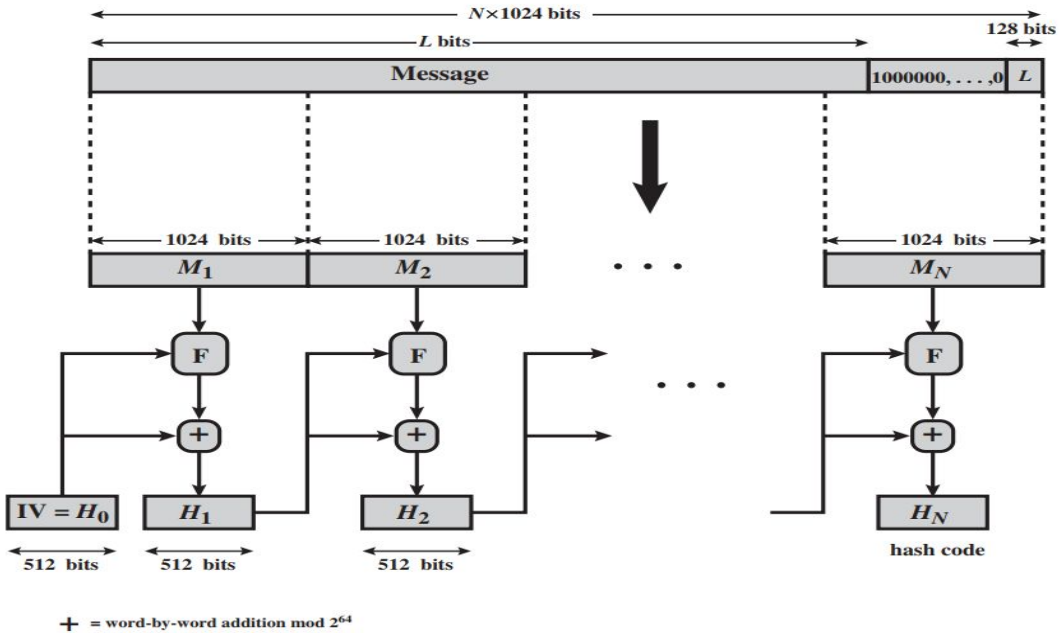
Anyone who knows the user's public key can verify the integrity of the message that is associated with the digital signature.

Examples of Digital Signature



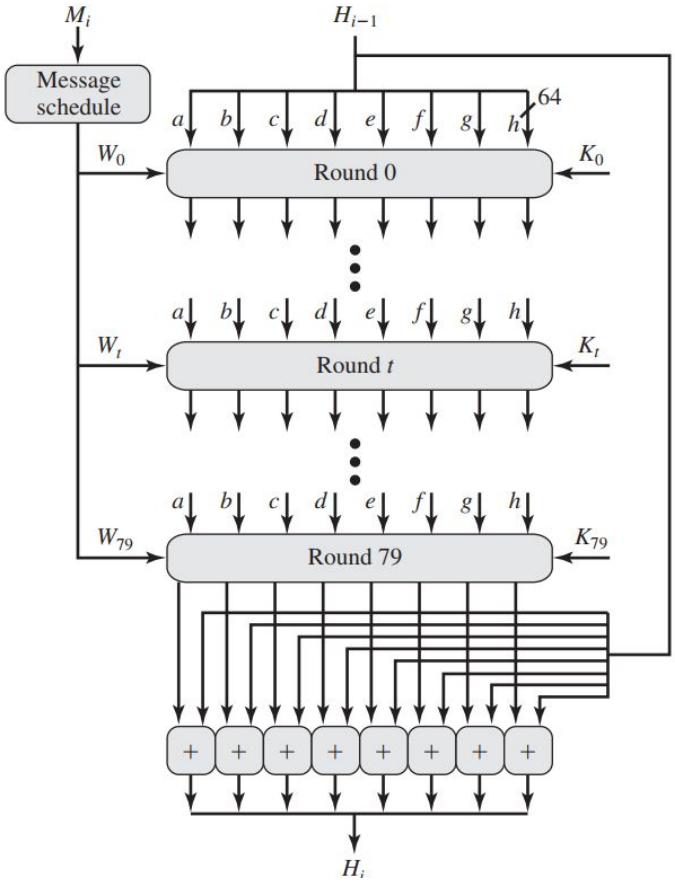
Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	$H(x)$ is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that $H(y) = h$.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.
Pseudorandomness	Output of H meets standard tests for pseudorandomness.

Message Digest Generation Using SHA-512



Processing of a Single 1024-Bit Block

After all 1024-bit blocks have been processed, the output from the th stage is the 512-bit message digest.



$$H_0 = \text{IV}$$

$$H_i = \text{SUM}_{64}(H_{i-1}, \text{abcdefgh}_i)$$

$$MD = H_N$$

where

IV	=	initial value of the abcdefgh buffer, defined in step 3
abcdefgh_i	=	the output of the last round of processing of the ith message block
N	=	the number of blocks in the message (including padding and length fields)
SUM_{64}	=	addition modulo 2^{64} performed separately on each word of the pair of inputs
MD	=	final message digest value

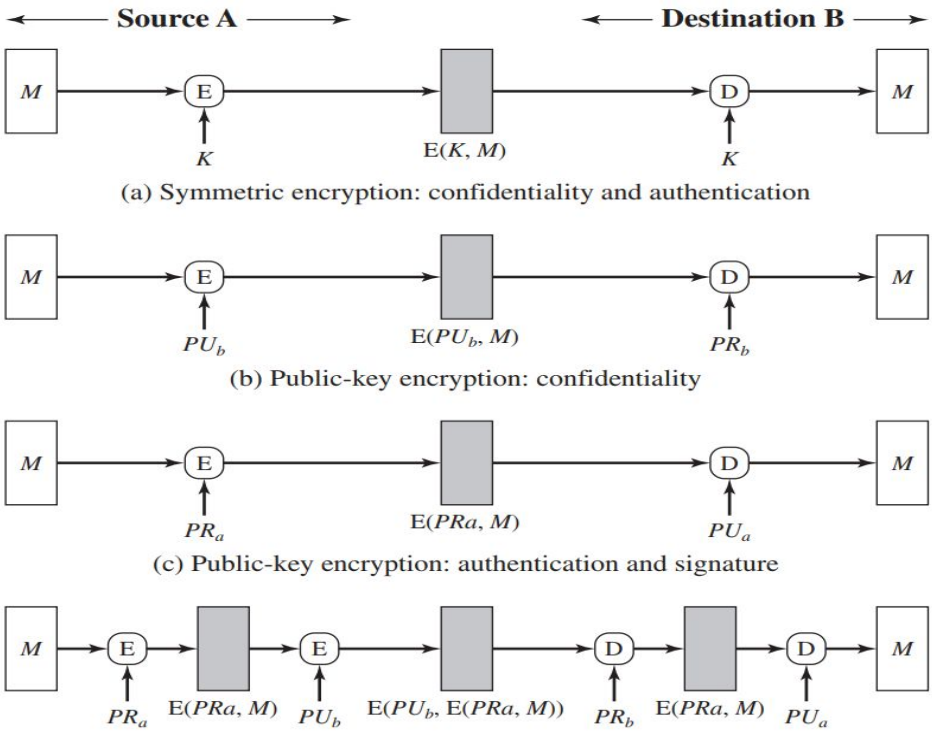
Message Authentication Code

A message authentication code (MAC) is an algorithm that requires the use of a secret key.

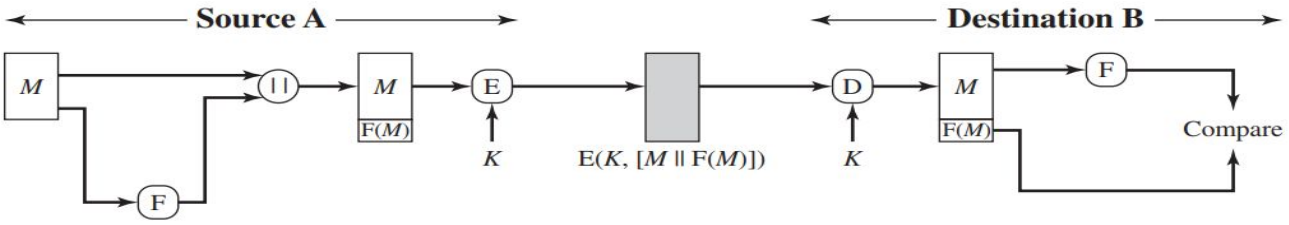
A MAC takes a variable-length message and a secret key as input and produces an authentication code.

A recipient in possession of the secret key can generate an authentication code to verify the integrity of the message

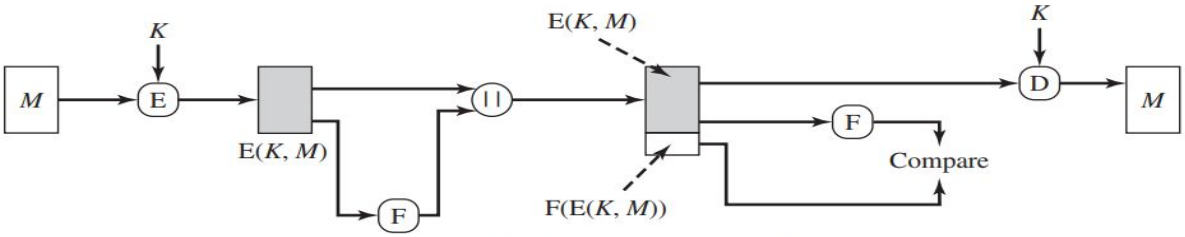
Basic Uses of Message Encryption



Internal and External Error Control



(a) Internal error control



(b) External error control

MAC

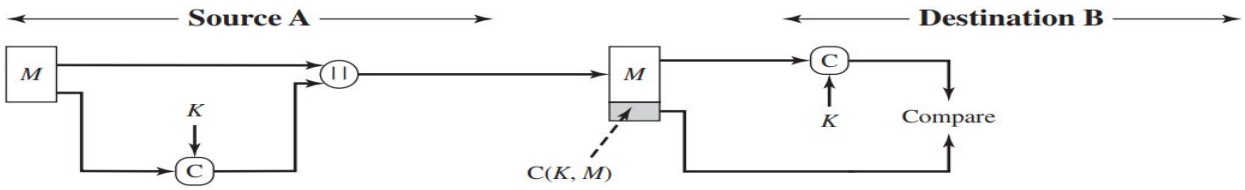
Involves the use of a secret key to generate a small fixed-size block of data, known as a cryptographic checksum or MAC, that is appended to the message.

$$\text{MAC} = \text{MAC}(K, M)$$

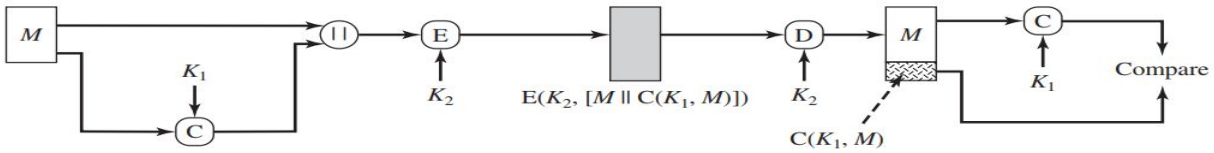
where

M = input message
C = MAC function
K = shared secret key
MAC = message authentication code

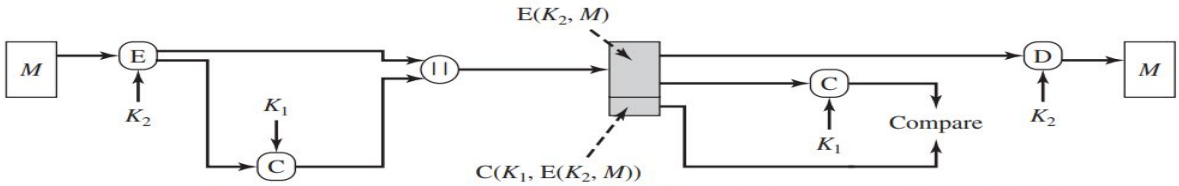
Basic Uses of Message Authentication code (MAC)



(a) Message authentication



(b) Message authentication and confidentiality; authentication tied to plaintext



(c) Message authentication and confidentiality; authentication tied to ciphertext

Security of Hash functions and MAC

Brute Force

the level of effort for brute-force attack on a MAC algorithm can be expressed as $\min(2^k, 2^n)$, n bit hash code and k bit secret.

Cryptanalysis

Due to the diversity in MAC structures and limited research on attacks, it is difficult to generalize the cryptanalysis of MACs,

MD5 Algorithm

Cryptographic hash functions take data input (or massage) and generate a fixed size result (or digest). The result is called checksum.

One thing to see here is that the hash functions are not encryption because you cannot decrypt the input from the output.

MD5 creates a 128-bit message digest from the data input which is typically expressed in 32 digits hexadecimal number.

MD5 hashes are unique for different inputs regardless of the size of the input.

Hexadecimal representation of input by md5

It is widely used to make sure that the transferred file in a software has arrived safely.

It is also used in database to store passwords as hash instead of the original input.

1 Append Padding Bits

The first step is to extend(padded) the b-bits message(input) so that the length of the message is equal to 448, modulo 512.

First a ’1’ bit is appended to the message and then a series of ’0’ bits

2 Append Length

Now we take the original message and make a 64-bit representation of the original b-bit message.

Now the message has a length that is exactly divisible by 512 or the message is multiple of 512.

3. Initialize MD Buffer

MD5 uses a four word buffer each 32-bits long constants. We denote them by A,B,C,D.

4. Process Message in 16-word Blocks

Auxiliary functions take three inputs of 32-bits word and gives an output of 32-bit word.

The auxiliary function apply logical and, or and xor to the inputs.

Later on we will show how we use each of these 4 functions in 4 rounds (each round has 16 operations).

$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$
$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$
$H(B,C,D) = B \oplus C \oplus D$
$I(B,C,D) = C \oplus (B \vee \neg D)$

The Table

The table consists of 64-elements where each element is computed using mathematical sin function:

$$abs(\sin(i+1)) \times 2^{32}$$

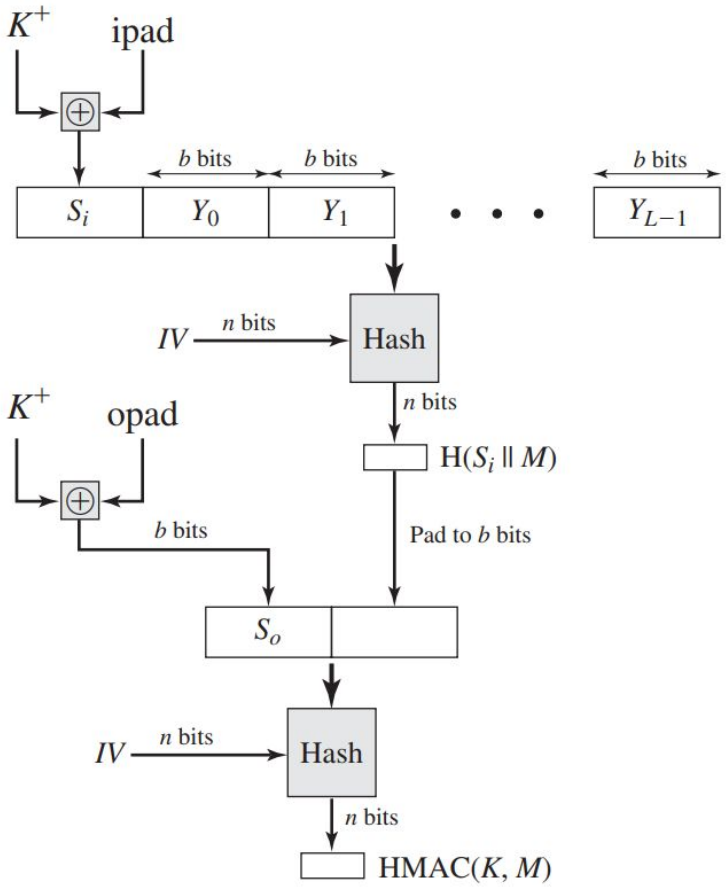
Recall from step 2, where we divided the message into blocks of 512-bits and then each 512-bits block to 16 words of 32-bits.

Those 16 word (each 32-bits) blocks are denoted as M[0....N-1].

Now for each word block we perform 4 rounds where each round has 16 operations. Each round follows basic pattern.

HMAC (Hash-based Message Authentication Code)

- H = embedded hash function (e.g., MD5, SHA-1, RIPEMD-160)
- IV = initial value input to hash function
- M = message input to HMAC (including the padding specified in the embedded hash function)
- Y_i = i th block of $M, 0 \leq i \leq (L - 1)$
- L = number of blocks in M
- b = number of bits in a block
- n = length of hash code produced by embedded hash function
- K = secret key; recommended length is $\geq n$; if key length is greater than b, the key is input to the hash function to produce an n-bit key


K^+
ipad
b bits
b bits
b bits
S_i
Y_0
Y_1
Y_{L-1}
IV
n bits
Hash
n bits
K^+
opad
$H(S_i \| M)$
b bits
Pad to b bits
S_o
IV
n bits
Hash
n bits
HMAC(K, M)

K^+ = K padded with zeros on the left so that the result is b bits in length

ipad = 00110110 (36 in hexadecimal) repeated $b/8$ times

opad = 01011100 (5C in hexadecimal) repeated $b/8$ times

Then HMAC can be expressed as

$$\text{HMAC}(K, M) = \text{H}[(K^+ \oplus \text{opad}) \| \text{H}[(K^+ \oplus \text{ipad}) \| M]]$$

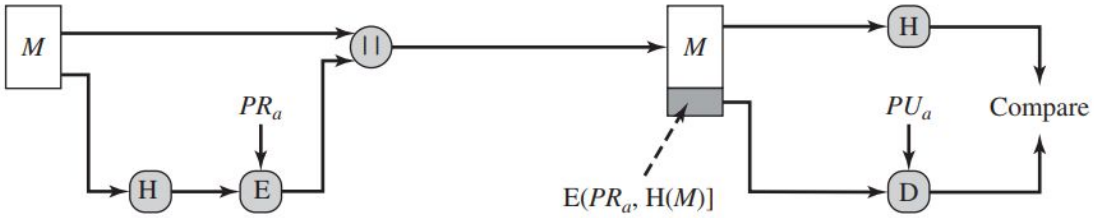
We can describe the algorithm as follows.

1. Append zeros to the left end of K to create a b-bit string K^+ (e.g., if K is of length 160 bits and $b = 512$, then K will be appended with 44 zeroes).
2. XOR (bitwise exclusive-OR) K^+ with ipad to produce the b-bit block S_i.
3. Append M to S_i.
4. Apply H to the stream generated in step 3.
5. XOR K^+ with opad to produce the b-bit block S_o.
6. Append the hash result from step 4 to S_o.
7. Apply H to the stream generated in step 6 and output the result.

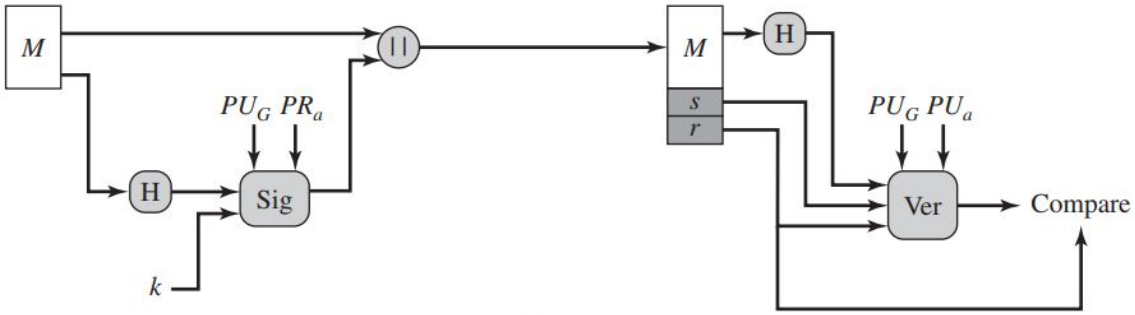
Digital Signature Standard

The DSS uses an algorithm that is designed to provide only the digital signature function.

Unlike RSA, it cannot be used for encryption or key exchange.



(a) RSA approach



(b) DSS approach

Global Public-Key Components

p prime number where $2^{L-1} < p < 2^L$ for $512 \leq L \leq 1024$ and L a multiple of 64; i.e., bit length of between 512 and 1024 bits in increments of 64 bits

q prime divisor of $(p - 1)$, where $2^{159} < q < 2^{160}$; i.e., bit length of 160 bits

g $= h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < (p - 1)$ such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudorandom integer with $0 < x < q$

User's Public Key

$y = g^x \bmod p$

User's Per-Message Secret Number

k = random or pseudorandom integer with $0 < k < q$

Signing

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1} (\mathrm{H(M)} + xr)] \bmod q$

Signature = (r, s)

Verifying

$w = (s')^{-1} \bmod q$

$\mathrm{u}_1 = [\mathrm{H(M')}w] \bmod q$

$\mathrm{u}_2 = (r')w \bmod q$

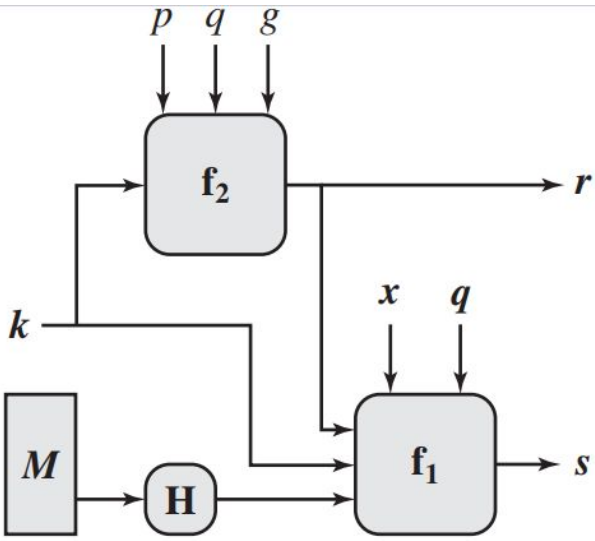
$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$

TEST: $v = r'$

M = message to be signed

$\mathrm{H}(M)$ = hash of M using SHA-1

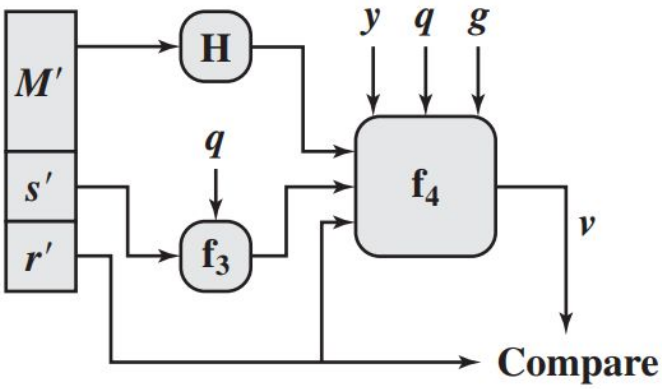
M', r', s' = received versions of M, r, s



$s = \mathrm{f}_1(\mathrm{H}(M), k, x, r, q) = (\mathrm{k}^{-1}\,(\mathrm{H}(M) + xr)) \bmod q$

$r = \mathrm{f}_2(k, p, q, g) = (g^k \bmod p) \bmod q$

(a) Signing



$w = \mathrm{f}_3(s', q) = (s')^{-1} \bmod q$

$v = \mathrm{f}_4(y, q, g, \mathrm{H}(M'), w, r')$

$= ((g^{(\mathrm{H}(M')w) \bmod q}\, y^{r'w \bmod q}) \bmod p) \bmod q$

(b) Verifying

Kerberos

Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network.

We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service

In this environment, a workstation cannot be trusted to identify its users correctly to network services.

1. A user may gain access to a particular workstation and **pretend to be another user** operating from that workstation.

2. A user **may alter the network address** of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation.

3. A user **may eavesdrop** on exchanges and use a replay attack to gain entrance to a server or to disrupt operations

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users.

Kerberos relies exclusively on symmetric encryption, making no use of public-key encryption.

Use an authentication server (AS) that knows the passwords of all users and stores these in a centralized database

(1) C → AS: $ID_C \| P_C \| ID_V$

(2) AS → C: $Ticket$

(3) C → V: $ID_C \| Ticket$

$Ticket = E(K_v, [ID_C \| AD_C \| ID_V])$

where

C = client

AS = authentication server

V = server

ID_C = identifier of user on C

ID_V = identifier of V

P_C = password of user on C

AD_C = network address of C

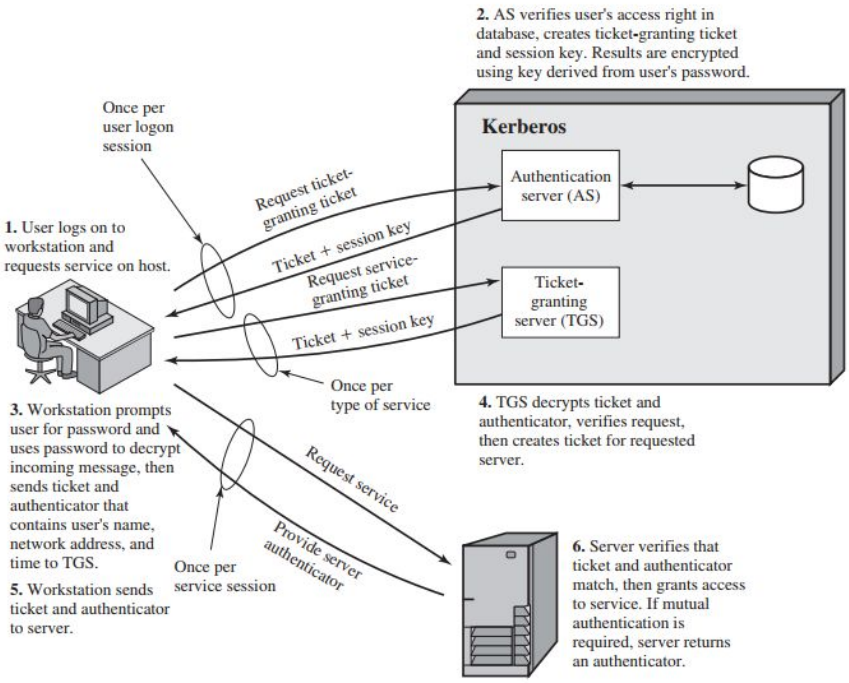
K_v = secret encryption key shared by AS and V

a user would need a new ticket for every different service.

An eavesdropper could capture the password and use any service accessible to the victim

To solve these additional problems :ticket-granting server (TGS)

Overview of Kerberos



Prime Numbers

Integer a can be factored as:(In terms of prime factors)

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$$

Relatively prime numbers, also known as **coprime numbers**, are two or more integers that have no common positive divisor other than 1