CRYPTOGRAPHY, NETWORK SECURITY AND CYBERLAW

Author- Bernard Menezes

Module-1

CHAPTER-1 INTODUCTION

CHAPTER-2 MATHEMATICAL BACKGROUND FOR CRYPTOGRAPHY

CHAPTER-3 BASICS OF CRYPTOGRAPHY

CHAPTER-4 SECRET KEY CRYPTOGRAPHY

CHAPTER-1 INTRODUCTION

1.1 Cyber Attacks

1.2 Defense Strategies and Techniques

1.3 Guiding Principles

1.1 CYBER ATTACKS

1.1.1 Motives

1.1.2 Common attacks

1.1.3 Vulnerabilities

1.1 Cyber Attack:

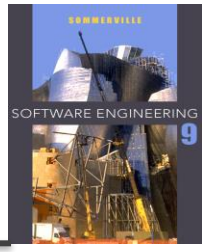
An attempt by hackers to damage or destroy a computer network or system.

1.1.1 Motives

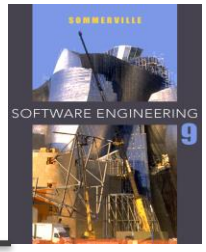
What are the main goals of an attacker?

- Most hackers were young adults, teens who had dropped out from school but otherwise they are intelligent and focused.
- Their goals are to damage the information system/communication system of financial and business institutions of their enemies.

Notable Cyber Attack



Year	Event
• **1988**	• Robert Morris, 23 year old American computer scientist and entrepreneur, released a worm that preventing normal functioning of almost 6000 computers.
• **1991**	• 31 year old David L Smith created the worm "**Melissa**" which infected thousands of computers causing damage of approximately $1.5 billion.

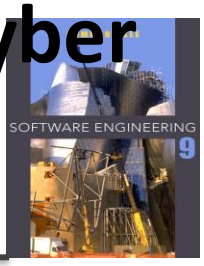


- **2001**

- This virus sent copies of itself to the 50 names of the recipient's address book.
- "**Anna Kournikova virus**"

  Promising photos of the tennis star mailed itself to the every person in the victim's address book.

Some of the main motives of launching cyber attacks are:



1. Theft of sensitive information.
2. Disruption of service.
3. Illegal access to or use of resources.

1. Theft of sensitive information.

- Many organizations store and communicate sensitive information.
- Information on new products being designed can be hugely advantageous to a company's competitors.
- Likewise, details of **military installations or precise military plans** can be of immense value to a nation's adversaries.
- Leakage of personal information such as ***credit card numbers, passwords.***

2. Disruption of service.

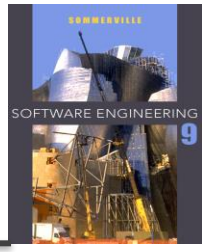
- Interruption or disruption of service is launched against an organization's servers so they are made unavailable or inaccessible.
- examples:- e-commerce websites.
- The goal here appears to be "***my competitor's loss is my gain.“***
- In 2001, there were a series of such attacks that targeted the websites of Yahoo, Microsoft, etc. in a short span of time.

3. Illegal access to or use of resources.

- The goal here is to obtain free access or service to paid services.
- Examples of this include free access to online digital products such as magazine or journal articles, free talk time on someone else's account etc.

1.1.2 Common Attacks

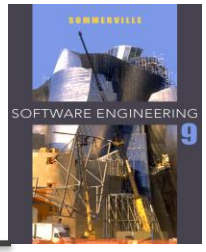
a) **Phishing attack**
b) **Pharming attack**
c) **Dictionary attacks**
d) **Denial of Service (DoS)**
e) **various types of malware**



a) **Phishing attack**:- is an attempt to obtain sensitive information such as usernames, passwords and credit card details often for malicious reasons by appearing as a trustworthy entity in an electronic communication.

b) **Pharming attack:-**is a cyber attack intended to redirect a website traffic to another fake site.

- Ex: ***an on-line bank.*** The fake site has the look and feel of the authentic bank with which the victim has an account. The victim is then induced to reveal sensitive information such as his/her login name and password, which are then passed on to fake website.



Union Bank of India

Good people to bank with

Visit Bank's website

1800 22 22 44 (In India-Toll Free)
» 1800 208 2244 (In India-Toll Free)
» 080-25300175 (In India-Chargeable)
» +91-80-25302510 (For NRIs)

Beware of Phishing attacks

Phishing is a fraudulent attempt, usually made through emails/calls/SMS to capture your confidential data like NetBanking Id/Password, mobile no, email Id/Password, Card no/PIN/CVV no, etc.

- ✗ Union Bank will never send you e-mails asking for confidential details of your account/ PIN/ Password or personal details.
- ✗ Never respond to e-mails/embedded links/calls asking you to update or verify UserIDs/Passwords/Card Number/CVV etc.
- ✗ Never click on any links in any e-mail to access the bank's site.
- ✗ Never enter login or other sensitive information in any pop up window.
- ✗ Do not be victim of SIM SWAPS, immediately investigate when you notice that you are not receiving call and message or getting SIM Registration fail. Keep your phone switched on and check alerts from Union Bank of India.
- ✗ Never respond to any SIM Swap Request even from mobile operators.
- ✓ Access your bank website only by typing the URL in address bar of browser.
- ✓ Always check the last log-in date and time in the post login page.
- ✓ Immediately change your passwords if you have accidentally revealed your credentials.
- ✓ Please report immediately on phishing[at]unionbankofindia[dot]com if you receive any such email/SMS or Phone call.

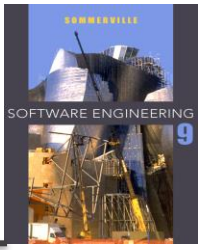
Continue to Login

Disclaimer!!

1. Our bank does not ask for the details of your account/PIN/password. Therefore any one pretending to be asking you for information from the bank/technical team may be fraudulent entities, so please beware. You should know how to operate net transactions and if you are not familiar you may refrain from doing so. You may seek bank's guidance in this regard. Bank is not responsible for online transactions going wrong.

2. We shall also not be responsible for wrong transactions and wanton disclosure of details by you. Viewing option and transactions option on the net are different. You may exercise your option diligently.

This site is best viewed on Microsoft® Internet Explorer 6.0 & above with resolution 1024 X 768.



c) Dictionary attack

- One means of having access into a computer system is through password-guessing attacks.

- The ultimate goal of the attacker is ***to impersonate his/her victim***.

- The attacker can then perform unauthorized logins, make on-line purchases, initiate banking transactions, etc., all under the assumed identity of the victim.

d) Denial of Service (DoS) :-

- the attacker performs a *interruption or disruption of the computing services on a system* .
- These attacks exhaust the *computing power, memory capacity, or communication bandwidth* of their targets so they are rendered unavailable.
- One version of this attack causes website defacement(changing visual appearance of the website).
- Dos attack on a web server slows down the web server so that its response time to requests from the outside world is unacceptably high.

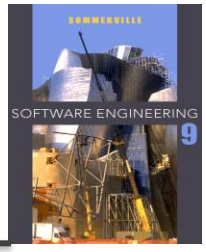
e) Attack caused by various types of malware.

- Worms and Virus are malware that replicate themselves.
- A worm is usually a stand-alone program that infects a computer, so a worm spreads from one computer to another.
- A Trojan is a kind of malware that masquerades as a utility .
  - Goals: modification of files, data theft.
  - Spyware , installed on a machine, can be used to monitor user activity and to recover valuable information such as passwords from user key strokes

1.1.3 Vulnerability

- A vulnerability is a **weakness** in a policy, procedure, protocol, hardware or software within an organization that has the potential to cause damage or loss.

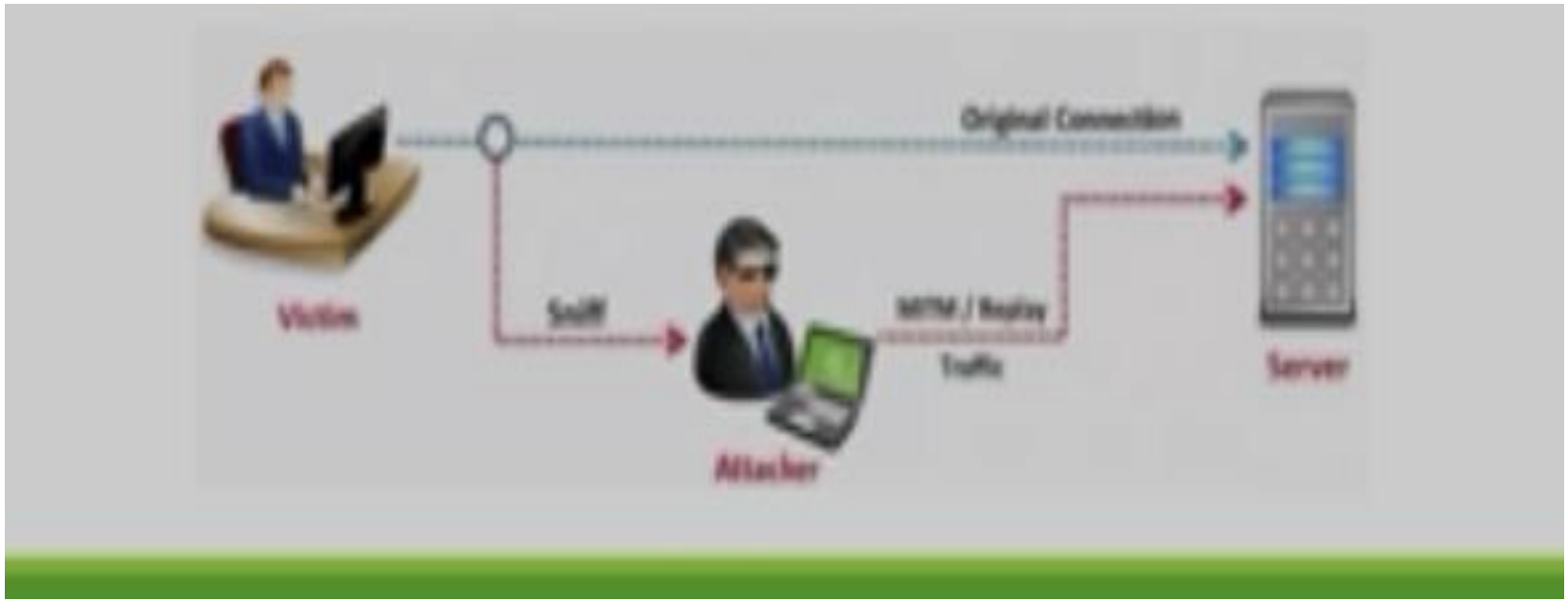
Vulnerability Types



1) **Human Vulnerabilities**
   - Introduced by careless/unthinking human behavior or action.
   - Ex. clicking on a link in an e-mail message from a questionable source
   - EX. clicking on an email attachment may open up a document causing a macro to be executed. The macro may be designed to infect other files on the system.
   - Related to **phishing** and cross-site scripting attacks

2) **Protocol Vulnerabilities**

- Attacks on commonly used networking protocols such as TCP, IP, ARP, ICMP and DNS
- Ex. Pharming attack and various hijacking attack
- Vulnerability in the design of security protocols that led to replay or man-in-the-middle attacks


Original Connection
Victim
Sniff
MITM / Replay
Traffic
Server
Attacker

3) **Software Vulnerabilities**

- Caused by **sloppily written** *system or application* **software**

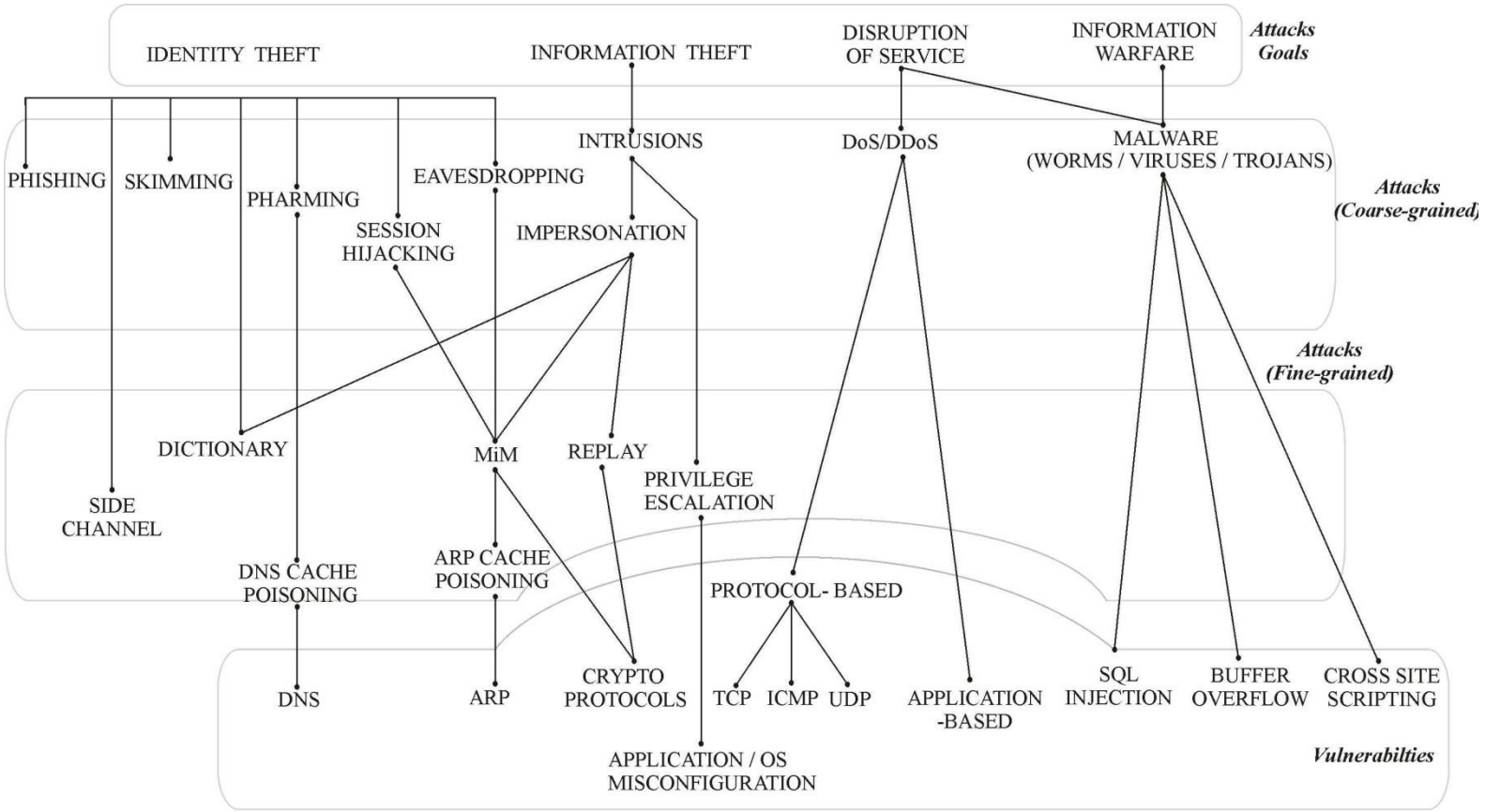
- Software may perform as expected under normal conditions but when provided with a specific input, it turns malicious

- Examples include **Buffer Overflow** vulnerability,

  A program declares an array of 100 elements. If the program does not check the length of the user input string; Buffer overflow occurs when we try to input values, which is more than the size of the array.

4) **Configuration Vulnerabilities**

- relate to settings on system/application software, on files, etc.
- Applications are often installed with default settings that attackers can use to attack them.
- Read-write-execute permissions on files (and other objects) may be too dangerous.
- This is particularly an issue with third party software where an attacker has easy access to a copy of the same application or framework we are running.


IDENTITY THEFT
INFORMATION THEFT
DISRUPTION OF SERVICE
INFORMATION WARFARE
Attacks Goals
PHISHING
SKIMMING
PHARMING
EAVESDROPPING
INTRUSIONS
DoS/DDoS
MALWARE (WORMS / VIRUSES / TROJANS)
Attacks (Coarse-grained)
SESSION HIJACKING
IMPERSONATION
Attacks (Fine-grained)
DICTIONARY
MiM
REPLAY
PRIVILEGE ESCALATION
SIDE CHANNEL
DNS CACHE POISONING
ARP CACHE POISONING
PROTOCOL- BASED
DNS
ARP
CRYPTO PROTOCOLS
TCP
ICMP
UDP
APPLICATION -BASED
SQL INJECTION
BUFFER OVERFLOW
CROSS SITE SCRIPTING
APPLICATION / OS MISCONFIGURATION
Vulnerabilties

1.2 Defence Strategies and Techniques

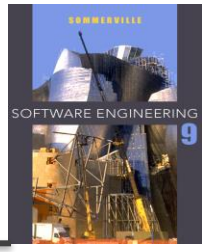
1) Access Control- Authentication and Authorization

2) Data Protection

3) Prevention and Detection

4) Response , Recovery and Forensics

1) Access Control- Authentication and Authorization



- The first defense strategy to prevent intrusions is **access control**.
- This implies the existence of a trusted third party that mediates access to protected system.
- The trusted third party is typically implemented in software and may be a part of the operating system and/or the application.

- First step in access control is to permit or deny entry into the system. This Involves some form of authentication-is providing password as a proof of identity. After success authentication we can access required resources.

- An important application of access control is to controlling n/w traffic which enters from the external insecure Internet into the protected environment of an organization.

- Example:- A device called firewall sits in between organization and Internet to filter packets based on the source/destination addresses and port numbers.

2) Data Protection

- The data in transit or storage needs to be protected.
- Dimensions of Data Protection. (This implies that data in transmit should not be tampered or modified.)
  - ***Data Integrity***: The data in transit should not be tampered with or modified.
  - ***Data confidentiality***: The data should not be readable by an intruder

- Cryptographic techniques are the best known ways to protect both the confidentiality and integrity of data.
- **Cryptography** is the Practice and study of hiding information.

- The **Encryption** operation is performed by the sender on a message to disguise it prior to sending it.

- The **Decryption** operation is performed on disguised message in order to recover the original message.

3) Prevention and Detection

- **Access control and Encryption are preventive strategies.**
- **Access Control** (against unauthorized access)
  1. Authentication:-keeps intruders out.
  2. Authorization:-limits what can be done by those who have been allowed in.

- **Encryption** (against eavesdropping)
  - it prevents intruders from eavesdropping on messages.

Intrusion detection:-

- Intrusion prevention may not always be practical or affordable, it may not always be effective.
- Example:- anti-virus products.

- **Cryptographic checksum**
  - detects tampering of messages.

- **Code Testing** (which detects vulnerabilities)

- Black box Testing:- (also known as Behavioural Testing) is a software testing method in which the internal structure/design implementation of the item being tested.

- White box Testing:- here, the security engineer has access to source code and can perform more elaborate testing by exercising different control paths in the source code.

4) Response , Recovery and Forensics

- Once an attack or infection has been detected, response measures should be taken immediately
- **These include shutting down all or part of the system.**
- If the system **infected by worm necessary patches need to be applied.**
- Many intrusion attempts leave finger prints just like a criminal does at the crime site.
- **Cyber forensics** is an emerging discipline with a set of tools that help to trace back the criminals of cyber crime

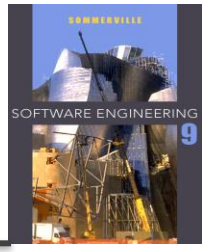
1.3 GUIDING PRINCIPLES

1. **Security is as much a human problem than a technological problem and must be addressed at various levels.**

- The **employees** within an organization should be educated on various do's and don'ts through periodically updated security awareness programs.
- In large organizations, security should be addressed by top-level **management**. Robust security policies should be formulated.
- **System administrators** handle day-to-day operations.

  -They should be proactive in crucial security practices such as patch application.

  -Their job also involves setting user/group permissions to various system resources such as files, configuring firewalls etc.

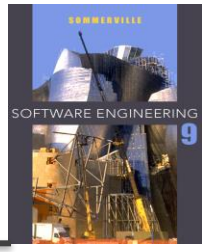


2) **Security should be factored in at inception, not as an afterthought**

- For several decades ago, security was not the priority for protocol designers. Later designer places, attention on functionality, correctness, performance and reliability.
- In general, security should be factored in early on during the design phase of a new product and then carried forward right through implementation and testing.

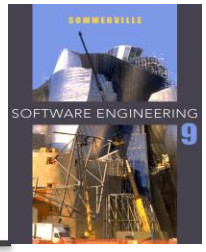
3) **Security by obscurity (or by complexity) is often bogus:-**

- There have been a number of cryptographic algorithms proposed by a small set of people.
- Those algorithms use was mandated in newly standardized protocols.



4) Always consider the "Default Deny" policy for adoption in access control:-

- Basically it means unless we specifically allow something, we deny it. It's the network version of **white listing.**
- **Back listing** is the network administration practice used to prevent the execution of undesirable programs.
- Back listing is the method used by most antivirus programs, intrusion prevention/detection systems.



5) **An entity should be given the least amount/level of permissions/privileges to accomplish a given task :-**

- RBAC(Role Based Access Control) is an idea of assigning system access to users based on their role in an organization.
- Access is assigned to each person based strictly on their role assignment.

6) **Use 'Defence in depth' to enhance security of an architectural design:-**

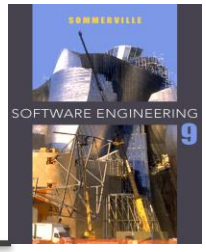
- This principle is used in many high-security installations and has been recently introduced in some airports.

- A passenger's ticket s checked before entering the airport terminal building. This is followed by verification of travel documents and bags etc.

- Defense in depth is applicable to cyber security.

  - Consider designing the firewall architecture for a mid-to-large size enterprise.

  -Every packet from the outside(Internet) should be intercepted by at least 2 firewalls.
- Firewalls may be from 2 different vendors and they have been configured by 2 different system administrators.
- They may have some overlapping functionality because of differences in the hardware/software design and in configuration what escapes from firewall 1 may be caught by Firewalls2 and vice versa.



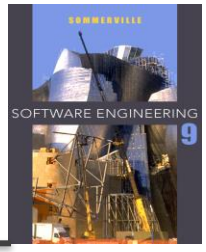
7) Identify vulnerabilities and respond appropriately:-

- Vulnerabilities in software are well researched. But equally important are shortcomings in policy, procedures and operations.
- Mobile devices and Bluetooth enabled gadgets may transmit malware to unsuspecting stations within the organizations.
- Likewise, USB enabled PCs may be victims of viruses residing on USB flash drives.

- Example:- the **Code Red worm** was a computer worm observed on the internet on July 2001
- It attacked computers running Microsoft's IIS web server.
- The other side of vulnerability identification is Risk Assessment.

Risk = Assets * Vulnerabilities* Threat

- If the assets impacted by a vulnerability are of low value or the threat perception is small, then associated risk is low.
- In such cases it may not make economic sense to address such vulnerabilities.



8) **Carefully study the tradeoffs (situational decision) involving security before making any:-**

- Engineering design often involves making tradeoffs- cost versus performance, functionality versus chip area etc.
- **Example:-** the area of electronic payment involving small purchases(say Rs 10 or less). Such payment called micropayments, may be made for digital goods such as on-line news paper articles.
- Payment schemes use some form of cryptography.
- The cryptographic overheads of theses schemes in terms of computation cost can be high.
- **Can we use cheaper Cryptography for micropayments?**
- In this case, we may be justified in trading off increased security for lower cost.

Module-1

CHAPTER-1 INTODUCTION

CHAPTER-3 MATHEMATICAL BACKGROUND FOR CRYPTOGRAPHY

CHAPTER-4 BASICS OF CRYPTOGRAPHY

CHAPTER-5 SECRET KEY CRYPTOGRAPHY

CHAPTER-3
MATHEMATICAL BACKGROUND FOR CRYPTOGRAPHY

3.1 Modulo Arithmetic
3.2 The Greatest Common Divisor
3.3 Useful Algebraic Structures
3.4 Chinese Remainder Theorem

3.1 Modulo Arithmetic

DIVISIBILITY EQUATION:-

$$d = n * q$$

$$32 = 8 * 4$$

Where, d is the dividend; n is the divisor; q is the quotient

- If the remainder is not zero, then 'n' does not divide 'd' and we can write the relations as,

$$d = n * q + r$$

$$42 = 5 * 8 + 2$$

Where 'r' is the remainder.

- In modular arithmetic, we are interested in only one of the outputs, the remainder r.
- This implies that we can change the above relation into a binary operator with 2 inputs ‘d’ and ‘n’ and one output ‘r’.
- And the congruence relation is **r ≡ d (mod n)**

  This says that **‘r’** is congruent to **d modulo n**
- In cryptography, we often use the concept of congruence instead of equality.

Example:-

- The result of 2 mod 10 = 2, 12 mod 10 =2, 22 mod 10 =2 and so on.

- In modular arithmetic , integers like 2,12,and 22 are called congruent mod 10; and the set itself is referred to as **congruent class.**

Properties

- If two integers are congruent modulo n, then they differ by an integral multiple of n.

  Algebraically, if a mod n=r and b mod n=r then

  $$a - b = n\,(q_1 - q_2)$$

Proof:

Let, $a = n*q_1 + r$ and

$b = n*q_2 + r$ where q_1 and q_2 are integers

Subtracting, we get $a - b = n\,(q_1 - q_2)$

*Since q_1 and q_2 are integers, a and b differ by an integral multiple of n

Properties

- Useful properties of modulo arithmetic:

$$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

$$(a - b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$$

$$(a * b) \bmod n = ((a \bmod n) * (b \bmod n)) \bmod n$$

(a *b) mod n = ((a mod n) * (b mod n)) mod n

- Proof:

  Let, $a = n*q_1 + r_1$ and $b = n*q_2 + r_2$

  then $a*b = n(n*q_1*q_2 + q_1 r_2 + q_2 r_1) + r_1 * r_2$

* We can eliminate the multiples of n when we take the mod n

$$(a*b) \bmod n = (r1 * r2) \bmod n$$

Substituting for a and b and applying property 3

LHS: $((n*q1 + r1) \bmod n) * ((n*q2 + r2) \bmod n)) \bmod n$

$= ((r1 \bmod n) * r2 \bmod n)) \bmod n$

$= (r1 * r2) \bmod n$

= RHS

(a *b) mod n = ((a mod n) * (b mod n)) mod n

Applications:

- multiplying a large number of terms, each term itself being a very large number
- Eg: we may have to multiply 50 integers, each about 1000 digits long.

$$(a_1 * a_2 * a_3 \ldots * a_{50}) \bmod n$$

then,

compute the product	$a_1 * a_2$
reduce, i.e., compute	b = (a1 * a2) mod n
compute the product	$b * a_3$
reduce, i.e., compute	$(b * a_3) \bmod n$

(a + b) mod n = ((a mod n) + (b mod n)) mod n

Example:

n = 8, a= 27 and b = 34

The LHS of Property 1 is

$$(27 + 34) \bmod 8$$
$$= 61 \bmod 8$$
$$= 5$$

The RHS of Property 1 is

$$((27 \bmod 8) + (34 \bmod 8)) \bmod 8$$
$$= (3 + 2) \bmod 8$$
$$= 5$$

3.2 GCD (Greatest Common Divisor)

- Two positive integers may have many common divisors but only one greatest common divisor.
- Example:

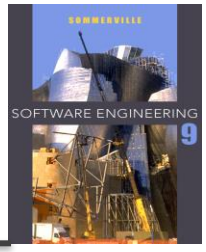
  24→ 2, 3, 4, 6, 8, 12, 24

  78→ 2, 3, 6, 13,26

  2, 3 and 6 are each common divisors of both 24 and78 then

  largest integer that divides both **is(24,78) = 6.**

Euclid's Algorithm



- Finding the greatest common divisor of two positive integers by listing all common divisors is not practical when the two integers are large.
- Solution to this problem is **Euclidean Algorithm**
- **Euclidean algorithm is based on the following two facts:-**

  1) gcd(a,0)=a. ← this tells that if the second integer is 0, then gcd is the first one.

  2) gcd(a,b) = gcd(b,r), where 'r' is the remainder of dividing a and b. ←- this allows us to change the value of a,b until b becomes 0.

Euclid's Algorithm

- Euclid's algorithm is used to find the gcd of two integers, b and c.
- If we divide *b* by *c* explicitly with quotient, *q*, and remainder, r.

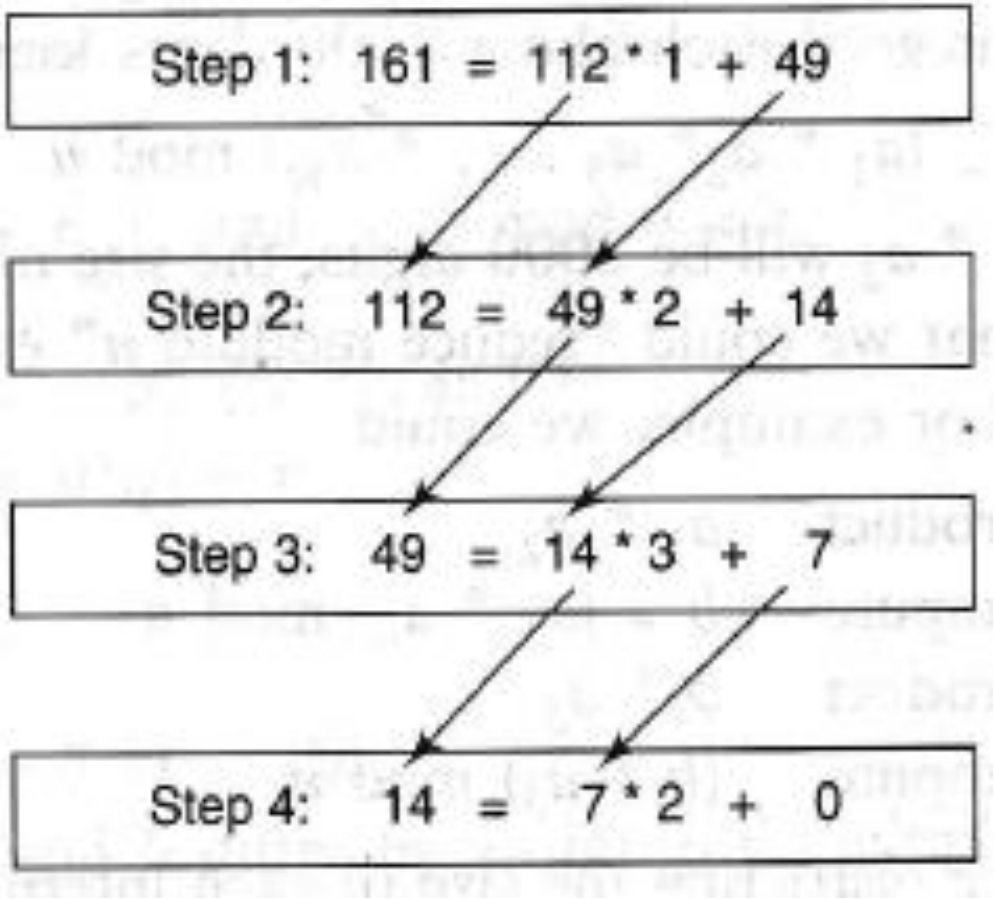
  Then $b = c * q + r$

- In each subsequent step, a similar equation is written.

- the new dividend (leftmost number) and new divisor are respectively the divisor and remainder from the previous step

Euclid's Algorithm

Example: GCD of 161 and 112



Let us now look at an example with relatively large numbers to see the power of this algorithm:

To find d = gcd (a,b) = gcd (1160718174,316258250)		
$a = q_1 b + r_1$	1160718174 = 3 × 316258250 + 211943424	d = gcd(316258250, 211943424)
$b = q_2 r_1 + r_2$	316258250 = 1 × 211943424 + 104314826	d = gcd(211943424, 104314826)
$r_1 = q_3 r_2 + r_3$	211943424 = 2 × 104314826 + 3313772	d = gcd(104314826, 3313772)
$r_2 = q_4 r_3 + r_4$	104314826 = 31 × 3313772 + 1587894	d = gcd(3313772, 1587894)
$r_3 = q_5 r_4 + r_5$	3313772 = 2 × 1587894 + 137984	d = gcd(1587894, 137984)
$r_4 = q_6 r_5 + r_6$	1587894 = 11 × 137984 + 70070	d = gcd(137984,70070)
$r_5 = q_7 r_6 + r_7$	137984 = 1 × 70070 + 67914	d = gcd(70070,67914)
$r_6 = q_8 r_7 + r_8$	70070 = 1 × 67914 + 2156	d = gcd(67914, 2156)
$r_7 = q_9 r_8 + r_9$	67914 = 31 × 2516 + 1078	d = gcd(2156, 1078)
$r_8 = q_{10} r_9 + r_{10}$	2156 = 2 × 1078 + 0	d = gcd(1078, 0) = 1078
Therefore, d = gcd(1160718174, 316258250) = 1078		

Extended Euclidean Algorithm

Formal procedure to obtain the inverse of **c** modulo **b** is called the Extended Euclidean algorithm.

Extended Euclidean Algorithm


```
ComputeInverse(b, c)          // Computes inverse of c mod b
{
    old1 = 1          new1 = 0
    old2 = 0          new2 = 1
    b' = b            c' = c
    r = 2
    while (r > 1) {
        q = b' / c'                          // compute quotient
        r = b' % c'                          // compute remainder
        temp1 = old1 – new1 * q
        old1 = new1
        new1 = temp1

        temp2 = old2 – new2 * q
        old2 = new2
        new2 = temp2

        b' = c'                  // update dividend
        c' = r                   // update divisor

        // At this point new1 * b + new2 * c = r
    }
    return new2
}
```

Extended Euclidean Algorithm

Example: Inverse of 12 modulo 79 (b=79 and c=12)

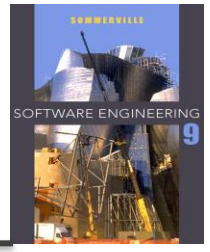
Iteration	b′	c′	q	r	old1	new1	old2	new2	Invariant new1 × b + new2 × c = r
—	79	12	—	2	1	0	0	1	—
1	12	7	6	7	0	1	1	–6	1 × 79 + (–6) × 12 = 7
2	7	5	1	5	1	–1	–6	7	(–1) × 79 + 7 × 12 = 5
3	5	2	1	2	–1	2	7	–13	2 × 79 + (–13) × 12 = 2
4	2	1	2	1	2	–5	–13	33	(–5) × 79 + 33 × 12 = 1

At the end of the last iteration r = 1, and the invariant is-

(-5) x 79 + 33 x 12 = 1

Or 12 * 33 = 1 + 5 * 79 ≡ 1 (mod79)

Thus, the inverse of 12 modulo 79 is 33.



Iteration	b'	c'	q	r	old1	new1	old2	new2	new1 x b + new2 x c = r
—	79	12	—	2	1	0	0	1	—
1	12	7	6	7	0	1	1	−6	

Compute inverse of 12 modulo 79

b = 79 ; c = 12.

ComputeInverse (79, 12).

old1 = 1 new1 = 0

old2 = 0 new2 = 1

b' = b = 79 c' = c = 12

r = 2

while (r > 1) {

$q = \frac{b'}{c'} = \frac{79}{12} = 6$

$r = b' \% c' = 7.$

temp1 = old1 − new1 * q

temp1 = 1 − 0 * 1

= 1

old1 = new1 = 0

new1 = temp1 = 1.

temp2 = old2 − new2 * q

= 0 − 1 * 6

= −6

old2 = new2 = 1

new2 = temp2 = −6

b' = d' = 12

c' = r. 7.

→ new1 * b + new2 * c = r

1 * 79 + (−6) * 12 = r

79 − 72 = 7.

3.3 Useful Algebraic Structures

3.3.1 GROUPS

3.3.2 RINGS

3.3.3 FIELDS

3.3 Useful Algebraic Structures

- The combination of the set and the operations that are applied to the elements of the set is called an **Algebraic Structure.**
- There are 3 common algebraic structures:-
  - Groups
  - Rings
  - Fields

3.3.1 Groups

A group is a pair <G, *>, where G is a set and * is a binary operation such that the following holds:

1. **Closure:** If a and b are elements of G, then **c= *a*b*** *is also an element of G.*

1. **Associativity:** If a, b, and c are elements of G then
   a*(b*c) = (a*b)*c
2. **Identity element:** There exists an element I in G such that for all b in G,
   I*b = b*I = b

4. **Inverse**: For each element b in G, there exists exactly one element c in G such that

   b*c = c*b = I (where c is the inverse of b)

- **Example: Finite group**

$< Z_n, +_n >$

where, Z_n = set represented as: { 0, 1, ……..n-1}

$+_n$ = The operation: addition modulo n

- **Identity** element of this group is **0** and the **inverse** of an element **b** is **-b**.

Example: $Z_5^* = \{1,2, 3, 4\}$ and $Z_6^* = \{1, 5\}$ It can be shown that $< Z^* , *_n >$ is a group.

Solution:-

Definition: The order of a group, (G, *) is the number of elements in G.

Definition: The Euler's Totient Function, denoted by Φ(n), is the order of $< Z_5^* , *_n >$

So, Φ(5) = 4 Φ(6) = 2

Lagrange's Theorem

- The order of any subgroup of a group divides the order of the parent group
- Consider $< Z_5^* , *_5 >$ $Z_5^* = \{1,2, 3, 4 \}$
  - Since its order is 4, no sub-group of it can have order = 3.
  - Its three subgroups have orders 1,2, and 4

- Let <G, *> be a finite group and let g be an element of G.
  - We use g^i to denote the element obtained by performing the operation * on g, i times.

$g * g * g \ldots\ldots\ldots\ldots * g$ *i* times

- Consider the elements:

$$g$$
$$g^2 = g * g$$
$$g^3 = g * g^2$$
$$g^4 = g * g^3$$
$$\ldots\ldots\ldots\ldots$$

- Each element in the above list is in G. Since the elements of <G, *> are closed under *.
- So, the list must repeat at some point.

Euler's theorem

- If m and n are relatively prime (co-prime), then **$m^{\Phi(n)} \bmod n = 1$.**

  Where $\Phi(n)$ denotes the order of the group.

- Example:- 7 and 10 are **relatively prime or co-prime.**

  7 → 1, 7

  10→ 1, 2, 5, 10

  the only positive integer that divides both of them is 1.

Fermat's Little theorem

Let p be prime and let m be a non-zero integer that is not a multiple of p then,

$$m^{p-1} \bmod p = 1$$

Examaple:- if m= 2 and p = 7

$2^{7-1} \bmod 7$

$2^{6} \bmod 7$

$64 \bmod 7$

1

Cyclic Group

Definition:

- A group <G, *> is cyclic if there is at least one element *g* in it such that <g> is <G, *>
- We refer to such an element of <G, *> as a generator of <G, *>

- (A group G is "Cyclic" if it's generated by a single element.)

- Example:- Z_7 = {0,1,2,3,4,5,6,} is cyclic order 7.

Since, 1+1 = 2 2 mod 7 = 2
1+1+1 = 3 3 mod 7 = 3
1+1+1+1=4 4 mod 7 = 4
1+1+1+1+1=5 5 mod 7 = 5
1+ 1+1+1+1+1=6 6 mod 7 = 6
1+1+1+1+1+1+1=7 7 mod 7 = 0
1+1+1+1+1+1+1+1=8 8 mod 7 = 1

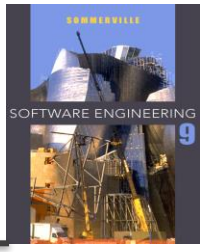
Here 1 is a generator.

Example: Consider $< Z_{13}^{*} , *_{13} >$. In this group,

$2^1 \ mod \ 13 = 2$
$2^2 \ mod \ 13 = 4$
$2^3 \ mod \ 13 = 8$
$2^4 \ mod \ 13 = 3$
$2^5 \ mod \ 13 = 6$
$2^6 \ mod \ 13 = 12$
$2^7 \ mod \ 13 = 11$
$2^8 \ mod \ 13 = 9$
$2^9 \ mod \ 13 = 5$
$2^{10} \ mod \ 13 = 10$
$2^{11} \ mod \ 13 = 7$
$2^{12} \ mod \ 13 = 1$

Hence, 2 is a generator of $< Z_{13}^{*}, *_{13} >$ However, 3 is not a generator of $< Z_{13}^{*} , *_{13} >$ and the group is cyclic.

Rings



- A ring is a triplet <R, +, *>, where + and * are binary operations and R is a set satisfying the following properties:

1. (R, +) is a commutative group. The additive identity is designated 0
2. For all x, y, and z in R,
   - x * y is also in R. (In other words, the set R is closed under *)
   - x * (y * z) = (x*y)*z. (In other words, * is an associative operation).
   - X* (y +z) = x*y + x*z= (y + z)*x. (We say that * distributes over+).

Few other properties of Rings:

- All rings that we use have a multiplicative identity designated as 1.

- the operation * does not need to be commutative. If * is commutative, the ring is called as a commutative ring.

- While each element, x, in R has an additive inverse (denoted by –x), an element need not have a multiplicative inverse

Fields

A field, <R, +, *>, is a commutative ring with the following additional properties:

•R has a multiplicative identity (denoted by 1) distinct from 0 (the additive identity)

•Each element, x, in R (except for 0) has an inverse element in R, denoted by x^{-1} , such that-

$$x * x^{-1} = x^{-1} * x = 1$$

- A field of size p^m is commonly denoted by $GF(p^m)$ or $F(p^m)$. Where GF means Galois Fields

- A prime or **irreducible polynomials** :- A polynomial with integer coefficients that cannot be factored into polynomials of lower degree, also with integer coefficients is called an irreducible polynomial.

x^3	$= (x)\ (x)\ (x)$
$x^3 + 1$	$= (x + 1)(x^2 + x + 1)$
$x^3 + x$	$= x(x + 1)^2$
$x^3 + x^2$	$= x^2(x + 1)$
$x^3 + x + 1$	
$x^3 + x^2 + 1$	
$x^3 + x^2 + x$	$= x(x^2 + x + 1)$
$x^3 + x^2 + x + 1$	$= (x + 1)^3$

- Writing polynomial equation in binary form:-

  10100001 = x^7+x^5+1

Multiplication table for all field elements of $GF(2^3)$

Multiplication table for elements in $GF(2^3)$ using irreducible polynomial $x^3 + x^2 + 1$

*	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	101	111	001	011
011	000	011	110	101	001	010	111	100
100	000	100	101	001	111	011	010	110
101	000	101	111	010	011	110	100	001
110	000	110	001	111	010	100	011	101
111	000	111	011	100	110	001	101	010

Multiplicative identity: **001 in every corresponding row.**

T o find the multiplicative inverse of a non-zero element for that we need to proceed along row, until we hit the shaded cell.

Example: **Inverse of 110 is 010.**

CHINESE REMAINDER THEOREM

Theorem is used in proving a number of results in cryptography.

Consider the factorization of an integer, N

$$N = n_1 * n_2 ..... N_k$$

where n1, n2, ... are pair wise relatively prime, i.e., $gcd(n_i, n_j) = 1$,

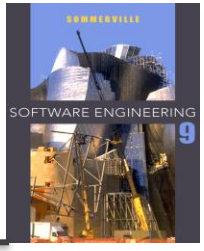
The mapping $f: Z_n \rightarrow Z_{n1} * Z_{n2} ……. Z_{nk}$ is defined as:

$$f(x) = (x \bmod n_1, x \bmod n_2, \ldots .. x \bmod n_k), \qquad 0 <= i < N$$

CHINESE REMAINDER THEOREM

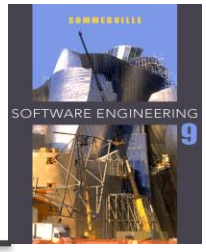
Example: Let N = 30. Choose n1 = 6 and n2 = 5 then f (i), 0 <= i < 30 are:

f(x)= (x mod n1, x modn2)
f(0)= (0 mod6, 0 mod 5)
f(0) = (0,0).
---
f(1)= (1 mod6, 1 mod 5)
f(1) = (1,1).
---
f(2)= (2 mod6, 2 mod 5)
f(2) = (2,2).
.....



$f(0) = (0, 0)$, $f(1) = (1, 1)$, $f(2) = (2, 2)$, $f(3) = (3, 3)$,
$f(4) = (4, 4)$, $f(5) = (5, 0)$, $f(6) = (0, 1)$, $f(7) = (1, 2)$,
$f(8) = (2, 3)$, $f(9) = (3, 4)$, $f(10) = (4,0)$, $f(11) = (5, 1)$,
$f(12) = (0, 2)$, $f(13) = (1, 3)$, $f(14) = (2, 4)$, $f(15) = (3, 0)$,
$f(16) = (4, 1)$, $f(17) = (5, 2)$, $f(18) = (0, 3)$, $f(19) = (1, 4)$,
$f(20) = (2, 0)$, $f(21) = (3, 1)$, $f(22) = (4, 2)$, $f(23) = (5, 3)$,
$f(24) = (0, 4)$, $f(25) = (1, 0)$, $f(26) = (2, 1)$, $f(27) = (3, 2)$,
$f(28) = (4, 3)$, $f(29) = (5, 4)$

- It is straight forward to compute f(x) given an x.



It is straightforward to compute $f(x)$ given an x. However, given a tuple in $Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_k}$, how do we reverse-map it to Z_N? At a more fundamental level, given a tuple $(x_1, x_2, \ldots, x_k) \in Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_k}$, does an $x \in Z_N$ even exist such that $f(x) = (x_1, x_2, \ldots x_k)$? We next show that such a reverse mapping does indeed exist.

Define

$$a_i = \frac{N}{n_i}, \quad 1 \leq i \leq k.$$

Let α_i denote the inverse of a_i in the modulo n_i sense, i.e.,

$$\alpha_i \times a_i \equiv 1 \pmod{n_i}, \quad 1 \leq i \leq k.$$

Then, given a tuple $(x_1, x_2, \ldots x_k) \in Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_k}$, compute

$$x = (x_1 \times a_1 \times \alpha_1 + x_2 \times a_2 \times \alpha_2 \ldots + x_k \times a_k \times \alpha_k) \bmod N$$

We claim that $f(x) = (x_1, x_2, \ldots x_k)$. To verify the claim, we note that

$$(x_1 \times a_1 \times \alpha_1 + x_2 \times a_2 \times \alpha_2 \ldots + x_k \times a_k \times \alpha_k) \bmod n_i = x_i$$

For a given n_i, the term, $x_i \times a_i \times \alpha_i \bmod n_i = x_i$ since, by definition, a_i and α_i are inverses modulo n_i. The other terms have the form, $x_j \times a_j \times \alpha_j \bmod n_i$, $i \neq j$. They are each zero. This is so since, by construction, each a_j, $j \neq i$, has n_i as a factor.

Solution follows these steps

1. Find N = n1* n2* n3
2. Find a1 = N/n1

   a2 = N/n2

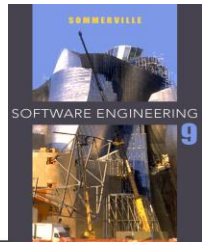
   a3 = N/n3

3. Find the multiplicative inverse of a1, a2,.....,ak using the corresponding modulus (n1,n2,....,nk) call the inverses α1,α2,... ,αk.

4. The solution :

$$x = (x1 * a1 * \alpha1 + x2 * a2 * \alpha2 + x3 * a3 * \alpha3) \pmod N$$

Problem on CRT



Let $N = 210$ and let $n_1 = 5$, $n_2 = 6$, $n_3 = 7$.
Compute $f^{-1}(3, 5, 2)$, i.e., given $x_1 = 3$, $x_2 = 5$, $x_3 = 2$, compute x.
We have

$$a_1 = N/n_1 = 42,$$
$$a_2 = N/n_2 = 35 \quad \text{and}$$
$$a_3 = N/n_3 = 30.$$

$$\alpha_1 = 42^{-1} \pmod 5 = 3$$
$$\alpha_2 = 35^{-1} \pmod 6 = 5 \quad \text{and}$$
$$\alpha_3 = 30^{-1} \pmod 7 = 4.$$

So,

$$\begin{aligned} x &= (x_1 \times a_1 \times \alpha_1 + x_2 \times a_2 \times \alpha_2 + x_3 \times a_3 \times \alpha_3) \pmod N \\ &= (3 * 42 * 3 + 5 * 35 * 5 + 2 * 30 * 4) \pmod{210} \\ &= 1493 \pmod{210} \\ &= 23 \end{aligned}$$

Procedure to find inverse

42*1 – 1 ÷ 5 = not whole number

42*2 – 1 ÷ 5 = not whole number

42***3*** – 1 ÷ 5 = whole number

35*1 – 1 ÷ 6 = not whole number

35*2 – 1 ÷ 6 = not whole number

35*3 – 1 ÷ 6 = not whole number

35*4 – 1 ÷ 6 = not whole number

35*5 – 1 ÷ 6 = whole number

CRYPTOGRAPHY, NETWORK SECURITY AND CYBERLAW

Author- Bernard Menezes

Module-1

CHAPTER-1 INTODUCTION

CHAPTER-3 MATHEMATICAL BACKGROUND FOR CRYPTOGRAPHY

CHAPTER-4 BASICS OF CRYPTOGRAPHY

CHAPTER-5 SECRET KEY CRYPTOGRAPHY

CHAPTER-4 BASICS OF CRYPTOGRAPHY

4.1 Preliminaries
4.2 Elementary Substitution Ciphers
4.3 Elementary Transposition Ciphers
4.4 Other Cipher Properties

4.1 Preliminaries

4.1.1 Secret versus “Public” Key Cryptography

4.1 Preliminaries

- Cryptography is a science and art of disguising messages so that only intended recipient can decipher the received message
- The message or document to be transferred is called **plaintext.** And its disguised version is called **cipher text**.
- Encryption involves the use of an encryption function or algorithm denoted by E, and decryption key e.
- Likewise, Decryption involves the use of an encryption function or algorithm denoted by D, and decryption key d.

C= Ee(P) and

P= Dd(C)

4.1.1 Secret versus “Public” Key Cryptography

- There are 2 types of Cryptography

1. Secret key cryptography
2. Public key cryptography

1. Secret key cryptography:-

- Both sender and receiver share a common secret. The same secret is used for encryption as well as for decryption.
- So, **e=d**. Hence this form of cryptography is also referred to a **symmetric key cryptography.**

2. **Public key cryptography:-**

- Two distinct keys forming a key pair are used, the **encryption key or public key and the decryption key or private key.**
- The public key of a user is used to encrypt messages to that user. It is intended to be known to the outside world.
- But the private key, should not be recovered to anyone. It is the private key of the recipient that is used to decrypt the message.
- The private key here has no relation with secret key cryptography. Because the public and private keys are distinct, this form of cryptography is also referred to as **asymmetric key cryptography.**

4.2 Elementary Substitution Ciphers

4.2.1 Monoalphabetic Ciphers

4.2.2 Polyalphabetic Ciphers

4.2 Elementary Substitution Ciphers

- A substitution cipher replaces one symbol with another.
- If the symbols in the plaintext are alphabetic characters, we replace one character with another.
- Substitution ciphers can be categorized as

1. Monalphabetic Cipher
2. Polyalphabetic Cipher

1. **Monoalphabetic Cipher:-**

- The simplest substitution cipher is one that replaces each alphabet in a text by the alphabet k positions away.

Ex: when k=3

PLAINTEXT : WHAT IS THE POPULATION OF MARS

CIPHERTEXT : ZKDW LV WKH SRSXODWLRQ RI PDUV

2) Polyalphabetic Cipher

- Here the cipher text corresponding to a particular character in the plain text is not fixed.
- The relationship between a character in the plaintext to a character in the cipher text is one-to-many.
- **Three examples of such ciphers are:-**

a) The vigenere cipher
b) The Hill cipher
c) One-time pad

a) The vigenere cipher

- The vigenere cipher is a poly alphabetic cipher that uses multi digit key k1,k2,k3,…km.
- Here k1,k2,….km are each integers.
- The plaintext is split into non overlapping blocks, each containing ‘m’ consecutive characters.
- Then the first letter of each block is replaced by the letter k1 positions to its right, the second letter of each block is replaced by the letter k2 positions to is right and so on...

Example:-

Plaintext: W I S H I N G Y O U

KEY : 4 19 03 22 07 12 05 11 04 19

Ciphertext: A B V D P Y L J S N

b) The Hill cipher

- The hill cipher is another polyalphatic cipher proposed by Lester hill.
- Here the plaintext is broken into blocks of size m. The key is m *m matrix of integers between 0 and 25.
- Let p1, P2,.....,Pn be the numeric representation of the characters in the plaintext .
- Let c1,c2,.....cn represent the corresponding characters in the cipher text.

- To compute the cipher text, we map each alphabet to an integer.
- We use the mapping, A->0, B->1, ...,z->25.
- The relationship between a block of plaintext and its cipher text is represented by,

c1= p1.k11 + p2.k21 + ……+ pm.km1 mod 26

c2= p1.k12 + p2.k22 + ……+ pm.km2 mod 26

.....

.....

c3= p1.k1m + p2.k2m + ……+ pm.kmm mod 26

- **C = P . K**

  where C → ♍♓◘♒♏❒ ♦♏☒♦

  P ☒ Plain text

  K ☒ m * m matrix comprising the key.
- At the receiver end, the plaintext can be recovered from the cipher text by using

  $P = C . K^{-1}$

Example:-

- Consider a Hill Cipher using a block size of 2 (m=2).

$$K = \begin{pmatrix} 3 & 7 \\ 15 & 12 \end{pmatrix}$$, Plain text be (H I).

Solution:-

Encryption:-

- The numeric equivalent of this block is (7 8).
- We obtain the corresponding cipher text using , **C = P . K**

$$C = (7\ 8) * \begin{pmatrix} 3 & 7 \\ 15 & 12 \end{pmatrix}$$

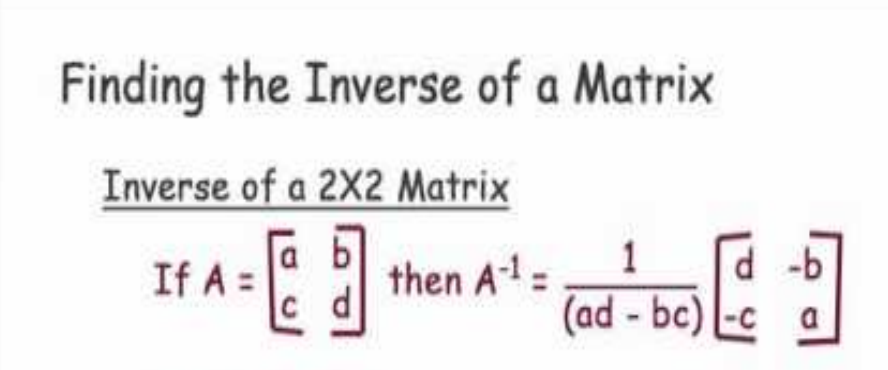
- (141 145) mod 26
  = (11 15) = **(L P)**

Decryption:-

$P = C \cdot K^{-1}$

- First we need to find K^{-1} = 1/ deter(K) * Adjoint(K)

- = 1/-69 * 12 -7
  -15 3



- **-69 inverse mod 26**

Note: -69*1 – 1 ÷ 26 = not whole number

-69*2 – 1 ÷ 26 = not whole number

-69*3 – 1 ÷ 26 = whole number

so, **-69 inverse mod 26 = 3.**

- In mod26 operation we cannot have negative number; for that we need to add 26 to that number.

Finally we have

$$K^{-1} = 3^{*} \begin{pmatrix} 12 & 19 \\ 11 & 3 \end{pmatrix} \quad \text{mod } 26 = \begin{pmatrix} 10 & 5 \\ 7 & 9 \end{pmatrix}$$

- $P = C \cdot K^{-1}$

$$P = (11 \quad 15) * \begin{pmatrix} 10 & 5 \\ 7 & 9 \end{pmatrix} \quad \text{mod } 26$$

$$P = (7 \quad 8) = (H \quad I)$$

C) One-time pad:-

- In cryptography, the **one-time pad** (**OTP**) is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key the same size as, or longer than, the message being sent.
- In this technique, a plaintext is paired with a random secret key (also referred to as *a one-time pad*).
- Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition.

Example:-


```
      H       E       L       L       O  message
   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= 30      16      13      21      25     message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) (message + key) mod 26
      E       Q       N       V       Z  → ciphertext
```

4.3 Elementary Transposition Ciphers

Elementary Transposition Ciphers

- The transposition cipher shuffles, rearranges or permutes the bits in block of plaintext.
- Example:-

Plaintext : Begin Operation at Noon

b	e	g	i
n	o	p	e
r	a	t	i
o	n	a	t
n	o	o	n

- Let us arrange the rows as follows

Row1→ ☼□◆→ ☼□◆→ ☼□◆→ ☼□◆→

a t n o

t i a r

g i e b

o n o n

p e o n

- The cipher text thus generated is A T N O T I A R G I E B O N O N P E O N
- To decrypt the message, the recipient would have to reverse the column shuffles, and then reverse the row shuffles.

4.4 Other Cipher Properties

4.4.1 Confusion and Diffusion

4.4.2 Block Ciphers and Stream Ciphers

4.4.1 Confusion and Diffusion

- Claude Shannon proposed the ideas of confusion and diffusion in the operation of cipher.

- **Confusion** is a property of cipher where it provides no clue regarding the relationship between the cipher text and key.
- Confusion is concerned with the relationship between the **key** and **cipher text.**

- **Diffusion** is concerned with relationship between **plaintext** and **cipher text**. Thus changing a single bit in a block of the plaintext will have the effect of changing each bit of the block of cipher text with probability of 0.5.

4.4.2 Block Ciphers and Stream Ciphers

In block cipher :-

- The plaintext is split into fixed size chunks called blocks and each are encrypted separately.
- Block size used in secret key cryptography are usually smaller like 64 bits in DES and 128 bits in AES.
- The block size of RSA is much larger 768 or more bits. While block size in ECC is 200 bits.

Stream cipher:-

- It operates on bits.
- The one time pad is example for stream cipher.
- The key is known to both sender and receiver.
- The per message string could be a message sequence number xor with key which generates Cipher text.
- An example of stream cipher is RC4 used in the wireless LAN protocol.

CRYPTOGRAPHY, NETWORK SECURITY AND CYBERLAW

Author- Bernard Menezes

Module-1

CHAPTER-1 INTODUCTION

CHAPTER-3 MATHEMATICAL BACKGROUND FOR CRYPTOGRAPHY

CHAPTER-4 BASICS OF CRYPTOGRAPHY

CHAPTER-5 SECRET KEY CRYPTOGRAPHY

CHAPTER -5

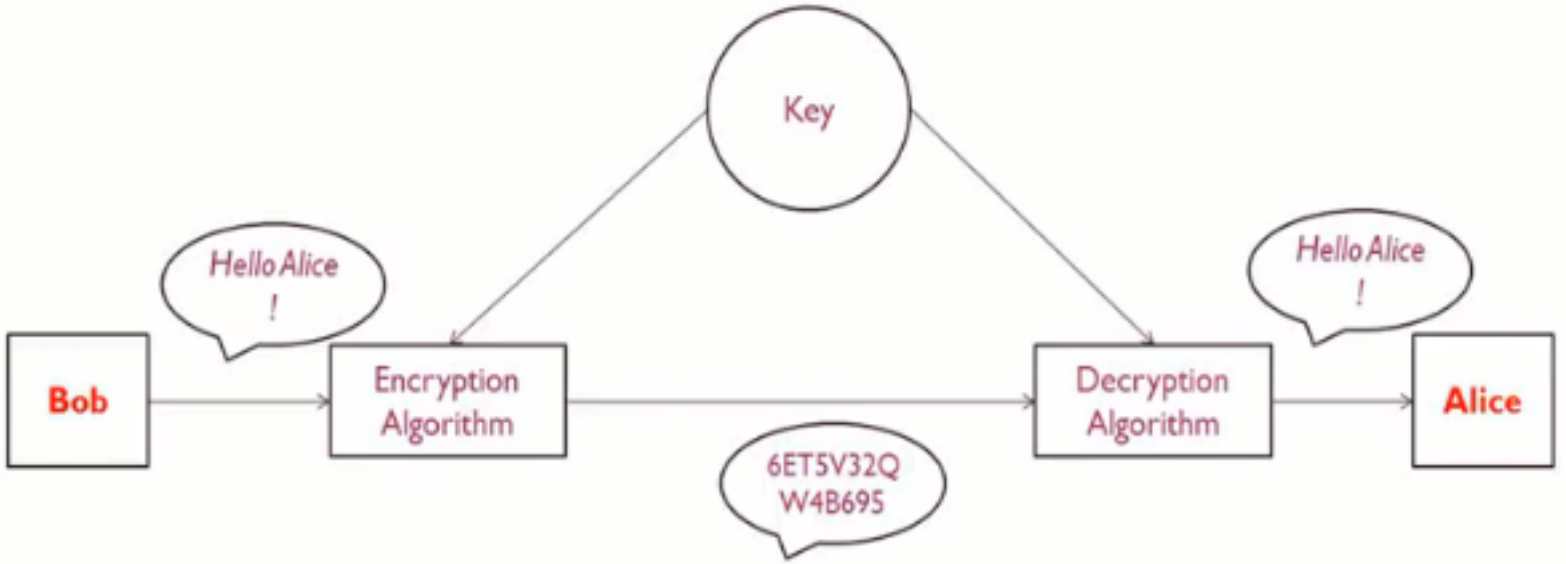
SECRET KEY CRYPTOGRAPHY

TWO TECHNIQUES

1. **Symmetric Cryptography.**
   - Also called secret key/private key cryptography.
   - Same key used for Encryption & Decryption.

2. **Asymmetric Cryptography.**
   - Also called public key cryptography.
   - A pair of keys is used for encryption and decryption.

Symmetric key/ Private key cryptography.



CHAPTER-5

5.1 Product Ciphers
5.2 DES Construction

5.1 Product Ciphers

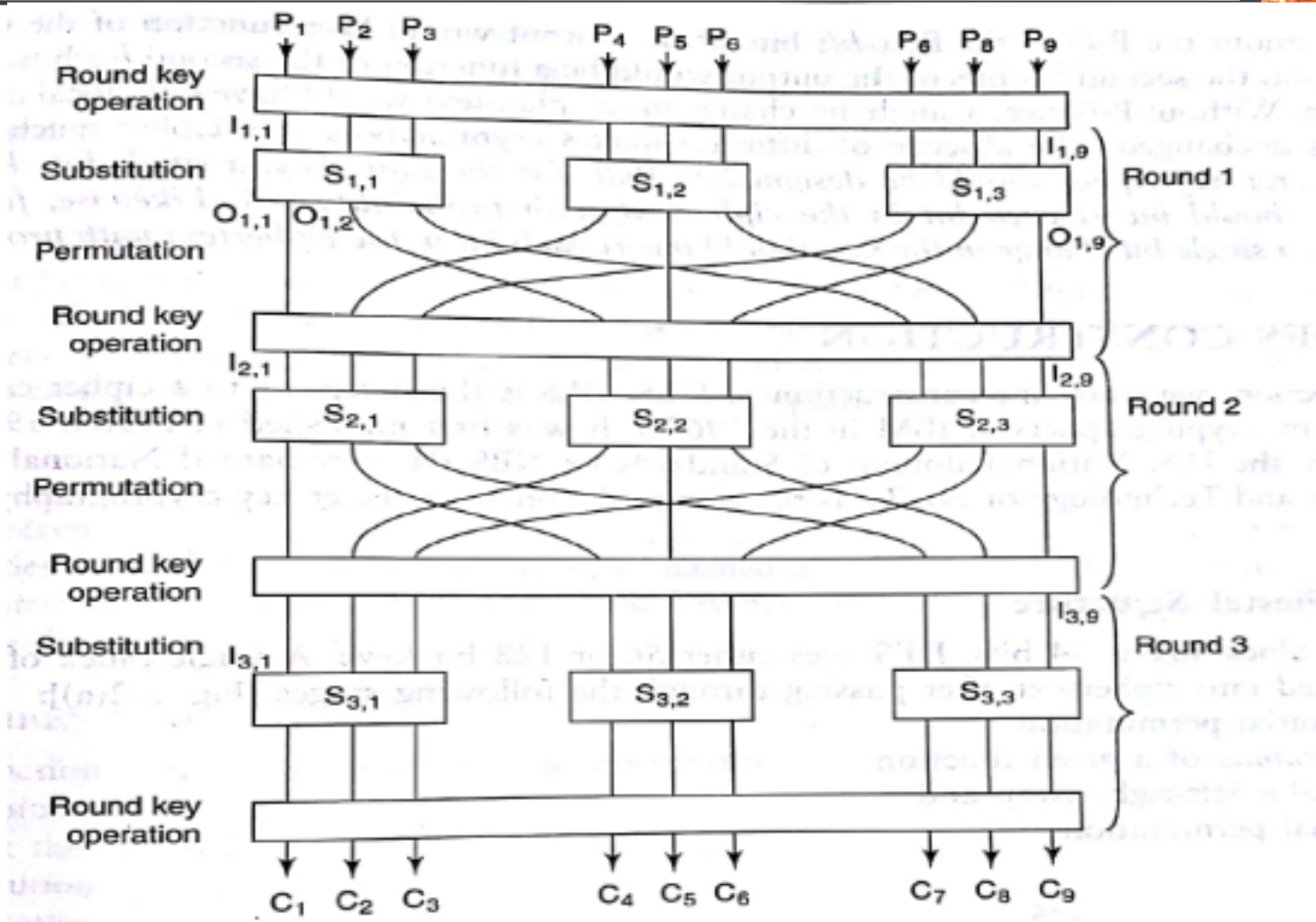
Product Ciphers

Product Ciphers

- ciphers using substitutions or transpositions are not secure because of language characteristics
- hence consider using several ciphers in succession to make harder, but:
  - two substitutions make a more complex substitution
  - two transpositions make more complex transposition
  - but a substitution followed by a transposition makes a new much harder cipher
- this is bridge from classical to modern ciphers

- An **Substitution** Box (S-Box) is a device that takes as input a binary string of length m and returns a binary string of length n.
- A P-Box performs a **permutation** or re-arrangement of the bits in the input.
- By cascading P-Boxes and S-Boxes alternately, the strength of a cipher can be greatly increased. Such a cipher is referred to as a **Product Cipher.**
- These operations are repeated over many rounds of iterations to make the cipher more stronger.
- Of the three operations, the **first** is the only one that involves the encryption key. It is actually an XOR of the input and the round key.
- **Second** step is the contribution of S-boxes which inject non-linearity into the design of the cipher.

- Non-linearity implies the absence of a linear relationship between any subset of bits in the plaintext, cipher text and key.
- Finally, the **third** step is permutation. A P-Box re-orders the inputs that it receives.



Three-round SPN network

5.2 DES CONSTRUCTION

DES CONSTRUCTION

Fiestel Structure:-

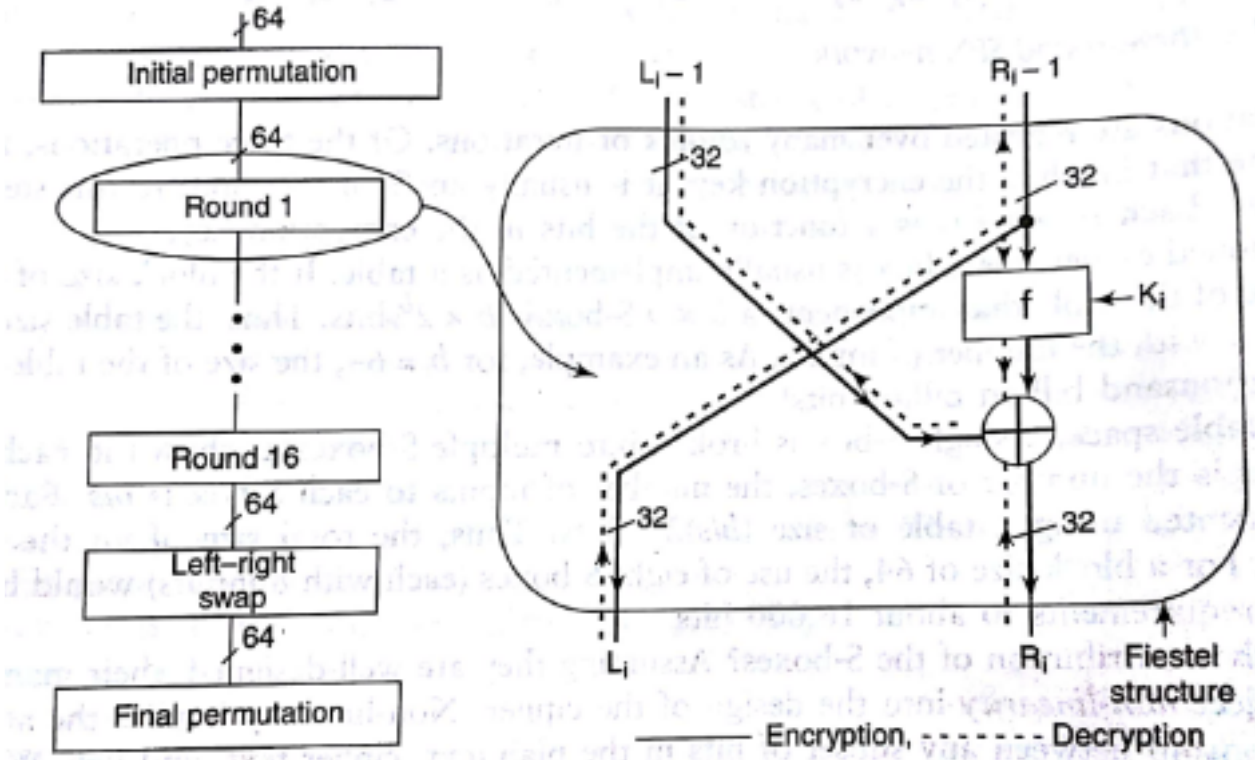
- The DES block size is 64 bits. DES uses either 56 or 128 bit keys.
- A single block of plaintext is transformed into cipher text after passing through the following stages:-
  - an initial permutation
  - 16 rounds of a given function
  - a 32-bit left-right swap
  - a final permutation

- Each of the 16 rounds is functionally identical.
- Let L_{i-1} and R_{i-1} be the left and right halves of the input to round i.

$$L_i = R_{i-1}$$

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

- The function f is applied at each round and is referred to as the “round” function.
- Each round uses a round key, which is one of the inputs to f.



DES operations

- The process of decryption involves obtaining L_{i-1} and R_{i-1} from L_i and R_i.
- Decryption proceeds from bottom to top and is summarized by the following equations.

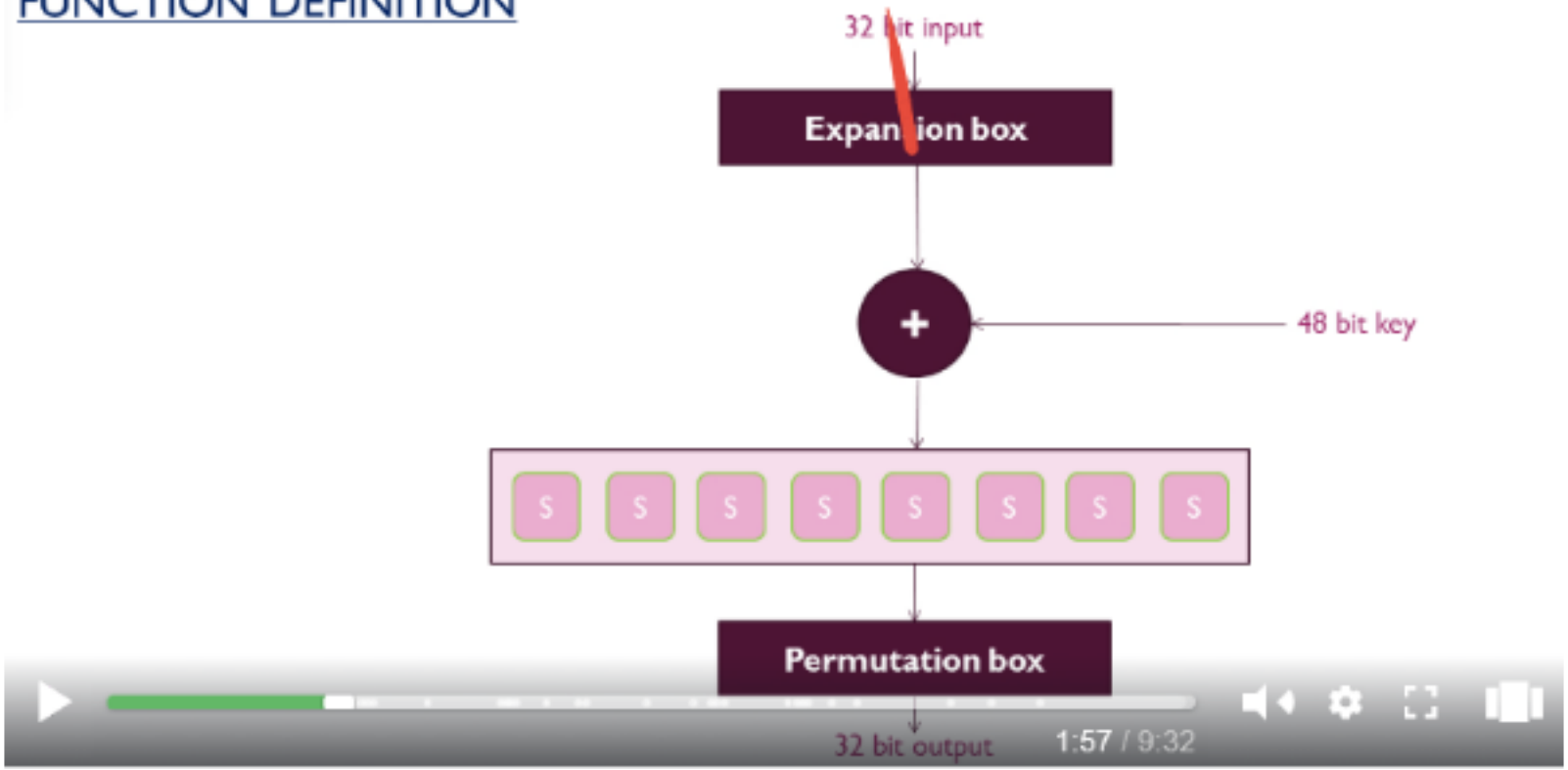
$$R_{i-1} = L_i$$

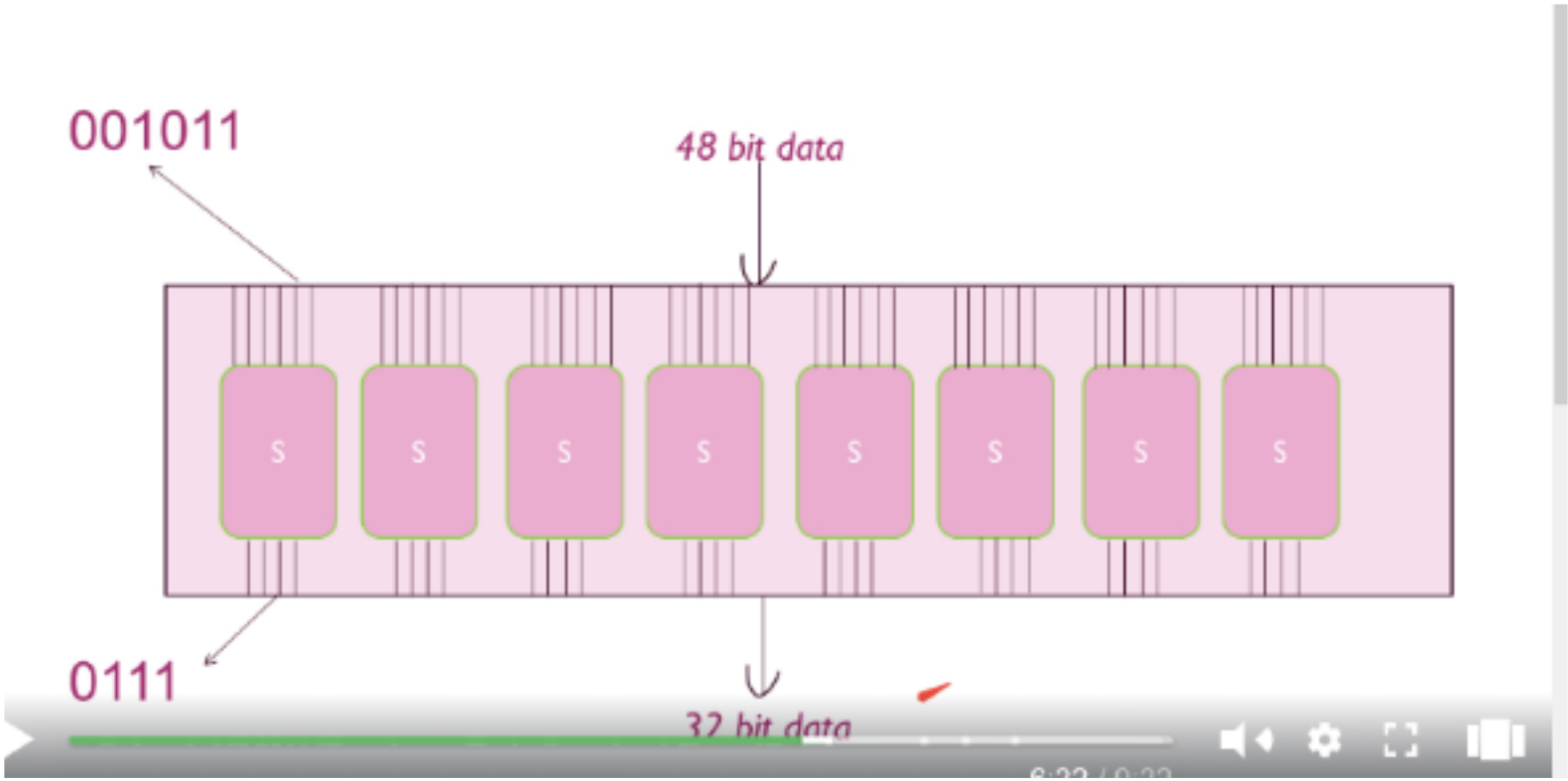
$$L_{i-1} = R_i \oplus f(L_i, K_i)$$

Round function

- A round function involves four operations:-
  - Expansion
  - ⊕ with the round key
  - Substitution
  - Permutation
- The input to the round function is Ri-1,a 32-bit quantity.
- This is first expanded into 48 bits by repeating some bits and interchanging their positions.
- The 48 bit quantity is then ⊕ed by with the round key, Ki.
- The result of the ⊕ operation is divided into eight 6-bit chunks.
- A total of 8 different S-boxes provide the eight substitutions.
- The output of the S-box is simply the 4-bit string that itself is the permuted value.

FUNCTION DEFINITION




001011
48 bit data
S
S
S
S
S
S
S
S
0111
32 bit data

S BOX (Substitution Box)

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011