Sinhgad Institutes

Sinhgad Technical Education Society's

SINHGAD ACADEMY OF ENGINEERING,

PUNE-411048

DEPARTMENT OF COMPUTER ENGINEERING

Laboratory manual (Instructor's Manual)

Course 310258:

INFORMATION SECURITY

Prepared by:

- Mr. V. K. Sambhar
- Mrs.V.S.Khandagale
- Ms. S.A. Mhaske

Vision

उत्तमपुरुषान् उत्तमाभियंत्रृन् निर्मातुं कटीबध्दः वयम् !

"We are committed to produce not only good engineersbut good human beings, also."

Mission

"Holistic development of students and teachers is what we believe in and work for. We strive to achieve this by imbibing a unique value system, transparent work culture, excellent academic and physical environment conducive to learning, creativity and technology transfer. Our mandate is to generate, preserve and share knowledge for developing a vibrant society."

Department of Computer Engineering

Vision

"To build the Department as a Centre of Excellence for students in Computer Engineering."

Mission

"We believe in developing value based system for student and staff by providing healthy and transparent work culture to cultivate new ideas in the field of engineering and technology which will contribute to build a vibrant Society."

Programme Outcomes (POs)

PO1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2. Problem analysis: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

PO6. The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professionalengineering practice.

PO7. Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9. Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10. Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11. Project management and finance: Demonstrate knowledge and understanding of the engineeringand management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12. Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Programme Specific Outcomes (PSOs)

Computer Engineering graduate will be able to,

PSO1: **Project Development:** Successfully complete hardware and/or software related system or application projects, using the phases of project development life cycle to meet the requirements of service and product industries; government projects; and automate other engineering stream projects.

PSO2: Domain Expertise: Demonstrate effective application of knowledge gained from different computer domains like, data structures, data bases, operating systems, computer networks, security, parallel programming, in project development, research and higher education.

PSO3: Career Development: Achieve successful Career and Entrepreneurship- The ability to employ modern computer languages, environments, and platforms in creating innovative career paths to be an entrepreneur, and a zest for higher studies

Savitribai Phule Pune University
Third Year of Computer Engineering (2019 Course)
310258:Laboratory Practice II

Home

Teaching Scheme	Credit: 02	Examination Scheme and Marks
Practical: 04 Hours/Week		**Term Work: 50 Marks** **Practical: 25 Marks**

Companion Course: Artificial Intelligence (310253), Elective II (310254)

Course Objectives:

- To learn and apply various search strategies for AI
- To Formalize and implement constraints in search problems
- To understand the concepts of Information Security / Augmented and Virtual Reality/Cloud Computing/Software Modeling and Architectures

Course Outcomes:

On completion of the course, learner will be able to

- **Artificial Intelligence**
  - **CO1:** Design a system using different informed search / uninformed search or heuristic approaches
  - **CO2:** Apply basic principles of AI in solutions that require problem solving, inference, perception, knowledge representation, and learning
  - **CO3:** Design and develop an interactive AI application
- **Information Security**
  - **CO4:** Use tools and techniques in the area of Information Security
  - **CO5:** Use the cryptographic techniques for problem solving
  - **CO6:** Design and develop security solution

OR

- **Augmented and Virtual Reality**
  - **CO4:** Use tools and techniques in the area of Augmented and Virtual Reality
  - **CO5:** Use the representing and rendering system for problem solving
  - **CO6:** Design and develop ARVR applications

OR

- **Cloud Computing**
  - **CO4:** Use tools and techniques in the area of Cloud Computing
  - **CO5:** Use cloud computing services for problem solving
  - **CO6:** Design and develop applications on cloud

OR

- **Software Modeling and Architectures**
  - **CO4:** Use tools and techniques in the area Software Modeling and Architectures
  - **CO5:** Use the knowledge of Software Modeling and Architectures for problem solving
  - **CO6:** Design and develop applications using UML as fundamental tool

Guidelines for Instructor's Manual

The instructor‘s manual is to be developed as a reference and hands-on resource. It should include prologue (about University/program/ institute/ department/foreword/ preface), curriculum of the course, conduction and Assessment guidelines, topics under consideration, concept, objectives, outcomes, set of typical applications/assignments/ guidelines, and references.

Guidelines for Student's Laboratory Journal

The laboratory assignments are to be submitted by student in the form of journal. Journal consists of Certificate, table of contents, and handwritten write-up of each assignment (Title, Date of Completion, Objectives, Problem Statement, Software and Hardware requirements, Assessment grade/marks and assessor's sign, Theory- Concept in brief, algorithm, flowchart, test cases, Test Data Set(if applicable), mathematical model (if applicable), conclusion/analysis. Program codes with sample output of all performed assignments are to be submitted as softcopy. As a conscious effort and little contribution towards Green IT and environment awareness, attaching printed papers as part of write-ups and

program listing to journal must be avoided. Use of DVD containing students programs maintained by Laboratory In-charge is highly encouraged. For reference one or two journals may be maintained with program prints in the Laboratory.

Guidelines for Laboratory /Term Work Assessment

Continuous assessment of laboratory work should be based on overall performance of Laboratory assignments by a student. Each Laboratory assignment assessment will assign grade/marks based on parameters, such as timely completion, performance, innovation, efficient codes, punctuality and

Guidelines for Practical Examination

Problem statements must be decided jointly by the internal examiner and external examiner. During practical assessment, maximum weightage should be given to satisfactory implementation of the problem statement. Relevant questions may be asked at the time of evaluation to test the student‘s understanding of the fundamentals, effective and efficient implementation. This will encourage, transparent evaluation and fair approach, and hence will not create any uncertainty or doubt in the minds of the students. So, adhering to these principles will consummate our team efforts to the promising start of student's academics.

Guidelines for Laboratory Conduction

The instructor is expected to frame the assignments by understanding the prerequisites, technological aspects, utility and recent trends related to the topic. The assignment framing policy need to address the average students and inclusive of an element to attract and promote the intelligent students. Use of open source software is encouraged. Based on the concepts learned. Instructor may also set one assignment or mini-project that is suitable to respective branch beyond the scope of syllabus.

Operating System recommended :- 64-bit Windows OS and Linux

Programming tools recommended: -

Information Security : - C/C++/Java

Augmented and Virtual Reality :- Unity, C#, Blender, VRTK, ARTK, Vuforia

VR Devices: HTC Vive, Google Daydream and Samsung gear VR.

Software Modeling and Architectures:-Front end:HTML5, Bootstarp, JQuery, JS etc.

Backend: MySQL /MongoDB/NodeJS

Virtual Laboratory:

Software Modeling and Architectures : http://vlabs.iitkgp.ernet.in/se

Information Security : http://cse29-iiith.vlabs.ac.in

Part I : Artificial Intelligence

Suggested List of Laboratory Experiments/Assignments

Sr. No.	Group A All assignments are compulsory
1.	Implement depth first search algorithm and Breadth First Search algorithm, Use an undirected graph and develop a recursive algorithm for searching all the vertices of a graph or tree data structure.
2.	Implement A star Algorithm for any game search problem.
3.	Implement Greedy search algorithm for any of the following application: I. Selection Sort II. Minimum Spanning Tree III. Single-Source Shortest Path Problem IV. Job Scheduling Problem V. Prim's Minimal Spanning Tree Algorithm VI. Kruskal's Minimal Spanning Tree Algorithm VII. Dijkstra's Minimal Spanning Tree Algorithm
	Group B
4.	Implement a solution for a Constraint Satisfaction Problem using Branch and Bound and Backtracking for n-queens problem or a graph coloring problem.
5.	Develop an elementary catboat for any suitable customer interaction application.

	Group C
6.	Implement any one of the following Expert System I. Information management II. Hospitals and medical facilities III. Help desks management IV. Employee performance evaluation V. Stock market trading VI. Airline scheduling and cargo schedules
	Part II : Elective II
	Suggested List of Laboratory Experiments/Assignments
Sr. No.	**Assignment Name**
	Information Security (Any five)
1.	Write a Java/C/C++/Python program that contains a string (char pointer) with a value \Hello World'. The program should AND or and XOR each character in this string with 127 and display the result.
2.	Write a Java/C/C++/Python program to perform encryption and decryption using the method of Transposition technique.
3.	Write a Java/C/C++/Python program to implement DES algorithm.
4.	Write a Java/C/C++/Python program to implement AES Algorithm.
5.	Write a Java/C/C++/Python program to implement RSA algorithm.
6.	Implement the different Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).
7.	Calculate the message digest of a text using the MD5 algorithm in JAVA.
	Cloud Computing (All assignments are compulsory)
1.	Case study on Microsoft azure to learn about Microsoft Azure is a cloud computing platform and infrastructure, created by Microsoft, for building, deploying and managing applications and services through a global network of Microsoft-managed data centers. OR Case study on Amazon EC2 and learn about Amazon EC2 web services.
2.	Installation and configure Google App Engine. OR Installation and Configuration of virtualization using KVM.
3.	Creating an Application in SalesForce.com using Apex programming Language.
4.	Design and develop custom Application (Mini Project) using Sales force Cloud.
5.	**Mini-Project** Setup your own cloud for Software as a Service (SaaS) over the existing LAN in your laboratory. In this assignment you have to write your own code for cloud controller using open-source technologies to implement **with HDFS**. Implement the basic operations may be like to divide the file in segments/blocks and upload/ download file on/from cloud in encrypted form.
	Augmented and Virtual Reality (Assignments 1,2, 3,7 are mandatory, any 2 from 4, 5 & 6)
1.	Installation of Unity and Visual Studio, setting up Unity for VR development, understanding documentation of the same.
2.	Demonstration of the working of HTC Vive, Google Daydream or Samsung gear VR.
3.	Develop a scene in Unity that includes:

	i.A cube, plane and sphere, apply transformations on the 3 game objects. ii.Add a video and audio source.
4.	Develop a scene in Unity that includes a cube, plane and sphere. Create a new material and texture separately for three Game objects. Change the color, material and texture of each Game object separately in the scene. Write a C# program in visual studio to change the color and material/texture of the game objects dynamically on button click.
5.	Develop and deploy a simple marker based AR app in which you have to write a C# program to play video on tracking a particular marker.
6.	Develop and deploy an AR app, implement the following using Vuforia Engine developer portal: i. Plane detection ii. Marker based Tracking(Create a database of objects to be tracked in Vuforia) iii. Object Tracking
7.	**Mini-Projects/ Case Study** Create a multiplayer VR game (battlefield game). The game should keep track of score, no. of chances/lives, levels(created using different scenes), involve interaction, animation and immersive environment. **OR** Create a treasure hunt AR application which should have the following features: i. A help button for instruction box to appear. ii. A series of markers which would give hints on being scanned. iii. Involve interaction, sound, and good UI.
	Software Modeling and Architectures **(Problem statement 1, 2 , 5 are mandatory and any one from 3 and 4)**
1.	Consider a library, where a member can perform two operations: issue book and return it. A book is issued to a member only after verifying his credentials. Develop a use case diagram for the given library system by identifying the actors and use cases and associate the use cases with the actors by drawing a use case diagram. Use UML tool.
2.	Consider online shopping system. Perform the following tasks and draw the class diagram using UML tool. Represent the individual classes, and objects Add methods Represent relationships and other classifiers like interfaces
3.	Consider the online shopping system in the assignment 2. Draw the sequence diagram using UML tool to show message exchanges
4.	Consider your neighboring travel agent from whom you can purchase flight tickets. To book a ticket you need to provide details about your journey i.e., on which date and at what time you would like to travel. You also need to provide your address. The agency has recently been modernized. So, you can pay either by cash or by card. You can also cancel a booked ticket later if you decide to change your plan. In that case you need to book a new ticket again. Your agent also allows you to book a hotel along with flight ticket. While cancelling a flight ticket you can also cancel hotel booking. Appropriate refund as per policy is made in case of cancellation. Perform the following tasks and draw the use case diagram using UML tool. a. Identify the use cases from a given non-trivial problem statement. b. Identify the primary and secondary actors for a system. **c.** Use to generalization of use cases and «include» stereotypes to prevent redundancy in the coding phase

Mini-Projects	
5.	Select a moderately complex system and narrate concise requirement Specification for the same. Design the system indicating system elements organizations using applicable architectural styles and design patterns with the help of a detailed Class diagram depicting logical architecture. Specify and document the architecture and design pattern with the help of templates. Implement the system features and judge the benefits of the design patterns accommodated.

Learning Resources

Text Books:

Artificial Intelligence

1. Stuart Russell and Peter Norvig, “Artificial Intelligence: A Modern Approach”, Third edition, Pearson, 2003, ISBN :10: 0136042597
2. Deepak Khemani, “A First Course in Artificial Intelligence”, McGraw Hill Education(India), 2013, ISBN : 978-1-25-902998-1
3. Elaine Rich, Kevin Knight and Nair, “Artificial Intelligence”, TMH, ISBN-978-0-07-008770-5

Information Security

1. Atul Kahate, “Cryptography and Network Security”, 3e, McGraw Hill Education
2. Prakash C. Gupta, “Cryptography and Network Security”, PHI
3. V.K. Pachghare, “Cryptography and Information Security”, PHI Learning

Cloud Computing

1. A. Srinivasan, J. Suresh,” Cloud Computing: A Practical Approach for Learning and Implementation”, Pearson, ISBN: 978-81-317-7651-3
2. Rajkumar Buyya, Christian Vecchiola, S. Thamarai Selvi, “Mastering Cloud Computing”, McGraw Hill Education, ISBN-13:978-1-25-902995-0

Augmented and Virtual Reality

1. William R Sherman and Alan B Craig, “Understanding Virtual Reality: Interface, Application and Design”, (The Morgan Kaufmann Series in Computer Graphics)”. Morgan Kaufmann Publishers, San Francisco, CA, 2002
2. Alan B Craig, “Understanding Augmented Reality, Concepts and Applications”, Morgan Kaufmann Publishers, ISBN:978-0240824086

Software Modeling and Architectures

1. Jim Arlow, Ila Neustadt, “UML 2 and the unified process –practical object-oriented analysis and design”, Addison Wesley, Second edition, ISBN 978-0201770605
2. Len Bass, Paul Clements, Rick Kazman, "Software Architecture in Practice", Second Edition, Pearson ,ISBN 978-81-775-8996-2
3. Hassan Gomaa, “Software Modeling and Design- UML, Use cases, Patterns and Software Architectures”, Cambridge University Press, 2011, ISBN 978-0-521-76414-8
4. Erich Gamma, “Design Patterns”, Pearson, ISBN 0-201-63361-2

Reference Books:

1. Nilsson Nils J , “Artificial Intelligence: A new Synthesis”, Morgan Kaufmann Publishers Inc. San Francisco, CA, ISBN: 978-1-55-860467-4
2. Patrick Henry Winston, “Artificial Intelligence”, Addison-Wesley Publishing Company, ISBN: 0-201-53377-4
3. Andries P. Engelbrecht, “Computational Intelligence: An Introduction”, 2nd Edition-Wiley India-

ISBN: 978-0-470-51250-0

Information Security

1. William Stallings, Lawrie Brown, "Computer Security Principles and Practice", 3rd_Edition, Pearson
2. William Stallings, "Cryptography and Network Security Principals and Practice", Fifth edition, Pearson
3. Nina Godbole, Sunit Belapure, "Cyber Security", Wiley, ISBN: 978-81-265-2179-1

Augmented and Virtual Reality

1. Steven M. LaValle, "Virtual Reality", Cambridge University Press, 2016
2. Alan B Craig, William R Sherman and Jeffrey D Will, "Developing Virtual Reality Applications: Foundations of Effective Design", Morgan Kaufmann, 2009.
3. Schmalstieg / Hollerer, "Augmented Reality: Principles & Practice", Pearson Education India; First edition (12 October 2016),ISBN-10: 9332578494
4. Sanni Siltanen, "Theory and applications of marker-based augmented reality", Julkaisija – Utgivare Publisher. 2012. ISBN 978-951-38-7449-0

Cloud Computing

1. James Bond ,"The Enterprise Cloud", O'Reilly Media, Inc. ISBN: 9781491907627
2. Dr. Kris Jamsa, "Cloud Computing: SaaS, PaaS, IaaS, Virtualization and more", Wiley Publications, ISBN: 978-0-470-97389-9
3. Anthony T. Velte Toby J. Velte, Robert Elsenpeter, "Cloud Computing: A Practical Approach", 2010, The McGraw-Hill.

Software Modeling and Architectures

1. Gardy Booch, James Rambaugh, Ivar Jacobson, "The unified modeling language user guide" , Pearson Education, Second edition, 2008, ISBN 0-321-24562-8.
2. Lan Sommerville, "Software Engineering", 9th edition, ISBN-13: 978-0-13-703515-1 ISBN-10: 0-13-703515-2.

@The CO-PO Mapping Matrix

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	-	2	-	3	-	-	2	2	2	1	2
CO2	1	-	2	2	3	2	-	2	2	2	1	2
CO3	1	-	2	2	3	2	-	2	2	2	2	2
CO4	1	-	2	-	3	-	-	2	2	2	2	2
CO5	1	-	2	-	3	-	-	2	2	2	2	2
CO6	1	-	2	-	3	-	-	2	2	2	2	2

INDEX

EX.NO:1

DISPLAY THE RESULT

AIM:

Write a Java/C/C++/Python program that contains a string (char pointer) with a value \Hello World9. The program should AND OR and XOR each character in this string with 127 and display the result

DESCRIPTION:

(a) String

The string is the one-dimentional array of characters terminated by null('\0'). Each and every character in the array consumes one byte of memory, and the last character must always be 0. The termination character('\0') is used to identify where the string ends. In C language string declaration can be done in two ways.

1. By char array
2. By string literal

EXAMPLE:

Let's see the example of declaring string by char array in C language.

Char ch[17]={'o','n','l','i','n','e','s','m','a','r','t','t','r','a','i','n','e','r','\0'};

As we know, array index starts from 0, so it will be represented as in the figure given below.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
o	n	l	i	n	e	s	m	a	r	t	t	r	a	i	n	e	r	\0

While declaring string, size is not mandatory. So we can write the above code as given below:

Char ch[]={,'n','l','i','n','e','s','m','a','r','t','t','r','a','i','n','e','r','\0'}

We can also define the string by the string literal in C language. For example: char str[]="onlinemarttrainer";

In such case, '\0' will be appended at the end of the string by the compiler.

(b) AND operation

There are two inputs and one output in binary AND operation. The inputs and result to a binary AND operation can only be 0 or 1. The binary AND operation will always produce a 1 output if both inputs are 1 and will produce a 0 output if both inputs are 0. For two different inputs, the output will be 0.

AND Truth table

Input		Output
X	Y	
0	0	0
0	1	0
1	0	0
1	1	1

C) XOR operation

There are two inputs and one output in binary XOR (exclusive OR) operation. It is similar to ADD operation which takes two inputs and produces one result. i.e. one output. The inputs and result to a binary AND operation can only be 0 or 1. The binary XOR operation will always produce a 1 output if either of its inputs are 1 and will produce a 0 output if both inputs are 0 or 1.

XOR Truth table

Input		Output
X	Y	
0	0	0
0	1	1
1	0	1
1	1	0

ALGORITHM:

STEP-1: Define the string

STEP-2: Perform AND operation

STEP-3: Perform XOR operation

STEP4: Display the result

CONCLUSION: Thus the AND or and XOR a string with a 127 had been implemented successfully using C language.

EX.NO:2

PERFORM ENCRYPTION AND DECRYPTION USING THE METHOD OF RAILFENCE– ROW & COLUMN TRANSPOSITION TECHNIQUE.

AIM:

Write a Java/C/C++/Python program to perform encryption and decryption using the method of Transposition technique

DESCRIPTION:

In the rail fence cipher, the plain text is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when were ach the bottom rail. When were ach the to p rail, the message is written downwards again until the whole plain text is written out. The message is then read off in rows.

EXAMPLE:

A	U	T	H	O	R
1	6	5	2	3	4
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	S	A	V
E	Y	O	U	R	S
E	L	F	A	B	C

yields the cipher

W I R E E R O S U A E V A R B D E V S C A C D O F E S E Y L .

ALGORITHM:

STEP-1: Read the Plain text.

STEP-2: Arrange the plain text in row column are matrix format.

STEP-3: Now read the keyword depending on the number of columns of the plain text.

STEP4: Arrange the characters of the key word in sorted order and the corresponding columns of the plain text.

STEP-5: Read the characters row wise or column wise in the former order to get the cipher text.

CONCLUSION:

Thus the railfence transposition algorithm had been executed successfully.

EX.NO:3

IMPLEMENTATION OF DES

AIM:

Write a Java/C/C++/Python program to implement DES algorithm.

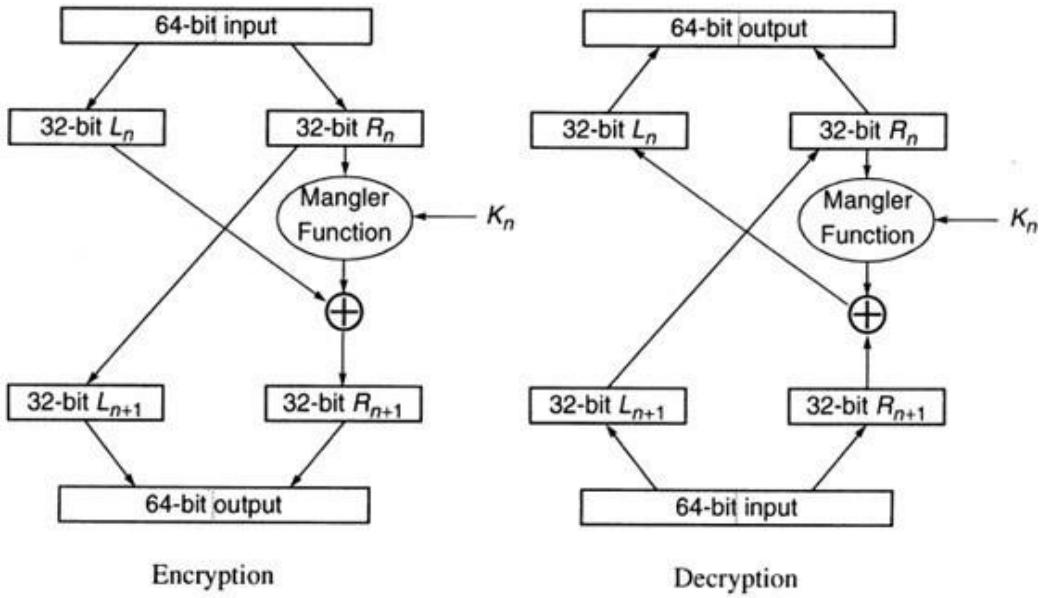
DESCRIPTION:

DES is a symmetric encryption system that uses64-bitblocks, 8bits of which are used for parity checks. The key therefore has a "useful" length of 56bits, which means that only 56 bits are actually used in the algorithm. The algorithm involves carrying out combinations, substitutions and permutations between the text to be encrypted and the key, while making sure the operations can be performed in both directions. The key is ciphered on 64 bits and made of 16 blocks of 4 bits, generally denoted k_1 to k_{16}. Given that "only" 56 bits are actually used for encrypting, there can be 2^{56} different keys.

The main parts of the algorithm are as follows:

- Fractioning of the text into 64-bit blocks
- Initial permutation of blocks
- Break down of the blocks into two parts: left and right ,named L and R
- Permutation and substitution steps repeated 16 times
- Re-joining of the left and right parts then inverse initial permutation

EXAMPLE:



Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a Symmetric-key block cipher issued by the national Institute of Standards & Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration −

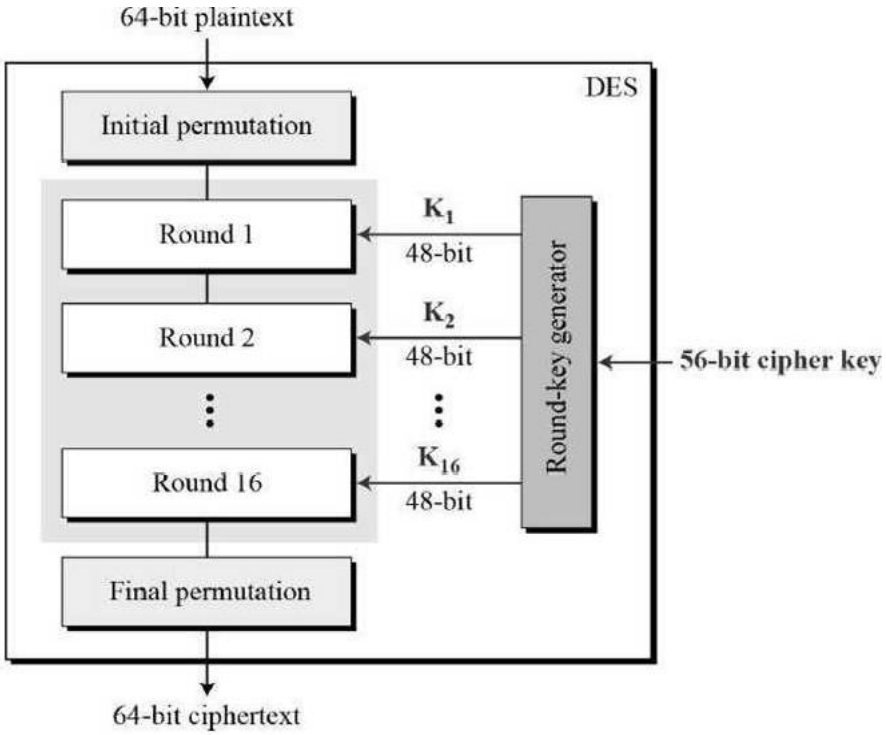


Figure 3.1: General Structure of DES

Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows

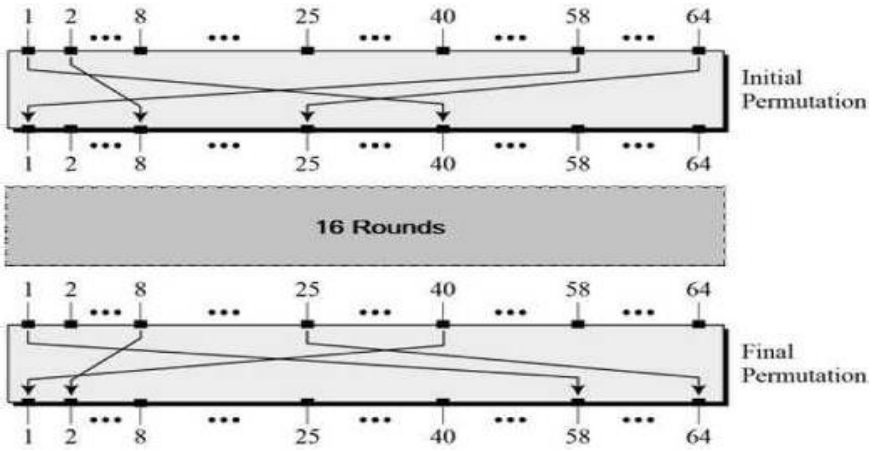


Figure 3.2 initial and final permutations

Round Function

The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

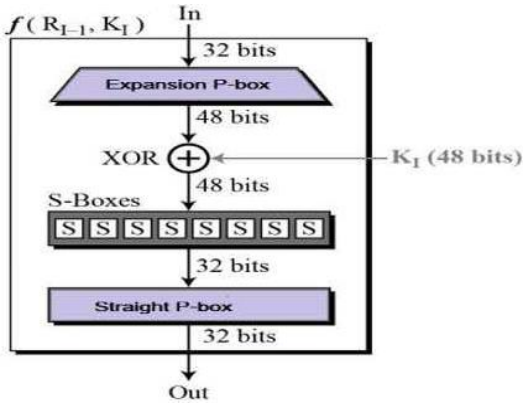
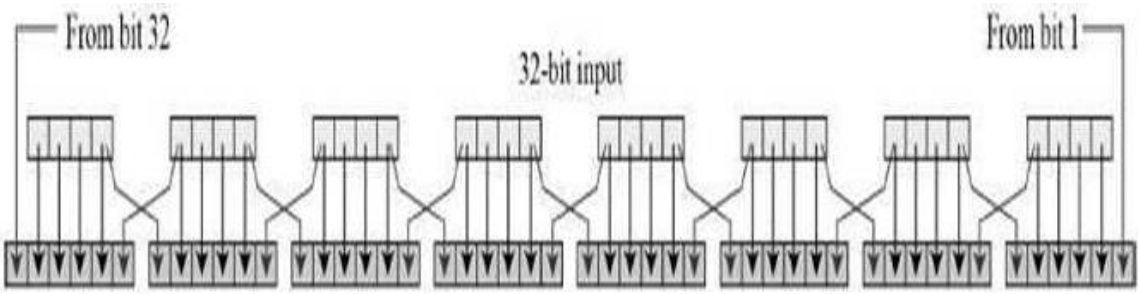


Figure 3.3 Round Functions

Expansion Permutation Box

Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits.



Permutation logic is graphically depicted in the following illustration:

Figure 3.4 Permutation logic

The graphically depicted Permutation logic is generally described as table in DES specification illustrated as shown:

Table 3.1 Permutation logic

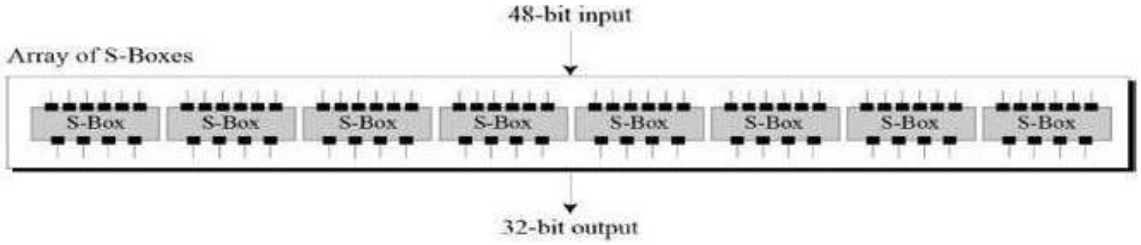
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

XOR(Whitener)

After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

Substitution Boxes

The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and



a 4-bit output. Refer the following illustration –

Figure 3.5 S-Boxes

The S-box rule is illustrated below –

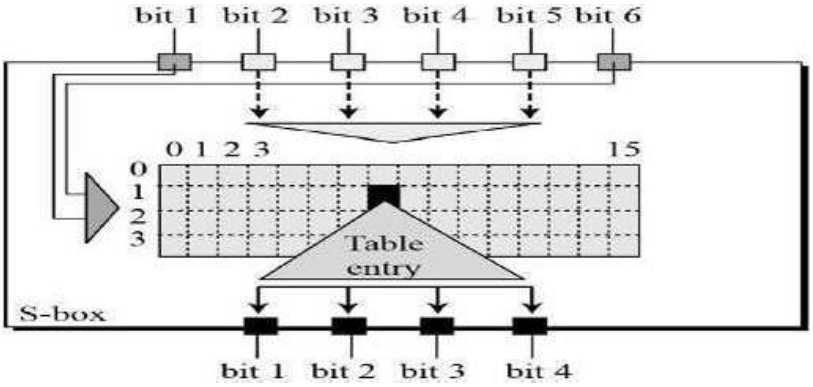


Figure 3.6 S-Box Rules

There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

Straight Permutation − The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:

Table 3.2 Straight Permutation

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −

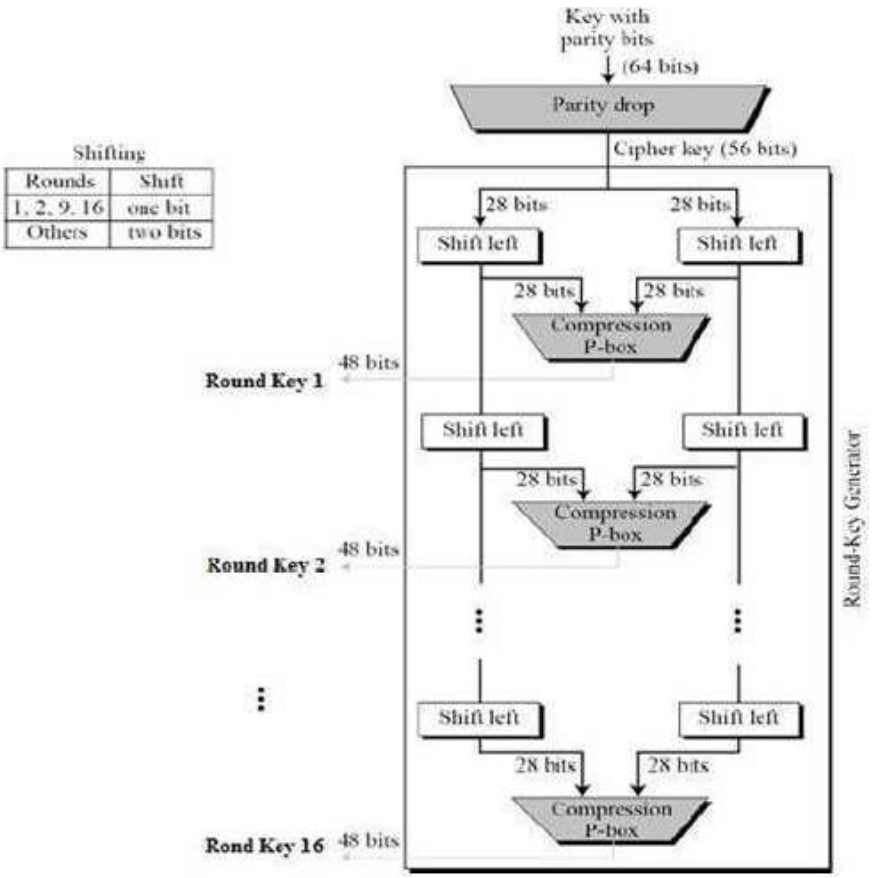


Figure 3.7 the process of key generation

The logic for Parity drops, shifting, and Compression P-box is given in the DES description

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

•Avalanche effect − A small change in plaintext results in the very great change in the cipher text.

•Completeness − Each bit of cipher text depends on many bits of plaintext.

During the last few years, cryptanalysis has found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

ALGORITHM:

STEP-1: Read the 64-bit plain text.

STEP-2: Split it into two 32-bit blocks and store it in two different arrays.

STEP-3: Perform XOR operation between these two arrays.

STEP-4: The output obtained is stored as the second 32-bit sequence and the original second 32-bit sequence forms the first part.

STEP-5: Thus the encrypted 64-bit cipher text is obtained in this way. Repeat the same process for the remaining plain text characters.

CONCLUSION:

Thus the data encryption standard algorithm had been implemented successfully using Java language.

EX.NO:4

IMPLEMENTATION OF AES

AIM:

Write a Java/C/C++/Python program to implement AES algorithm.

.

DESCRIPTION:

Theory Concepts:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C ,Java and Python

Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration −

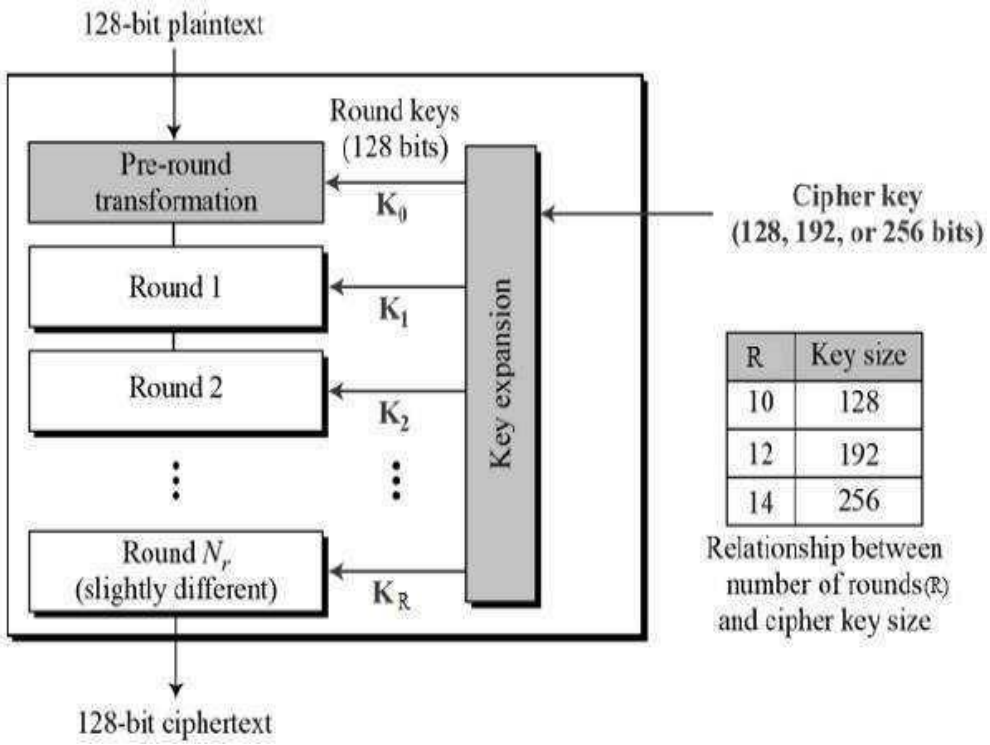
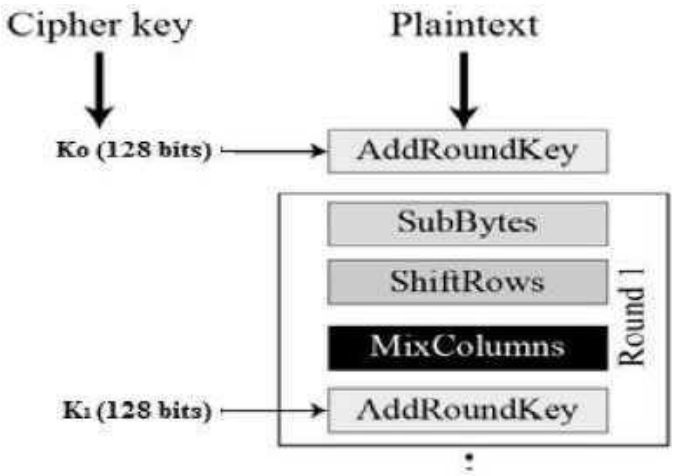


Figure 4.1 AES structure

Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −



CONCLUSION:

Thus the Advanced encryption standard algorithm had been implemented successfully using Java language

EX.NO:5

IMPLEMENTATION OF RSA

AIM:

To write a C program to implement the RSA encryption algorithm.

DESCRIPTION:

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. A basic principle behind RSA is the observation that it is practical to find three very large positive integers e, d and n such that with modular exponentiation for all integer m:

$$(m^e)^d = m(\mathrm{mod} n)$$

The public key is represented by the integers n and e; and, the private key, by the integer d. m represents the message. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

RSA(Rivest, Shamir & Adleman)

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the integers are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

- RSA makes the public and prívate keys by multiplying two large prime numbers *p* and *q*
  - It's easy to find & multiply large prime No. ($n=pq$)
  - It is very difficult to factor the number *n* to find *p* and *q*
  - Finding the private key from the public key would require a factoring operation
  - The real challenge is the selection & generation of keys.

- RSA is complex and slow, but secure
- 100 times slower than DES on s/w & 1000 times on h/w

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secures public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (*e*,*n*), the algorithm is as follows:

1. Represent the message as an integer between 0 and (*n*-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the *e*th power modulo *n*. The result is a ciphertext message C.
3. To decrypt ciphertext message C, raise it to another power *d* modulo *n*

The encryption key (*e*,*n*) is made public. The decryption key (*d*,*n*) is kept private by the user.

How to Determine Appropriate Values for *e*, *d*, and *n*

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as *p* and *q*.
2. Set *n* equal to *p* * *q*.
3. Choose any large integer, *d*, such that GCD(*d*, ((*p*-1) * (*q*-1))) = 1
4. Find *e* such that *e* * *d* = 1 (**mod** ((*p*-1) * (*q*-1)))

Rivest, Shamir, and Adleman provide efficient algorithms for each required operation[4].

How secure is a communication using RSA?

Cryptographic methods cannot be proven secure. Instead, the only test is to see if someone can figure out how to decipher a message without having direct knowledge of the decryption key. The RSA method's security rests on the fact that it is extremely difficult to factor very large numbers. If 100 digit numbers are used for *p* and *q*, the resulting *n* will be approximately 200 digits. The fastest known factoring algorithm would take far too long for an attacker to ever break the code. Other methods for determining *d* without factoring *n* are equally as difficult.

Any cryptographic technique which can resist a concerted attack is regarded as secure. At this point in time, the RSA algorithm is considered secure.

How Does RSA Works?

RSA is an **asymmetric** system, which means that a key pair will be generated (we will see how soon) , a **public** key and a **private** key , obviously you keep your private key secure and pass around the public one.

The algorithm was published in the 70's by Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman, hence RSA, and it sort of implement's a trapdoor function such as Diffie's one.

RSA is rather slow so it's hardly used to encrypt data, more frequently it is used to encrypt and pass around **symmetric** keys which can actually deal with encryption at a **faster** speed.

RSA Security:

- It uses prime number theory which makes it difficult to find out the key by reverse engineering.
- Mathematical Research suggests that it would take more than 70 years to find P & Q if N is a 100 digit number.

Algorithm

The RSA algorithm holds the following features −

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

You will have to go through the following steps to work on RSA algorithm −

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown −

N=p*q

Here, let N be the specified large number.

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1

Step 3: Public key

The specified pair of numbers **n** and **e** forms the RSA public key and it is made public.

Step 4: Private Key

Private Key **d** is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows −

ed = 1 mod (p-1) (q-1)

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is **(n,e).** To encrypt the plain text message in the given scenario, use the following syntax −

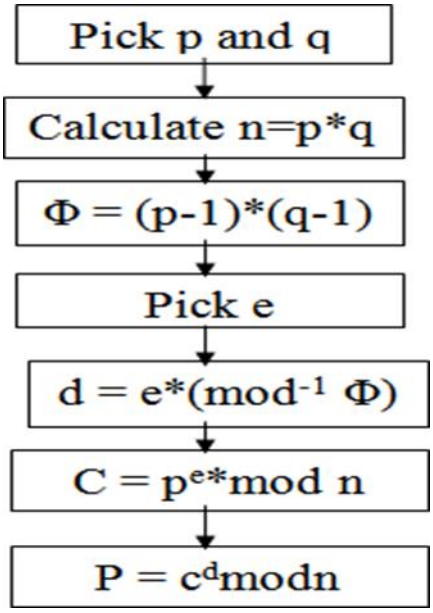
C = Pe mod n

Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver **C** has the private key **d**, the result modulus will be calculated as −

Plaintext = Cd mod n

Example



1. P=7, Q=17
2. 119=7*17
3. (7-1)*(17-1)= 6*16 =96 factor 2 & 3, so E=5
4. (D*5) mod (7-1)*(17-1)=1, so D=77
5. CT=10^5 mod 119 =100000 mod 119 =40
6. Send 40
7. PT=40^{77} mod 119 = 10

ALGORITHM:

STEP-1: Select two co-prime numbers as p and q.

STEP-2: Compute n as the product of p and q.

STEP-3: Compute (p-1)*(q-1) and store it in z.

STEP-4: Select a random prime number e that is less than that of z.

STEP-5: Compute the private key,dase*mod^{-1}(z).

STEP-6: The cipher text is computed as $message^{e}$*mod n.

STEP-7: Decryption is done as $cipher^{d}$ mod n.

CONCLUSION:

Thus we learn that to how to Encrypt and Decrypt the message by using RSA Algorithm.

EX.NO:6

IMPLEMENTATION OF DIFFIEHELLMAN KEY EXCHANGE ALGORITHM

AIM:

To implement the Diffie-Hellman Key Exchange algorithm using C language.

DESCRIPTION:

Diffie–Hellman Key Exchange establishes a shared secret between two parties that can be used for secret communication for exchanging data over a public network. It is primarily used as a method of exchanging cryptography keys for use in symmetric encryption algorithms like AES. The algorithm in itself is very simple. The process begins by having the two parties, Alice and Bob. Let's assume that Alice wants to establish a shared secret with Bob.

Diffie-Hellman key Exchange (DH)

In the mid- 1970's, Whitefield Diffie, a student at the Stanford University met with Martin Hellman, his professor &the two began to think about it. After some research & complicated mathematical analysis, they came up with the idea of AKC. Many experts believe that this development is the first & perhaps the only truly revolutionary concept in the history of cryptography

Silent Features of Diffie-Hellman key Exchange (DH)

1. Developed to address shortfalls of *key distribution* in symmetric key distribution.
2. A *key exchange algorithm*, not an encryption algorithm
3. Allows two users to share a *secret key* securely over a public network
4. Once the key has been shared Then both parties can use it to encrypt and decrypt messages using symmetric cryptography
5. Algorithm is based on "difficulty of calculating discrete logarithms in a finite field"
6. These keys are mathematically related to each other.
7. ''Using the public key of users, the session key is generated without transmitting the private key of the users.''

Diffie-Hellman Key Exchange/Agreement Algorithm with Example

1. Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.

   Let n = 11, g = 7.

2. Alice chooses another large random number x, and calculates A such that:
   $A = g^x \bmod n$

   Let x = 3. Then, we have, $A = 7^3 \bmod 11 = 343 \bmod 11 = 2$.

3. Alice sends the number A to Bob.

   Alice sends 2 to Bob.

4. Bob independently chooses another large random integer y and calculates B such that:
   $B = g^y \bmod n$

   Let y = 6. Then, we have, $B = 7^6 \bmod 11 = 117649 \bmod 11 = 4$.

5. Bob sends the number B to Alice.

   Bob sends 4 to Alice.

6. A now computes the secret key K1 as follows:
   $K1 = B^x \bmod n$

   We have, $K1 = 4^3 \bmod 11 = 64 \bmod 11 = 9$.

7. B now computes the secret key K2 as follows:
   $K2 = A^y \bmod n$

   We have, $K2 = 2^6 \bmod 11 = 64 \bmod 11 = 9$.

Diffie -Hellman Key exchange

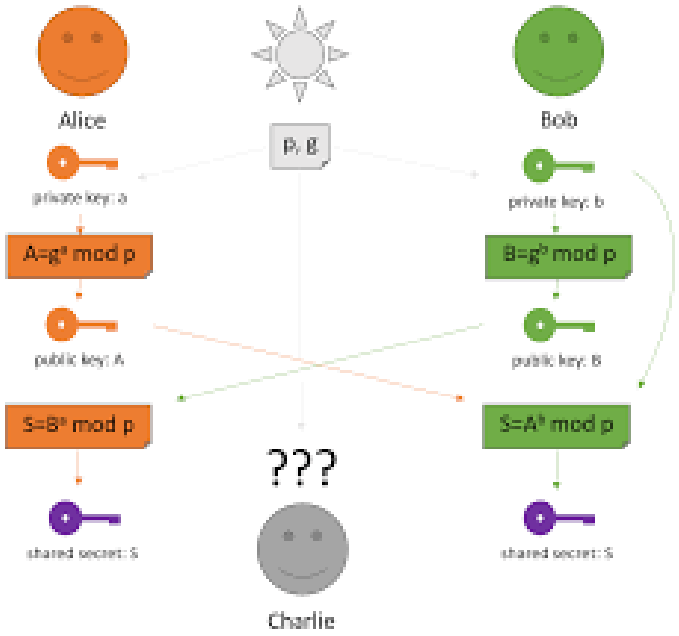
1. Public values:

- large prime p, generator g (primitive root of p)

2. Alice has secret value x, Bob has secret y
3. Discrete logarithm problem: given x, g, and n, find A
4. A $\rightarrow$ B: $g^x \pmod n$
5. B $\rightarrow$ A: $g^y \pmod n$
6. Bob computes $(g^x)^y = g^{xy} \pmod n$
7. Alice computes $(g^y)^x = g^{xy} \pmod n$
8. Symmetric key= $g^{xy} \pmod n$

Limitation: Vulnerable to "man in the middle" attacks*

EXAMPLE:



ALGORITHM:

STEP-1: Both Alice and Bob shares the same public keys g and p.

STEP-2: Alice selects a random public key a.

STEP-3: Alice computes his secret key A as g^a mod p.

STEP-4: Then Alice sends A to Bob.

STEP-5: Similarly Bob also selects a public key b and computes his secret key as B and sends the same back to Alice.

STEP-6 : Now both of them compute their common secret key as the other one's secret key power of a mod p.

CONCLUSION:

Thus we have studied and implement Diffie-Hellmen key exchange algorithm

EX.NO:7

IMPLEMENTATION OF MD5

AIM:

To write a C program to implement the MD5 hashing technique.

DESCRIPTION:

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks. The message is padded so that its length is divisible by 512.The padding works as follows: first a single bit ,1 ,is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message upto 64 bits less than a multiple of 512.The remaining bits are filled up with 64bits representing the length of the original message, modulo 2^{64}.
The main MD 5 algorithm

operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C, and D. These are initialized to certain fixed constants. The main algorithm then uses each 512-bit message block in turn to modify the state.

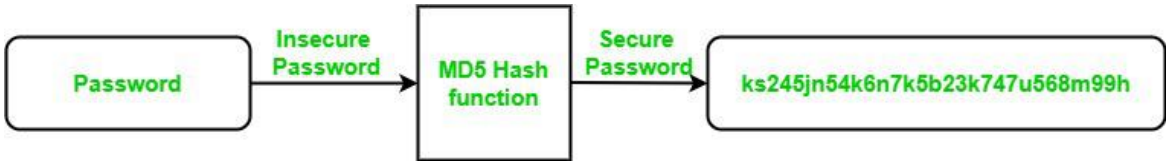
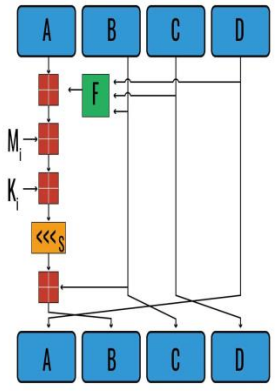


Fig 7.1 Simplified Block diagram



EXAMPLE:

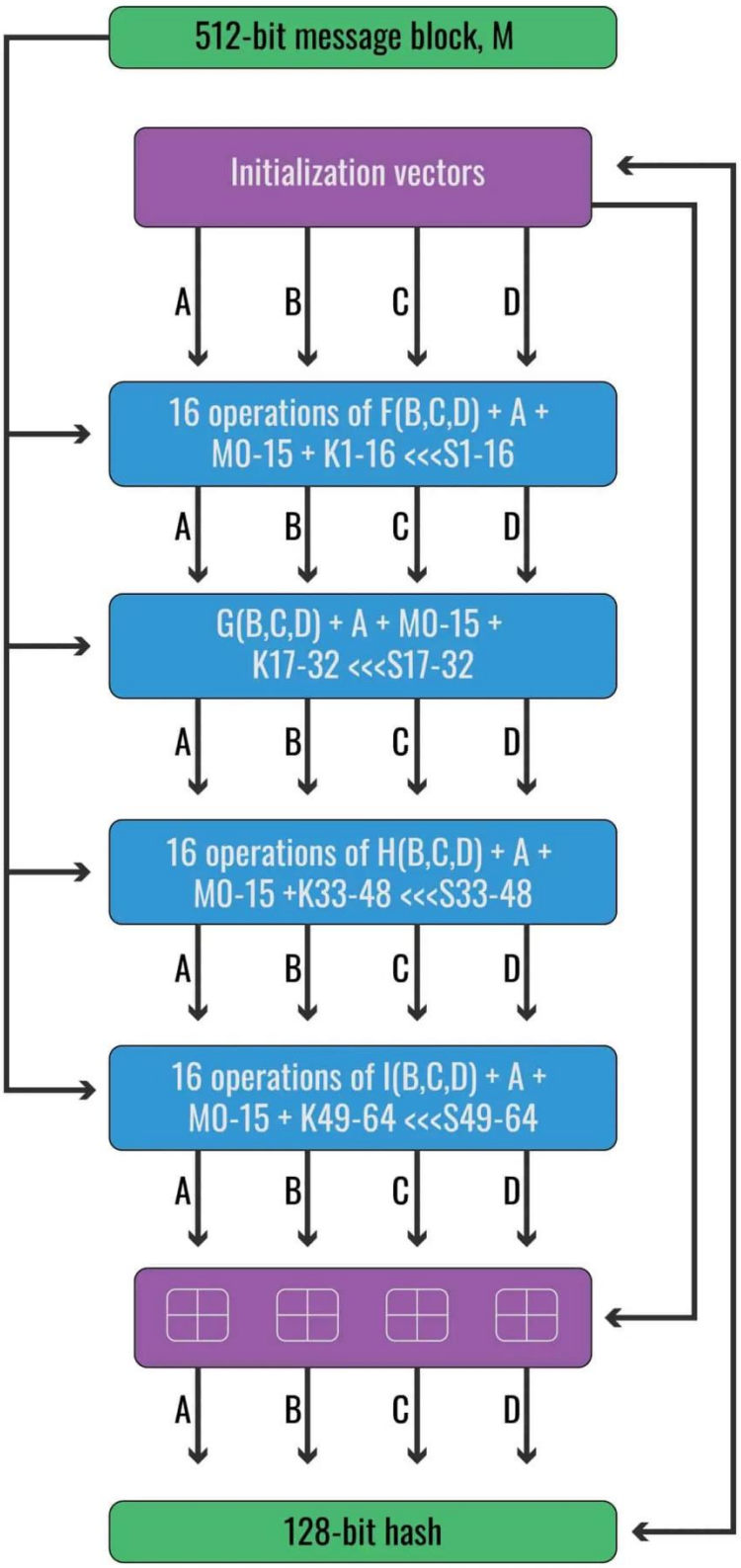


Fig 7.3 Structure of MD5

ALGORITHM:

STEP-1: Read the 128-bit plain text.

STEP-2: Divide into four blocks of 32-bits named as A,B,C and D.

STEP3: Compute the functions f, g, hand I with operations such as, rotations, permutations, etc,.

STEP4: The output of these functions are combined together as F and performed circular shifting and then given to key round.

STEP-5: Finally, right shift of‘ s’times are performed and the results are combined together to produce the final output.

CONCLUSION:

Thus we have studied and implement of MD5 hashing algorithm

STEP3: Compute the functions f, g, hand I with operations such as, rotations, permutations, etc,.

STEP4: The output of these functions are combined together as F and performed circular shifting and then given to key round.

STEP-5: Finally, right shift of' s'times are performed and the results are combined together to produce the final output.

CONCLUSION:

Thus we have studied and implement of MD5 hashing algorithm