Discrete Mathematics

SC205

Project-2023

prof. Manish K. Gupta
prof. Prosenjit Kundu
prof. Manoj Raut

- **Project Name**

Application of Cryptography

- **Group Members**

Het Shah
202201515

Manoj Dhundhlava
202201503

Nitin Kanzariya
202201181

Zeel Boghara
202201201

Kashyap Trivedi
202201191

Kartik Bariya
202201202

1 Introduction to cryptography

- Definition :

  Cryptography is the practise of securing communication in the presence of adversaries, according to the definition. It entails strategies and procedures for converting information into an incomprehensible form for unauthorised individuals, known as ciphertext, and then decrypting it back into its original form, known as plaintext.

1. Cryptography protects and conceals information. Unauthorised individuals gained access.

2. Cryptography also ensures that data has not been altered or interfered with during transmission or storage.

3. It aids in the identification of communication parties and guarantees messages originate from reliable sources. They conveyed a message.

4. Different types of cryptography exist, such as using the same key for both encryption and decryption (symmetric encryption) or using separate keys for each (asymmetric encryption).

2 Types of Cryptography:

- Symmetric Encryption: Uses the same key for encryption and decryption.
- Asymmetric Encryption: Uses different keys for encryption and decryption.
- Cryptographic Hash Functions: Transforms data into fixed-size codes.
- Key Management: Involves securely generating, sharing, and storing encryption keys.

2.1 Symmetric Cryptography

- Symmetric cryptography, also known as secret-key cryptography, uses the same key for both encryption and decryption. It involves the following steps:

  1. The sender encrypts the plaintext message using the shared secret key.
  2. The encrypted message, known as ciphertext, is transmitted to the receiver.
  3. The receiver decrypts the ciphertext using the same secret key to obtain the original plaintext message.

  Examples of symmetric encryption algorithms include Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

2.2 Asymmetric Cryptography

- Asymmetric cryptography, often known as public-key cryptography, encrypts and decrypts using separate keys. It consists of the following steps:

  1. The receiver generates a key pair consisting of a public and a private key.
  2. The receiver shares the sender's public key while keeping the sender's private key private.
  3. The sender encrypts the plaintext message using the receiver's public key.
  4. The encrypted message, referred to as ciphertext, is sent to the receiver.r.
  5. Using their private key, the receiver decrypts the ciphertext to recover the original plaintext message.

  Secure key exchange and digital signatures are two advantages of asymmetric cryptography. RSA is the most extensively used asymmetric encryption algorithm. (Rivest-Shamir-Adleman)

3 Introduction of AES and DES

3.1 AES (Advanced Encryption Standard)

- What exactly is AES ?

  ⇒ The National Institute of Standards and Technology (NIST) in the United States picked AES as an encryption standard to secure sensitive information. It is frequently recognised as an effective algorithm for encrypting sensitive data.

  ⇒ It is a block cypher that encrypts and decrypts using a 128-bit block size.

  ⇒ Each round consists of the same operations.

  The Advanced Encryption Standard (AES) is a symmetric encryption technology that is widely used for secure data transfer and storage. It succeeded the Data Encryption Standard (DES) due to its improved security and efficiency. AES works using data blocks and a secret key for encryption and decryption.

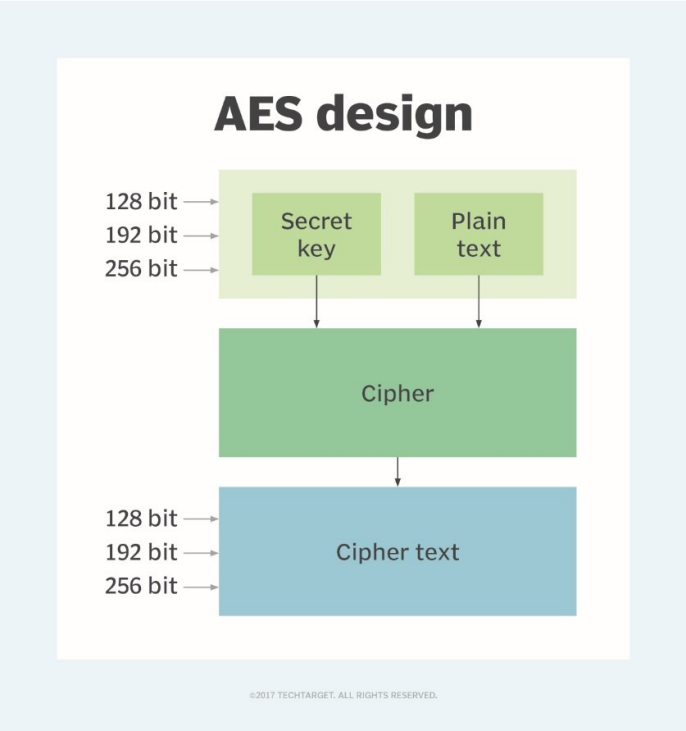


Figure 1: AES Logo

3.2 DES (Data Encryption Standard)

- Before AES, the Data Encryption Standard (DES) was a popular symmetric encryption technique. It operates on 64-bit data blocks and has a 56-bit secret key. To encrypt and decrypt data, DES employs numerous rounds of substitution, permutation, and XOR operations.

3.2.1 Description

- DES is a Feistel network structure block cypher. It employs a 56-bit key, with 8 bits for parity and the remaining 48 bits for encryption. DES supports 16 rounds of operations, including substitution, permutation, and XOR.

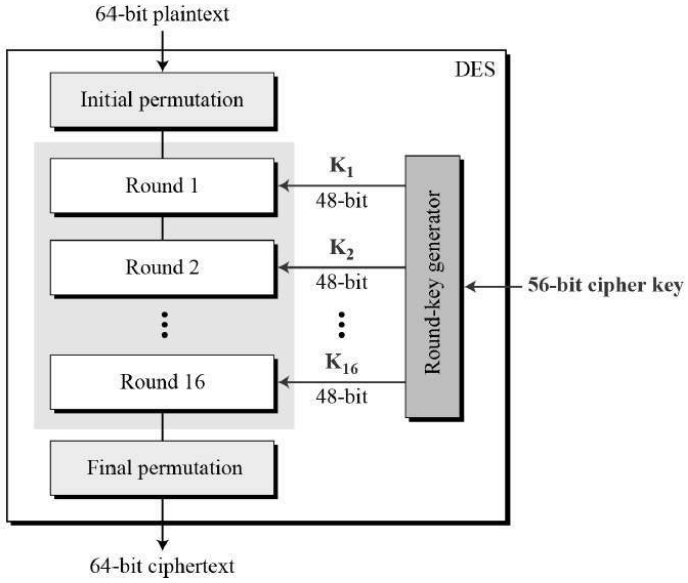


Figure 2: DES Logo

4 AES Algorithm

4.1 Description

- AES is a symmetric encryption algorithm that operates on blocks of data. It uses a substitution-permutation network (SPN) structure to achieve secure encryption and decryption. The algorithm consists of several rounds, with the number of rounds depending on the key size.

4.2 What is the procedure?

- To encrypt data, AES fundamentally repeats four major processes. It takes a 128-bit block of data and a key [the layman's term for password] and outputs ciphertext. The functions are as follows:

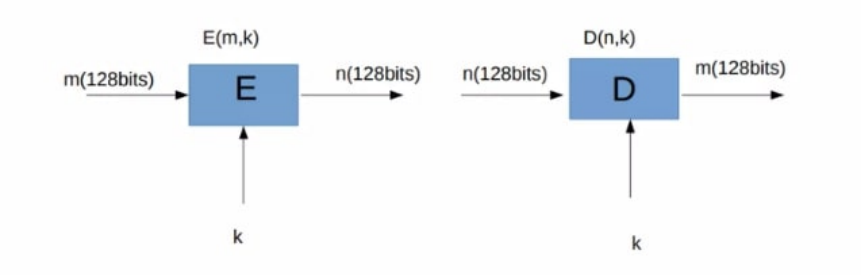
  1. Sub Bits
  2. Row Shifts
  3. Columns of Mix
  4. Insert Key

  ⇒ The number of rounds performed by the algorithm is tightly determined by the size of the key.

  ⇒ The following table gives overview of number of rounds performed with the input of varying key lengths:

Key Size (in bits)	Rounds
128	10
192	12
256	14

The greater the number of keys, the more secure the data. The time it takes s/w to encrypt will rise as the number of rounds increases.



Here,

E = the encryption function for a symmetric block cipher

m = a 128-bit plain text message

n = cipher text

k = a 128-bit key that is used for both encryption and decryption.

D = symmetric block cypher decryption function.

- Steps For Incryption And Decryption :

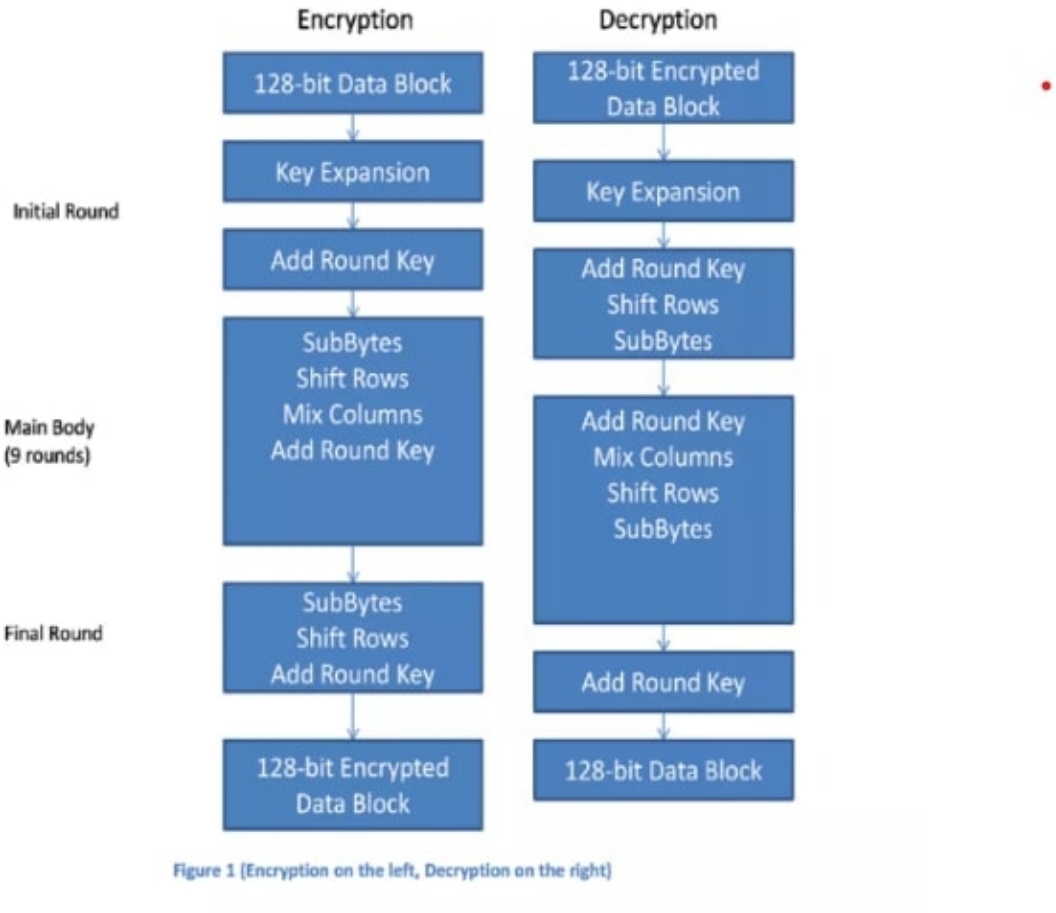


Figure 3: Example Figure

4.3 Step Analysis

- Key Expansion- During the expansion process, the given 128-bit cypher key is stored in a matrix of [4]X [4] bytes (16*8 = 128 bits), and the four column word of the key matrix is extended into a schedule of 44 words (44*4 = 176), resulting in 11 round keys (176/11 = 16 bytes or 128 bits).

- $N_r + 1$ = the number of round keys. Where N_r is the number of rounds (which is 10 in the case of a 128-bit key size), the round keys are 11.

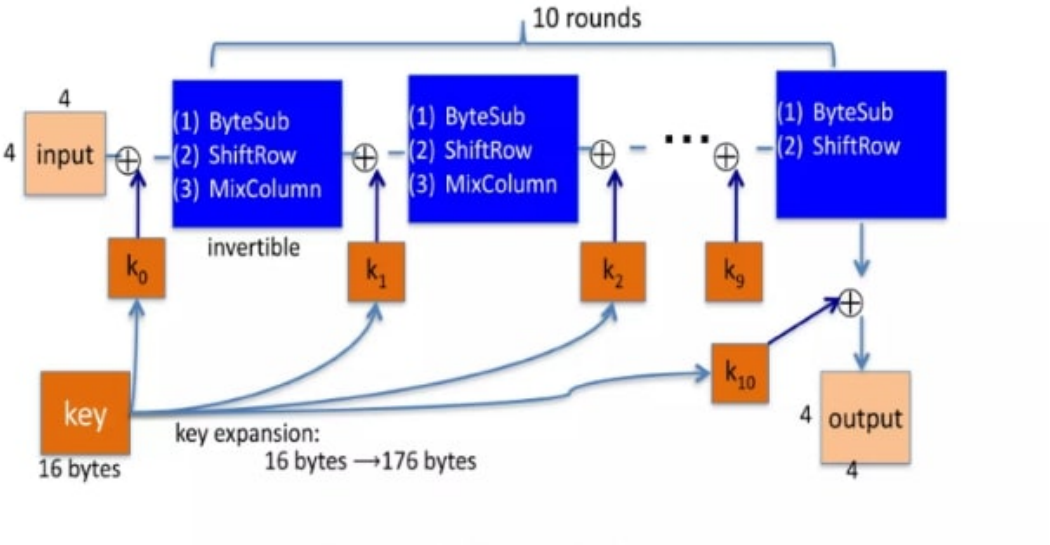
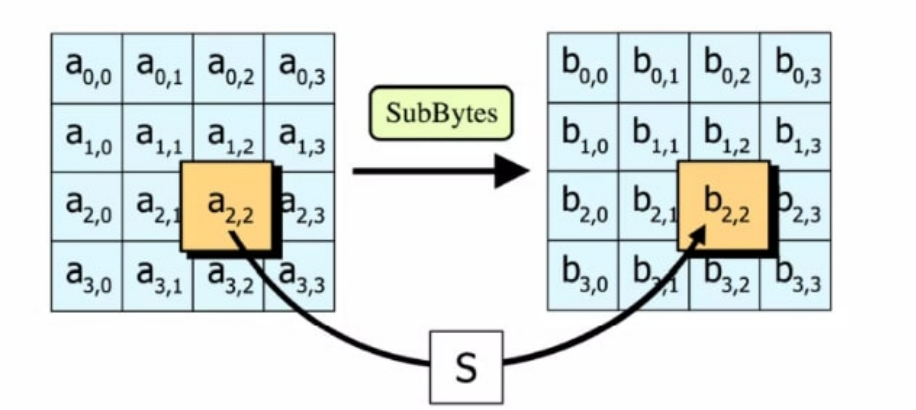


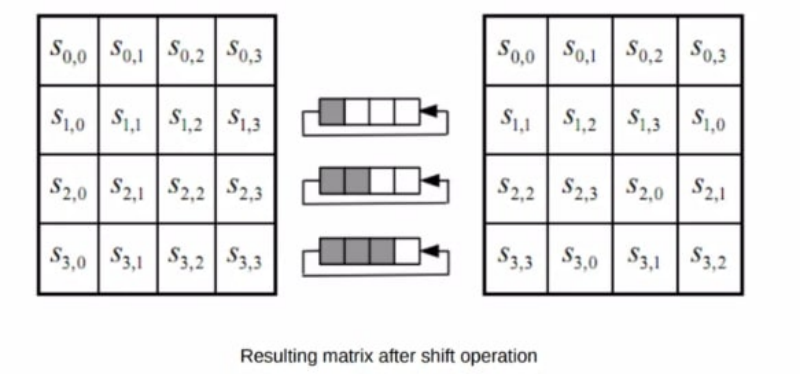
Figure 4: Example Figure

SubBytes: Each matrix element is replaced by an s-box matrix element.



- The S-box is a special look up table which is constructed by Galois fields.
- The generating function used in this algorithm is GF(256).
- For shift row, In this step rows of the block are cylindrically shifted in left direction.

The first row is untouched, the second by one shift, third by two and fourth by 3.



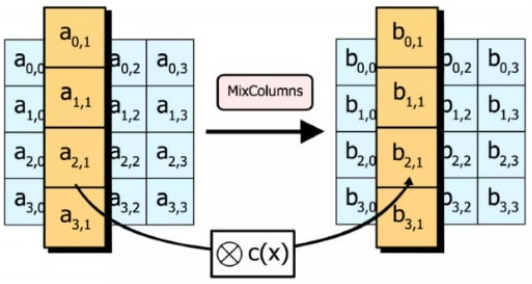
- Shift Rows
- Mix columns

This is the most critical portion of the algorithm since it causes the bit flipping to spread throughout the block.

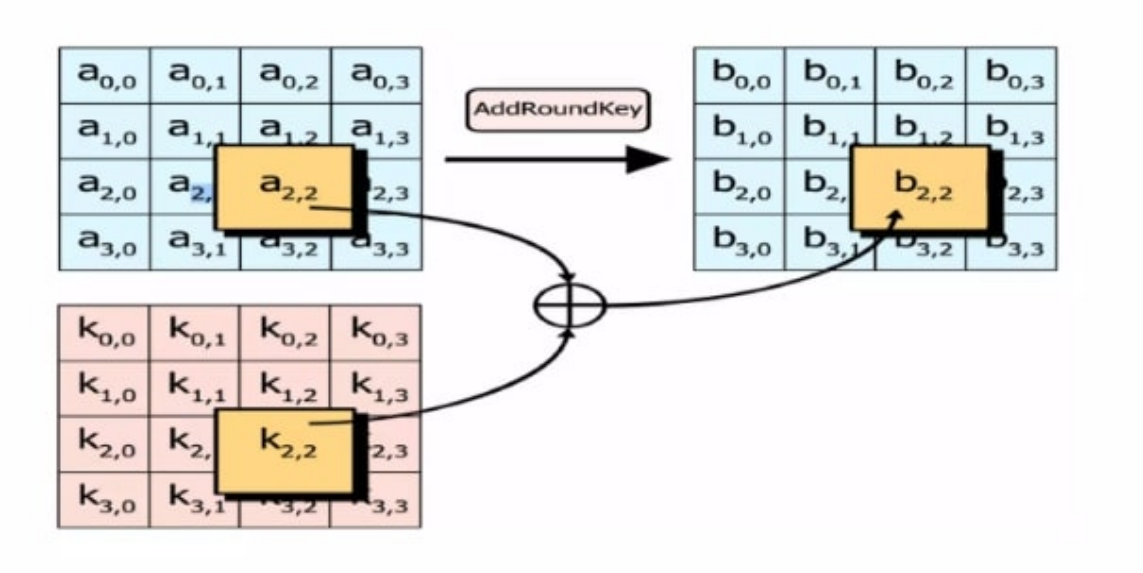
In this phase, the block is multiplied using a fixed matrix.

In the Galois field, the multiplication is field multiplication.

There are 16 multiplications, 12 XORs, and a 4-byte output for each row.



- Add round key



In this stage, each byte is XOR-ed with the relevant element of the key's matrix.

Once this step is completed, the keys for this phase are no longer available. Using the same key will cause the algorithm to fail.

To address this issue, the keys are enlarged.

The mix column step is skipped in the final round.

It is not recorded why this is done, although a paper was recently produced against this practise, exposing the weakening of cipher text.

5 DES Algorithm

- The DES cryptosystem is a slightly modified Feistel cipher with alphabet {O, 1} and block length 64. In this section, we explain in detail how DES works.

0	0	0	1	0	0	1	1
0	0	1	1	0	1	0	0
0	1	0	1	0	1	1	1
0	1	1	1	1	0	0	1
1	0	0	1	1	0	1	1
1	0	1	1	1	1	0	0
1	1	0	1	1	1	1	1
1	1	1	1	0	0	0	1

Figure 5: Valid DES key

5.1 Plaintext and Ciphertext Space

- The plaintext and ciphertext spaces of DESare P = C = $\{0,1\}^{64}$. The DES keys are all bitstrings oflength 64 with the following property. If a 64-bit DES key is divided into eight bytes, then the sum of the eight bits of each byte is odd. This means that seven of the eight bits determine the value of the eighth bit. Transmission errors of one bit can be corrected. Therefore, the key space is

$$\mathcal{K} = \{(b_1, \ldots, b_{64}) \in \{0,1\}^{64} : \sum_{i=1}^{8} b_{8k+i} \equiv 1 \mod 2, 0 \leq k \leq 7\}.$$

The number of DES keys is $2^{56} \sim 7.2 * 10^{16}$.

Example :

A valid hexadecimal DES key is 0.5cm33457799BBCDFFI. Its binary expansion can be found in Figure 5.

5.2 Initial Permutation

- Given a plaintext p, DES works in three steps. Prior to the Feistel encryption, DES applies an initial permutation (IP) to p . This is a bit permutation on bit vectors of length 64 that is independent of the chosen key . The permutation IP and its inverse are shown in given below figure. Below figure is read as follows: If p $\in\{O, 1\}^{64}$, P = P_1 P_2 $P_3 \cdot \cdot P_{64}$, then IP(P) = P_{58} P_{50} $P_{42} \cdot \cdot \cdot P_7$.

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

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

A 16-round Feistel cipher is applied to the permuted plaintext. Finally, the ciphertext is constructed using the inverse permutation IP^{-1}:

$$c = IP^{-1}(R_{16}L_{16}).$$

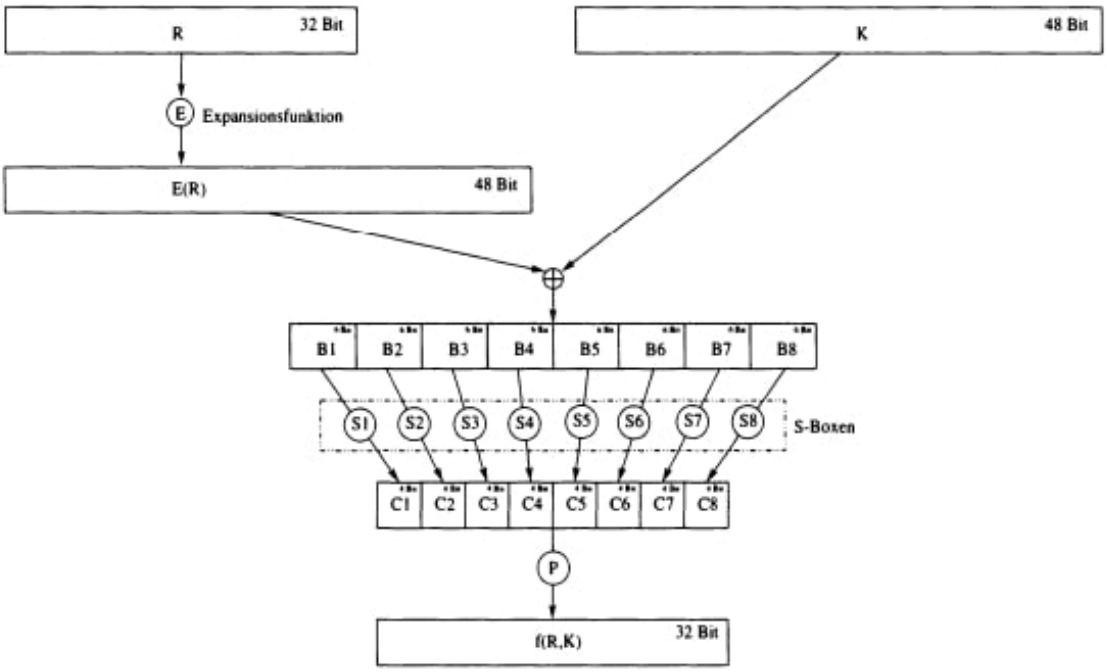
5.3 Internal Block Cipher

- We describe the block cipher on which the DES Feistel cipher is based . Its alphabet is O,1, its block length is 32, and its key space is $\{O, 1\}^{48}$. We explain the encryption function f_k : $\{O, 1\}^{32}$ $\rightarrow${O,1}^{32} for a key K $\in${O, 1}^{48}

The argument R $\in\{0,1\}^{32}$ is expanded by the expansion function E : $\{0,1\}^{32} \rightarrow\{0,1\}^{48}$. This function is shown in s-box Figure . If R = R_1 R_2 ... R_{32} , then E(R) = R_{32} R_{31} R_2 . . . R_{32} R_1.

Next, E(R) $\oplus$ K is computed, and the result is divided into eight blocks B_i, 1 $\leqslant$ i $\leqslant$ 8 of length 6 namely,

$$\mathrm{E(R)} \oplus \mathrm{K} = B_1\ B_2\ B_3\ B_4\ B_5\ B_6\ B_7\ B_8$$



is computed with $B_i \in\{0,1\}^6$, 1 $\leqslant$ i $\leqslant$ 8. In the next step, functions S_i : $\{0,1\}^6 \rightarrow\{0,1\}^4$, 1 $\leqslant$ i $\leqslant$ 8

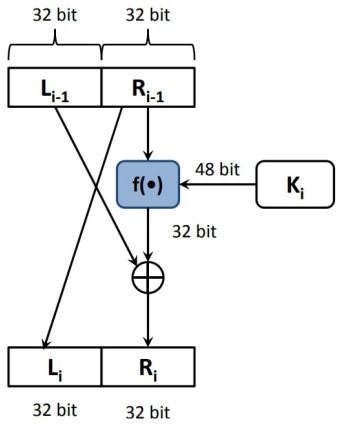
are used (the so-called S-boxes). They are described below. Using those functions, the string

$$\mathrm{C} = C_1\ C_2\ C_3\ C_4\ C_5\ C_6\ C_7\ C_8$$

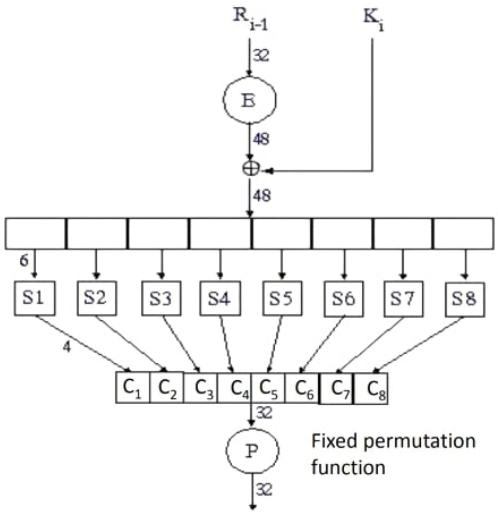
is determined, where $C_i = S_i(B_i)$, 1 $\leqslant$ i $\leqslant$ 8. It has length 32. The permutation P from below figure is applied to this string. The result is f_k(R).

5.3.1 DES ROUND i

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



5.3.2 DES "f(•)"*Function*



- E is an expansion function that generates a block of 48 bits from a block of 32 bits of input.
- 16 bits appear twice, in the expansion.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	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	30	31	32	1

5.4 s-boxes

- Now we describe the S-boxes s_i, $1 \leqslant i \leqslant 8$. They are the heart of DES because they are highly nonlinear . They are shown in figure 6. Each S-box is represented by a table with four rows and 16 columns. For each string B = b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 , the value S_i(B) is computed as follows. The integer with binary expansion b_1 b_6 is used as the row index. The integer with binary expansionb_2 b_3 b_4 b_5 is used as the column index . The entry of the S-box in this row and column is written in binary expansion. This expansion is padded with leading zeros such that its length is four. The result is S_i(B).

- The functions E and P.

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	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	30	31	32	1

P			
16	7	10	21
29	12	28	17
1	15	23	26
5	18	31	20
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Row	Column															
	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
S_1																
[0]	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
[1]	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
[2]	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
[3]	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
[0]	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
[1]	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
[2]	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
[3]	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
[0]	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
[1]	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
[2]	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
[3]	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
[0]	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
[1]	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
[2]	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
[3]	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																
[0]	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
[1]	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
[2]	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
[3]	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
[0]	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
[1]	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
[2]	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
[3]	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
[0]	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
[1]	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
[2]	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
[3]	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
[0]	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
[1]	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
[2]	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
[3]	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Figure 6: S-box of DES

5.5 Keys

- Finally, we explain how the round keys are computed. Let k $\in \{0,1\}^{64}$ be a DES key. We generate the round keys K_i , $1 \leqslant$ i $\leqslant 16$, oflength 48. We define the values V_i, $1 \leqslant$ i $\leqslant 16$, as follows .

  The round keys are computed by the following algorithm using the functions

  PC1 : $\{0,1\}^{64} \to \{0,1\}^{64} \times \{0,1\}^{64}$, PC2 : $\{0,1\}^{64} \times \{0,1\}^{64} \to \{0,1\}^{64}$,

$$v_i = \begin{cases} 1 & \text{for } i \in \{1, 2, 9, 16\} \\ 2 & \text{otherwise.} \end{cases}$$

which are described later.

1. Set (C_o, D_o) = PC1(k).

2. For1 $\leqslant$ i $\leqslant$ 16, do the following:

   (a) Let C_i be the string that is obtained from D_{i-1} by a circular left shift of V_i positions

PC1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Figure 7: The functions PC1 and PC2

   (b) Let D_i be the string that is obtained from D_{i-1} by a circular left shift of V_i positions.

   (c) Determine K_i = PC2(C_i, D_i) .

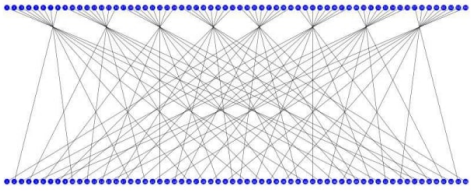
The function PCI maps a bit string k of length 64 to two bit strings C and D of length 28. This is done according to above table. The upper half of the table describes C. If k = k_1 k_2 . . . k_{64}, then C = k_{57} k_{49}...k_{36} . The lower half of the table represents D, so D =k_{63} k_{55} ... k_4. The function PCZ maps a pair (C, D) of bit strings of length 28 (i.e., a bit string of length 56) to a bit string of length 48. The function is shown in above Table . The value PC2(b_1 ...b_{56}) is b_{l4} b_{l7} .. . b_{32} .

This concludes the description of the DES encryption algorithm.

5.6 Final Permutation(IP^{-1})

- The table is read in a manner that is comparable to how the end permutation is the inverse of the starting permutation.

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



- In other words, the first bit of the output of the final permutation is bit 40 of the preoutput block, the second bit is bit 8, the third is bit 9, and so on, ending with bit 25 of the preoutput block as the last bit.

5.7 Security of DES

- Brute-force attacks: With today's computational power, it is easy to run DES through a thorough key search attack, testing every potential key until the right one is discovered.
- Attacks based on cryptanalysis: A number of cryptanalysis methods, including meet-in-the-middle attacks, linear cryptanalysis, and differential cryptanalysis, have been created to take advantage of DES's flaws.
- 3 DES (Triple DES): 3 DES, which employs DES encryption three times with distinct keys, was invented to increase security. This improves security over DES alone by increasing the effective key size to 168 bits.
- AES Replacement: The Advanced Encryption Standard (AES) has replaced DES and 3DES as the industry-standard encryption algorithms because it provides greater security. AES may use keys that are 128, 192, or 256 bits long, which makes it more resilint to brute-force assaults.
- DES Limitations: DES has other restrictions in addition to the key length. It uses blocks of 64 bits, which might be limited for some applications. Additionally, it lacks integrated support for functions like data integrity and authentication.

6 MATH BEHIND AES AND DES

- AES and DES involves advanced concepts from algebra, number theory, finite fields, and cryptography.The types of algebra is modular arithmetic(modulus) , Boolean algebra(AND($*$) , OR($+$) , XOR($\wedge$) , XNOR($\vee$)) , finite fields(Galois field GF($2\wedge8$)).

6.1 MODULAR ARITHMETIC EXAMPLE:

- Suppose we want to perform modular arithmetic on the numbers 17 , with a modulus of 5. In this case, we are interested in finding the remainder when dividing 17 by 5.

To do this, we divide 17 by 5: $17 \div 5 = 3$ with a remainder of 2. In modular arithmetic, we only consider the remainder.

Therefore, the result of 17 modulo 5 is 2.Another way to express this is: $17 \equiv 2 \pmod 5$, which reads as "17 is congruent to 2 modulo 5.

6.2 BOOLEAN ALGEBRA EXAMPLE :

- Boolean algebra is like a set of rules for working with two states: ON and OFF.

AND Operation : If both switches are turned on (1), the result is ON (1). Otherwise, the result is OFF (0).

OR Operation : If at least one switch is turned on (1), the result is ON (1). If both switches are turned off (0), the result is OFF (0).

XOR Operation : If the switches have different states (one is ON and the other is OFF), the result is ON (1). If both switches have the same state (both ON or both OFF), the result is OFF (0).

6.3 FINITE FIELD EXAMPLE :

1. Additional in the finite field

   When you add two numbers within this finite field, if the result goes beyond 3, we wrap around and start again from 0.
   For example:

   2 + 3 = 1 (since 2 + 3 = 5, but we wrap around to 1 within our finite field)

   3 + 3 = 2 (since 3 + 3 = 6, but we wrap around to 2)

   In this finite field, the highest number we can reach is 3. Once we go beyond that, we loop back to the beginning.

2. Multiplication in the Finite Field

   When you multiply two numbers within this finite field, if the result goes beyond 3, we wrap around as well.
   For example:

   2 * 3 = 2 (since 2 * 3 = 6, but we wrap around to 2 within our finite field)

   3 * 3 = 1 (since 3 * 3 = 9, but we wrap around to 1)

   Again, the multiplication operation follows the wrapping-around rule within our limited set of numbers.

7 What exactly is the issue ?

- Here are some examples of challenges that AES and DES can help with:

1. Data Confidentiality : AES and DES ensure that data remains private while being sent or stored. Unauthorised individuals cannot access the information without the accompanying decryption key because the data is encrypted using these algorithms.
2. Secure Communication : AES and DES are commonly used in secure communication protocols such as SSL/TLS, VPNs, and encrypted email. They provide a secure conduit for transmitting sensitive data across public networks, preventing eavesdropping and unauthorised access.
3. Compliance and Standards : For data encryption, AES and DES have been adopted as industry standards. They assist businesses in meeting security requirements and standards such as the Payment Card Industry Data Security Standard (PCI DSS) and the Federal Information Processing Standard (FIPS).

8 Solution of problem using AES and DES

- solution of third problem secure communication

AES and DES are like secret codes used to protect messages sent over networks. They ensure that only the intended recipients can read the messages, while keeping them hidden from others who might try to intercept or eavesdrop.

When you send a message using secure communication protocols like SSL/TLS or VPNs, AES or DES is used to encrypt the message before it travels across the network. This encryption process transforms the message into a scrambled form that is unreadable without a special key.

At the receiving end, the encrypted message is decrypted using the same encryption algorithm (AES or DES) and the corresponding key. The decrypted message is then revealed in its original, readable form to the intended recipient.

The use of AES and DES in secure communication allows for confidential and secure exchanges of sensitive information, protecting it from unauthorized access and maintaining the privacy and integrity of the data being transmitted.

9 Maths in solving problem

1. Number Theory : Number theory plays a significant role in cryptography. Concepts like prime numbers, modular arithmetic, modular inverses, Euler's totient function, and the Chinese Remainder Theorem are utilized in tasks like generating and manipulating encryption keys, factoring large numbers, and analyzing the mathematical properties of cryptographic

algorithms.

Example: In RSA encryption, the security is based on the difficulty of factoring large composite numbers into their prime factors. Number theory techniques are used to analyze the properties of large numbers and identify factors that can compromise the encryption.

2. Algebraic Structures : Algebraic structures, such as finite fields, rings, and groups, are employed in cryptography. Finite fields, in particular, play a crucial role in symmetric encryption algorithms like AES and DES. Finite fields involve operations like addition, multiplication, and exponentiation performed on finite sets of elements.

   Example: AES and DES utilize the mathematics of finite fields to perform substitution and permutation operations, which shuffle and transform the data during encryption. Finite field arithmetic ensures that computations stay within a specific range, enhancing the security of the algorithms.

10 Disadvantages of AES and DES

1. Disadvantages of AES:

   AES can be slow and computationally demanding, especially with larger key sizes, which can be a disadvantage in devices with limited processing power.

   AES requires careful key management practices to ensure the security of encryption keys, which can be challenging to implement correctly.

2. Disadvantages of DES:

   DES has a relatively short key length, which makes it susceptible to brute-force attacks. Advances in computing power have made it easier to crack DES encryption.

   DES is an older algorithm that lacks some modern security features found in newer encryption algorithms, making it less secure overall.

   Known attacks, such as differential and linear cryptanalysis, have been successful against DES, compromising its security.

11 CONCLUSION

- In conclusion, cryptography is an essential tool for ensuring the confidentiality, integrity, and authenticity of sensitive information. It plays a critical role in protecting data in an increasingly digital world and continues to evolve to address new challenges and threats.

HOW CAN WE COMMERCIALIZE OUR SOLUTION AND CONVERT IT IN STARTUP ?

- By leveraging the strong demand for secure data encryption solutions, the software can be positioned as a valuable product in the market. With a well-crafted business plan,more improved software and a skilled team, the startup can help businesses and people to secure their data. By developing a scalable and user-friendly software platform that prioritizes data security, the startup can meet the needs of various industries. Effective marketing and sales strategies will help reach potential clients and showcase the software's advantages.

12 More Information

- You tube video : https://youtu.be/drkR91C9bRo
- Website Link : https://dm-project-of-cryptography-2023.netlify.app/
- Drive Link : https://drive.google.com/file/d/1ZHXVw$_{Iq}$9EvwGJwqRZ3v−2W4pC8CewK/view?usp = drivesdk

13 Contribution

- Het shah : Task-Website
- Manoj Dhundhalva :Task-(Website + Software)
- Nitin Kanzariya : Task-Latex
- Zeel Boghara : Task-Latex
- Kashyap Trivedi : Task-PPT
- Kartik Baria : Task-Video

These are References that we used during making LateX file [1] , [2] ,[3] ,[4] ,[5].

References

[1] V. R. Joan Daemen, The Design of Rjindael: AES.

[2] B. Schneier, Applied Crytography.

[3] R. Rivest, AES: the secret Algorithm.

[4] https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/.

[5] https://www.slideshare.net/talhasaleem09/cryptography-discrete-mathematics.