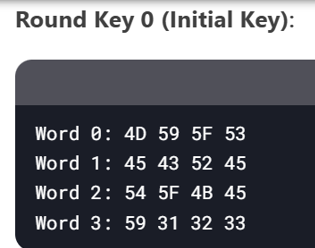
OOP COURSE PROJECT

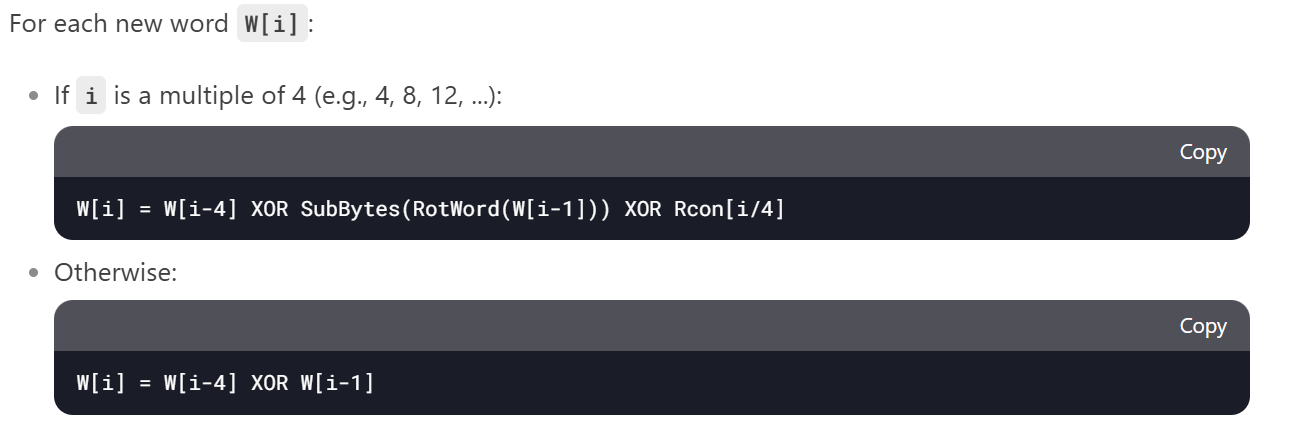
First let’s understand the problem, by studying the algorithms of each encryption algorithm, to see how they work.

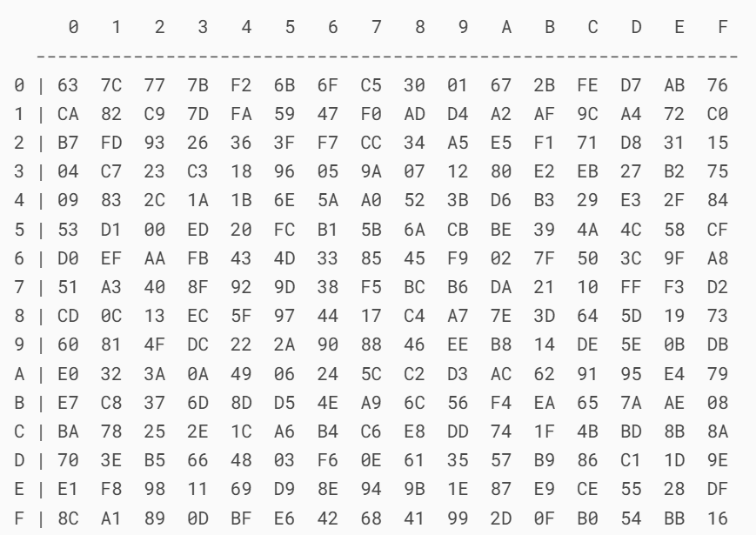
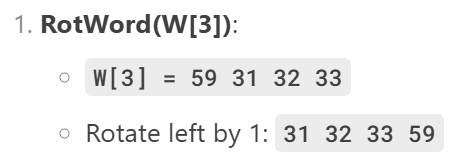
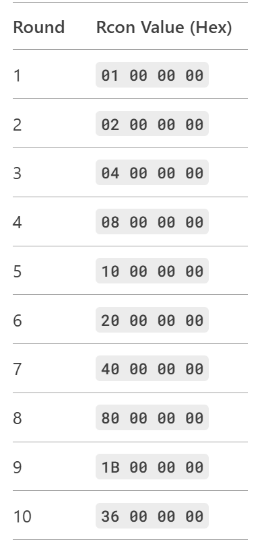
Note: Each encryption/decryption algorithm can only be implemented on a specific amount of characters. In order to work on large amount of texts, the........

##### AES (128 bit)

**MAKING OF ROUNDKEYS**

1. INPUT A 16 BYTE KEY FROM THE USER AND CONVERT IT TO HEXADECIMAL. THIS WILL BE ROUNDKEY 0
2. 10 MORE ROUNDKEYS ARE MADE TO CONDUCT THE ENCRYPTION PROCESS, USING THE FORMULAS BELOW

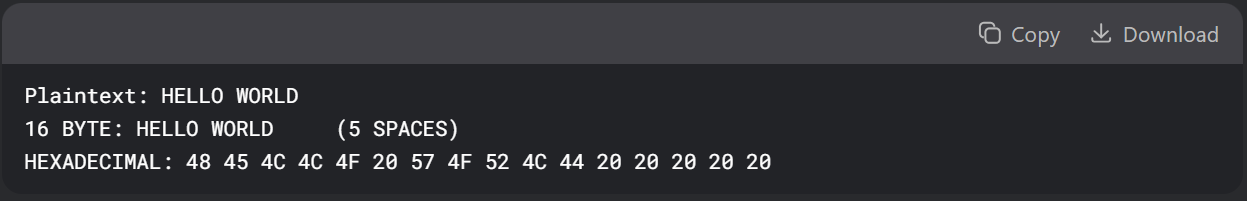


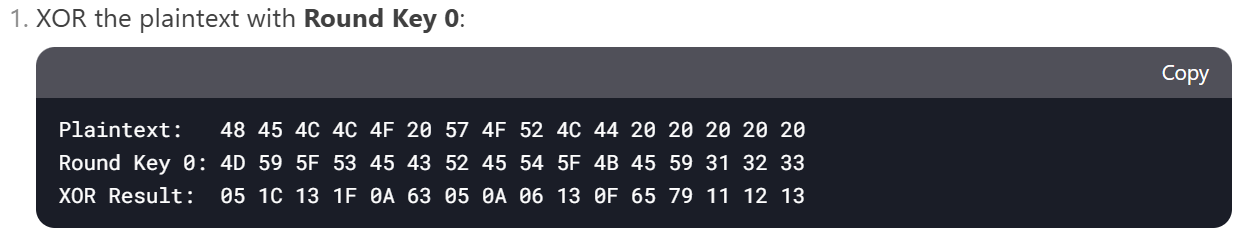


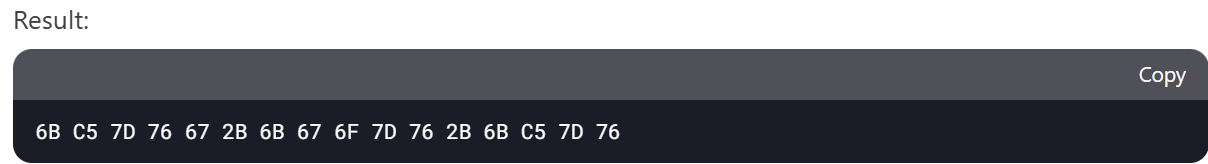
S BOX

**ENCRYPTION**

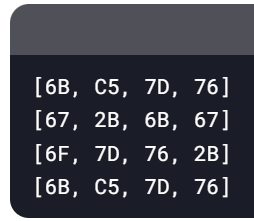
1. INPUT PLAIN TEXT FROM THE USER, MAKE IT 16 BYTES, AND CONVERT TO HEXADECIMAL



1.  ROUND 0
2. ROUND (1-9) (REPEAT 9 TIMES)

* Apply S Box on the result of previous round.

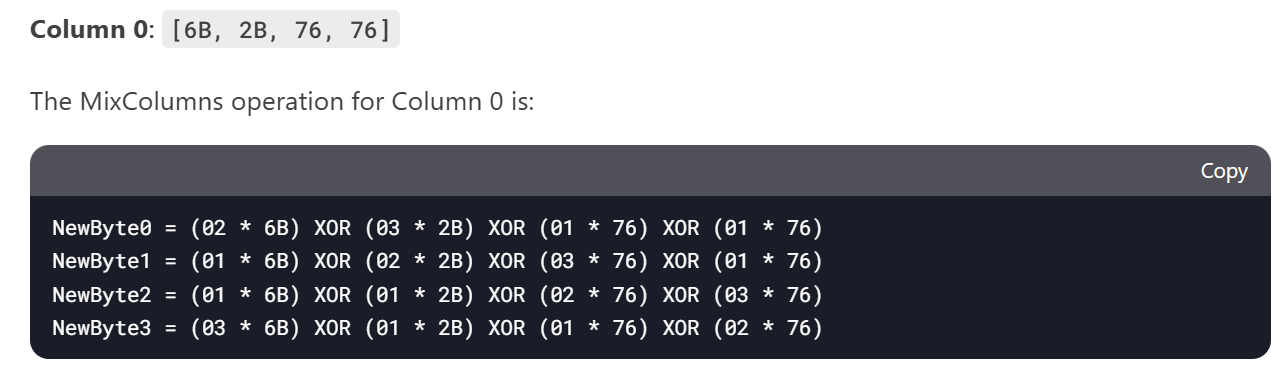
* A screenshot of a computer

  AI-generated content may be incorrect.Shift Rows



* **Row 0**: No shift.
* **Row 1**: Shift left by 1 byte.
* **Row 2**: Shift left by 2 bytes.
* **Row 3**: Shift left by 3 bytes.
* Mix Columns:

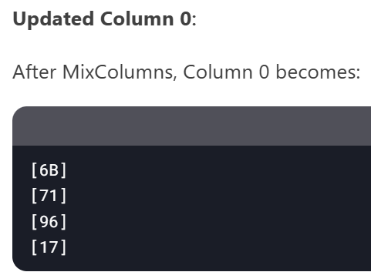
0 1 2 3



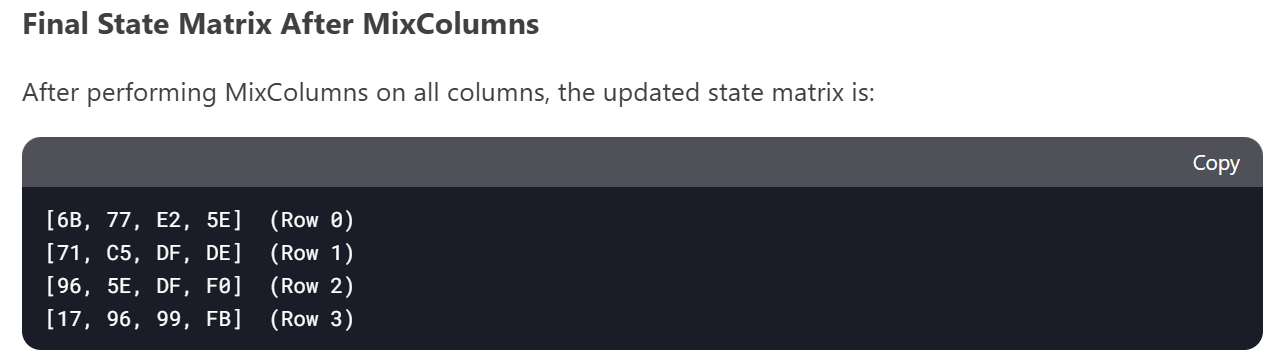
Yellow values differ subject to column (The rest remain same)

0 1 2 3

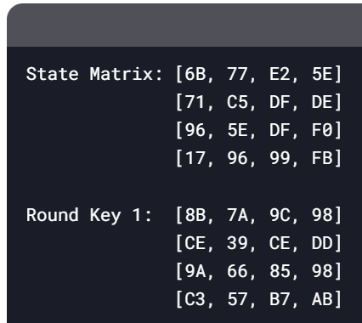


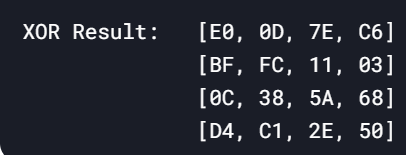


(Repeat for all columns)



* XOR WITH RESPECTIVE ROUNDKEY (IN THIS CASE, ROUNDKEY 1)





XOR

1. ROUND 10

* Repeat step 3 (EXCEPT THE MIXCOLUM PART)
* THE RESULT OF ROUND 10 WILL BE THE FINAL ENCRYPTED TEXT

**DECRYPTION**

1. STARTS WITH ROUNDKEY 10 AND ENDS WITH ROUNDKEY 1
2. A black rectangular object with white letters

   AI-generated content may be incorrect.ROUND 10
3. ROUND 9-1 (REPEAT 9 TIMES)

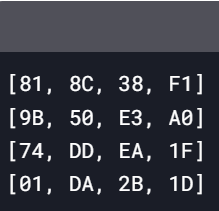
* A black and white screen with white text

  AI-generated content may be incorrect.Inverse Shift Rows

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

* Apply Inverse S Box

A table of numbers and letters

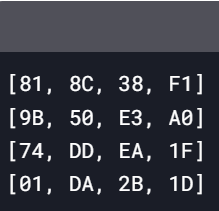
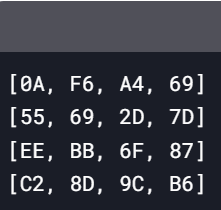
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* XOR with respective Round Key

A black and white screen with white text

AI-generated content may be incorrect.

**Round Key 9 (Example)**



XOR



* Inverse Mix Column



0 1 2 3

Column 0: [0A, 55, EE, C2]

Yellow values differ subject to column (The rest remain same)

A black and white screen with white text

AI-generated content may be incorrect.The Inverse Mix Column operation for Column 0 is

0 1 2 3

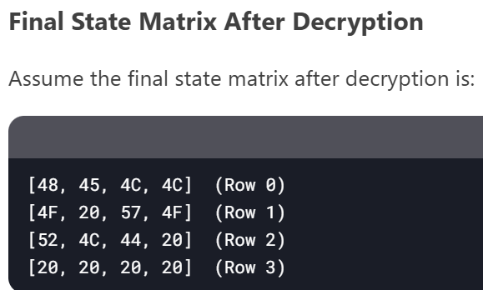


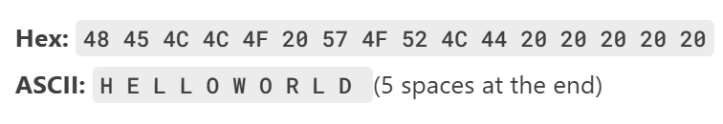
A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
 4. ROUND 0

* Repeat Step 4 (EXCEPT INVERSE MIX COLUMN PART)

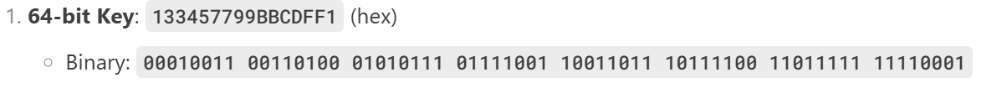
  
  
  
  
  
  
  
  
  
 5. CONVERT HEXADECIMAL TO ASCII TO ACHIEVE FINAL DECRYPTED TEXT

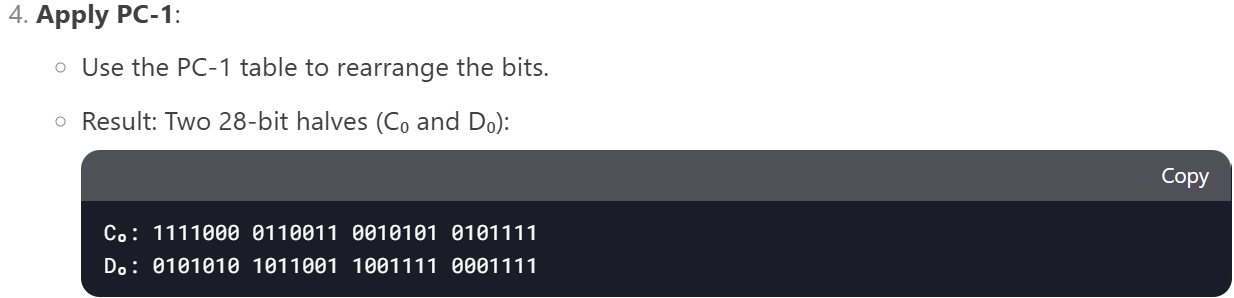


##### DES (56 bit)

**MAKING OF SUBKEYS**

1. Make a 16 digit hexa key (convert to 64 bit binary key)

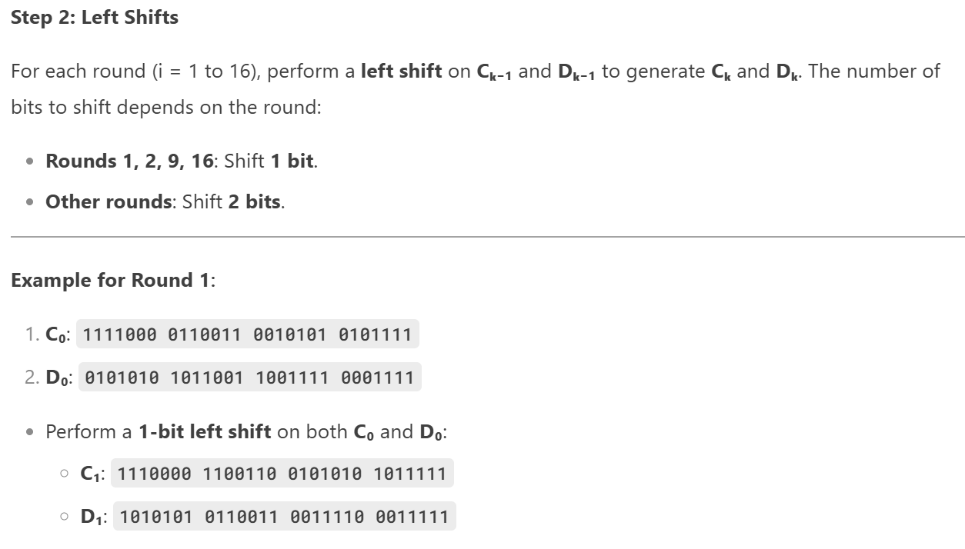


1. A screenshot of a computer

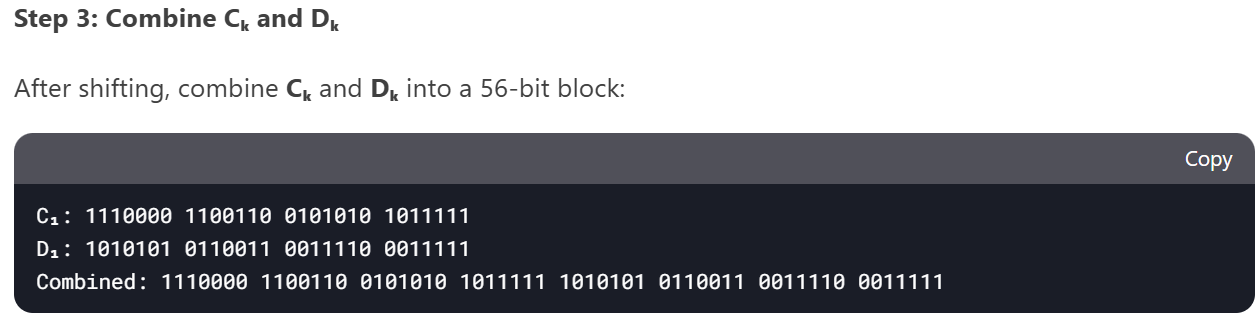
   AI-generated content may be incorrect.Rearrange bits according to PC-1 table, and split in half (This step turns the 64 bit key to a 56 bit key)  
     
    PC-1 TABLE (ORDER OF BITS)

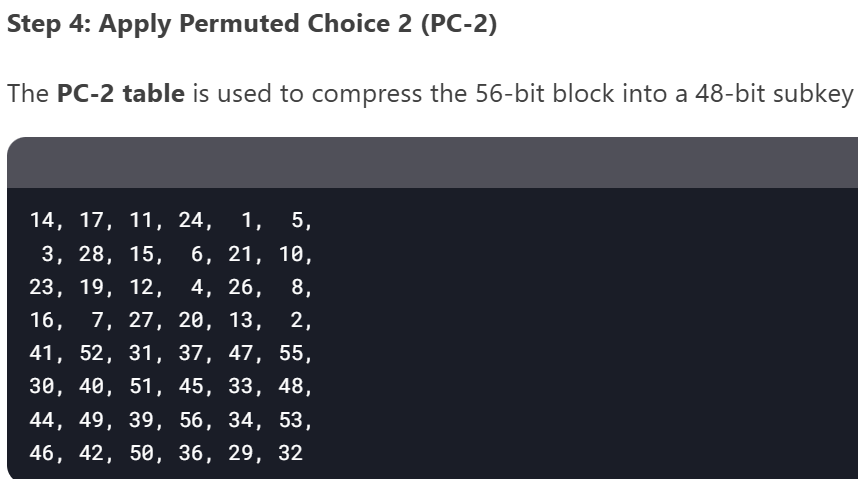
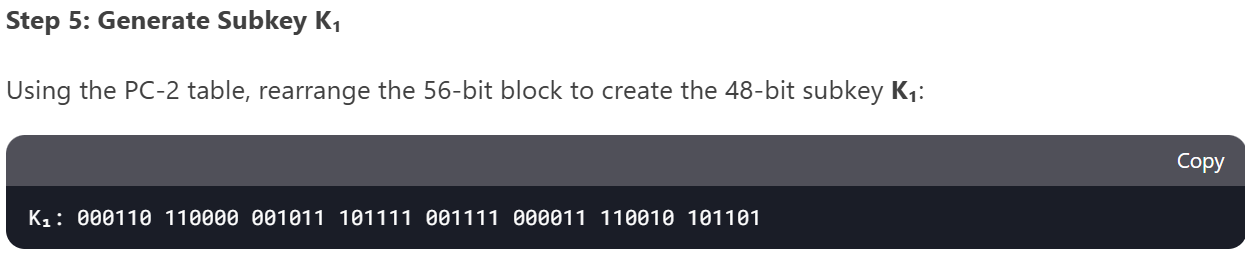
Actually 56

1. Left Shift and PC-2 (repeat 16 times for 16 rounds)

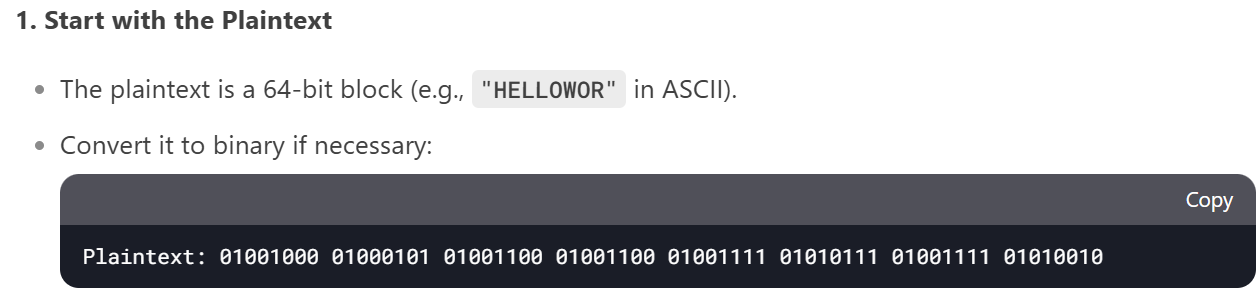
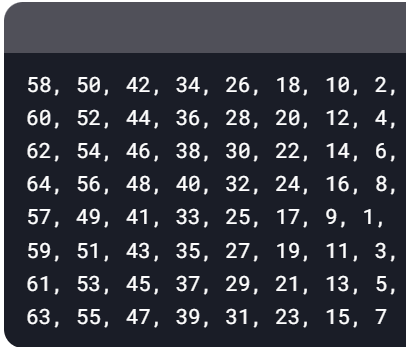
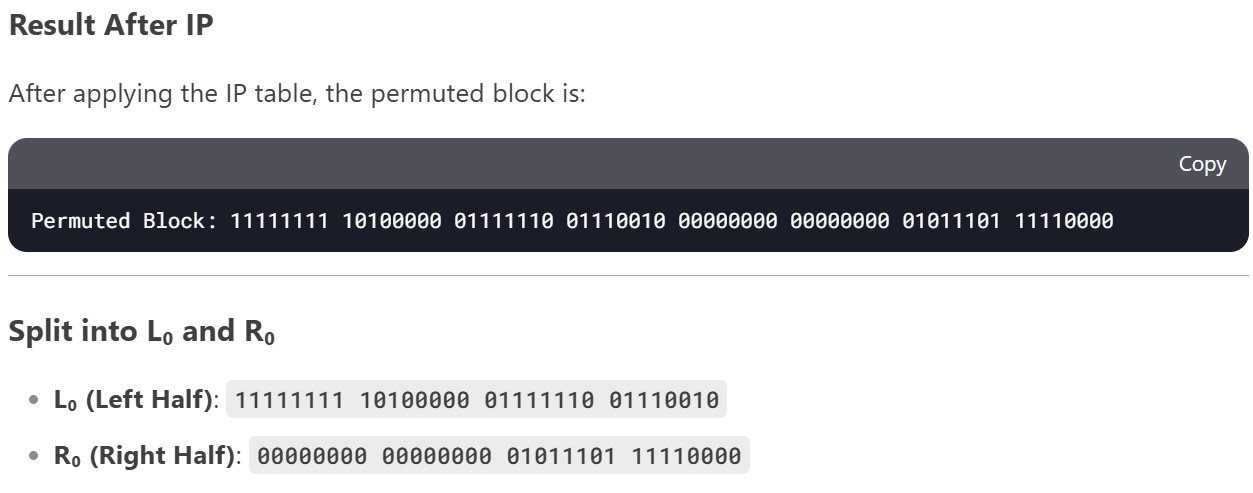
* Perform either 1 or 2 left shifts on the previous 28-bit halves (Ck-1, Dk-1) according to squared data (So for left shift for Round 2, left shift will be applied on C1, D1)



* Combine Ck and Dk
* Rearrange According to PC-2 Table (This step shortens the 56 bit key to 48 bit subkey)

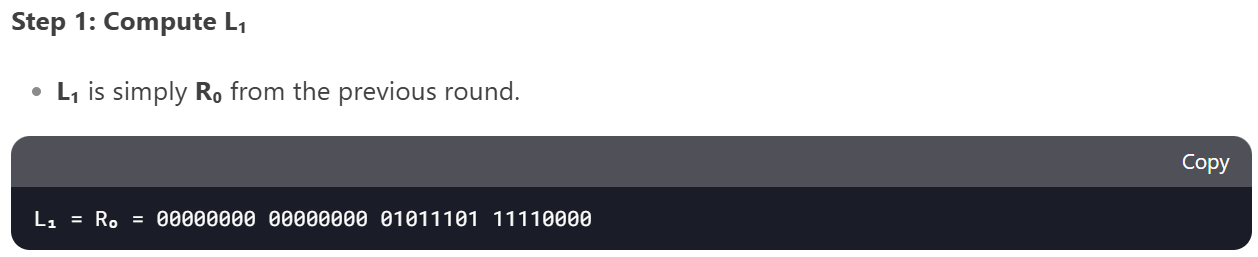
  
 PC-2 TABLE (ORDER OF BITS)

**ENCRYPTION**

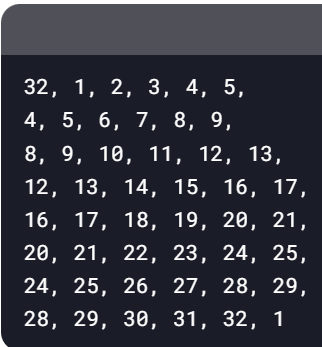
1. Convert Chosen 8 character Text to Binary
2. Rearrange bits according to IP table, and split in half

IP TABLE

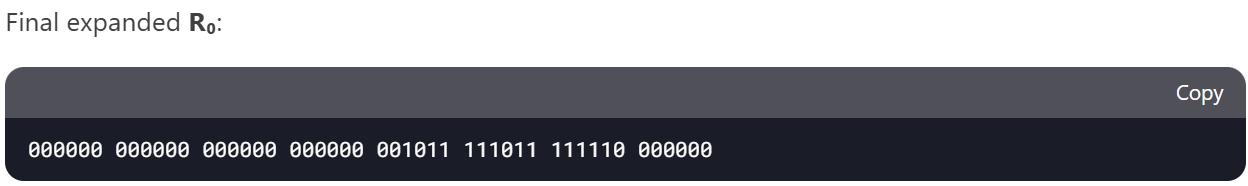
# STEP 3 AND 4 TO BE REPEATED 16 TIMES TILL ROUND 16

1. Find L1 (ROUND 1)

1. Find R1 (ROUND 1)

* Apply E Table

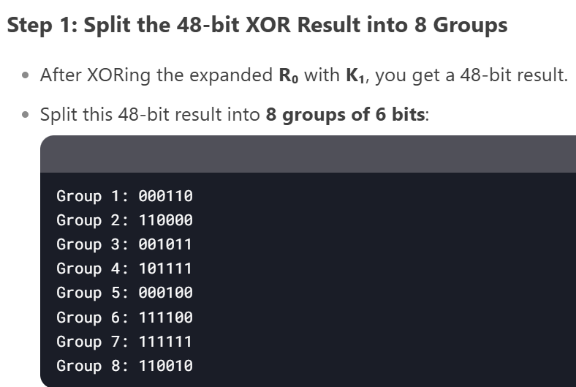
E TABLE (Expands R0)

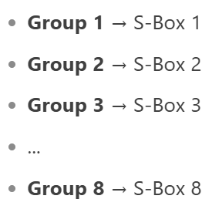


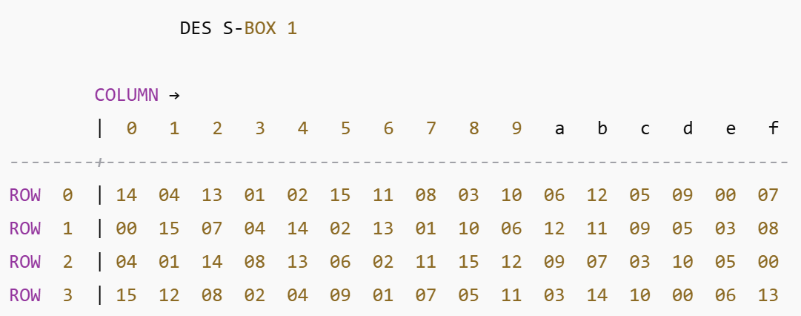
* A black rectangular object with white numbers

  AI-generated content may be incorrect.XOR with respective Sub-Key
* Apply appropriate S boxes

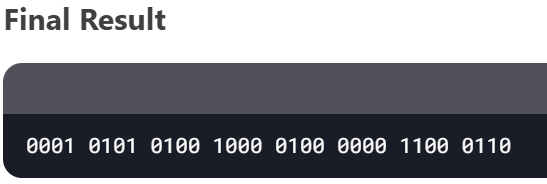
A white background with black text

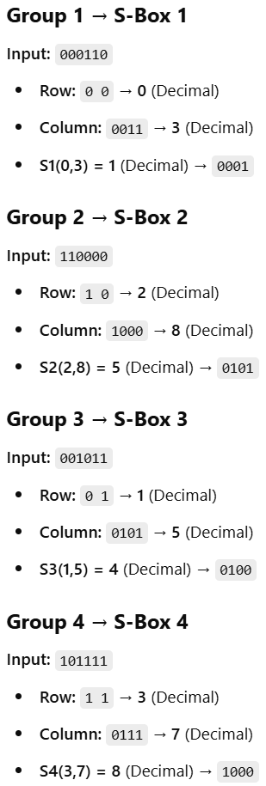
AI-generated content may be incorrect.

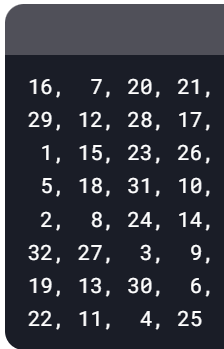




Only S box 1 included for clarity

  
  
  
  
  
  
  
  
  
  
  
A screenshot of a computer

AI-generated content may be incorrect.

* Apply P Table

P TABLE

A close-up of a credit card

AI-generated content may be incorrect. The permutated output is:

* XOR With L0 to achieve R1

A black and white screen with white text

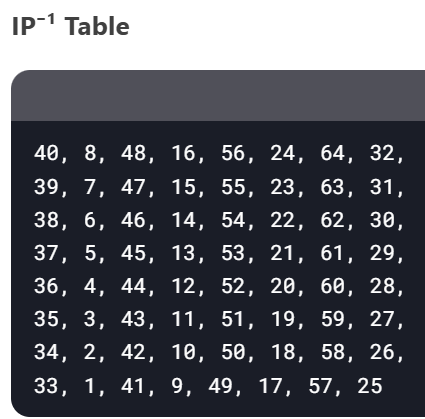
AI-generated content may be incorrect.

1. A black rectangular object with a white background

   AI-generated content may be incorrect.Combine L16 and R16

A close-up of a credit card

AI-generated content may be incorrect.

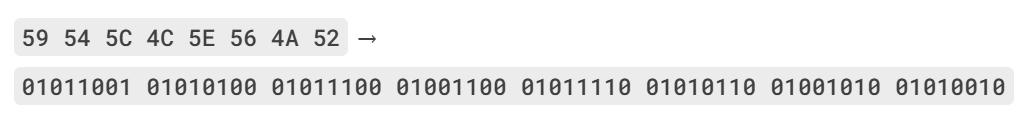
1. Apply IP⁻¹ Table

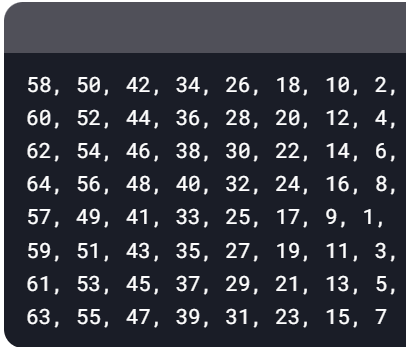


1. Convert to Hexadecimal to achieve final encrypted text

**DECRYPTION**

1. Convert cipher text to Binary



1. Rearrange bits according to IP table, and split in half

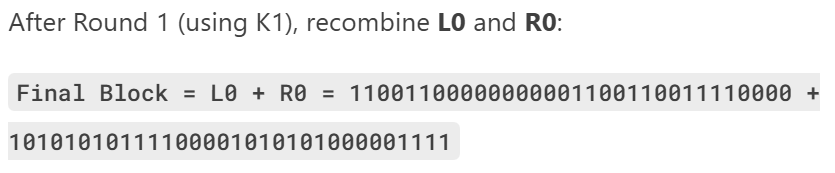
IP TABLE

A close-up of numbers

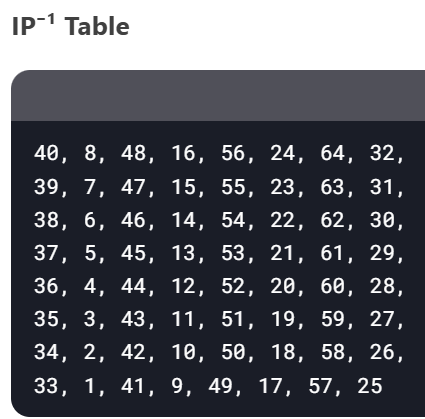
AI-generated content may be incorrect.

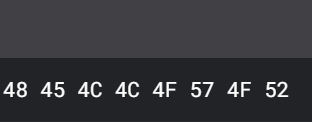
1. A screenshot of a computer

   AI-generated content may be incorrect.Compute Lk and Rk till L0 and R0 are achieved (Repeated 16 times)  
     
    ROUND 16
2. Combine L0 and R0

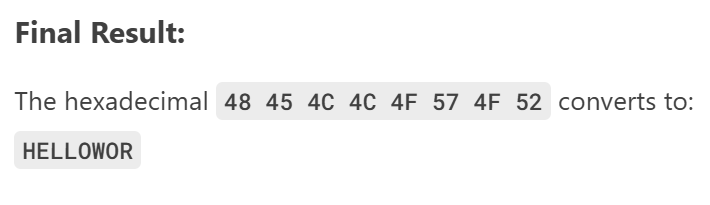


1. Apply IP-1 Table to achieve decrypted text in hexadecimal



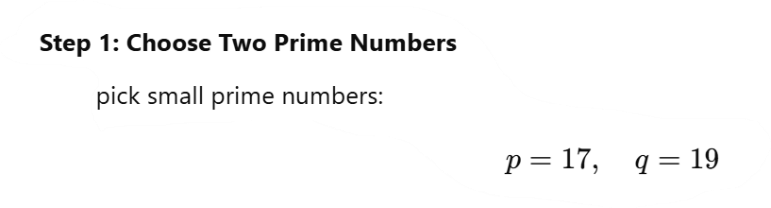


1. Convert the hexadecimal to ASCII to achieve Final Decrypted Text



##### RSA (9 bit) :/

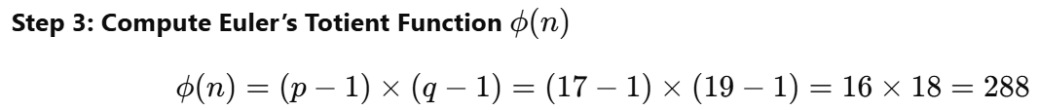
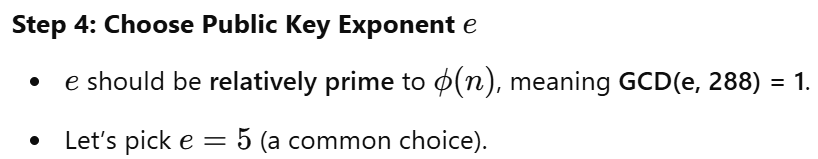
**MAKING OF PUBLIC AND PRIVATE KEYS**

1. Select two prime numbers, p and q

1. Multiply p and q

A white and black background with black text

AI-generated content may be incorrect.

1. Multiply (p-1) with (q-1)
2. Choose e (Public key), where e and ϕ(n) must not have a common factor (other than 1)  
      
    Greatest Common Devisor
3. Calculate d (Private key), by performing Modular Inverse

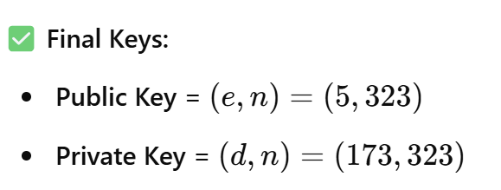
A close-up of a sign

AI-generated content may be incorrect.



A black text on a white background

AI-generated content may be incorrect.

1. Final Keys

**ENCRYPTION**

1. A screenshot of a computer

   AI-generated content may be incorrect.Convert text to ASCII
2. Encrypt each letters ASCII value (must be less than n, else make smaller blocks so that it is less than n), using formula and public key

A white paper with black text and black text

AI-generated content may be incorrect.

A number and numbers on a white background

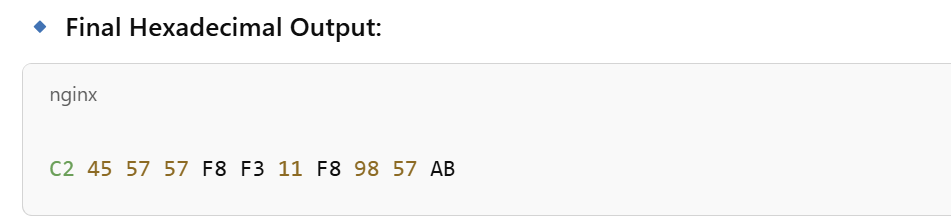
AI-generated content may be incorrect.

And rest of the letters...

1. Encrypted Text in Decimal



1. Convert to Hexadecimal for final Encrypted Text



**DECRYPTION**

1. Reclaim decimal RSA encrypted text



1. Decrypt each number using decryption formula and private key

A white background with black text

AI-generated content may be incorrect.

A white background with black text

AI-generated content may be incorrect.

And rest of the blocks...

1. Final Decrypted data

A close-up of a sign

AI-generated content may be incorrect.