PROBLEM STATEMENT : Data Encryption System: Rahul wants to send encoded messages to his friend Ram. Develop an algorithm to encode all the digits, special characters, lower and upper case alphabets.

Documentation:
Security is top of mind for anyone in IT these days.Encryption is one aspect of security technology that every computer user should understand.

What is Encryption

Encryption is a way for data—messages or files—to be made unreadable, ensuring that only an authorized person can access that data.
Encryption uses complex algorithms to scramble data and decrypts the same data using a key provided by the message sender.
Encryption ensures that information stays private and confidential, whether it's being stored or in transit. Any unauthorized access to the data will only see a chaotic array of bytes.

Common Encryption Algorithms

DES (data encryption standard)
Introduced in 1976, DES (data encryption standard) is one of the oldest symmetric encryption methods.
DES uses a 56-bit encryption key
DES converts 64-bit blocks of plaintext data into ciphertext by dividing the block into two separate 32-bit blocks and applying the encryption process to each independently.
This involves 16 rounds of various processes — such as expansion, permutation, substitution, or an XOR operation with a round key —that the data will go through as it’s encrypted.
64-bit blocks of encrypted text is produced as the output.

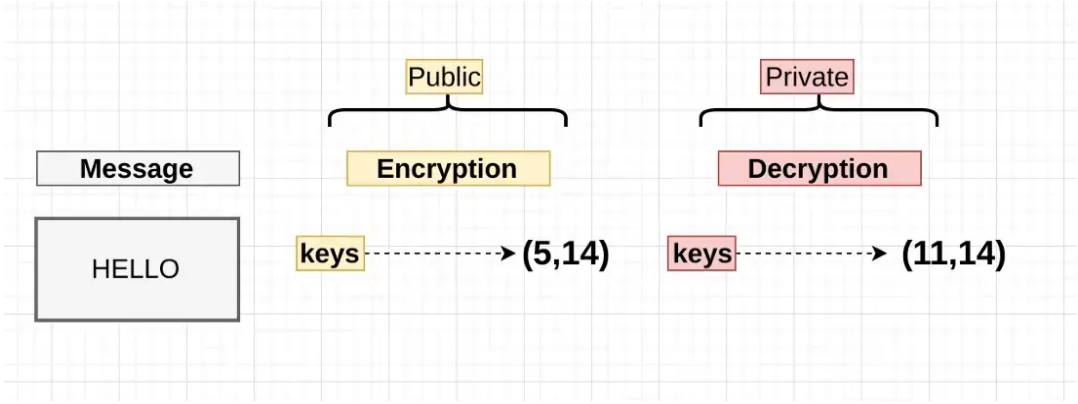
3DES
Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits

AES Advanced Encryption Standard

It is highly efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy-duty encryption purposes.
AES is largely considered impervious to all attacks, except for brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher.

RSA Security

RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet.
Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys.
The bits of encryption is based on the how large the prime numbers considered.
The AES key lengths – 128, 192, and **256 bits** – may change accordingly.



RSA (Rivest- Shamir - Adleman) Algo

Encryption :
C(cipher text) = Ppow(e)mod n

Decryption :
P= Cpow(d) mod n

e=public key { e, n }
d=private key {d , n}

Key Generation
1) Consider 2 large prime numbers
2) Calculate n= p*q

3) pi(n) = (p-1)(q-1) Eulers Totient Function

4) Choose a small number e, co- prime to pi(n)
   with GCD(pi(n),e)=1 and 1<e<pi(n)

5) Find d , such that d*e mod pi(n)=1

The block size is simply the amount of bits or bytes that can be transformed by the block cipher. It is the input and output size of the keyed block cipher.

	Key Type	Key Size	Block Size
AES	Symmetric	128 bits	256 bits
DES	Symmetric	56 bits	64 bits
RSA	Asymmetric	Var((256 bits)	256 bits

RSA has highest key size of 256bits and block size of 256 meaning it is highly encrypted and impossible to crack.
I used RSA algorithm since it is of Asymmetric type i.e it has both private and public key which is most suitable for encrypted message transfer between sender and receiver.