RAISONI GROUP
— a vision beyond —

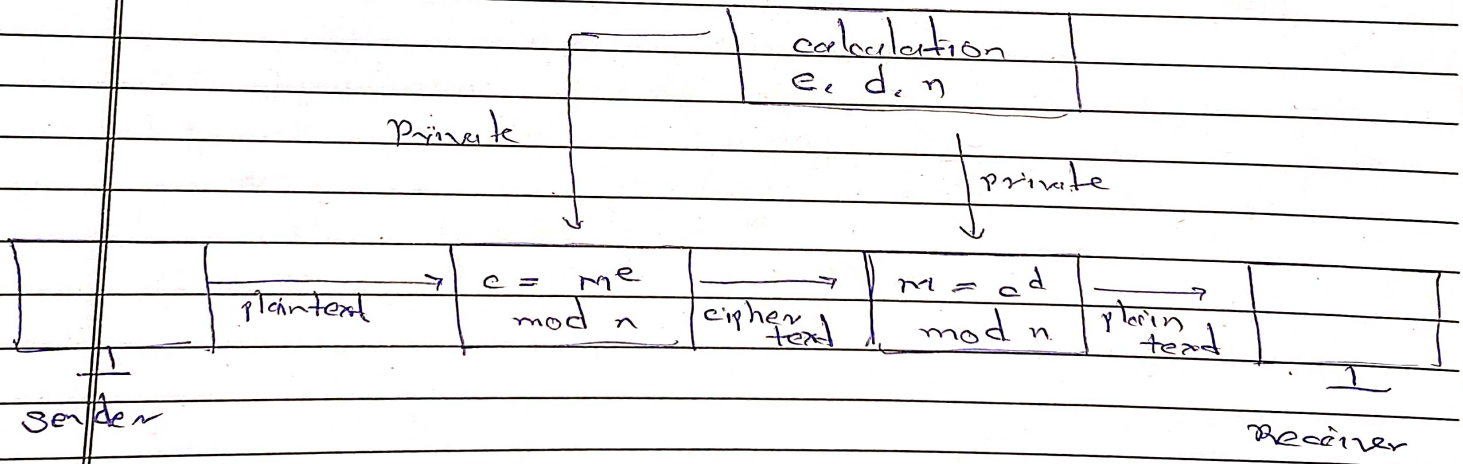
Assignment no. 07

* Aim:

write a program to develop secure system by applying RSA cryptography Algo.

* Theory:

RSA encryption algorithm is a type of public key encryption algorithm. The public key is used for encryption and the private key is used for decryption. RSA is the most common public key algorithm.



RSA Algorithm:

- Select two large prime numbers, p and q.
- Multiply these numbers to find $n = p \times q$, where n is called modulus for encryption and decryption.

- choose number e less than n, such that n is relatively prime to $(p-1) \times (q-1)$. It means that e and $(p-1) \times (q-1)$ have no common factor except 1.
- If $n = p \times q$, then the public key is $\langle e, n \rangle$. A plaintext message m is encrypted using public key $\langle e, n \rangle$. To find ciphertext from the plain text:

$$c = m^e \bmod n$$

m must be less than n.

- To determine the private key, we use the following formula to calculate the d such that: $De \bmod \{(p-1) \times (q-1)\} = 1$ OR

$De \bmod \varphi(n) = 1$

- The private key is $\langle d, n \rangle$. A cipher text message c is decrypted using private key $\langle d, n \rangle$. To calculate plain text m from cipher text c following formula is used to get plain text m.

$$m = c^d \bmod n.$$

★ conclusion:

Hence, we successfully learned and able to implement the public and private key using RSA and to encrypt and decrypt the message.

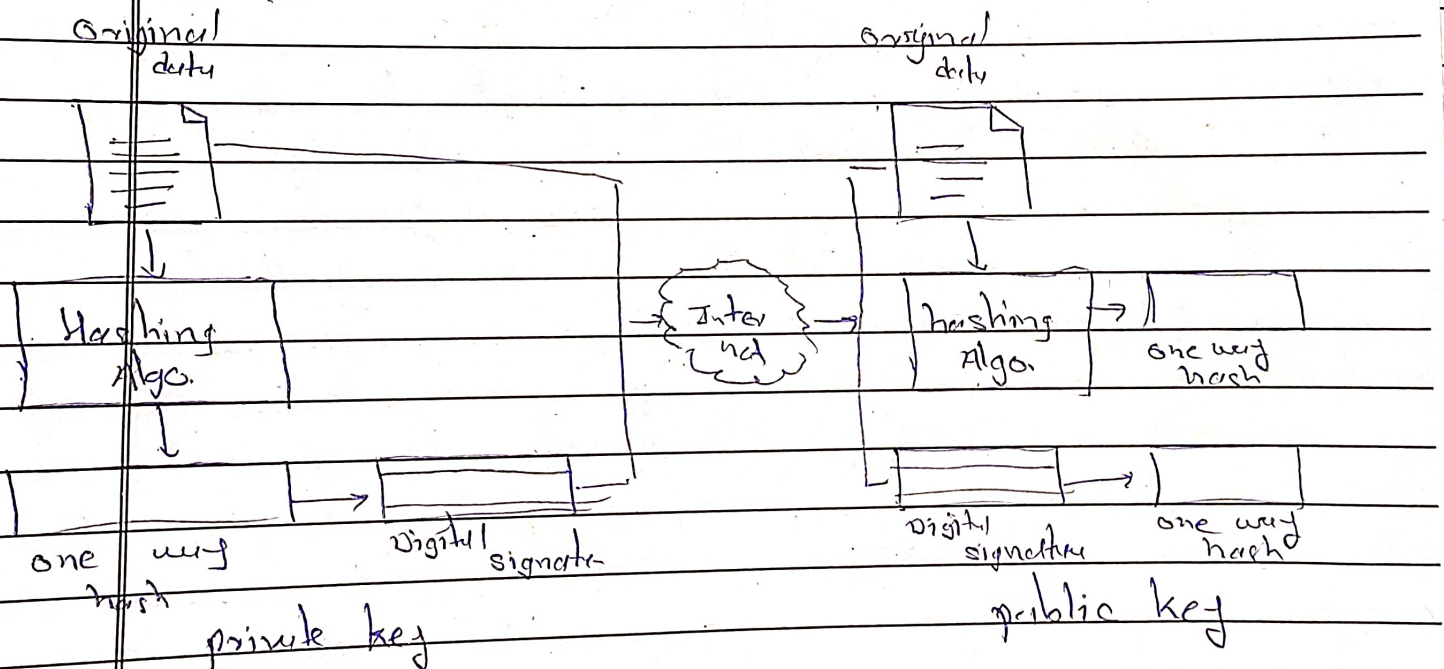
RAISONI GROUP
— a vision beyond —

Assignment No 08

★ Aim: Implement Digital Signature algorithm in Java.

★ Theory:

A digital signature is a mathematical technique used to validate the authenticity and integrity of message, software or digital signature.



Authentication: Authentication is any process by which a system verifies the identity of user who wishes to access it.

Non repudiation: Non repudiation means to ensure that transferred message has been sent & received by parties claiming to have sent &

RAISONI GROUP
—a vision beyond—

Signing Algo:

To create digital signature, signing algorithm like email program create a one way hash of the electronic data which is to be signed. The signing algo then encrypts the hash value using the private key.

This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to verifier.

Benefits of digital signature:

- Legal documents and contracts: Digital signature are legally binding.
- Sales contract: Digital signing of contracts and sales authenticates the identity of the seller and buyer.
- Financial Documents: Financial department digitally sign invoices so customers can trust that the payment request is from the right seller.

★ conclusion:

Hence, we successfully learn about the digital signature and successfully implement the signature using signing algorithm.

RAISONI GROUP
—a vision beyond—

Assignment No. 09

★ Aim: Write a program to implement Elliptic curve based arithmetic.

★ Theory:

Elliptic curve cryptography (ECC) is widely used cryptographic technique that relies on the algebraic structure of elliptic curves to provide secure communication and data protection.

ECC is particularly popular for its strong security and efficiency, making it suitable for various applications, such as secure key exchange and digital signatures.

Some key points

- Elliptic Curve:

A Elliptic curve is mathematical curve defined by an equation of the form: $y^2 = x^3 + ax + b$. The curve is typically defined by over a finite field, which means that all the arithmetic operations are performed modulo a prime number.

- Points on the curve:

The points on an elliptic curve form a group. The group operation, is typically represented as + and is defined geometrically, similar to addition in the cartesian plane.

RAISONI GROUP
— a vision beyond —

- Scalar Multiplication:
  Scalar Multiplication is the core operation in ECC. It involves multiplying a point on the curve by an integer (scalar) which results in another point on curve.
- Discrete logarithm:
  The security of ECC relies on the difficulty of solving the discrete logarithm problem on the elliptic curve.
- key Exchange:
  ECC is commonly used for key exchange protocols like Elliptic curve diffie-Hellman.
- Digital Signature:
  ECC can also be used for digital signatures using schema like Elliptic curve digital Signature Algorithm (ECDSA).
- Efficiency:
  One of the key advantages of ECC is its efficiency. ECC operation can be performed with shorter key algorithm compared to other cryptographic system like RSA while still providing strong security.

★ conclusion:
Hence, we Successfully learn about the Elliptic Curve and Successfully implemented a program for Elliptic curve based Arithmetic.

RAISONI GROUP
—a vision beyond—

Assignment NO. 10

★ Aim: Write a program to implement Diffie Hellman key Exchange

★ Theory:

Diffie Hellman key exchange is a method of digital encryption that securly exchanges cryptographics key between two parties over a public channel without their conversation being transmitted over internet.

Diffie Hellman key exchange raises numbers to selected power to produce decryption key. The components of key are never directly transmitted, making the task of would be code breaker mathematically.

Diffie Hellman Algorithm:

The Diffie-Hellman algo. is being used to establish a shared key that can be used for secret communication while exchanging data over public network using the elliptic curve to generate points and get the secret key using the parameters

RAISONI GROUP
—a vision beyond—

step by step explanation :

Alice	Bob
public keys available = p, G	public key avail. = p, G
private key selected = a	private key selected = b
key generated = $x = G^a \bmod p$	key generated = $y = G^b \bmod p$
Exchange of generated key takes place	
key received = y	key recived = x
Generated secret $k_a = y^a \bmod p$	Generated secret = $k_b = x^b \bmod p$
Algebraically it can be shown that $k_a = k_b$	
users now have symmetric key to encrypt	

p and G are both publicly available numbers. users pick private values a and b and they generate a key and exchange it publicly

conclusion :

Hence, we successfully learn about the Diffie Hellman key exchange algo and successfully implemented using Java