Tutorial #5

Security in Computing COSC2356/2357

1. Discuss some of the scenarios where privacy preservation of sensitive data is required.

(Discuss with your peers and do it yourself)

RSA Homomorphism (Multiplying two numbers secretly)

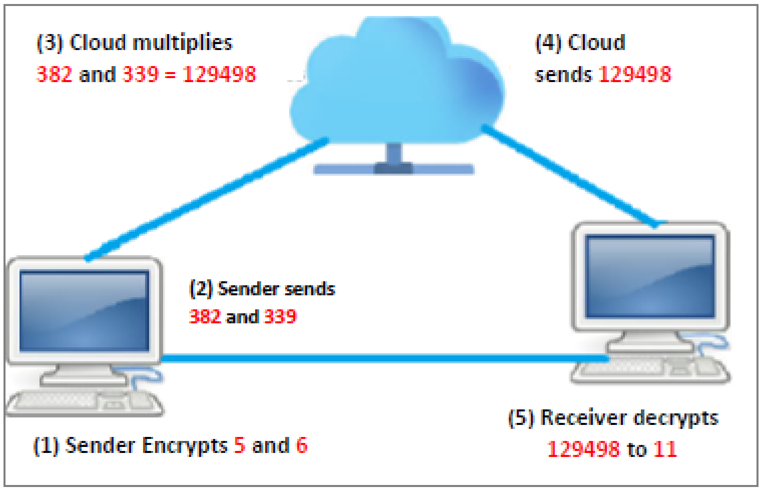
2. Alice, the sender, has two messages $m_1 = 5$ and $m_2 = 8$. She wants to **multiply** the messages (5*8=40) securely using Homomorphic properties of **RSA** cryptosystem and send to Bob, the receiver. The Cloud Server, who has computation power, will perform the homomorphic multiplication and send the encrypted results to Bob. Bob should find 40 after performing decryption. Bob chooses two prime numbers: $p = 17, q = 23$ and public parameter $e = 7$. Show the encryption, homomorphic multiplication and decryption process.

ElGamal Homomorphism (Multplying two numbers secretly)

3. Alice the sender has two messages $m_1 = 3$ and $m_2 = 4$. She wants to **multiply** the messages (3*4=12) securely using Homomorphic properties of **ElGamal** cryptosystem and send to Bob, the receiver. The Cloud Server, who has computation power, will perform the homomorphic multiplication and send the encrypted results to Bob. Bob should find 12 after performing decryption. Bob chooses public parameters $p = 2879, g = 2585$ and private key $x = 47$. Alice chooses two random numbers $r_1 = 154$ and $r_2 = 96$ encrypt the two messages. Show the encryption, homomorphic multiplication and decryption process.

Paillier Homomorphism (Adding two numbers secretly)

4. Alice has two messages $m_1 = 5$ and $m_2 = 6$. She wants to add the messages (5+6=11) securely using Homomorphic properties of Paillier. The Cloud Server, who has computation power, will perform the homomorphic addition and send the encrypted results to Bob. Bob Should find 11 after performing decryption. Bob chooses $p = 5, q = 7$ and an integer $g = 164.$ Alice chooses two random numbers $r_1 = 17$ and $r_2 = 19$ to encrypt the two messages. Show the encryption, homomorphic additions and decryption process.


(3) Cloud multiplies
382 and 339 = 129498
(4) Cloud
sends 129498
(2) Sender sends
382 and 339
(1) Sender Encrypts 5 and 6
(5) Receiver decrypts
129498 to 11