Tutorial #5

<u>Security in Computing COSC2356/2357</u>

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

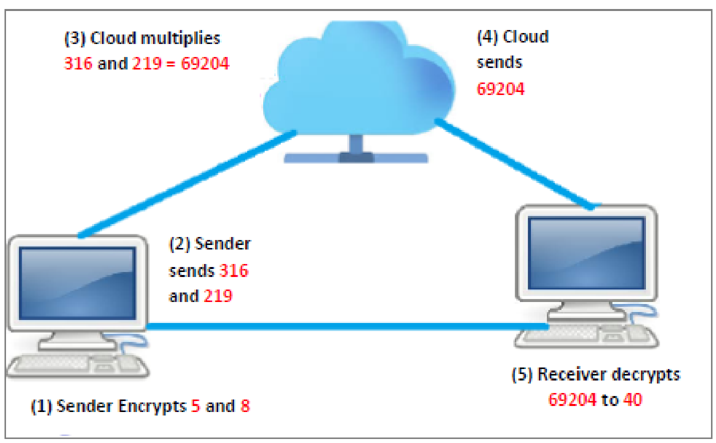
Answer:

Few of the scenarios are listed below where privacy preservation of sensitive data is required. Please go through from the **slide number 24** to **52** to get some idea about privacy-preservation techniques.

a) Privacy-preserving online voting
b) Privacy-preserving revenue calculation
c) Privacy-preserving Item Recommendation
d) Privacy-preserving Data analysis
e) Privacy-preserving medical data mining
f) Privacy-preserving Cloud-based Billing Model for Smart Meters
g) Privacy-preserving Biometric Matching

RSA Homomorphism (Multplying 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.



Answer:

Bob chooses two prime numbers: $p = 17, q = 23$

Bob calculates $n = 17 * 23 = 391$

Bob calculates: $\varphi(n) = (p-1) \times (q-1) = (17-1) \times (23-1) = 352$

Bob chooses: $e = 7$

Bob calculates: $d = e^1 \, mod \, \varphi(n) = 7^{-1} \, mod \, 352$ = 151

Bob's public key: ***(n,e) = (391, 7)***

Bob sends public key ***(n,e)*** to Alice.

<u>@Sender:</u>

Alice calculates two ciphertexts for two messages, M_1 and M_2 , as follows:

$$C_1 = M_1^e \, mod \, n = 5^7 \, mod \, 391 = 316$$
$$C_2 = M_2^e \, mod \, n = 8^7 \, mod \, 391 = 219$$

Alice sends (C_1, C_2) to the cloud for multiplication.

<u>@Cloud:</u>

The cloud calculates: $C = C_1 . C_2 = 316 . 219 = 69204$

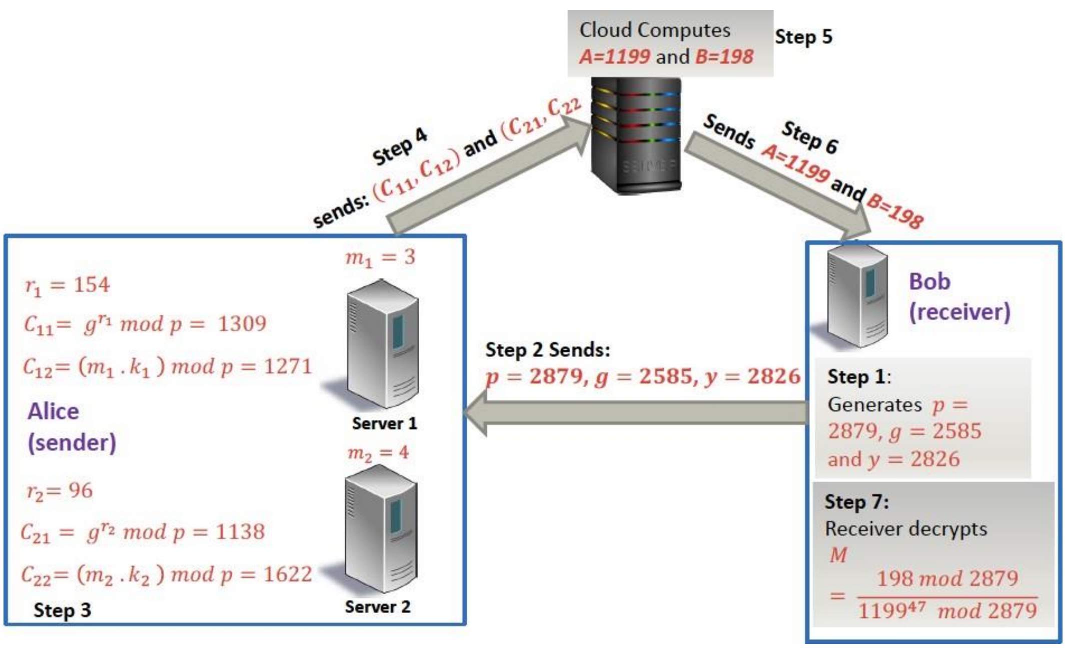
The cloud sends ***C*** to Bob.

@Receiver:

Bob decrypts the message as follows:
$M = C^d \; mod \; n = 69204^{151} \; mod \; 391 = 40$
The result of the multiplication is M = 40

ElGamal Homomorphism (Multiplying 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.



Answer:

Receiver generates: $p = 2879, g = 2585$

Secret key $x = 47$

Receiver computes: $y = g^x \; mod \; p = \; 2585^{47} \; mod \; 2879 = 2826$

Receiver sends: $p = 2879, g = 2585$ and $y = 2826$ to sender

Sender chooses two random numbers $r_1 = 154 \; and \; r_2 = 96$

Sender calculates: $k_1 = \; y^{r_1} \; mod \; p = \; 2826^{154} \; mod \; 2879 = 2343$

and $k_2 = \; y^{r_2} \; mod \; p = \; 2826^{96} \; mod \; 2879 = 1845$

Sender calculates C_1 and C_2two messages $m_1 = 3$ and $m_2 = 4$ as follows:

$$C_{11} = \; g^{r_1} \; mod \; p = \; 2585^{154} \; mod \; 2879 = 1309$$

$$C_{12} = (m_1 \,.\, k_1 \,) \; mod \; p = (3 \,.\, 2343) \; mod \; 2879 = 1271$$

$$C_{21} = \; g^{r_2} \; mod \; p = \; 2585^{96} \; mod \; 2879 = 1138$$

$$C_{22} = (m_2 \,.\, k_2 \,) \; mod \; p = (4 \,.\, 1845) \; mod \; 2879 = 1622$$

Sender sends: (C_{11}, C_{12}) and (C_{21}, C_{22}) to cloud server.

Cloud server computes ***A*** and ***B*** as follows:

$$A = (C_{11}.\, C_{21}) \; mod \; p = (1309 \,.\, 1138) \; mod \; 2879 = 1199$$

$$B = (C_{12}.\, C_{22}) \; mod \; p = (1271 \,.\, 1622) \; mod \; 2879 = 198$$

Cloud server sends ***A*** and ***B*** to receiver.

Receiver computes the result ***M = m₁ * m₂*** as follows:

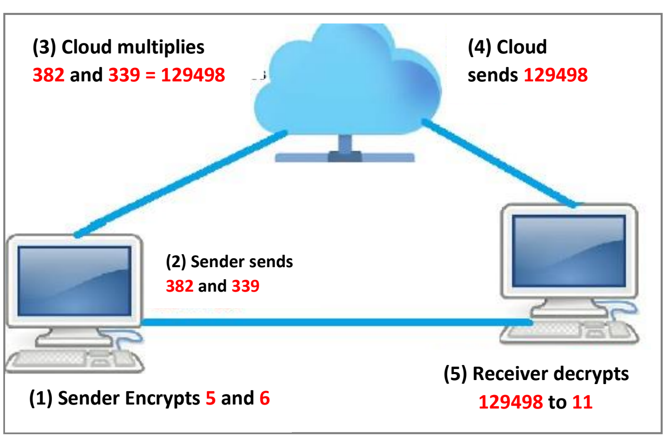
$$M = \frac{B \; mod \; p}{A^x \;\; mod \; p} = \frac{198 \; mod \; 2879}{1199^{47} \;\; mod \; 2879} = \frac{198 \; mod \; 2879}{1456 \;\; mod \; 2879}$$

$$= \big((198 \; mod \; 2879).\, (1456^{-1} \; mod \; 2879)\big) \; mod \; 2879 = (198 \,.\, 698) \; mod \; 2879 = \mathbf{12}$$

The final result is: ***M = 12.***

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.



Answer:

Bob chooses : $p = 5$ and $q = 7$ and generates $n = pq = 5 \times 7 = 35$

Bob selects an integer $g = 164$

Bob sends public key $(n, g) = (35,164)$ to Alice and Cloud server.

Bob computes: $\lambda = lcm(p-1, q-1) = lcm(5-1, 7-1) = lcm(4, 6) = 12$

Bob computes: $k = L(g^{\lambda} \; mod \; n^2)$ using function $L(u) = (u-1)/n$

Let, $u = g^{\lambda} \; mod \; n^2 = 164^{12} \; mod \; 35^2 = 1121$

Therefore, $k = L(g^{\lambda} \; mod \; n^2) = L(u) = \frac{u-1}{n} = \frac{1121-1}{35} = 32$

Bob Computes: $\mu = k^{-1} \; mod \; n = 32^{-1} \; mod \; 35 = 23$

Bob stores private key: $(\lambda, \mu) = (12,23)$

Now, Alice has two messages $m_1 = 5$ and $m_2 = 6$. She wants to add the messages securely using Homomorphic properties of Paillier Cryptosystems.

Alice has public key $(n, g) = (35,164)$

Alice selects two random numbers: $r_1 = 17$ and $r_2 = 19$

Alice encrypts $m_1 = 5$ as follows to produce C_1

$C_1 = g^{m_1}.{r_1}^{n} \; mod \; n^2$ = $164^5.17^{35} \; mod \; 35^2$

$= ((164^5 \; mod \; 35^2).(17^{35} \; mod \; 35^2)) \; mod \; 35^2 = 474 \,.\, 68 \; mod \; 35^2 = 382$

Alice encrypts $m_2 = 6$ as follows to produce C_2

$C_2 = g^{m_2}.{r_2}^{n} \; mod \; n^2$ = $164^6.19^{35} \; mod \; 35^2$

$= ((164^6 \; mod \; 35^2).(19^{35} \; mod \; 35^2)) \; mod \; 35^2 = 561 \,.\, 374 \; mod \; 35^2 = 339$

Alice sends $(C_1, C_2) = (382,339)$ to the Cloud Server.

Cloud Server Computes: $C = C_1 \,.\, C_2 = 382 \,.\, 339 = 129498$

Cloud Server sends $C = 129498$ to Bob

Bob computes the addition of two numbers (M) from $C = 129498$ as follows:

$$M = L\left(C^{\lambda} \; mod \; n^2\right).\mu \; mod \; n$$

Let, $u = C^{\lambda} \; mod \; n^2 = 129498^{12} \; mod \; 35^2 = 71$

Therefore, $L\left(C^{\lambda} \; mod \; n^2\right) = L(u) = \frac{u-1}{n} = \frac{71-1}{35} = 2$

and $M = L\left(C^{\lambda} \; mod \; n^2\right).\mu \; mod \; n = 2 \,.\, 23 \; mod \; 35 = 46 \; mod \; 35 = 11$

Here, $M = 11$ is our answer which is equal to $5 + 6 = 11$