Quiz#3-Chap3-PPML-HomomorphicEncryptionAlgorithms

p22cs013@coed.svnit.ac.in Switch account

Draft saved

Your email will be recorded when you submit this form

Quiz#3-Chap3-PPML-HomomorphicEncryptionAlgorithms

Quiz#3-Chap3-PPML-HomomorphicEncryptionAlgorithms
Scheduled for 4:00 pm, 10th April 2023, Duration: Strictly 50 minutes.
1. The quiz must be attempted using your SVNIT email ID only. If attempted using any other email ID, it would NOT be considered. There will not be any exceptions to this. If you are not visible on the Meet link for the purpose, then also no marks would be graded.
2. Please attend the quiz that is assigned to you.
3. Total Questions: 30, Total Marks:60. There is NO negative marking.
4. Google classroom may not show the correct scores. Please do not assume that is your real score.
5. Any quiz **that is received 2 minutes after the deadline, shall NOT be graded and shall be considered as Not Attempted**. Therefore, DO NOT continue attempting after the deadline - in order to ensure that your quiz is submitted and received in the next two minutes. No excuses would be tolerated. **Thus, any delay in receiving the quiz on classroom beyond the time specified would render the submission invalid and yield zero marks.**

In El Gammal Homomorphic encryption algorithm if the public key chosen is pk = {ρ, α, β } = { 107 , 9 , 94 }, and the other parameters are as shown, and if the two pairs of ciphertexts to be aggregated are (26,101) and (15,31), then the output of the node aggregating the ciphertext is ___________.

2 points

ElGamal code for Exams

- Prime p = 107 and primitive root $\alpha = 2$
- Private key is chosen at random from {1..p-1} i.e. S_k= a
- $\beta = \alpha^a \bmod p = 2^{67} \bmod 107 = 94$
- Public Key is $\{p, \alpha, \beta\}$ = {107, 2, 94}

Encryption is as follows: If Public Key $p_k = \{p, \alpha, \beta\}$

$$C_1 = \alpha^r \bmod p$$
$$C_2 = m * \beta^r \bmod p$$

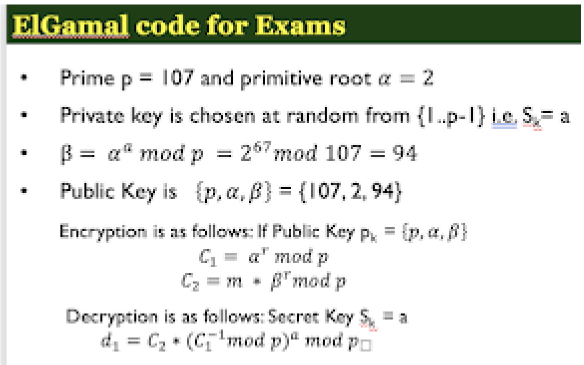
Decryption is as follows: Secret Key S_k = a

$$d_1 = C_2 * (C_1^{-1} \bmod p)^a \bmod p$$

- ( ) (15,19)
- ( ) none of these
- ( ) (10,17)
- (x) (69,28)

Clear selection

In El Gammal Homomorphic encryption algorithm if the public key chosen is pk = {ρ, α, β } = { 107 , 9 , 94 }, then ________ cryptosystem. 2 points



ElGamal code for Exams

- Prime p = 107 and primitive root $\alpha = 2$
- Private key is chosen at random from {1..p-1} i.e. S_k = a
- $\beta = \alpha^a \bmod p = 2^{67} \bmod 107 = 94$
- Public Key is $\{p, \alpha, \beta\}$ = {107, 2, 94}

Encryption is as follows: If Public Key $p_k = \{p, \alpha, \beta\}$

$$C_1 = \alpha^r \bmod p$$
$$C_2 = m * \beta^r \bmod p$$

Decryption is as follows: Secret Key S_k = a

$$d_1 = C_2 * (C_1^{-1} \bmod p)^a \bmod p$$

- [x] is not a valid
- [ ] is a valid

Clear selection

IF $C_1=Ek_{pu\beta}(X_1)$ and $C_2=Ek_{pu\beta}(X_2)$, then the crypto-system is multiplicatively homomorphic if ________ .[Here, C_1, C_2 are ciphertexts and X_1, X_2 are the associated plaintexts and $EK_{pu\beta}$ and EK_{pri} are the public and private keys.] 2 points

- [ ] $X_1+X_2=Ek_{pu\beta}(C_1)*Ek_{pu\beta}(C_2)$
- [ ] C_1+C2=Dk_{pri} [$Ek_{pu\beta}(X_1)+Ek_{pu\beta}(X_2)$]
- [ ] $C_1+C_2=Ek_{pu\beta}(X_1)+Ek_{pu\beta}(X_2)$
- [x] $X_1+X_2=Dk_{pri}$ [$Ek_{pu\beta}(X_1)*Ek_{pu\beta}(X_2)$]

Clear selection

In Domingo Ferrer's algorithm, if the plaintext values obtained after splitting the input plaintext is (11,3,6), the value of n is 39, the secret parameter r = 7, and the intermediate ciphertext communicated to the destination node is (c_1, c_2, c_3), then (c_1, c_2, c_3) = ________ .

2 points

Algorithm Domingo-Ferrer ()
Parameters:
Public Key: integer d ≥ 2, *large integer M*
Secret Key: g that divides M; r so that r^{-1} *exists in* Z_M
Encryption: Split m into d parts $m_1..m_d$ *such that*
$\sum_{i=1}^{d}(m_i) \bmod g = m$
$C = [c_1, ..., c_d] = [m_1 r^1 modM, m_2 r^2 modM, .., m_d r^d modM]$
Decryption: $m = (c_1 r^{-1} + c_2 r^{-2} + ... + c_d r^{-d})$: mod M
Aggregation: Scalar addition modulo M: $C_{12} = C_1 + C_2 =$
$[(c_1 1 + c_2 1) modM, ..., (c_1 d + c_2 d) modM]$

- (38, 21, 3)
- (39, 21, 42)
- (40, 19, 4)
- (77, 20, 3)

Clear selection

Stefeen Peter's homomorphic encryption algorithm is _________ homomorphic.

2 points

Algorithm Casstelluccia+Domingo-Ferrer ()

Parameters:

Public Key: integer $d \geq 2$, *large integer* M

Secret Key: g that divides M; r so that r^{-1} *exists in* Z_M

Encryption: Randomly generated key stream $k \in [0, M-1]$

e1 = (k + m) mod M

Split e1 into d parts $m_1..m_d$ *such that*

$\sum_{i=1}^{d} (m_i) \bmod g = m$

$C = [c_1, ..., c_d] = [m_1 r^1 modM, m_2 r^2 modM, .., m_d r^d modM]$

Aggregation: Scalar addition modulo M: $C_{12} = C_1 + C_2 =$

$[(c_1 1 + c_2 1) modM, ..., (c_1 d + c_2 d) modM]$

Decryption: $d_1 = (c_1 r^{-1} + c_2 r^{-2} + ... + c_d r^{-d}$ mod M

m=$(d_1 - k) \bmod M$

where k is the sum of aggregated key streams

- ○ non-homomorphic
- ◉ additively
- ○ Fully
- ○ multiplicatively

Clear selection

In Castellucia's scheme, given that n=303, k_1=50, k_2=50, plaintexts m_1=30, m_2=30, and if the ciphertext received at the destination node(base station) is C_i, then the expression for decryption that would get the plaintext at the base station as __________, and the resulting plaintext, computed from the ciphertext received at the base station is__________.

2 points

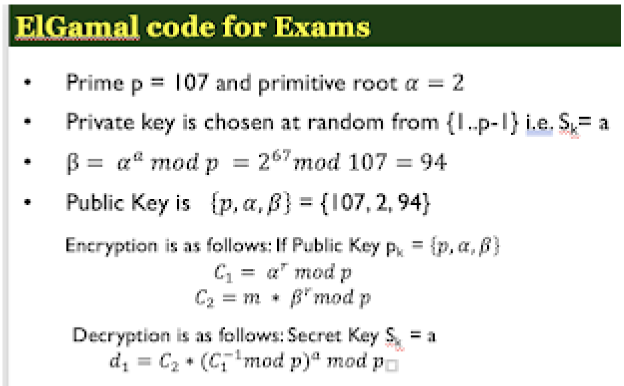
Algorithm Casstelluccia ()
Parameters: Select large integer M
Encryption: Message $m \in [0, M-1]$,
Randomly generated key stream $k \in [0, M-1]$
$c = (m + k) \bmod M$
Decryption: $m = (c\text{-}k) \bmod M$
Aggregation: $c_{12} = (c_1 + c_2) mod M$

- C_i-10, 60
- C_i-50, 100
- C_i-100, 60
- C_i-60, 100

Clear selection

In El Gammal Homomorphic encryption algorithm if the public key chosen is pk = {ρ, α, β } = { 107 , 9 , 94 }, and the other parameters are as shown, and if the two pairs of ciphertexts to be aggregated are (104,29) and (68,67), then the output of the node aggregating the ciphertext is ___________.

2 points



ElGamal code for Exams

- Prime p = 107 and primitive root $\alpha = 2$
- Private key is chosen at random from {1..p-1} i.e. S_k = a
- $\beta = \alpha^a \bmod p = 2^{67} \bmod 107 = 94$
- Public Key is $\{p, \alpha, \beta\}$ = {107, 2, 94}

Encryption is as follows: If Public Key $p_k = \{p, \alpha, \beta\}$

$$C_1 = \alpha^r \bmod p$$
$$C_2 = m * \beta^r \bmod p$$

Decryption is as follows: Secret Key S_k = a

$$d_1 = C_2 * (C_1^{-1} \bmod p)^a \bmod p$$

- ( ) (15,19)
- ( ) (69,28)
- ( ) (10,17)
- (•) none of these

Clear selection

In Castellucia's scheme, given that n = 200, m = 300, k = 50, the Ciphertext C = ____________ .

2 points

- ( ) 45
- ( ) 91
- (•) 100
- ( ) 41
- ( ) cannot be computer

Clear selection

A cryptosystem that uses an encryption scheme, viz. C=E(x)=e^x, is ________ homomorphic, where e is an exponent operation and x is any integer. 1 point

- ◯ not homomorphic
- ◉ multiplicatively
- ◯ fully
- ◯ additively

Clear selection

In Paillier homomorphic encryption algorithm, if the public key pk = {n,g} = {77, 5652}, random r=19 and the plaintext m=25, then the ciphertext c is __________ . 2 points

Algorithm Paillier ()

Key Generation:

1 Choose two large prime numbers p and q randomly and independently of each other such that gcd(pq,(p-1)(q-1))=1.

2 This property is assured if both primes are of equivalent length, i.e. $p, q \in 1||\{0,1\}^{(s-1)}$ for security parameter s.

3 Compute n=pq and $\lambda = lcm(p-1, q-1)$.

4 Select random integer g where $g \in Z^*_{n^2}$.
Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse:
$\mu = (L(g^\lambda mod\, n^2))^{-1} mod\, n$,
where function L is defined as, L(u) = (u-1)/n

5 The public (encryption) key is (n,g).

6 The private (decryption) key is (λ, μ).

Message Encryption: Let m be a message to be encrypted where $m \in Z_n$.
Select a random r where r $\in Z_{n^*}$
Compute ciphertext as: $c = g^m . r^n \; mod\, n^2$

Decryption: Ciphertext c $\in Z^*_{n^2}$
Compute message: $m = L(c^\lambda \; mod\, n^2).\mu \; mod\, n$

- ◯ 3052
- ◯ 2976
- ◯ 2526
- ◉ 3390

Clear selection

In Castellucia's scheme, given that n=303, k_1=40, k_2=34, plaintexts m_1=30, m_2=46, the ciphertext value received at the destination node(base station) is ________ .

2 points

Algorithm Casstelluccia ()

Parameters: Select large integer M

Encryption: Message $m \in [0, M-1]$,

Randomly generated key stream $k \in [0, M-1]$

$c = (m + k) \bmod M$

Decryption: $m = (c\text{-}k) \bmod M$

Aggregation: $c_{12} = (c_1 + c_2) mod M$

- (selected) 150
- 80
- 153
- 70

Clear selection

When using Castellucia's homomorphic encryption algorithm, say the key values used by two sensor nodes node1 and node2 are k_1= 220 and k_2 = 320 respectively. Let the large integer **n** for the system is chosen to be 2048. If the plaintext values sensed are 480 and 540 respectively, then the ciphertext at the base station computed is _________.

2 points

Algorithm Casstelluccia ()
Parameters: Select large integer M
Encryption: Message $m \in [0, M-1]$,
Randomly generated key stream $k \in [0, M-1]$
$c = (m + k) \bmod M$
Decryption: $m = (c\text{-}k) \bmod M$
Aggregation: $c_{12} = (c_1 + c_2) mod M$

- (selected) 1560
- 1600
- 1500
- 1650

Clear selection

In Castellucia's scheme, given that n=303, k_1=50, k_2=50, plaintexts m_1=100, m_2=100, and if the ciphertext received at the destination node(base station) is C_i, then the expression for decryption that would get the aggregated plaintext at the base station is __________, and the resulting plaintext, computed from the aggregated ciphertext received at the base station is__________.

2 points

- C_i-100, 50
- C_i-200, 200
- C_i-60, 100
- (selected) C_i-100, 200

Clear selection

Castellucia's scheme is ________ homomorphic, whereas the Domingo Ferrer scheme is ___________, whereas _____________ scheme is also multiplicatively homomorphic. 1 point

Algorithm Domingo-Ferrer ()

Parameters:

Public Key: integer $d \geq 2$, *large integer* M

Secret Key: g that divides M; r so that r^{-1} *exists in* Z_M

Encryption: Split m into d parts $m_1..m_d$ *such that*

$$\sum_{i=1}^{d} (m_i) \bmod g = m$$

$$C = [c_1, ..., c_d] = [m_1 r^1 mod M, m_2 r^2 mod M, .., m_d r^d mod M]$$

Decryption: $m = (c_1 r^{-1} + c_2 r^{-2} + ... + c_d r^{-d})$ **mod M**

Aggregation: Scalar addition modulo M: $C_{12} = C_1 + C_2 =$

$$[(c_1 1 + c_2 1) mod M, ..., (c_1 d + c_2 d) mod M]$$

- ◯ multiplicatively, additively, RSA
- ◯ multiplicatively, multiplicatively, RSA
- ◯ additively, multiplicatively, Goldwasser-Micali
- ◯ multiplicatively, additively, Goldwasser-Micali
- ◉ additively, additively, RSA

Clear selection

Castellucia's scheme is _______ key based scheme. 1 point

- ◯ Asymmetric-key based
- ◉ Symmetric-key based

Clear selection

Castellucia's scheme is ________ homomorphic, whereas the Stefeen Peter's scheme is ___________, whereas _____________ scheme is multiplicatively homomorphic.

2 points

- ○ multiplicatively, additively, Goldwasser-Micali
- ○ multiplicatively, multiplicatively, RSA
- ◉ additively, additively, RSA
- ○ additively, multiplicatively, Goldwasser-Micali
- ○ multiplicatively, additively, RSA

Clear selection

In Castellucia's scheme, given that n = 193, m = 45, k = 41, the Ciphertext C = ____________ .

1 point

Algorithm Casstelluccia ()
Parameters: Select large integer M
Encryption: Message m $\in [0, M-1]$,
Randomly generated key stream k $\in [0, M-1]$
c = (m + k) mod M
Decryption: m = (c-k) mod M
Aggregation: $c_{12} = (c_1 + c_2) mod M$

- ○ 41
- ○ 45
- ○ 91
- ◉ 86

Clear selection

Consider the multiplicative group Z^*_{11} Given that 8 is one of the generators of this group, the set of Quadratic residues of Z^*_{11} is _________. 2 points

- ( ) {1,3,4,5,11}
- (•) {1,3,4,5,9}
- ( ) {1,2,4,5,9}
- ( ) {1,3,4,5,9,10}
- ( ) {1,3,4,5,12}

Clear selection

If RSA system modulus n=91, and if the encryption key selected is (5, ϕ (n)) then the decrytion key must be _________ , considering the value of ϕ(n) = ______. 2 points

- ( ) (27,90)
- ( ) (29,90)
- ( ) (29,72)
- ( ) (27,72)

Compute the following moduli: −14 mod 3 ≡ _______ mod3. 73 mod 23 ≡ _______ mod 23. (3) − 82 mod 9 ≡ _________ mod9. 2 points

- ( ) 1, 4, 1
- (•) 1, 4, 8
- ( ) 3, 4, 1
- ( ) 4, 1, 8

Clear selection

_______ homomorphic cryptosystems are those that allow for either addition OR multiplication operation ONLY to be performed on the ciphertext, but not both.

2 points

- ◯ Asymmetric-key based
- ◯ Fully
- ◯ Symmetric-key based
- ◉ Partially

Clear selection

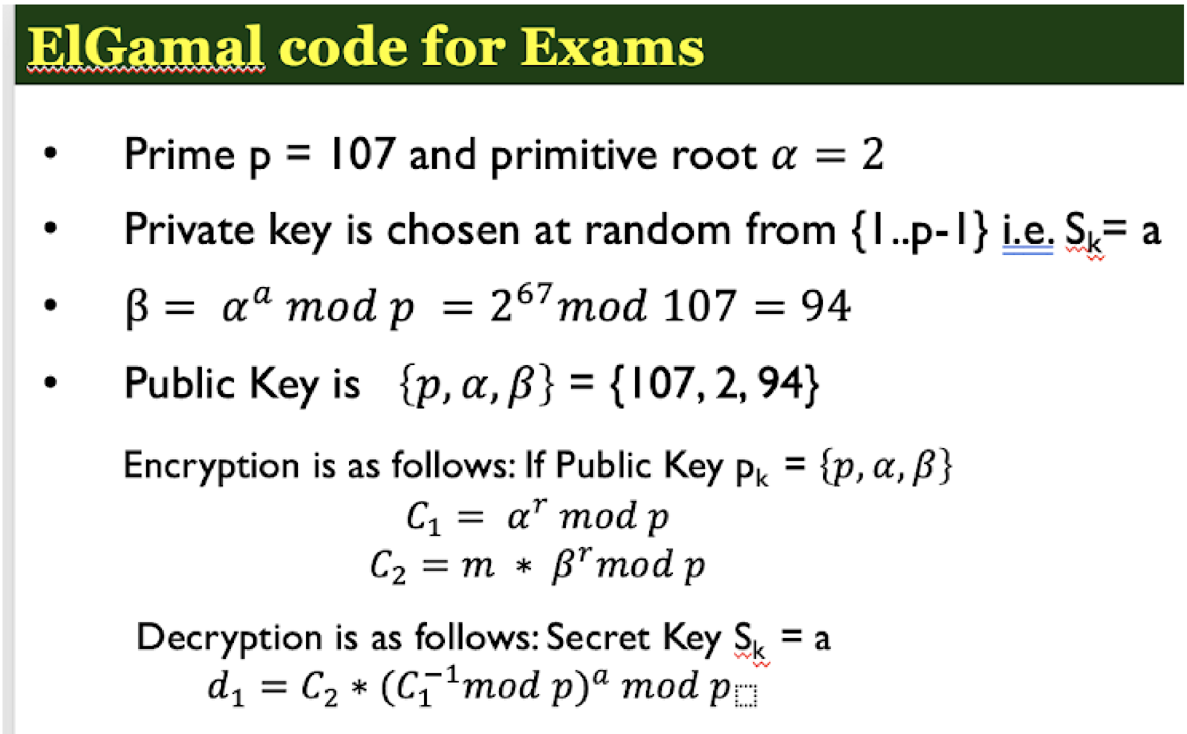
Consider the multiplicative group $\mathbb{Z}^*_{19}$. This is _______ group, because ____________. The number of of generators in this group is equal to ___________; one of which is ________.

2 points

- ◯ acyclic, the number p $\mathbb{Z}^*_p$ is a non-prime, 5, 12
- ◯ acyclic, the number p $\mathbb{Z}^*_p$ is a nonprime, 5, 12
- ◯ cyclic, the number p $\mathbb{Z}^*_p$ is a prime, 5, 12
- ◉ cyclic, the number p $\mathbb{Z}^*_p$ is a prime, 6, 15
- ◯ acyclic, the number p $\mathbb{Z}^*_p$ is a prime, 6, 14
- ◯ cyclic, the number p $\mathbb{Z}^*_p$ is a nonprime, 6, 15

Clear selection

Consider the El Gammal cryptosystem as per the scheme shown in the figure. If the plaintext m=66 and the random r = 45 then the ciphertext pairs are _____________. 2 points



- {97,84}
- {97,85}
- {96,85}
- {96,84}

_______ homomorphic cryptosystems are those that allow for either addition OR multiplication operation ONLY to be performed on the ciphertext, but not both. 1 point

- Asymmetric-key based
- Symmetric-key based
- (selected) Partially
- Fully

Clear selection

As per the design of the RSA homomorphic algorithm, if the system modulus n=15, then it is NOT possible to have an encryption key with value (e,ϕ(n)) = ___________ . 2 points

- (4,8)
- (3,10)
- (5,8)
- (11,14)

Clear selection

In Stefeen 's algorithm, if the input plaintext value is 7, n=39, the key k=2, the value of d=3 and the secret parameter n'=13, then the plaintext values that could be obtained after splitting is ________ . 2 points

Algorithm Casstelluccia+Domingo-Ferrer ()
Parameters:
Public Key: integer $d \geq 2$, *large integer M*
Secret Key: g that divides M; r so that r^{-1} *exists in* Z_M
Encryption: Randomly generated key stream $k \in [0, M-1]$
$e1 = (k + m) \bmod M$
Split e1 into d parts $m_1..m_d$ *such that*
$\sum_{i=1}^{d} (m_i) \bmod g = m$
$C = [c_1, ..., c_d] = [m_1 r^1 modM, m_2 r^2 modM, .., m_d r^d modM]$
Aggregation: Scalar addition modulo $M: C_{12} = C_1 + C_2 =$
$[(c_1 1 + c_2 1) modM, ..., (c_1 d + c_2 d) modM]$
Decryption: $d_1 = (c_1 r^{-1} + c_2 r^{-2} + ... + c_d r^{-d}$ mod M
$m = (d_1 - k) \bmod M$
where k is the sum of aggregated key streams

- (6,11,11)
- (5,9,8)
- (16,17,12)
- (9,12,11)

Clear selection

IF C_1=$Ek_{pu\beta}(X_1)$ and C_2=$Ek_{pu\beta}(X_2)$, then the crypto-system is additively homomorphic if ________ .[Here, C_1, C_2 are ciphertexts and X_1, X_2 are the associated plaintexts and $EK_{pu\beta}$ and EK_{pri} are the public and private keys.]

2 points

- ◯ C_1+C2=Dk_{pri} [$Ek_{pu\beta}(X_1)$+$Ek_{pu\beta}(X_2)$]
- ◯ X_1+X_2=$Ek_{pu\beta}(C_1)$+$Ek_{pu\beta}(C_2)$
- ◉ X_1+X_2=Dk_{pri} [$Ek_{pu\beta}(X_1)$+$Ek_{pu\beta}(X_2)$]
- ◯ C_1+C_2=$Ek_{pu\beta}(X_1)$*$Ek_{pu\beta}(X_2)$

Clear selection

In El Gammal Homomorphic encryption algorithm if the public key chosen is pk = {p, α, β } = { 107 , 9 , 94 }, and the other parameters are as shown, and if the two pairs of ciphertexts to be aggregated are (42,104) and (8,65), then the output of the node aggregating the ciphertext is __________.

2 points

ElGamal code for Exams

- Prime p = 107 and primitive root $\alpha = 2$
- Private key is chosen at random from {1..p-1} i.e. S_k= a
- $\beta = \alpha^a \bmod p = 2^{67} \bmod 107 = 94$
- Public Key is $\{p, \alpha, \beta\}$ = {107, 2, 94}

Encryption is as follows: If Public Key $p_k = \{p, \alpha, \beta\}$

$$C_1 = \alpha^r \bmod p$$
$$C_2 = m * \beta^r \bmod p$$

Decryption is as follows: Secret Key S_k = a

$$d_1 = C_2 * (C_1^{-1} \bmod p)^a \bmod p$$

- ◯ none of these
- ◯ (10,17)
- ◯ (69,28)
- ◉ (15,19)

Clear selection

A natural application of homomorphic encryption is ______________ . 1 point

- ○ encrypting data using an asymmetric key cipher.
- ○ outsourcing computations to a trusted third party.
- ◉ outsourcing computations to an untrusted third party.
- ○ generating a keyed MAC using a hash function.
- ○ encrypting data using a symmetric key cipher.

Clear selection

In Goldwasser-Micali Homomorphic encryption algorithm, if the chosen random r = 51 where 1 < r < n, the public KeyPk=(a,n)=(80,851) & plaintext bit m=1, then the ciphertext c= __________ . 2 points

Key generation [edit]

The modulus used in GM encryption is generated in the same manner as in the RSA cryptosystem. (See RSA, key generation for details.)

1. Alice generates two distinct large prime numbers p and q, randomly and independently of each other.
2. Alice computes $N = p\,q$.
3. She then finds some non-residue x such that the Legendre symbols satisfy $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1$ and hence the Jacobi symbol $\left(\frac{x}{N}\right)$ is +1. The value x can for example be found by selecting random values and testing the two Legendre symbols. If p, q = 3 mod 4 (i.e., N is a Blum integer), then the value $N - 1$ is guaranteed to have the required property.

The *public key* consists of (x, N). The secret key is the factorization (p, q).

Message encryption [edit]

Suppose Bob wishes to send a message m to Alice:

1. Bob first encodes m as a string of bits (m_1, ..., m_n).
2. For every bit m_i, Bob generates a random value y_i from the group of units modulo N, or $\gcd(y_i, N) = 1$. He outputs the value $c_i = y_i^2 x^{m_i} \pmod{N}$.

Bob sends the ciphertext (c_1, ..., c_n).

Message decryption [edit]

Alice receives (c_1, ..., c_n). She can recover m using the following procedure:

1. For each i, using the prime factorization (p, q), Alice determines whether the value c_i is a quadratic residue; if so, m_i = 0, otherwise m_i = 1.

Alice outputs the message m = (m_1, ..., m_n).

- ○ 173
- ○ 273
- ○ 171
- ◉ 436

Clear selection

In Domingo Ferrer's algorithm, if the plaintext values obtained after splitting the sensed plaintext at the leaf node is (2,4,8), the value of n is 39, the secret parameter r is 7, then the intermediate ciphertext communicated to the parent node by this leaf node node is ______ . 2 points

Algorithm Domingo-Ferrer ()
Parameters:
Public Key: integer $d \geq 2$, *large integer M*
Secret Key: g that divides M; r so that r^{-1} *exists in* Z_M
Encryption: Split m into d parts $m_1..m_d$ *such that* $\sum_{i=1}^{d}(m_i) \bmod g = m$
$C = [c_1, ..., c_d] = [m_1 r^1 modM, m_2 r^2 modM, .., m_d r^d modM]$
Decryption: $m = (c_1 r^{-1} + c_2 r^{-2} + ... + c_d r^{-d})$: mod M
Aggregation: Scalar addition modulo M: $C_{12} = C_1 + C_2 = [(c_1 1 + c_2 1) modM, ..., (c_1 d + c_2 d) modM]$

- (14, 196, 2744)
- (14,28,17)
- (14, 28, 56)
- (14, 1, 14)

Clear selection

If RSA system modulus n=21, and the encryption exponent chosen could be ________ (a valid e). Then the value of decryption exponent is ______ . 2 points

- 4,5
- 6,7
- 7, 7
- 7,3

In Stefeen Peter's algorithm, if the plaintext values obtained after splitting the input plaintext is (11,7,6), the value of n is 39, the secret parameter r = 5, and the intermediate ciphertext communicated to the destination node is (c_1, c_2, c_3), then (c_1, c_2, c_3) = __________ .

2 points

Algorithm Casstelluccia+Domingo-Ferrer ()
Parameters:
Public Key: integer $d \geq 2$, *large integer* M
Secret Key: g that divides M; r so that r^{-1} *exists in* Z_M
Encryption: Randomly generated key stream $k \in [0, M-1]$
$e1 = (k + m) \bmod M$
Split e1 into d parts $m_1..m_d$ *such that*
$\sum_{i=1}^{d} (m_i) \bmod g = m$
$C = [c_1, ..., c_d] = [m_1 r^1 modM, m_2 r^2 modM, .., m_d r^d modM]$
Aggregation: Scalar addition modulo M: $C_{12} = C_1 + C_2 =$
$[(c_1 1 + c_2 1) modM, ..., (c_1 d + c_2 d) modM]$
Decryption: $d_1 = (c_1 r^{-1} + c_2 r^{-2} + ... + c_d r^{-d}$ mod M
$m = (d_1 - k) \bmod M$
where k is the sum of aggregated key streams

- ( ) (30,2,10)
- (•) (16,19,9)
- ( ) (21,36,18)
- ( ) (25,30,25)

Clear selection

Page 2 of 2

Back Submit Clear form