عنوان الدرس:..... اليوم:..... التاريخ: / / ١٤

Subject:..... Day:..... Date: / /20 الموافق: / / ٢٠م

Q 1 Define RSA algorithm and explain setp briefly.

RSA is public key encryption algorithm (asymmetric) based on the difficulty of factoring large number

steps:

1. chose two prime number p and q
2. Compute $n = p * q$
3. compute Euler's totient $\varphi(n) = (p-1)(q-1)$
4. choose a public key e such that $1 < e < \varphi(n)$ and $gcd(e, \varphi(n)) = 1$
5. compute the ~~pri~~ private key d, where $d \times e = 1 \pmod{\varphi(n)}$
6. encryption $c = m^e \bmod n$
7. dencryption $m = c^d \bmod n$

Q 2: what the homomorphic propetry in cryptography?

Solve:

It means operation on ciphertexts correspond to operation on plaintexts

Q.3 Expain why RSA is multiplicatively homomorphy ?

Solve:

because: $E(m) = m^e \bmod n$

$\Rightarrow E(m_1) \times E(m_2) = (m_1^e \bmod n)(m_2^e \bmod n)$

$= ((m_1^e)(m_2^e)) \bmod n = (m_1 \times m_2)^e \bmod n$

$= E(m_1 \times m_2)$

Q4 what the advantage and risk of homomorphy encryption?

Solve:

Advantage:

1. compute on encrypted data
2. privacy include and data analysis

Risk:

1. vulnerable to manipulate (malleability) and choosen ciphertext attacks
2. slow for large data

عنوان الدرس: ..... اليوم: ..... التاريخ: / / ١٤

Subject: ..... Day: ..... Date: / / 20 الموافق: / / ٢٠م

5. Why use mod in RSA ?

Solve

To keep result whin range prevent overflow and ensure reversibility,

It the base of RSA security and math properties

6. Compute manually for small case (p=3, q = 11, e=7 , m1 = 2 , m2 = 5)

$n = p \times q \Rightarrow n = 3 \times 11 = 33$, $\varphi(n) = (3-1)(11-1) = 20$

$d = 3$ [illegible]

$E(m1) = 2^7 \bmod 33 = 128 \bmod 33 = 29$

$E(m2) = 5^7 \bmod 33 = 78125 \bmod 33 = 14$

~~Now~~ multiply both ciphertext:

$E(m_1) \times E(m_2) \bmod 33 = 29 \times 14 \bmod 33 = 10$

$E(m_1 \times m_2) = E(2 \times 5) = E(10) = 10^7 \bmod 33$

$= 10000000 \bmod 33 = 10$

decryption

$dec(29) = 29^3 \bmod 33 = 24389 \bmod 33 = 2$

$dec(14) = 14^3 \bmod 33 = 2744 \bmod 33 = 5$

Q7. why is key size important for security?

* solve:

Large keys make factring n header → strong security

Q8. Explin what happens if e and φ(n) are not coprime

If e and φ(n) are not coprime then there is no modular inverse for e, so d ... be calculated without d decryption is impossible and the key pair is invalid

Q9. Describe one-real-word application of ... homomorphic encryption.

secure cloud data processing:
it allows storing encrypted data in the cloud and preforming calculation on searches on it without decryption, keep the data safe and private

```python
# Dencrypt function
def decrypt(c,d,n):
    m= (c**d) % n
    return m

# Encrypt function
def encrypt(m,e,n):
    c= (m**e) % n
    return c
# Generate p, q, n, ϕ(n), and keys (e, d)

def genate_key():
    p=7
    q=11
    n=p*q
    phi=(p-1)*(q-1)
    e=17
    d=2753
    return p,q,n,phi ,e,d
```

```python
def main():
    #Generate p, q, n, ϕ(n), and keys (e, d) by genate_key function
    p,q,n,phi ,e,d=genate_key()
    #choose the m1 and m2
    m1=6
    m2=8
    # Encrypt m1 and m2
    cm1=encrypt(m1,e,n)
    cm2=encrypt(m2,e,n)
    # Multiply ciphertexts and decrypt the result
    mult_cm= (cm1*cm2) % n
    dec_mult= decrypt(mult_cm,d,n)
    # Calculate expected result
    excepted_mult= (m1*m2) % n
```

```
    print("p:",p," q:",q)
    print("n:",n," ϕ:",phi)
    print("public key (e,n):(",e,",",n,")")
    print("private key (d,n):(",d,",",n,")\n\n")

    print("m1:",m1," m2:",m2)
    print("E(m1) = ",cm1," E(m2) = ",cm2)
    print ("E(m1)*E(m2) mod n = ",mult_cm)
    print("decrypeted rusute = ",dec_mult)
    print("expected (m1*m2 mod n) = ",excepted_mult)
    # Check homomorphic property
    if dec_mult == excepted_mult:
        print("\nHomomorphic property done")
    else:
        print("Homomorphic property failed")

if __name__ == "__main__":
    main()
```

```
p: 7  q: 11
n: 77  ϕ: 60
public key (e,n):( 17 , 77 )
private key (d,n):( 2753 , 77 )


m1: 6  m2: 8
E(m1) =  41  E(m2) =  57
E(m1)*E(m2) mod n =  27
decrypeted rusute =  48
expected (m1*m2 mod n) =  48

Homomorphic property done
```