RSA Class Activity

APT3090 CRYPTOGRAPHY AND NETWORK SECURITY

1. Provide the notation for generating RSA key pair, Encryption and Decryption

i. Select two large prime numbers p and q.
ii. Compute their product n: where $n = p \times q$
iii. Calculate Euler's totient function $\phi(n)$ where $\phi(n)=(p-1) \times (q-1)$
iv. Choose an integer e such that $1<e<\phi(n)$and GCD $(e, \phi(n))=1$.
v. Determine d such that $d \times e \equiv 1 \pmod{\phi(n)}$

Encryption

To encrypt a plaintext message m:

1. Convert the plaintext message m into an integer m such that $0 \leq m < n$
2. Compute the ciphertext c:

   c=m^e mod n

Decryption

To decrypt a ciphertext c:

1. Compute the plaintext message m:

   m = c^d mod n

2. Decoding in RSA

Decode the three ciphertext symbols 5, 9 and 3 using the private RSA key (7, 11). What are the corresponding plaintext symbols?

i. Decrypt the ciphertext 5:

   m = 5^11 mod 7= 3

   The plaintext symbol for ciphertext 5 is 3.

ii. Decrypt the ciphertext 9:

   m = 9^11 mod 7 = 4

   The plaintext symbol for ciphertext 9 is 4.

iii. Decrypt the ciphertext 3:

   m = 3^11 mod 7 = 5

   The plaintext symbol for ciphertext 3 is 5.

3. Matching RSA Keys

Which of the following private RSA keys matches the public RSA key (5, 91)?

- (19, 91)
- (24, 91)
- (29, 91)
- (19, 81)
- (24, 81)
- (29, 81)

Solution

The modulus n should be the same for both public and private keys. So I eliminate options where n = 81:

- (19, 81)
- (24, 81)
- (29, 81)

Now I’m left with:

- (19, 91)
- (24, 91)
- (29, 91)

In RSA, e and d are related by the equation: $e * d \equiv 1 \pmod{\varphi(n)}$ where $\varphi(n)$ is Euler's totient function

For n = 91; ϕ(n): 91 = 7 * 13 (prime factorization)

Φ (91) = (7-1) * (13-1) = 6 * 12 = 72

5 * d ≡ 1 (mod 72)

5 * 29 = 145 ≡ 1 (mod 72)

The correct private key is (29, 91).

4. Generate Your Own RSA Key Pair

Use the procedure as described in the lecture to generate a RSA key pair, using primes in the range from 20 to 100. Test the correctness of your key pair by encoding and decoding a number. If your key pair is correct, after decoding an encoded number, you should arrive at the number you started from.

Solution

two prime numbers p and q;
p=23 and q =47.

n = 23×47=1081

$\phi(n)= (23-1) \times (47-1) = 22 \times 46 = 1012$

Choose e such that 1<e<ϕ(n) and GCD (e, ϕ(n)) =1:
e=3
GCD (3,1012) =1

Determine d such that $d \times e \equiv 1 (\mod \phi(n))$

I will use Euclidean Algorithm to find d

Q	A	B	R	T1	T2	T
337	1012	3	1	0	1	-337
3	3	1	0	1	-337	1014
	1	0		-337	1014	

-337+1012=675

675*3 mod 1012=1
So, d =675

Testing

m =5

encrypt c=5^3 mod 1081 =125
c=125
decrypt m=125^675 mod 1081 = 5
m= 5