NETWORK PROTOCOLS & SECURITY
23EC2210 R/A/E

Topic:

RSA algorithm

Session – 38

RSA Encryption

RSA Algorithm

- Asymmetric encryption method
- Also know as Public Key Cryptography
- Uses two different keys are used for encryption and decryption.
  - Public key
  - Private(secret) key
- Encryption is done using public key and decryption is done using secret key.
- Ron Rivest, Adi Shamir and Len Adleman have developed this algorithm(Rivest-Shamir-Adleman).

RSA...

This algorithm works as follows:

Key Generation:

1. Select any two prime numbers p and q where $p \neq q$.
2. Calculate $n = p*q$.
3. Calculate $\Phi(n) = (p-1) * (q-1)$.
4. Select e such that, e is relatively prime to $\Phi(n)$

   i.e., $\gcd(e, \Phi(n)) = 1$ and $1<e< \Phi(n)$
5. Calculate $d = e^{-1} \bmod \Phi(n)$ or $ed = 1 \bmod \Phi(n)$
6. Public key = {e,n} ; Private key = {d,n}

7. Encryption:

$C = M^e \bmod n$, where $M<n$

Where,
C = Ciphertext,
M = Plaintext,
e = Encryption key.
n = Block size

---

8. Decryption :

$M = C^d \bmod n$
Where d = decryption key

RSA Example1

1. Select any two prime numbers p and q where, $p \neq q$.
2. Calculate n = p*q.
3. Calculate $\Phi(n) = (p-1) * (q-1)$.
4. Select e such that, e is relatively prime to $\Phi(n)$

   i.e., gcd(e, $\Phi(n)$) =1 and $1<e<\Phi(n)$
5. Calculate $d = e^{-1} \bmod \Phi(n)$ or $ed = 1 \bmod \Phi(n)$

   $d = ((\Phi(n) * i) + 1) / e$

   Stop calculating d when you get a numerical value.
6. Public Key(Pu) = {e,n}
   Private Key(Pk) = {d,n}

1. p = 13, q = 11
2. n = 13*11 = 143
3. $\Phi(n) = (13-1) * (11-1) = 12*10 = 120$
4. Select e =13 ; gcd(13,120) =1
5. $d = ((\Phi(n) * i) + 1) / e$
   $d = (120 * 1) + 1) / 13 = 9.3$ (for i =1)
   $d = (120 * 2) + 1) / 13 = 18.5$ (for i=2)
   $d = (120 * 3) + 1) / 13 = 27.7$ (for i=3)
   $d = (120 * 4) + 1) / 13 = 37$ (for i = 4)
   Therefore d = 37
6. Public Key(Pu) = {13,143}
   Private Key(Pk) = {37,143}

RSA Example1

7. Encryption:

$C = M^e \bmod n$, where $M<n$

8. Decryption :

$M = C^d \bmod n$

7. Encryption:

Choose Plaintext M = 13

$C = 13^{13} \bmod 143 = 52$

Therefore, **C =52**

8. Decryption:

$M = 52^{37} \bmod 143 = 13$

Therefore, **M = 13**

RSA Exercise

Example-2:

P and Q are two prime numbers. P=7 and Q=17. Take public key E=5. If the plaintext value is 6, then what will be the cipher text value according to RSA algorithm? Again, calculate plaintext value from cipher text.

RSA Exercise...

Example-3:

In a public key crypto system using RSA algorithm, user uses two prime numbers 5 and 7. He chooses 11 as encryption key, find out decryption key. What will be the cipher text, if the plaintext is 2? Decrypt the cipher text, what will be the plaintext value?


THANK
YOU