Asymmetric Key Cryptography for IT 7th sem Students

Developed and Presented By:

Dileep Kumar Yadav

Assistant professor

Dept. of CSE

V.B.S PU,Jaunpur

Mb. No.8726943272

Email-dileep1482@gmail.com

Asymmetric Key Cryptography

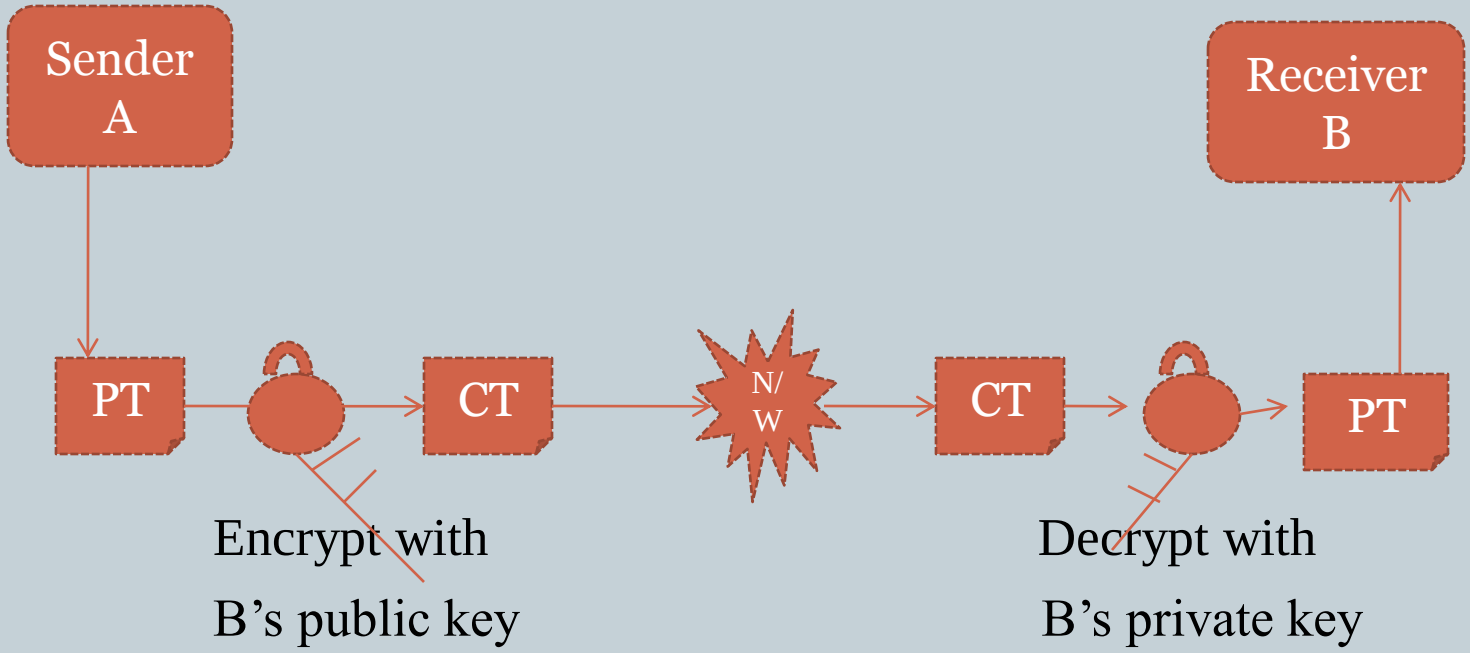
- If two different keys are used in a cryptographic mechanism where one key is used for encryption and other different key is used for decryption then this mechanism is called asymmetric key cryptography.
- It is also called public key cryptography, two different keys are used. One key is used for encryption and only other corresponding key must be used for decryption. No other key can decrypt the message not even the original i.e. first key used for decryption.

Cont…

- The beauty of this scheme is that every communicating party needs just a key pair for communicate with any number of other communicating parties. Once someone a key pair he or she can communicate with anyone else.
- There is a simple mathematical basis for this scheme. If you have an extremely large number that has only two factors, which are prime numbers you can generate a pair of keys.
- For example consider a number 10. the number 10 has only two factors i.e.5 and 2 which are prime numbers.

Cont…

- One of the two keys are called as public key and other is the private key.



RSA Algorithm

- Choose two large prime numbers P and Q.
- Calculate N=P×Q.
- Select the public key i.e. the encryption key E such that it is not a factor of (P-1) × (Q-1).
- Select the private key i.e. the decryption key D such that the following equation is true..

  $(D \times E) \bmod (P-1) \times (Q-1) = 1$

- For encryption calculate the cipher text CT from the plain text PT as follows:

  $CT = PT^{E} \bmod N$

Cont…

- Send CT as the cipher text to the receiver.
- For decryption calculate the plain text PT from the cipher text CT as follows:

$$PT=CT^{D} \bmod N$$

For Example

- Let P=7 and Q=17.
- Calculate N=P×Q i.e. 7×17=119.
- Select the public key i.e. E such that it is not factor of

  (P-1) ×(Q-1) i.e.(7-1) ×(17-1)=6×16=96
- The factors of 96 are 2,2,2,2,2 and 3 because(96=2×2×2×2×2×3).
- Thus we have to choose E such that none of the factors of E is 2 and 3.
- Let us choose E as 5,7,11,13,17,19,23,25,29 and so on…

Cont…

- Select the private key i.e. decryption key D such that
- $(D \times E) \bmod (P-1) \times (Q-1) = 1$
- Let substitute the values of E,P and Q in this equation
- $(D \times 5) \bmod (7-1) \times (17-1) = 1$
- i.e. $(D \times 5) \bmod (6 \times 16) = 1$
- i.e. $(D \times 5) \bmod 96 = 1$
- For satisfy this equation we will choose D=77 then..
- $77 \times 5 \bmod 96 = 1$
- i.e. $385 \bmod 96 = 1$ which satisfy this equation.

Cont…

- For encryption calculate the cipher text CT from the plain text PT as follows:
- CT=PT^E mod N
- i.e. CT=10^5 mod 119, let us take PT=10
- i.e. CT= 100000 mod 119
- i.e. CT=40
- Send CT i.e. 40 on the receiver side
- For decryption calculate the plain text PT from CT as follows:

Cont…

- PT= CT^D mod N
- i.e. PT=40^77mod119
- i.e. PT=10.

Security of RSA

- Brute Force Attack
- Mathematical Attack
- Timing Attack
- Chosen Cipher text Attack

Reference

- Cryptography and network security “Atul Kahate” 3e,Mc Graw hill education.