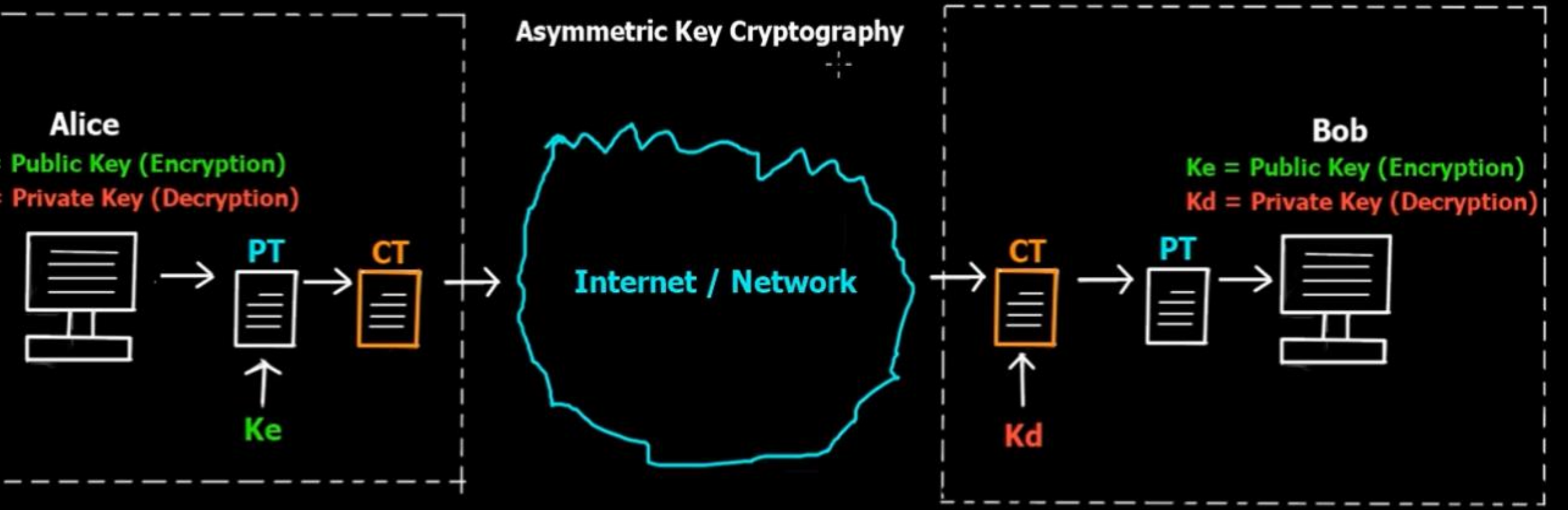
RSA

RSA Algorithm - Asymmetric Cryptography Algorithm

A Algorithm -

- Ron Rivest, Adi Shamir and Len Adlemen developed the method called as RSA algorithm
- Most popular and proven asymmetric key cryptography algorithm
- Based on the mathematical fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product.



RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

1. Choose two large prime numbers P and Q.
2. Calculate N = P * Q
3. Select the public key (i.e. the encryption key) E such that it is not a factor of (P – 1) & (Q – 1).
4. Select the private key (i.e. the decryption key) D such that the following equation is true: (D * E) mod (P – 1) * (Q – 1) = 1

Encryption -

>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

1. Choose two large prime numbers P and Q.
2. Calculate N = P * Q
3. Select the public key (i.e. the encryption key) E such that it is not a factor of (P – 1) & (Q – 1).
4. Select the private key (i.e. the decryption key) D such that the following equation is true: (D * E) mod (P – 1) * (Q – 1) = 1

Encryption -

>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

1. P = 7, Q = 17

RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

1. Choose two large prime numbers P and Q.
2. Calculate N = P * Q
3. Select the public key (i.e. the encryption key) E such that it is not a factor of (P – 1) & (Q – 1).
4. Select the private key (i.e. the decryption key) D such that the following equation is true: (D * E) mod (P – 1) * (Q – 1) = 1

Encryption -

>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

1. P = 7 Q = 17
2. N = 7 * 17 = 119

RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

1. Choose two large prime numbers P and Q.
2. Calculate N = P * Q
3. Select the public key (i.e. the encryption key) E such that it is not a factor of (P – 1) & (Q – 1).
4. Select the private key (i.e. the decryption key) D such that the following equation is true: (D * E) mod (P – 1) * (Q – 1) = 1

Encryption -

>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

1. P = 7, Q = 17

2. N = 7 * 17 = 119

3. (P – 1) * (Q – 1) = 6 * 16 = 96

   Let us choose the public key value of E as 5.

   E = 5 ⟶ Encryption Key (Public Key)

RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

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

Encryption -

>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

1. P = 7, Q = 17

2. N = 7 * 17 = 119

3. (P – 1) * (Q – 1) = 6 * 16 = 96

   Let us choose the public key value of E as 5.

   E = 5 ⟶ Encryption Key (Public Key)

4. (D * E) mod (P – 1) * (Q – 1) = 1

   Let us choose D as 77 because (77 * 5) mod 96 = 385 mod 96 = 1

   D = 77 ⟶ Decryption Key (Private Key)

RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

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

Encryption -

>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

1. P = 7, Q = 17

2. N = 7 * 17 = 119

3. (P – 1) * (Q – 1) = 6 * 16 = 96

   Let us choose the public key value of E as 5.

   E = 5 → Encryption Key (Public Key)

4. (D * E) mod (P – 1) * (Q – 1) = 1

   Let us choose D as 77 because (77 * 5) mod 96 = 385 mod 96 = 1

   D = 77 → Decryption Key (Private Key)

RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

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

Encryption -

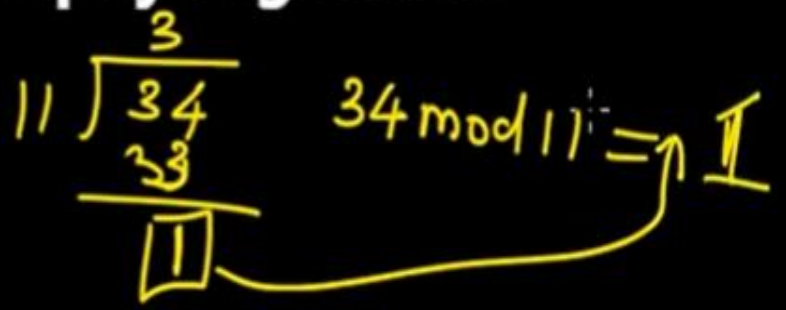
>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

1. P = 7, Q = 17



2. N = 7 * 17 = 119

3. (P – 1) * (Q – 1) = 6 * 16 = 96

   Let us choose the public key value of E as 5.

   E = 5 ⟶ Encryption Key (Public Key)

4. (D * E) mod (P – 1) * (Q – 1) = 1

   Let us choose D as 77 because (77 * 5) mod 96 = 385 mod 96 = 1

   D = 77 ⟶ Decryption Key (Private Key)

RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

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

Encryption -

>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

1. P = 7, Q = 17

2. N = 7 * 17 = 119

3. (P – 1) * (Q – 1) = 6 * 16 = 96

   Let us choose the public key value of E as 5.

   E = 5 ⟶ Encryption Key (Public Key)

4. (D * E) mod (P – 1) * (Q – 1) = 1

   Let us choose D as 77 because (77 * 5) mod 96 = 385 mod 96 = 1

   D = 77 ⟶ Decryption Key (Private Key)

Based on the above values, consider an encryption and decryption process as follows: A = 1, B = 2 etc

C=3 D=4 E=5 F=6 ....

PT = F = 6

Encryption -

$CT = PT^E \bmod N$

Decryption -

$PT = CT^D \bmod N$

RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

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

Encryption -

>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

1. P = 7, Q = 17
2. N = 7 * 17 = 119
3. (P – 1) * (Q – 1) = 6 * 16 = 96

   Let us choose the public key value of E as 5.

   E = 5 ⟶ Encryption Key (Public Key)
4. (D * E) mod (P – 1) * (Q – 1) = 1

   Let us choose D as 77 because (77 * 5) mod 96 = 385 mod 96 = 1

   D = 77 ⟶ Decryption Key (Private Key)

Based on the above values, consider an encryption and decryption process as follows: A = 1, B = 2 etc

C=3 D=4 E=5 F=6 ....

PT = F = 6

Encryption -

$CT = PT^E \bmod N$

$CT = 6^5 \bmod 119$

CT = 41

Decryption -

$PT = CT^D \bmod N$

RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

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

Encryption -

>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

1. P = 7, Q = 17
2. N = 7 * 17 = 119
3. (P – 1) * (Q – 1) = 6 * 16 = 96

   Let us choose the public key value of E as 5.

   E = 5 ⟶ Encryption Key (Public Key)
4. (D * E) mod (P – 1) * (Q – 1) = 1

   Let us choose D as 77 because (77 * 5) mod 96 = 385 mod 96 = 1

   D = 77 ⟶ Decryption Key (Private Key)

Based on the above values, consider an encryption and decryption process as follows: A = 1, B = 2 etc

C=3 D=4 E=5 F=6 ....

PT = F = 6

Encryption -

$CT = PT^E \bmod N$

$CT = 6^5 \bmod 119$

$CT = 41$

Decryption -

$PT = CT^D \bmod N$

$PT = 41^{77} \bmod 119$

$PT = 6$

RSA Algorithm - Asymmetric Cryptography Algorithm

Algorithm -

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

Encryption -

>> Calculate the cipher text CT from the plain text PT as follows: $CT = PT^E \bmod N$

Decryption -

>> Calculate the plain text PT from the cipher text CT as follows: $PT = CT^D \bmod N$

Example -

1. P = 7, Q = 17
2. N = 7 * 17 = 119
3. (P – 1) * (Q – 1) = 6 * 16 = 96

   Let us choose the public key value of E as 5.

   Alice

   E = 5 → Encryption Key (Public Key)
4. (D * E) mod (P – 1) * (Q – 1) = 1

   Let us choose D as 77 because (77 * 5) mod 96 = 385 mod 96 = 1

   Bob

   D = 77 → Decryption Key (Private Key)

Based on the above values, consider an encryption and decryption process as follows: A = 1, B = 2 etc

C=3 D=4 E=5 F=6 ....

PT = F = 6

Encryption -

$CT = PT^E \bmod N$

$CT = 6^5 \bmod 119$

CT = 41

Decryption -

$PT = CT^D \bmod N$

$PT = 41^{77} \bmod 119$

PT = 6

RSA Algorithm - Asymmetric Cryptography Algorithm

RSA Algorithm -

>> Ron Rivest, Adi Shamir and Len Adlemen developed the method called as RSA algorithm
>> Most popular and proven asymmetric key cryptography algorithm
>> Based on the mathematical fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product.