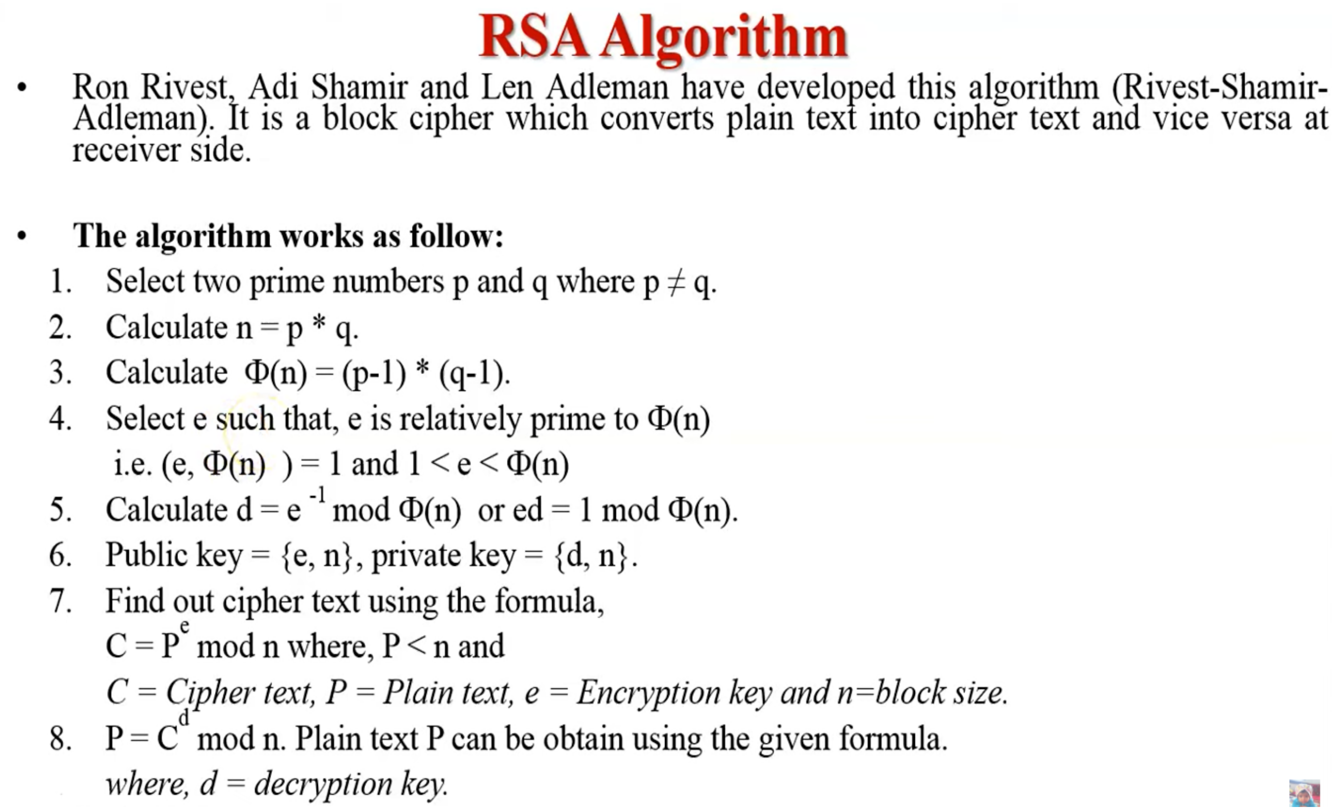
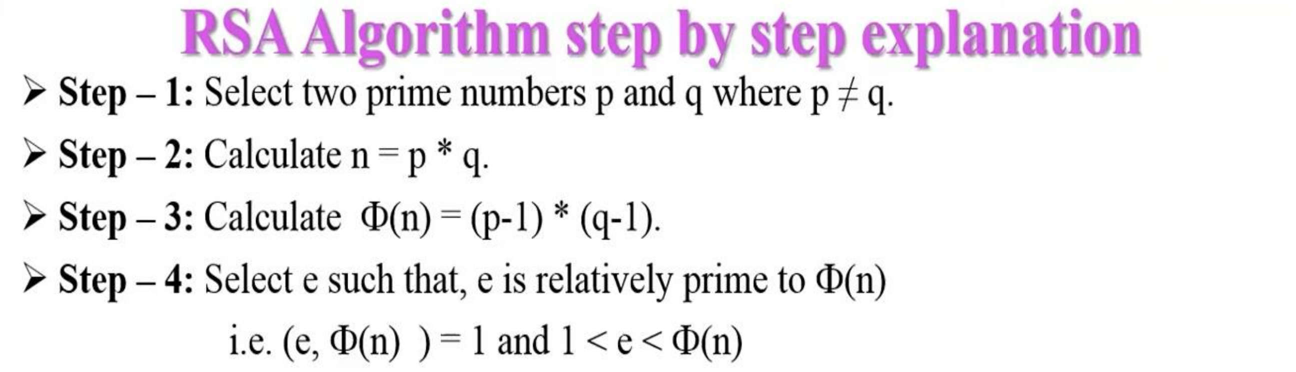


RSA Algorithm

- Ron Rivest, Adi Shamir and Len Adleman have developed this algorithm (Rivest-Shamir-Adleman). It is a block cipher which converts plain text into cipher text and vice versa at receiver side.

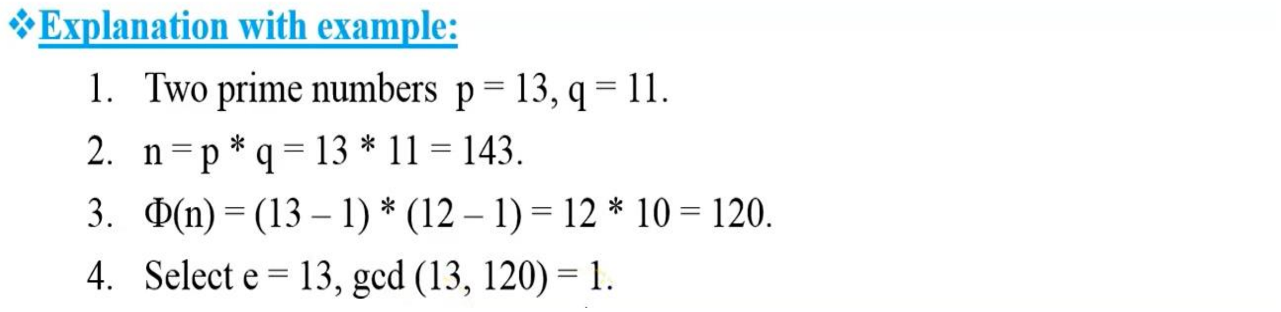
- **The algorithm works as follow:**
  1. Select two prime numbers p and q where $p \neq q$.
  2. Calculate $n = p * q$.
  3. Calculate $\Phi(n) = (p-1) * (q-1)$.
  4. Select e such that, e is relatively prime to $\Phi(n)$
     i.e. $(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$
  5. Calculate $d = e^{-1} \bmod \Phi(n)$ or $ed = 1 \bmod \Phi(n)$.
  6. Public key = {e, n}, private key = {d, n}.
  7. Find out cipher text using the formula,
     $C = P^e \bmod n$ where, $P < n$ and
     C = Cipher text, P = Plain text, e = Encryption key and n=block size.
  8. $P = C^d \bmod n$. Plain text P can be obtain using the given formula.
     where, d = decryption key.

- **It is a public key (Asymmetric) encryption technique.**
- **RSA key Can be typically 2024 or 2048 bits long.**



RSA Algorithm step by step explanation

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



❖Explanation with example:

1. Two prime numbers $p = 13, q = 11$.
2. $n = p * q = 13 * 11 = 143$.
3. $\Phi(n) = (13 – 1) * (12 – 1) = 12 * 10 = 120$.
4. Select $e = 13$, gcd $(13, 120) = 1$.

➢ **Step – 5:** Calculate $d = e^{-1} \bmod \Phi(n)$ or $ed = 1 \bmod \Phi(n)$.

❖Explanation with example:

5. Finding d:

➔ $e * d \bmod \Phi(n) = 1$

➔ $13 * d \bmod 120 = 1$

(How to find: $d * e = 1 \bmod \Phi(n)$ ➔ $d = ((\Phi(n) * i) + 1) / e$

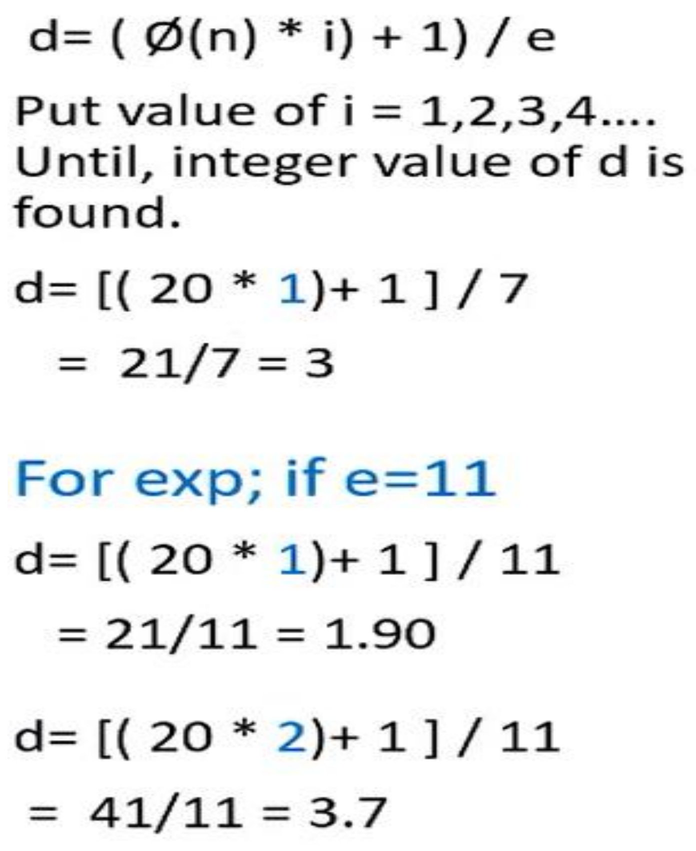
$d = (120 + 1) / 13 = 9.30$ ($\because i = 1$)

$d = (240 + 1) / 13 = 18.53$ ($\because i = 2$)

$d = (360 + 1) / 13 = 27.76$ ($\because i = 3$)

$d = (480 + 1) / 13 = 37$ ($\because i = 4$))

How to find D



d= (Ø(n) * i) + 1) / e

Put value of i = 1,2,3,4.... Until, integer value of d is found.

d= [(20 * 1)+ 1] / 7

= 21/7 = 3

For exp; if e=11

d= [(20 * 1)+ 1] / 11

= 21/11 = 1.90

d= [(20 * 2)+ 1] / 11

= 41/11 = 3.7

- **Step – 6:** Public key = {e, n}, private key = {d, n}.
- **Step – 7:** Find out cipher text using the formula,

  $C = P^{e} \bmod n$ where, $P < n$

  C = Cipher text, P = Plain text, e = Encryption key and n=block size.
- **Step – 8:** $P = C^{d} \bmod n$. Plain text P can be obtain using the given formula.

  where, d = decryption key.

❖Explanation with example:

6. Public key = {13, 143} and private key = {37, 143}.

7. **Encryption :** Plain text ***P = 13***. (where, $P < n$)

   $C = P^{e} \bmod n = 13^{13} \bmod 143 = 52$. $\boxed{C = 52}$

8. **Decryption:**

   $P = C^{d} \bmod n = 52^{37} \bmod 143 = 13$. $\boxed{P = 13}$

Exercise - 1

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

Solution:

1. Two prime numbers P=7, Q=17
2. n = P * Q = 17 * 7 = 119 **n = 119**
3. Φ(n) = (P–1) * (Q –1) = (17 – 1) * (7 – 1) = 16 * 6 = 96 **Φ(n) = 96**
4. Public key E = 5. **E= 5**
5. Calculate d = 77. d = ((Φ(n) * i) + 1) / e **d= 77**

   d = ((96*1)+1) / 5 = 19.4

   d = ((96*2)+1) / 5 = 38.6

   d = ((96*3)+1) / 5 = 57.8

   d = ((96*4)+1) / 5 = 77 (Stop finding d because getting integer value)
6. Public key = {e, n} = {5, 119}, private key = {d, n} = {77, 119}.
7. Plain text PT = 6, $CT = PT^{E} \bmod n = 6^{5} \bmod 119 = 41$. **Cipher Text = 41**
8. Cipher text CT = 41, $PT = CT^{d} \bmod n = 41^{77} \bmod 119 = 6$. **Plain Text = 6**

Exercise - 2

Question: In a public key cryptosystem 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 value of plain text?

Solution:

1. Two prime numbers $p = 5, q = 7$
2. $n = p * q = 5 * 7 = 35$ **n = 35**
3. $\Phi(n) = (p-1) * (q-1) = (5-1) * (7-1) = 4 * 6 = 24$ **Φ(n) = 24**
4. Public key $e = 11$. **e= 11**
5. Calculate $d = 11$. $d = ((\Phi(n) * i) + 1) / e$ **d= 11**
6. Public key = $\{e, n\} = \{11, 35\}$, private key = $\{d, n\} = \{11, 35\}$.
7. Plain text $P = 2$, $C = P^e \bmod n = 2^{11} \bmod 35 = 18$. **Cipher Text = 18**
8. Cipher text $C = 18$, $P = C^d \bmod n = 18^{11} \bmod 35 = 2$. **Plain Text = 2**

Exercise - 3

Question: P and Q are two prime numbers. P=17, and Q=11. Take public key E=7. If plain text value is 5, then what will be cipher text value & private key value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

1. Two prime numbers $p = 17, q = 11$
2. $n = p * q = 17 * 11 = 187$ **n = 187**
3. $\Phi(n) = (p-1) * (q-1) = (17-1) * (11-1) = 16 * 10 = 160$ **Φ(n) = 160**
4. Public key $e = 7$. **e= 7**
5. Calculate $d = 23$. $d = ((\Phi(n) * i) + 1) / e$ **d= 23**
6. Public key = $\{e, n\} = \{7, 187\}$, private key = $\{d, n\} = \{23, 187\}$.
7. Plain text $P = 5$, $C = P^e \bmod n = 5^7 \bmod 187 = 146$. **Cipher Text = 146**
8. Cipher text $C = 146$, $P = C^d \bmod n = 146^{23} \bmod 187 = 5$. **Plain Text = 5**

Exercise - 4

Question: P and Q are two prime numbers. P=3, and Q=11. Take public key E=3. If original message is 00111011, then what will be cipher text value & private key value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

1. Two prime numbers p = 3, q = 11
2. n = p * q = 3 * 11 = 33 **n = 33**
3. $\Phi(n) = (p-1) * (q-1) = (3-1) * (11-1) = 2 * 10 = 20$ **$\Phi(n) = 20$**
4. Public key e = 3. **e= 3**
5. Calculate d =7. d = (($\Phi(n)$ * i) + 1) / e **d= 7**
6. Public key = {e, n} = {3, 33}, private key = {d, n} = {7, 33}.
7. Plain text P = $(00111011)_2 = (59)_{10}$, C = P^e mod n = 59^3 mod 33 = 20. **Cipher Text = 20**
8. Cipher text C = 20, P = C^d mod n = 20^7 mod 33 = 26. **Plain Text = 26**

Exercise - 5

Question: P and Q are two prime numbers. P=13, and Q=17. Take public key E=19. If original message is 12, then what will be cipher text value & private key value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

1. Two prime numbers p = 13, q = 17
2. n = p * q = 13 * 17 = 221 **n = 221**
3. $\Phi(n) = (p-1) * (q-1) = (13-1) * (17-1) = 12 * 16 = 192$ **$\Phi(n) = 192$**
4. Public key e = 19. **e= 19**
5. Calculate d =91. d = (($\Phi(n)$ * i) + 1) / e **d= 91**
6. Public key = {e, n} = {19, 221}, private key = {d, n} = {91, 221}.
7. Plain text P = 12 , C = P^e mod n = 12^{19} mod 221 = 181. **Cipher Text = 181**
8. Cipher text C = 181, P = C^d mod n = 181^{91} mod 221 = 12. **Plain Text = 12**