CSE 4215

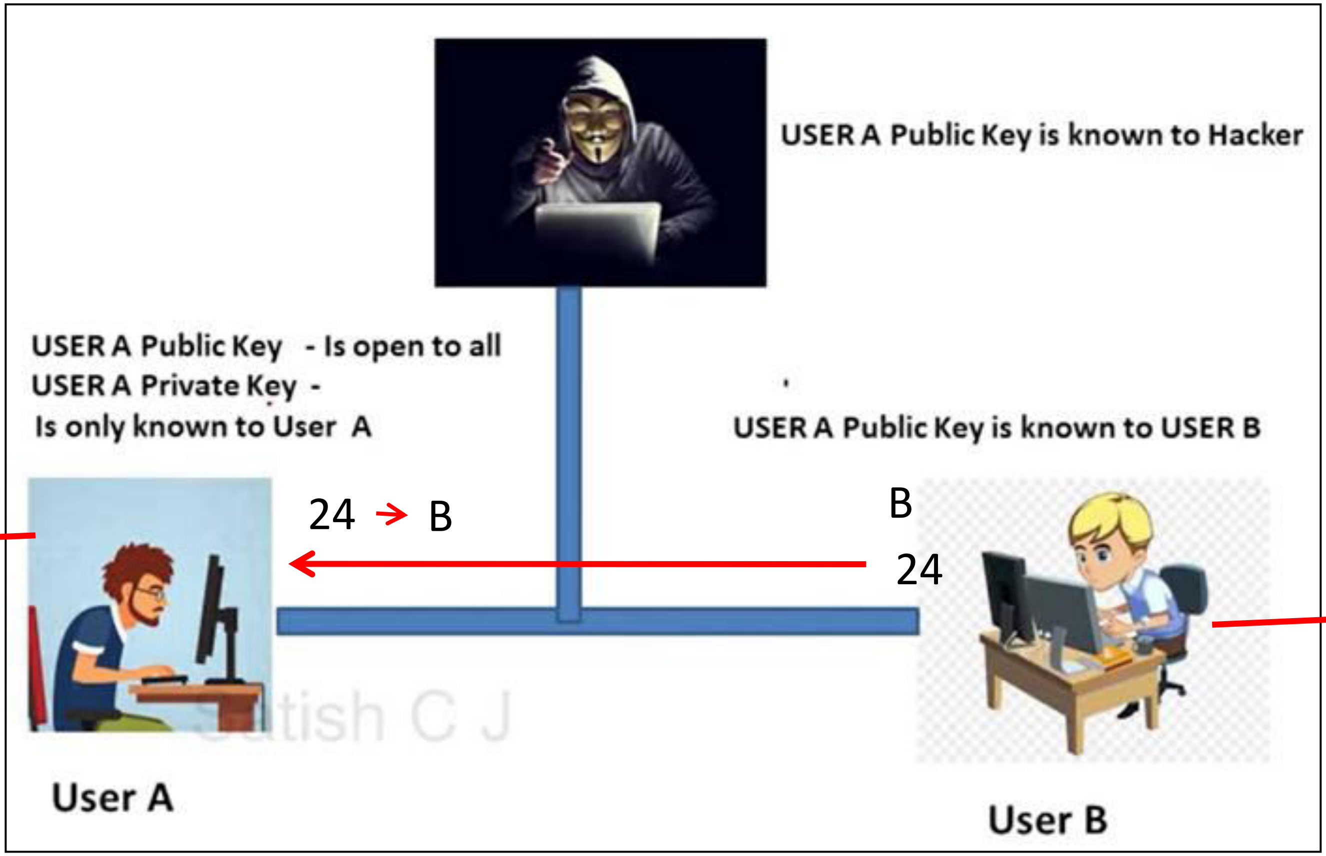
Chapter 3

RSA Algorithm

Lecture 9

Public Key Cryptography

User A decrypt the message using Private key



User B encrypt message using public key of user A. Suppose B is the message and 24 is the ciphertext

Suppose user A wants to communicate using insecured channel

But someone can try to access the data

Public Key Cryptography

- Public-key cryptography, or **asymmetric cryptography**, is a cryptographic system that uses pairs of keys:
- public keys, which may be disseminated widely, and
- private keys, which are known only to the owner.
- In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key.

Euler's Totient Function

- Denoted as $\Phi(n)$.
- $\Phi(n)$ = Number of positive integers less than 'n' that are relatively prime to n.

Example 1: Find $\Phi(5)$.

Solution:

Here n=5.

Numbers less than 5 are 1, 2, 3 and 4.

GCD	Relatively Prime?
GCD (1, 5) = 1	✓
GCD (2, 5) = 1	✓
GCD (3, 5) = 1	✓
GCD (4, 5) = 1	✓

$\therefore \Phi(5) = 4.$

Example 2: Find $\Phi(11)$.

Solution:

Here n=11.

Numbers less than 11 are 1, 2, 3, 4, 5, 6, 7, 8, 9 and 10.

GCD	Relatively Prime?
GCD (1, 11) = 1	✓
GCD (2, 11) = 1	✓
GCD (3, 11) = 1	✓
GCD (4, 11) = 1	✓
GCD (5, 11) = 1	✓

GCD	Relatively Prime?
GCD (6, 11) = 1	✓
GCD (7, 11) = 1	✓
GCD (8, 11) = 1	✓
GCD (9, 11) = 1	✓
GCD (10, 11) = 1	✓

$\therefore \Phi(11) = 10.$

Euler’s Totient Function

- Denoted as $\Phi(n)$.
- $\Phi(n)$ = Number of positive integers less than ‘n’ that are relatively prime to n.

Example 3: Find $\Phi(8)$.

Solution:

Here n=8.

Numbers less than 8 are 1, 2, 3, 4, 5, 6, and 7.

GCD	Relatively Prime?
GCD (1, 8) = 1	✓
GCD (2, 8) = 2	✗
GCD (3, 8) = 1	✓
GCD (4, 8) = 4	✗

GCD	Relatively Prime?
GCD (5, 8) = 1	✓
GCD (6, 8) = 2	✗
GCD (7, 8) = 1	✓

$\therefore \Phi(8) = 4$.

If n is prime then $\Phi(n)=n-1$

Multiplicative Inverse

$5 \times 5^{-1} = 1$

$5 \times \frac{1}{5} = 1$

$A \times \frac{1}{A} = 1$

1/5 is multiplicative inverse of 5

Under mod n

$A \times A^{-1} \equiv 1 \bmod n$

$3 \times ? \equiv 1 \bmod 5$

$3 \times 2 \equiv 1 \bmod 5$ — 2 is the Multiplicative Inverse of 3 mod 5

$2 \times ? \equiv 1 \bmod 11$

$2 \times 6 \equiv 1 \bmod 11$ — 6 is the Multiplicative Inverse of 2 mod 11

$4 \times ? \equiv 1 \bmod 5$

$4 \times 4 \equiv 1 \bmod 5$ — 4 is the Multiplicative Inverse of 4 mod 5

$5 \times ? \equiv 1 \bmod 10$ — No MI as 5 & 10 are not relatively prime

Modular Exponentiation

Example 1

Solve 23^3 mod 30.

23^3 mod 30 = -7^3 mod 30 || 23 mod 30 can be 23 or -7.
= -7^3 mod 30
= -7^2 x -7 mod 30
= 49 x -7 mod 30
= -133 mod 30
= -13 mod 30
= 17 mod 30

23^3 mod 30 = 17

Example 2

Solve 31^{500} mod 30.

31^{500} mod 30 = 1^{500} mod 30
= 1 mod 30
= 1

31^{500} mod 30 = 1

Example 3

Solve 242^{329} mod 243.

242^{329} mod 243 = -1^{329} mod 243
= -1^{329} mod 243 || -1^{328} x -1^1
= -1 mod 243
= 242

242^{329} mod 243 = 242

Example 4

Solve 11^7 mod 13.

11^7 mod 13 = 11 mod 13 x 11 mod 13 x 11 mod 13 x 11 mod 13 x 11 mod 13 x 11 mod 13 x 11 mod 13
= -2 x -2 x -2 x -2 x -2 x -2 x -2 mod 13
= -128 mod 13
= -11 mod 13
= 2

11^7 mod 13 = 2

Modular Exponentiation (extended)

Example 1

Solve 88^7 mod 187.

$88^1 \bmod 187 = 88$

$88^2 \bmod 187 = 88^1 \times 88^1 \bmod 187 = 88 \times 88 = 7744 \bmod 187 = 77$

$88^4 \bmod 187 = 88^2 \times 88^2 \bmod 187 = 77 \times 77 = 5929 \bmod 187 = 132$

$88^7 \bmod 187 = 88^4 \times 88^2 \times 88^1 \bmod 187 = (132 \times 77 \times 88) \bmod 187$

$= 894{,}432 \bmod 187$

$88^7 \bmod 187 = 11$

Example 2

What is "the last two digits" of 29^5?

$29^1 \bmod 100 = 29$ or -71

$29^2 \bmod 100 = 29^1 \times 29^1 \bmod 100 = 29 \times 29 = 841 \bmod 100 = 41$ or -59

$29^4 \bmod 100 = 29^2 \times 29^2 \bmod 100 = 41 \times 41 = 1681 \bmod 100 = 81$ or -19

$29^5 \bmod 100 = 29^4 \times 29^1 \bmod 100$

$= -19 \times 29 \bmod 100$

$= -551 \bmod 100$

$= -51 \bmod 100$

$= 49$

$88^7 \bmod 187 = 49$

Example 3

Solve 3^{100} mod 29.

$3^1 \bmod 29 = 3 \bmod 29 = 3$ or -26.

$3^2 \bmod 29 = 3^1 \times 3^1 \bmod 29 = 3 \times 3 \bmod 29 = 9 \bmod 29 = 9$ or -20.

$3^4 \bmod 29 = 3^2 \times 3^2 \bmod 29 = 9 \times 9 \bmod 29 = 81 \bmod 29 = 23$ or -6.

$3^8 \bmod 29 = 3^4 \times 3^4 \bmod 29 = -6 \times -6 \bmod 29 = 36 \bmod 29 = 7$ or -22.

$3^{16} \bmod 29 = 3^8 \times 3^8 \bmod 29 = 7 \times 7 \bmod 29 = 49 \bmod 29 = 20$ or -9.

$3^{32} \bmod 29 = 3^{16} \times 3^{16} \bmod 29 = -9 \times -9 \bmod 29 = 81 \bmod 29 = 23$ or -6.

$3^{64} \bmod 29 = 3^{32} \times 3^{32} \bmod 29 = -6 \times -6 \bmod 29 = 36 \bmod 29 = 7$ or -22.

$3^{100} \bmod 29 = 3^{64} \times 3^{32} \times 3^4 \bmod 29.$

$= 7 \times -6 \times -6 \bmod 29$

$= 252 \bmod 29$

$3^{100} \bmod 29 = 20$

Example 4

Solve 23^{16} mod 30

$23^{16} \bmod 30 = (((23^2)^2)^2)^2 \bmod 30$

$= (((-7^2)^2)^2)^2 \bmod 30$

$= ((49^2)^2)^2 \bmod 30$

$= ((19^2)^2)^2 \bmod 30$

$= ((-11^2)^2)^2 \bmod 30$

$= (121^2)^2 \bmod 30$

$= (1^2)^2 \bmod 30$

$= 1 \bmod 30$

$23^{16} \bmod 30 = 1$

RSA Algorithm

- **RSA** (Rivest–Shamir–Adleman) is an **algorithm** used to encrypt and decrypt messages.
- This algorithm was described in 1977.
- It is an asymmetric cryptographic **algorithm**. Asymmetric means that there are two different keys.
- This is also called public key cryptography, because one of the keys can be given to anyone.

RSA Algorithm

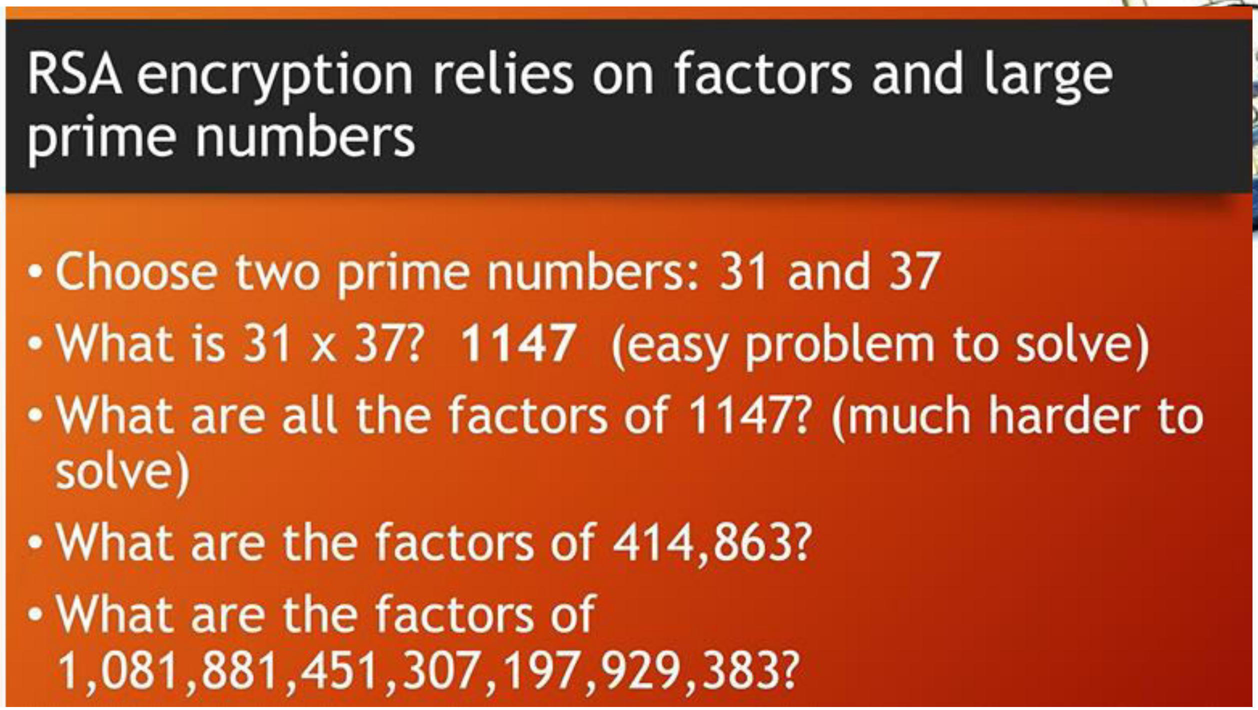
If it is asked that what the prime factors of 35?

The answer is very easy and simple, it is 5 & 7 because the number is very small but consider the following 256 digit number, it is very difficult, the RSA algorithm is based on this

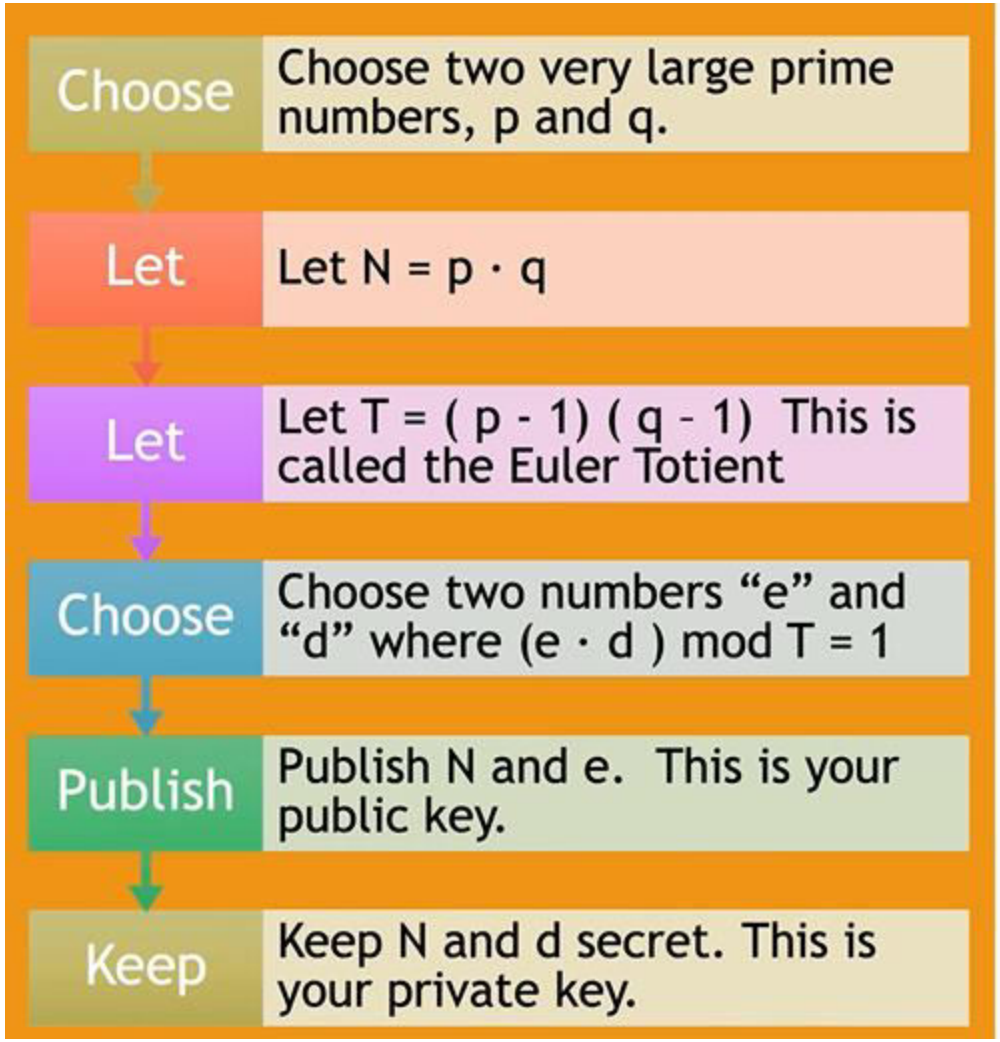
What is the prime factors of 256?

2140324650240744961264423072839333563008614715144755017797754920881418023447
1401366433455190958046796109928518724709145876873962619215573630474547705208
0511905649310668769159001975940569345745223058932597669747168173806936489469
9871578494975937497937

It is very difficult to find prime factors



RSA Algorithm



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.

RSA Algorithm

- **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: $d * e = 1 \bmod \Phi(n)$ → $d = ((\Phi(n) * i) + 1) / e$
   $d = (120 + 1) / 13 = 9.30$ ($\because i = 1$)
   $d = (240 + 1) / 13 = 18.53$ ($\because i = 2$)
   $d = (360 + 1) / 13 = 27.76$ ($\because i = 3$)
   $d = (480 + 1) / 13 = 37$ ($\because i = 4$))

- **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.

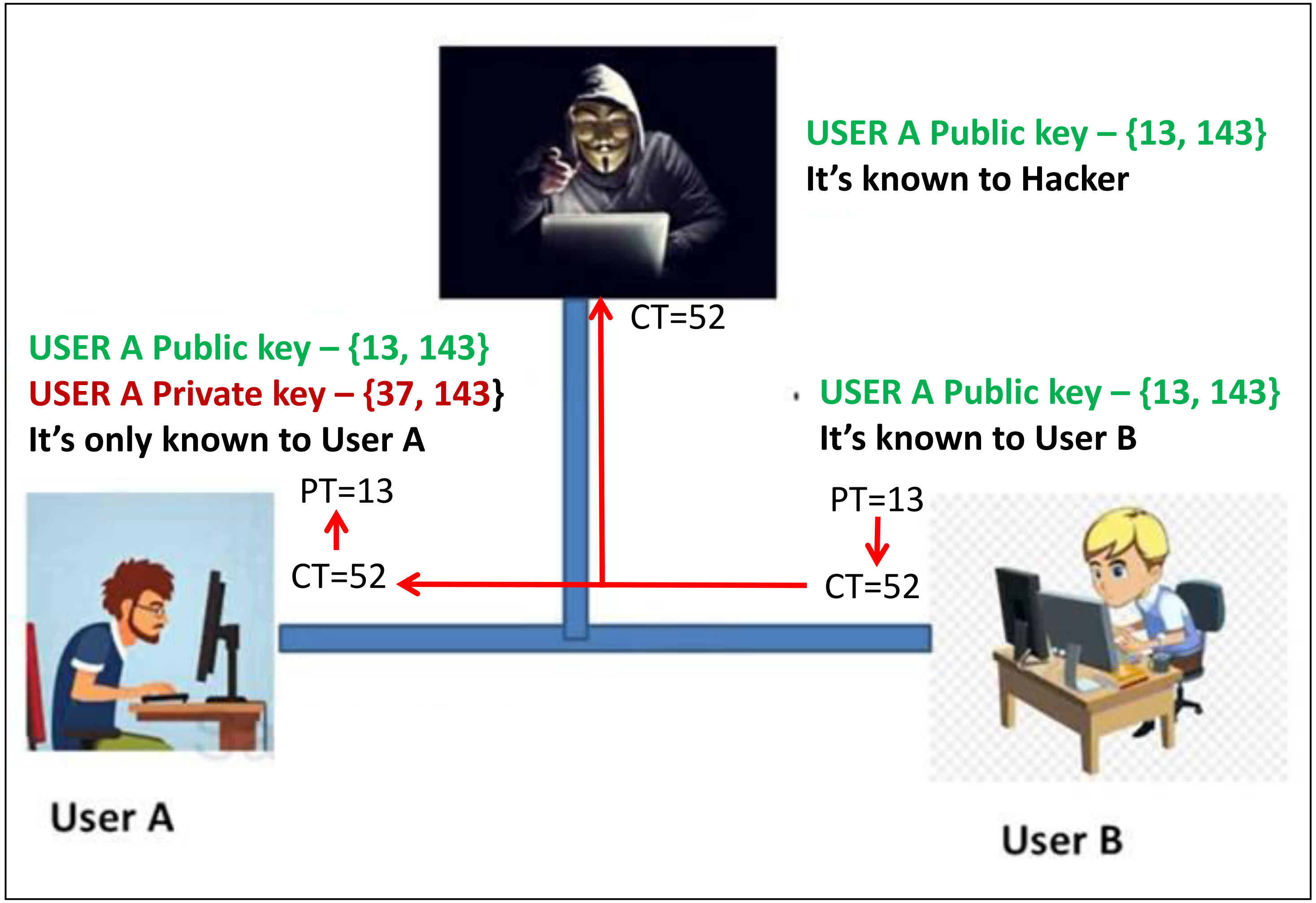
❖ **Explanation with example:**

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

Test the result online use the link

https://umaranis.com/rsa_calculator_demo.html

RSA Algorithm



Hacker doesn't have private key to decrypt the message

RSA Algorithm

If it is asked that what the prime factors of 35?

The answer is very easy and simple, it is 5 & 7 because the number is very small but consider the following 256 digit number, it is very difficult, the RSA algorithm is based on this

2140324650240744961264423072839333563008
6147151447550177977549208814180234471
4013664334551909580467961099285187247091
4587687396261921557363047454770520805
1190564931066876915900197594056934574
5223058932597669747168173806936489469
9871578494975937497937

RSA Algorithm

2140324650240744961264423072839333563008
614715144755017797754920881418023447
1401366433455190958046796109928518724709
14587687396261921557363047454770520805
1190564931066876915900197594056934574
52230589325976697471681738069364894699
87157849497593749793 7

RSA-250 =
6413528947707158027879019017057738908482501474294344720811685963202
453234463 0238623598752668347708737661925585694639798853367
×
3337202759497815655622601060535511422794076034476755466678452098702
384172921 0037080257448673296881877565718986258036932062711

Very difficult the big prime numbers

The more bigger prime number makes more difficult for Hacker to decrypt

Go to the website for RSA factoring challenge
https://en.wikipedia.org/wiki/RSA_Factoring_Challenge

End