Experiment 5: RSA algorithm

Aim: Write a program to implement RSA algorithm.

Learning Outcomes:

After completion of this experiment, student should be able to

1. Differentiate between symmetric and asymmetric key cryptography.
2. Describe working of RSA algorithm.
3. Understand application of RSA along with its advantage and limitations.

Theory:

Algorithm for RSA is given below.

- Choose two large prime numbers p, q
  - Let $n = pq$; then $\phi(n) = (p–1)(q–1)$
  - Choose $e < \phi(n)$ such that e is relatively prime to $\phi(n)$.
  - Compute d such that $ed \bmod \phi(n) = 1$
- Public key: (e, n); private key: (d,n)
- Encipher: $c = m^e \bmod n$
- Decipher: $m = c^d \bmod n$

Example:

- Take $p = 7$, $q = 11$, so $n = 77$ and $\phi(n) = 60$
- Alice chooses $e = 17$, making $d = 53$
- Bob wants to send Alice secret message HELLO (07 04 11 11 14)
  - $07^{17} \bmod 77 = 28$
  - $04^{17} \bmod 77 = 16$
  - $11^{17} \bmod 77 = 44$
  - $11^{17} \bmod 77 = 44$
  - $14^{17} \bmod 77 = 42$
- Bob sends 28 16 44 44 42
- Alice receives 28 16 44 44 42
- Alice uses private key, $d = 53$, to decrypt message:
  - $28^{53} \bmod 77 = 07$
  - $16^{53} \bmod 77 = 04$
  - $44^{53} \bmod 77 = 11$
  - $44^{53} \bmod 77 = 11$
  - $42^{53} \bmod 77 = 14$
- Alice translates message to letters to read HELLO

Procedure:

1. Write a program to implement RSA algorithm.
2. Accept two integer numbers from user.
3. Validate the input provided by user is a prime number. If not, ask user to reenter prime number.
4. Generate public key and private key.
5. Display public key.
6. Ask user to input message for encryption.
7. Display the cipher text.
8. Ask user to input cipher text for decryption.

9. Display the plain text.
10. Create a word document for your observation and answer the following questions. Upload your document on Student Portal along with your code.

Note: Code should have proper comments

Questions:

1. Compare and contrast symmetric key encryption and asymmetric key encryption.
2. Explain few of the application of RSA.
3. List advantages and limitations of RSA?
4. What are the more popular values of e in practice? Why?
5. Why decryption using RSA takes more time as compared to encryption?