

Experiment No 3

Aim : Implementation and analysis of RSA cryptosystem and digital signature scheme using RSA.

Lab Outcome :

LO2 : Demonstrate Key management, distribution and user authentication.

Theory :

1. Explain the steps of RSA key generation?

RSA (Rivest-Shamir-Adleman) is a widely used asymmetric cryptographic algorithm that relies on a pair of keys: a public key and a private key. RSA key generation involves a series of steps that ensure secure communication and data encryption. Below, I'll provide a detailed explanation of the key generation process:

1. Choosing Prime Numbers (p and q): The first step in RSA key generation is to select two distinct prime numbers, usually denoted as p and q. These prime numbers are critical to the security of the algorithm. They need to be large and chosen randomly to prevent attackers from factoring the modulus and breaking the encryption.
2. Calculating Modulus (n): The modulus (n) is computed as the product of the two prime numbers: $n = p * q$. The modulus is used in both the public and private keys. It provides the size of the "space" in which the encryption operates, making the encryption stronger with larger values of n.
3. Calculating Euler's Totient Function ($\phi(n)$): Euler's totient function ($\phi(n)$) is calculated as $\phi(n) = (p - 1) * (q - 1)$. This function is crucial for ensuring that the public and private keys are relatively prime. $\phi(n)$ represents the count of numbers less than n that are coprime to n.
4. Selecting Public Exponent (e): The public exponent (e) is a small odd integer that is coprime to $\phi(n)$. A common choice for e is 65537 ($2^{16} + 1$). This choice of e provides good security properties while ensuring efficient encryption and decryption operations.
5. Calculating Private Exponent (d): The private exponent (d) is computed as the modular multiplicative inverse of e modulo $\phi(n)$. In other words, it satisfies the equation $(e * d) \% \phi(n) = 1$. The private exponent d is what allows the decryption of messages encrypted with the public key.

6. **Public Key Generation:** The public key consists of the pair (e, n) . It is distributed to anyone who wishes to send an encrypted message to the key owner. The public key is used for encrypting messages, ensuring only the private key holder can decrypt them.
7. **Private Key Generation:** The private key consists of the pair (d, n) . This key must be kept secret and secure. The private key is used for decrypting messages encrypted with the corresponding public key. Losing the private key could compromise the security of encrypted communications.

The RSA key generation process is fundamental to the security and effectiveness of RSA encryption. It leverages the mathematical properties of prime numbers and modular arithmetic to create a secure communication channel between parties. The strength of RSA lies in the difficulty of factoring large semiprime numbers (the product of two large prime numbers), which makes it practically impossible for attackers to deduce the private key from the public key.

2. Explain the steps of Digital signature generation and verification process:

Digital signatures play a crucial role in ensuring data integrity, authenticity, and nonrepudiation in the digital world. They provide a way to verify that a digital document or message was indeed generated by a specific sender and has not been tampered with during transmission. The process involves two main steps: digital signature generation and digital signature verification.

Digital Signature Generation:

1. **Hashing the Message:** The sender begins by creating a cryptographic hash of the message they want to sign. A hash function, such as SHA-256, is used to produce a fixed-size digest that uniquely represents the content of the message.
2. **Private Key Encryption:** The sender then encrypts the hash value using their private key. This encrypted hash forms the digital signature. The use of the private key ensures that only the sender, who possesses the corresponding private key, can create the signature.
3. **Attaching the Signature:** The encrypted hash (digital signature) is attached to the original message. This combination forms the digitally signed message. Any alteration to the message will result in a different hash, making it evident that the message has been tampered with.

Digital Signature Verification:

1. Hashing the Received Message: The recipient of the digitally signed message starts by computing the hash value of the received message using the same hash function as the sender. This generates a digest that represents the content of the received message.
2. Public Key Decryption: The recipient then decrypts the digital signature using the sender's public key. This process yields the original hash value that the sender encrypted using their private key during the signature generation.
3. Comparing Hashes: The recipient compares the decrypted hash value with the hash value they calculated from the received message. If the two hash values match, it indicates that the message has not been tampered with and that the signature is valid. A mismatch suggests either tampering or the use of an incorrect signature.

Benefits and Security:

The digital signature process provides several benefits:

- Data Integrity: Any alteration to the message or document will lead to a mismatch between the computed hash and the decrypted hash in the signature.
- Authenticity: The use of the sender's private key ensures that only the sender could have created the signature.
- Non-Repudiation: The sender cannot deny having sent the digitally signed message since the signature is tied to their private key.

Output:

Name: Aman Singh

Batch : T23

Roll No: 128

Digital Signature:

Document x WhatsApp x PlayFair Cipher - Online x Vigenere Cipher - Online x Virtual Labs x

cse29-iiith.vlabs.ac.in/exp/digital-signatures/simulation.html

Digital Signatures Scheme

Digitally sign the plaintext with Hashed RSA.

Plaintext (string):

attackpostponed SHA-1

Hash output(hex):

d1852d8bfb03f7450fbecdb69742ec9f16af37f3

Input to RSA(hex):

d1852d8bfb03f7450fbecdb69742ec9f16af37f3 Apply RSA

Digital Signature(hex):

31b4ef479d501506cdfed8dcea64037e20ddf844ef32df7f1dc479570d648211
1646ad07ed40fe6eaf3b9b6e66fc82df6a2c840928528dafbe13574cd61533e

Digital Signature(base64):

MbTVR51QFQbN/tjc6mQDFiDd+ETvMt9/HcR5Vw1kghEWRq3wftQP5urzubmb8gt
9qLIQJKFNr74TV0zWFTPg==

28°C Partly cloudy Search 23:52 25-08-2023

Document x WhatsApp x PlayFair Cipher - Online x Vigenere Cipher - Online x Virtual Labs x

cse29-iiith.vlabs.ac.in/exp/digital-signatures/simulation.html

Digital Signatures Scheme

Digital Signature(hex):

31b4ef479d501506cdfed8dcea64037e20ddf844ef32df7f1dc479570d648211
1646ad07ed40fe6eaf3b9b6e66fc82df6a2c840928528dafbe13574cd61533e

Digital Signature(base64):

MbTVR51QFQbN/tjc6mQDFiDd+ETvMt9/HcR5Vw1kghEWRq3wftQP5urzubmb8gt
9qLIQJKFNr74TV0zWFTPg==

Status:

Time: 4ms

RSA public key

Public exponent (hex, F4=0x10001):

3

Modulus (hex):

BC86E3DC782C446EE756B874ACECF2A115F613021EAF1ED5EF295BEC28ED899D
26FE2EC896BF9DE84FE381AF67A7B7CB848D85235E72AB595ABF8FE840D5F8DB

1024 bit 1024 bit (e=3) 512 bit 512 bit (e=3)

28°C Partly cloudy Search 23:52 25-08-2023

Name: Aman Singh

Batch : T23

Roll No: 128

RSA key generation and decode

The screenshot shows the 'Public-Key Cryptosystems (PKCSv1.5)' simulation interface. The browser address bar displays 'cse29-iiith.vlabs.ac.in/exp/pkcs/simulation.html'. The interface includes a sidebar with a menu icon and the Virtual Labs logo. The main content area displays the following parameters for key generation:

- Private exponent (hex):
7daf4292fac82d9f44e47af87348a1c0b9440cac1474bf394a1b929d729e5bbc
f402f29a9300e11b478c091f7e5dacd3f8edae2effe3164d7e0eeada87ee817b
- P (hex):
ef3fc61e21867a900e01ee4b1ba69f5403274ed27656da03ed88d7902cce693f
- Q (hex):
c9b9fcc298b7d1af568f85b50e749539bc01b10a68472fe1302058104821cd65
- D mod (P-1) (hex):
9f7fd9696baefc6009569edcbd19bf8d576f89e1a439e6ad4905e50ac8899b7f
- D mod (Q-1) (hex):
867bffd7107a8bca39b503ce09a30e267d567606f02f7540cac03ab5856bde43
- 1/Q mod P (hex):
412d6b551d93ee1bd7dcca63d7a6d031fc66035ecc630dd7f5f949a378cd9d

The Windows taskbar at the bottom shows the system clock as 23:43 on 25-08-2023, with a temperature of 28°C and 'Partly cloudy' weather.

The screenshot shows the 'Public-Key Cryptosystems (PKCSv1.5)' simulation interface. The browser address bar displays 'cse29-iiith.vlabs.ac.in/exp/pkcs/simulation.html'. The interface includes a sidebar with a menu icon and the Virtual Labs logo. The main content area displays the following information:

- A 'decrypt' button is visible.
- Decrypted Plaintext (string):
chandrayaanisland
- Status:
Decryption Time: 4ms
- RSA private key**
 - Buttons: 1024 bit, 1024 bit (e=3), 512 bit, 512 bit (e=3), Generate, bits = 512
 - Modulus (hex):
BC86E3DC782C446EE7560874ACECF2A115E613021EAF1ED5EF295BEC2BED899D
26FE2EC8968F9DE84FE381AF67A7B7C8B48D85235E72AB595ABF8FE840D5F8DB
 - Public exponent (hex, F4=0x10001):
3
 - Private exponent (hex):
7daf4292fac82d9f44e47af87348a1c0b9440cac1474bf394a1b929d729e5bbc
f402f29a9300e11b478c091f7e5dacd3f8edae2effe3164d7e0eeada87ee817b

The Windows taskbar at the bottom shows the system clock as 23:43 on 25-08-2023, with a temperature of 28°C and 'Partly cloudy' weather.

Name: Aman Singh

Batch : T23

Roll No: 128

The screenshot shows a web browser window with the URL `cse29-iiith.vlabs.ac.in/exp/pkcs/simulation.html`. The page title is "Public-Key Cryptosystems (PKCSv1.5)". The interface includes the following sections:

- Plaintext (string):** A text input field containing "chandraanislanded" and an "encrypt" button.
- Ciphertext (hex):** A text input field containing the hexadecimal string "714804a48356c44f88d6e546ea716ce84ed9138718330fb914f90922887f9b8d3afe405eadcd12e8acf21a3043ace8ed37640edc56f2f50cb8b56b924c5ef73b" and a "decrypt" button.
- Decrypted Plaintext (string):** A text input field containing "chandraanislanded".
- Status:** A text input field containing "Decryption Time: 4ms".
- RSA private key:** A section with buttons for "1024 bit", "1024 bit (e=3)", "512 bit", and "512 bit (e=3)", a "Generate" button, and a "bits = 512" label.
- Modulus (hex):** A text input field.

The bottom of the browser window shows a Windows taskbar with various application icons, a search bar, and system tray information including "28°C Partly cloudy", "ENG IN", and the date "25-08-2023".

Conclusion:

Learnt about RSA scheme and RSA cryptosystem , explored steps involved in digital key generation and verification , generated and verified digital signature using software and also implemented RSA scheme.

Name: Aman Singh

Batch : T23

Roll No: 128