Experiment No.16

B. Encrypt and Decrypt message using key pair

Theoretical Background

What is Encryption

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting plaintext to ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of an encryption key: a set of mathematical values that both the sender and the recipient of an encrypted message know.

What is Decryption

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

Public key Encryption

When the two parties communicate to each other to transfer the intelligible or sensible message, referred to as plaintext, is converted into apparently random nonsense for security purpose referred to as cipher text. The process of changing the plaintext into the cipher text is referred to as encryption. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext. Once the cipher text is produced, it may be transmitted.

Public key Decryption

The process of changing the cipher text to the plaintext that process is known as decryption. Asymmetric is a form of Cryptosystem in which encryption and decryption are performed using different keys-Public key (known to everyone) and Private key (Secret key). This is known as Public Key Encryption.

Private key Encryption

In an age where breaches occur daily, businesses need to protect confidential information including customer data, intellectual property, research and development, future business plans, and all sorts of other information. Confidential information needs to be secured at rest, as well as when it is exchanged between employees, executives, partners, and others, via phone call, text

message or email. Data is secured in many different ways, one of which is private key encryption. What, exactly, is private key encryption.

Private key Decryption

A private key, also known as a secret key, is a variable in cryptography that is used with an algorithm to encrypt and decrypt code. Secret keys are only shared with the key's generator, making it highly secure. Private keys play an important role in symmetric cryptography, asymmetric cryptography and cryptocurrencies.

There are two types of Encryption and Decryption:

1. **Symmetric Encryption/Decryption**

Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages. By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original and understandable form. The secret key that the sender and recipient both use could be a specific password/code or it can be random string of letters or numbers that have been generated by a secure random number generator (RNG).

2. **Asymmetric Encryption/Decryption**

Asymmetric Encryption is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt. Frequently (but not necessarily), the keys are interchangeable, in the sense that if key A encrypts a message, then B can decrypt it, and if key B encrypts a message, then key A can decrypt it. While common, this property is not essential to asymmetric encryption. Asymmetric Encryption is also known as Public Key Cryptography, since users typically create a matching key pair, and make one public while keeping the other secret. Users can "sign" messages by encrypting them with their private keys. This is effective since any message recipient can verify that the user's public key can decrypt the message, and thus prove that the user's secret key was used to encrypt it. If the user's secret key is, in fact, secret, then it follows that the user, and not some impostor, really

sent the message. Users can send secret messages by encrypting a message with the recipient's public key.

Conclusion

We have conclude that how should we perform Encrypt and Decrypt using key pair in windows 7 operating system.

Exercise

1. What is meant by Encryption?
2. What is meant by Decryption?
3. What is Public key and Private Key?

Answers

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Marks obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total(25)**	

Network and Information Security(22620)