WRITEUP

Prathik Kallepalli - pkallepa

February 27, 2023

1 Introduction

In this document, I will discuss my concerns, learning's, and achievements that I learned from this assignment.

2 Public-Private Cryptography in today's world

Public-private cryptography, also known as asymmetric cryptography, has many applications in modern technology and communication. It enables secure communication and authentication between parties over insecure networks, such as the internet.

Here are some of the major applications of public-private cryptography:

1. Secure communication: Public-private cryptography is used in many applications for secure communication, such as email encryption, secure messaging apps, and virtual private networks (VPNs). By encrypting messages using a recipient's public key, only the intended recipient can decrypt and read the message using their private key.

2. Digital signatures: Public-private cryptography is used for digital signatures, which are used to verify the authenticity and integrity of digital documents and transactions. A digital signature is created using the sender's private key, and can be verified using the sender's public key.

3. Secure online transactions: Public-private cryptography is used to secure online transactions, such as e-commerce purchases and online banking. SSL/TLS, the security protocol used to secure web connections, uses public-private cryptography to establish a secure connection between a web server and a client.

4. Access control: Public-private cryptography can be used for access control, such as secure authentication for remote access to computer systems, secure login to websites, and secure access to physical locations.

Overall, public-private cryptography has revolutionized the way we communicate and do business online, and has made it possible to secure sensitive information and transactions in a world where cyber threats are a constant threat. Its applications are wide-ranging, from secure communication to secure online transactions and access control, and it continues to play a vital role in shaping the future of technology and communication.

3 Key Generation

The SS algorithm generates a pair of keys - a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret. The public key is used for encrypting messages, while the private key is used for decrypting them.

4 Encryption

In public key cryptography, the sender uses the recipient's public key to encrypt the message. This encrypted message can only be decrypted using the recipient's private key.

5 Digital signatures

Public key cryptography can also be used to create digital signatures. The sender uses their private key to encrypt a hash of the message. The recipient can then use the sender's public key to verify the signature by decrypting the hash and comparing it to the hash of the message.

6 Popular Applications of Public-Private Cryptography

1. Secure communication: Public key cryptography is widely used to secure communication over insecure networks like the internet. SSL/TLS, SSH, and PGP are some of the popular protocols that use public key cryptography.
2. Digital signatures: Digital signatures are widely used to authenticate digital documents, contracts, and transactions. For example, when you sign a document electronically, the document is hashed and encrypted with your private key, and the recipient can verify the signature using your public key.
3. Secure online transactions: Public key cryptography is used to secure online transactions like online shopping, banking, and payment processing. For example, when you make an online payment, your credit card information is encrypted using the merchant's public key and can only be decrypted using their private key.

Personally I use cryptogtography on a daily base as I use many applications and websites that require my login information as it is securing a lot of my personal information.