CSE 13S: Assignment 5 Write-Up

Johnny Li

February 26, 2023

1 Introduction

SS and RSA are a type of cryptography that involves the use of a pair of public and private keys to encrypt and decrypt messages. The public key can be shared with anyone without compromising the private key, whereas the private key is kept secret. Due to the math behind it (P=?NP) it's much easier to encrypt information using the key than it is to decrypt it without the keys. The system works by encrypting messages using the public key, which can then only be decrypted using the private key. This allows for secure communication between two parties, as only the intended recipient can decrypt the message.

During the exploration of public-private cryptography, we delved into the specific implementation of the RSA/SS algorithms. We learned that RSA is one of the most commonly used algorithms in public-private cryptography due to its strength and efficiency. While there are other encryption methods which are harder to break, RSA strikes a good balance between speed and security.

Generating the keys necessary for RSA encryption and decryption requires the generation of two large prime numbers. These numbers are multiplied to produce a number that serves as the modulus for the public and private keys. The public key consists of the modulus and a smaller number known as the public exponent. The private key, on the other hand, consists of the modulus and a larger number known as the private exponent.

Once the keys have been generated, messages can be encrypted and decrypted using these keys. The encryption process involves converting the message into a numerical form and raising it to the power of the public exponent, modulo the modulus. The resulting ciphertext can only be decrypted by raising it to the power of the private exponent, modulo the modulus.

In addition to encrypting and decrypting messages, we also learned how to apply this system to files. By encrypting a file with the public key, only the holder of the private key can decrypt the file and access its contents. This is particularly useful in situations where sensitive information needs to be shared securely between two parties.

2 Applications of Public-Private Cryptography

Public-private cryptography has become an essential tool for ensuring secure communication and data protection in the digital age. In this regard, public-private cryptography finds its use in various applications, ranging from e-commerce to online banking, secure communication, and data storage.

One of the significant applications of public-private cryptography is in the field of e-commerce, where secure online transactions are essential. By using public-private cryptography, online stores and businesses can securely transmit sensitive information, such as credit card details, from the customer to the merchant. The customer's sensitive information is encrypted with the merchant's public key, ensuring that only the intended recipient can decrypt and access the information.

Another critical application of public-private cryptography is in online banking, where the safety of sensitive financial information is crucial. Online banking platforms employ public-private cryptography to secure their transactions, ensuring that the financial information of customers is well-protected. This is accomplished by encrypting the sensitive information with the bank's public key, which can only be decrypted by the bank's private key.

Secure communication is another application of public-private cryptography. End-to-end encryption, for instance, relies on public-private cryptography to provide secure communication. End-to-end encryption ensures that only the intended recipient can decrypt a message, even if the message is intercepted by an attacker.

Public-private cryptography is also employed in data storage to protect sensitive information. Data encryption ensures that sensitive information stored in the cloud or on a device is not easily accessible to unauthorized persons. The encryption process involves encrypting the data with a unique key that can only be decrypted by the intended recipient, ensuring that sensitive information is well-protected.

In conclusion, the applications of public-private cryptography are numerous, and as a Computer Science student, I have come to appreciate its importance in securing communication and data. From e-commerce to online banking, secure communication, and data storage, public-private cryptography plays a significant role in ensuring that sensitive information is well-protected. Its applications continue to grow as the digital age progresses, making it an essential tool in computer science and technology.

3 Personal Application

Secure messaging apps have become increasingly popular in recent years, particularly in the wake of numerous high-profile data breaches and privacy scandals. These apps use end-to-end encryption, which means that messages are encrypted on the sender's device and can only be decrypted on the recipient's device. This ensures that even if a message is intercepted by a third party, it cannot be read without the appropriate decryption key.

The use of public-private cryptography in secure messaging apps is particularly important for individuals who value their privacy and security. In today's world, where sensitive information is often shared over digital platforms, it is essential to have strong encryption measures in place to protect personal data. This is particularly true for individuals who may be at risk of surveillance or hacking, such as journalists, activists, and whistleblowers.

Aside from secure messaging apps, public-private cryptography has numerous other applications in modern society. It is used in online banking to ensure the security of financial transactions, in e-commerce to protect credit card information, and in digital signatures to authenticate electronic documents. Public-private cryptography is also used in the creation of virtual private networks (VPNs) and in the protection of sensitive government communications.

In recent years, there has been a growing debate about the balance between privacy and security in the use of public-private cryptography. Some argue that strong encryption measures are essential for protecting individual privacy, while others argue that encryption can hinder law enforcement efforts to combat crime and terrorism. This debate has been particularly contentious in the United States, where the government has sought to gain access to encrypted data in criminal investigations.

Despite this debate, public-private cryptography remains a crucial tool for protecting individual privacy and security in the digital age. It is essential that individuals and organizations continue to use strong encryption measures to protect their sensitive information and communications.