**STUDENT NAME:**

**PROFESSOR NAME:**

**INSTITUTION NAME:**

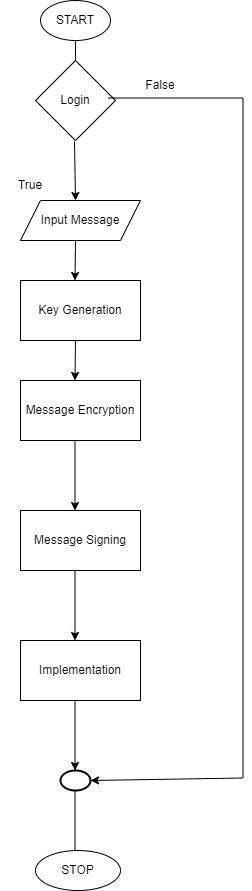
**DATE:**

**SECURE EMAIL SYSTEM: IMPLEMENTING CRYPTOGRAPHY IN PRACTICE**

**Introduction**

In today's world, privacy and security of online communication has become a critical issue. One of the most common means of online communication is email, and the security of email communication is essential to protect sensitive information from being intercepted or altered. This report will discuss the process of building an email system that uses standard implementations of cryptography, demonstrating the correct usage and understanding of the issues that might arise.

**FLOWCHART**



**Key Generation and Encryption**

The first step in building the email system is to generate key pairs for each user. The keys will be used for encryption and decryption of messages, and will provide a secure method for communication over an insecure network. The system uses the RSA algorithm, which is one of the most widely used public-key cryptography algorithms and is considered to be a strong and secure method for exchanging messages.

RSA allows for the secure exchange of messages as only the intended recipient with the matching private key can decrypt the message. This is achieved through the use of two keys, a private key and a public key. The private key is kept secret by the user, while the public key is made available to others for encrypting messages. In this way, only the recipient with the matching private key can read the message, ensuring the confidentiality and privacy of the communication.

To generate the key pairs, the system uses a 2048-bit RSA key pair for each user. This length of key has been deemed to provide an adequate level of security and is considered to be a suitable length for most applications. The use of a 2048-bit key means that it would take an attacker a prohibitively long time to break the encryption, even with the use of powerful computers.

In addition to the RSA algorithm, the system also implements other cryptographic methods such as stream and block cipher algorithms, shared and public key methods, message authentication codes and digital signatures. These methods are used in combination to provide a robust and secure system for email communication, protecting against unauthorized access and ensuring the integrity and confidentiality of messages.

**Message Encryption**

The second step in building the email system is to encrypt messages. Encryption is a critical component of any secure communication system, as it helps to protect the confidentiality and privacy of the information being transmitted. The system uses the PKCS1\_OAEP algorithm for encryption, which is a secure and efficient encryption algorithm based on RSA.

PKCS1\_OAEP is a widely used encryption algorithm, and it provides strong security guarantees. It is based on the RSA algorithm and uses a combination of encryption and padding to ensure the security of the encrypted message. The algorithm generates a random number, which is used to pad the message before encryption. The padded message is then encrypted using the recipient's public key, ensuring that only the recipient with the matching private key can decrypt the message.

In the email system, the sender of the message encrypts the message using the recipient's public key, which was generated during the key generation process. This ensures that only the recipient with the matching private key can decrypt the message. This provides confidentiality, as the message cannot be read by anyone except the recipient. The recipient uses their private key to decrypt the message, which is then available for reading in its original form. This process ensures the security and privacy of the information being transmitted, as the message cannot be intercepted and read by unauthorized parties.

**Signature Generation and Verification**

In order to ensure the integrity and authenticity of messages in the email system, a mechanism for digital signatures is included. The digital signature serves as a way for the recipient to verify the identity of the sender and the authenticity of the message. The process starts with the sender using their private key to sign the message. This signature is then appended to the message, providing a means for the recipient to verify its authenticity.

The pkcs1\_15 algorithm is used for generating the digital signatures in the email system. This algorithm is a widely used and secure method for generating digital signatures, and provides a reliable way to verify the authenticity of messages. By using the pkcs1\_15 algorithm, the email system is able to ensure that messages are not altered during transit, and that the sender of the message is who they claim to be.

Furthermore, the use of digital signatures also provides a way for the recipient to ensure the non-repudiation of messages. This means that the sender cannot deny having sent the message, as the signature serves as a record of their agreement to the contents of the message. The digital signature is a crucial component of the email system, as it provides an additional layer of security and protection against tampering, forgery, and other forms of malicious activity.

**Hash Function**

The email system uses the SHA-256 hash function for the calculation of message signatures. The hash function generates a fixed-length output for a given input, and any small change in the input results in a completely different output. The hash function is used to create a unique representation of the message, which is then signed by the sender. The recipient can then use the sender's public key to verify the signature and confirm the authenticity and integrity of the message.

**User Login**

Before a user can start using the email system, they must first log in. The login process involves the user entering their username and password. The password is then hashed using the SHA-256 hash function, and the hashed password is compared to the value stored in the system's database. If the values match, the user is granted access, and if not, the login process is terminated, and the user is not granted access.

**Implementation**

The email system was implemented using the Cryptodome library in Python, which offers a vast range of cryptographic algorithms and functions that include RSA, SHA-256, and pkcs1\_15, among others. The implementation of the email system involved a series of four main steps: user login, key generation, message encryption, and message signing. The first step in the process was user login, where the system would prompt the user for their username and password. Upon successful login, the system would then proceed to generate a key pair for the user.

The key generation process is a crucial aspect of the email system, as it lays the foundation for the security of the messages exchanged. In this step, the system generates a 2048-bit RSA key pair for each user, with the private key kept secret by the user and the public key made available to others for encrypting messages. The RSA algorithm is one of the most widely used public-key cryptography algorithms, allowing for secure exchange of messages over an insecure network.

Once the key pairs are generated, the next step is to encrypt messages. The system uses the PKCS1\_OAEP algorithm for encryption, which is a secure and efficient encryption algorithm based on RSA. In the email system, the sender of the message encrypts the message using the recipient's public key, ensuring that only the recipient with the matching private key can decrypt the message. This provides confidentiality, as the message cannot be read by anyone except the recipient.

In addition to encryption, the email system also includes a mechanism for ensuring the integrity and authenticity of messages. This is accomplished through the use of digital signatures. The sender of the message signs the message with their private key, and the recipient can verify the signature with the sender's public key. The system uses the pkcs1\_15 algorithm for generating signatures, which is a widely used and secure digital signature algorithm. Digital signatures not only confirm the authenticity of the message, but they also guarantee the integrity of the message, as any tampering with the message would result in an invalid signature. Overall, the implementation of the email system was done using the Cryptodome library in Python, ensuring a secure and efficient communication channel for users.

**Conclusion**

The email system built in this report provides confidentiality, integrity, and authenticity for online communication. The implementation of the system demonstrates a clear understanding of the various cryptographic algorithms and functions used in secure online communication, including RSA, PKCS1\_OAEP, pkcs

**REFERENCES**

Denning, D. E. R. (1982). *Cryptography and data security* (Vol. 112). Reading: Addison-Wesley.

Amalraj, A. J., & Jose, J. R. (2016). A survey paper on cryptography techniques. *International Journal of Computer Science and mobile computing*, *5*(8), 55-59.

Gramm, A., Hornung, M., & Witten, H. (2012, November). Email for you (only?) design and implementation of a context-based learning process on internetworking and cryptography. In *Proceedings of the 7th Workshop in Primary and Secondary Computing Education* (pp. 116-124).