

# Al Imam Mohammad Ibn Saud Islamic University College of Computer and Information Sciences

Information Systems Department

***IS380: Cybersecurity***

***The Term Project –***

**Instructions:**

1. This is a group work project worth **20%** of the total mark.
2. Submission due: Monday 09/05/2022, 9:00 PM
3. Read and sign for Part (A) and note that: **Any Cheating will result in** ZERO **grade for the whole project** (The work will be checked for plagiarism, and I will only accept **40%** and less in SafeAssign)
4. Submit **both softcopy** (via Blackboard) (use MS word format)

|  |  |  |  |
| --- | --- | --- | --- |
| **Section: 172** | | | |
| **Students Names** | **Students IDs** | **Read and accept**  **Part (A) (Signature)** | **Deserved Marks out**  **of 20** |
| Mohammed Ali Alghamdi | 443018152 | Accept |  |
| Meshal Abdulaziz Alghaith | 443014782 | Accept |  |
| Asseil Osama Sardidi | 443015799 | Accept |  |

**Part A (Plagiarism Declaration):**

**I declare that the proposed document is my own work and I own the copy right of it with no copy rights violation or plagiarism from other resources**

Page **1** of **3**





|  |  |  |
| --- | --- | --- |
| **Project Evaluation's Sheet** | | |
| **Criteria** | **Deserved Points** | **Criteria's Points** |
| **Phase 1** | **5** | |
| * Clarity of project description |  | 2 |
| * Clarity of the proposed solution |  | 2 |
| * Language and writing style |  | 1 |
| **Phase 2** | **10** | |
| * Introduction |  | 2 |
| * Background |  | 2 |
| * Case study/Example |  | 2 |
| * Implementation |  | 2 |
| * Reference |  | 1 |
| * Language and writing style |  | 1 |
| **PRESENTATION** | **5** | |
| * Summarize main points. |  | 1 |
| * Design details (Colours, Font, Format...etc) |  | 1 |
| * Delivery, clarity of language, and use of   time |  | 1 |
| * Answering the question |  | 1 |
| **Total** |  | **20** |

Page **2** of **3**





# Introduction:

# In the present time and in our daily lives, we notice that the transfer of information is considered one of the most important, if not the most important things, whether in universities, banking transactions, or even entertainment and commercial websites. Therefore, it is essential to focus on protecting this information from any external interference.

# The RSA encryption algorithm is a mathematical algorithm used to encrypt and decrypt data using mathematical equations. This algorithm protects the process of transferring data from the sender to the recipient, making the message readable but in an unreadable format.

# Background

RSA Encryption Algorithm, RSA appeared for the first time in 1977 by Leonard Adleman, Adi Shamir and Ronald Rivest, RSA uses both the public and the private keys, the public key used for encrypting the massage and the private key decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method to assure confidentiality, integrity, and authenticity. This means that messages encrypted with the public key can only be decrypted using the private key, ensuring that the person with the private key is the only person who can read the message, thus protecting the information from unauthorized access. RSA uses Many protocols such as Secure Shell and SSL/TLS, rely on RSA for encryption and digital signature functions.

SHL: is a cryptographic network protocol that provides secure login and command execution on remote systems, RSA is used for key exchange, where the public key is shared to encrypt data, allowing secure access to the remote system.

SLL/TLS: are protocols that secure the communication between web browsers and servers, most commonly in HTTPS. RSA is a part of establishing a secure connection, encrypting data between the client and server.

# Case study or example of use

1. RSA encryption is a key security method that banks rely on to keep electronic transactions safe and protect customer information. The main purpose of this technology is to encrypt financial details and maintain confidentiality while data travels over the internet.

When a financial transfer happens, the bank generates a pair of RSA keys, public and private to ensure everything is secure. The public key is used to encrypt the financial data being sent, while the private key is what decrypts it. So, when a customer enters the amount and the recipient's account info, that data gets encrypted with the RSA keys and sent =securely to the bank's servers.

Once the bank server gets the encrypted info, it uses its private key to decrypt and handle the transaction safely. The transaction's validity is checked and processed based on the decrypted data, ensuring everything goes smoothly.

By using RSA encryption in banking, customer data and financial transactions are well-protected during transfers, keeping information confidential and safe from unauthorized access. This approach helps secure financial activities and maintain data integrity in the fast-paced and complex online world.

# the implementation

Implementing RSA requires two prime numbers p and q and computing their product, in RSA encryption, the public exponent e is typically set to 65537 for both efficiency and security.

RSA Key:

two prime numbers p and q.

Calculate n=p\*q.

Compute ϕ(n)=(p−1) (q−1).

Choose an integer e such that 1 < e <ϕ(n) and gcd(e,ϕ(n)) = 1

Compute d, the modular inverse of e modulo ϕ(n).

RSA Encryption:

To encrypt a message m: c = m^e mod n Where c is the ciphertext.

RSA Decryption:

To decrypt the ciphertext c: m= c^d mod n Where m is the original message.

**Advantages**

1. **Security**:

RSA provides a high level of security

1. **Asymmetric Encryption**:

RSA is an asymmetric algorithm, meaning it uses two keys: a public key for encryption and a private key for decryption.

1. **Digital Signatures:** RSA is used not only for encryption but also for generating digital signatures
2. **Key Distribution**:

Since RSA uses a public and private key system, the public key can be distributed freely without compromising the security of the encrypted messages.

**Disadvantages**

1. **Key Size:**

To maintain high levels of security, RSA requires large key sizes

1. **Message Size Limitation**:

RSA can only encrypt data smaller than the key size

3.  **Key Management**:

Managing large RSA keys can be complex

# References

[1] Ajay Sarangam. 2020. RSA algorithm: Working and Use Cases

From: [https://u-next.com/blogs/cyber-security/rsa- algorithm/#:~:text=Now%20let%20us%20explain%20the%20RSA%20algorithm%20with%20an%20example:-](https://u-next.com/blogs/cyber-security/rsa-%20%20%20%20algorithm/#:~:text=Now%20let%20us%20explain%20the%20RSA%20algorithm%20with%20an%20example:-)

[2] Practical Networking. 2019. RSA Example

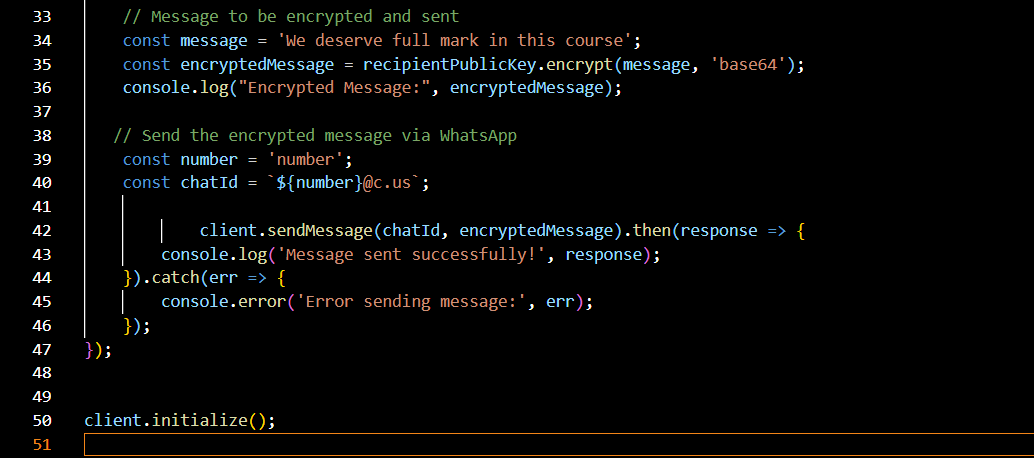
From:<https://www.practicalnetworking.net/series/cryptography/rsa-example/#:~:text=How%20do%20we%20generate%20RSA%20Keys?%20How%20do%20we%20use>

[3] Encryption Consulting.2024. What is RSA? How does an RSA work?

From:<https://www.encryptionconsulting.com/education-center/what-is-rsa/>

Appendix

Encryption code:



A screenshot of a computer

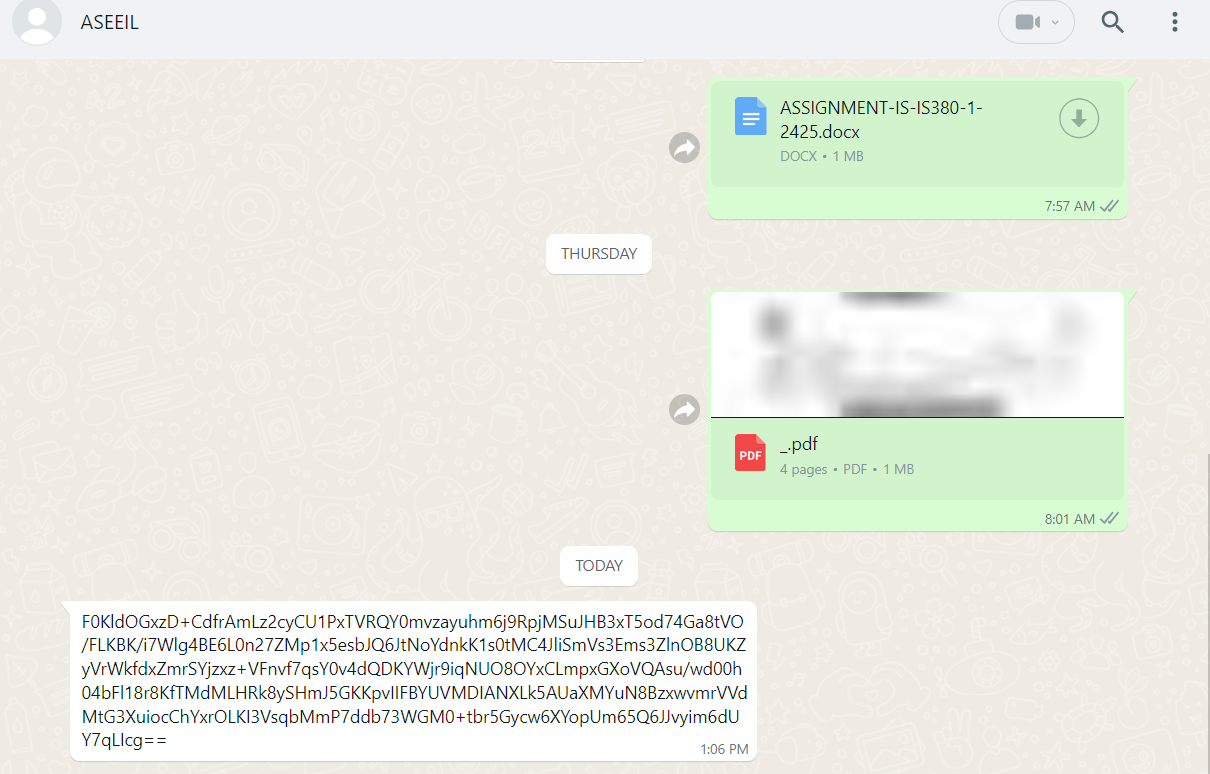
Description automatically generated

Result of encryption:

A screenshot of a qr code

Description automatically generated

Ciphertext (the encrypted message):



Private key with the plaintext (decrypted message) and the decryption code :

A screenshot of a computer

Description automatically generated

Page **3** of **3**