**COMPUTER ENGINEERING**

**Title of Micro-Project:** Micro-Project on Cryptography Tool.

**GROUP MEMBERS**

|  |  |  |
| --- | --- | --- |
| **ROLL NO** | **CLASS** | **NAME OF MEMBER** |
| 3111 | CO6I | Shreyash Kotain |
| 3112 | CO6I | Darshana Kure |
| 3113 | CO6I | Sahil Mahatre |
| 3114 | CO6I | Omkar Moolya |
| 3115 | CO6I | Aman Pandey |
| 3116 | CO6I | Priyanka Patil |
| 3117 | CO6I | Heramb Pawar |
| 3118 | CO6I | Aditya Raut |
| 3119 | CO6I | Pawan Salve |
| 3120 | CO6I | Ameya Sawant |

**Guide Name**: - Mrs. Ashwini Parkar

**Part A Plan**

**Aim of Micro-Project:** Implement client server communication using cryptography tool

**Brief description**: -

1. Data Encryption Ensures Confidentiality. Basically, It Is Transforming Intelligible Data into Encrypted Form That Is Not Easy to Decipher.
2. The Data Is Encrypted So That Only Intended User Can Read It. In This Era of Technology Encryption Is A Necessity. It Is One of The Most Powerful Way to Keep Out Data Safe from Intruders. This comes under Cryptography
3. Cryptography Is About Constructing and Analyzing [Protocols](https://en.wikipedia.org/wiki/Communications_protocol) That Prevent Third Parties or The Public from Reading Private Messages
4. Various Aspects in information security such as Data [Confidentiality](https://en.wikipedia.org/wiki/Confidentiality), [Data Integrity](https://en.wikipedia.org/wiki/Data_integrity), [Authentication](https://en.wikipedia.org/wiki/Authentication), And [Non-Repudiation](https://en.wikipedia.org/wiki/Non-repudiation) Are Central To Modern Cryptography.
5. RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e., **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

**Aim** **of Micro-Project: -**

The Micro-Project Aims To: -

* Study the importance of client server communication using cryptography tool.
* Study various properties of cryptography tool for client server communication.
* Study functioning of cryptography tool.
* Study the process of data encryption.

**Action Plan: -**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr No** | **Detail of Activities** | **Plan start date** | **Plan end date** | **Name of Team Members** |
| 1 | Group formed according to roll no & group leaders were elected also detailed information on micro project was given |  |  | Heramb Pawar |
| 2 | Finalization of micro project as well as detailed discussion regarding topic |  |  | Shreyash Kotain |
| 3 | Planning of micro-project regarding, resources, software used, submission date and completing part a plan of micro – project |  |  | Aditya Raut |
| 4 | Complete analysis of design part of micro-project & distribution of module among group members |  |  | Priyanka Patil |
| 5 | Getting it finalized by the guide |  |  | Shreyash Kotain |
| 6 | Implementation of Project report |  |  | Sahil Mhatre |
| 7 | Presentation of 1st part of micro-project Infront of guide by each group member and Preparing of part b plan for micro-project |  |  | Aman Pandey |
| 8 | Submission of micro-project |  |  | Aditya Raut |

**Resources used: -**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr No** | **Name of Resources Required** | **Specification** | **Quantity** | **Remarks** |
| 1 | Computer | **Processor-**Amd  **Hard Disk-**2 Tb  **Ram-**16gb  **Operating System-**Windows 10 Pro | 1  1  1  1 | Hardware used |
| 2 | Microsoft word | MS office 2010 | -- | Software used |
| 3 | Cokolov | Cryptography and Communication Tool | --- | Software  Used |

**PART B**

**Aim of The Project**: Implement client server communication using cryptography tool

**Brief description**: -

1. Data Encryption Ensures Confidentiality. Basically, It Is Transforming Intelligible Data into Encrypted Form That Is Not Easy to Decipher.
2. The Data Is Encrypted So That Only Intended User Can Read It. In This Era of Technology Encryption Is A Necessity. It Is One of The Most Powerful Way to Keep Out Data Safe from Intruders. This comes under Cryptography
3. Cryptography Is About Constructing and Analyzing [Protocols](https://en.wikipedia.org/wiki/Communications_protocol) That Prevent Third Parties or The Public from Reading Private Messages
4. Various Aspects in information security such as Data [Confidentiality](https://en.wikipedia.org/wiki/Confidentiality), [Data Integrity](https://en.wikipedia.org/wiki/Data_integrity), [Authentication](https://en.wikipedia.org/wiki/Authentication), And [Non-Repudiation](https://en.wikipedia.org/wiki/Non-repudiation) Are Central To Modern Cryptography.
5. RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e., **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

**Aim** **of Micro-Project: -**

The Micro-Project Aims To: -

* Study the importance of client server communication using cryptography tool.
* Study various properties of cryptography tool for client server communication.
* Study functioning of cryptography tool.
* Study the process of data encryption.

**Course Outcome Integrated:**

1. Identify risk related to computer security and Information hazard in various situation
2. Apply cryptographic algorithm and protocols to maintain computer security**.**

**Actual Procedure Followed:**

1. **Group Formation: -** NIS is a subject that teaches us about basic security principals, various threat to security and techniques to address this threat. The basic aim of micro- project is to accelerate the attainment of the various outcomes in the course. In the first 2 weeks of April the subject was introduced. The syllabus as well as details of micro-project were discussed. A group of 10 members was formed and the group leaders were selected. The schedule of plan “a”,” b” & “presentation of micro-project” were finalized. The various micro-project topics related to subject were discussed our guide gave us the opportunity to select the topic of our choice.
2. **Finalization of Micro-Project: -** After attending the lectures for 2 weeks. We selected the topic for micro-project. We discussed the topic with our guide regarding the concept which we are going to apply in the project. We individually tried to explain the basic platform of project.
3. **Planning: -** After finalization of the project we started working on the project. We started the planning phase. We discussed among ourselves regarding the resources such as testing material, software requirements, etc. In this week we completed ‘part a plan’ of the micro-project which is nothing but an initial description about the project. We submitted it to the guide.
4. **Module Distribution &Analysis Part: -** Once the planning was over regarding resources, etc. We finalized the module which we will be writing. According to members we distributed the modules. We started the analysis of project.
5. **Design Part: -** In this part we focused on designing the structure of the project. We planned to apply some formatting to give an attractive look to the structure.
6. **Implementation: -** In the week we actually started the technical phase. In this phase we technically applied the formatting as decided. Each member was designing project modules which were assigned to them. Finally, the project was within the schedule time.
7. **Presentation: -** In this week we had to present the micro-project. Each member of group presented their own parts with confidence in front of guide. She asked us various queries regarding the topics. We explained her about the various components of the project. She asked us to do some changes regarding some topics.
8. **Submission: -** This week was submission week. We submitted our project along with ‘part a & b plan’ to the guide. We also submitted the hard copies and soft copies of project to the guide

**Actual Resources Used:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr No** | **Name of Resources Required** | **Specification** | **Quantity** | **Remarks** |
| 1 | Computer | **Processor-**Amd  **Hard Disk-**2 Tb  **Ram-**16gb  **Operating System-**Windows 10 Pro | 1  1  1  1 | Hardware used |
| 2 | Microsoft word | MS office 2010 | -- | Software used |
| 3 | Cokolov | Communication and Cryptography Tool | -- | Software Used |

**Report**

**Introduction:**

1. **What Is Data Encryption?**

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by organizations. Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption.

1. **What Is Primary Function of Data Encryption?**

The purpose of data encryption is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks. The outdated data encryption standard (DES) has been replaced by modern encryption algorithms that play a critical role in the security of IT systems and communications. These algorithms provide confidentiality and drive key security initiatives including authentication, integrity, and non-repudiation. Authentication allows for the verification of a message’s origin, and integrity provides proof that a message’s contents have not changed since it was sent. Additionally, non-repudiation ensures that a message sender cannot deny sending the message.

1. **The Process of Data Encryption:**

Data, or plaintext, is encrypted with an encryption algorithm and an encryption key. The process results in ciphertext, which only can be viewed in its original form if it is decrypted with the correct key. Symmetric-key ciphers use the same secret key for encrypting and decrypting a message or file. While symmetric-key encryption is much faster than asymmetric encryption, the sender must exchange the encryption key with the recipient before he can decrypt it. As companies find themselves needing to securely distribute and manage huge quantities of keys, most data encryption services have adapted and use an asymmetric algorithm to exchange the secret key after using a symmetric algorithm to encrypt data. On the other hand, asymmetric cryptography, sometimes referred to as public-key cryptography, uses two different keys, one public and one private. The public key, as it is named, may be shared with everyone, but the private key must be protected. The Rivest-Sharmir-Adleman (RSA) algorithm is a cryptosystem for public-key encryption that is widely used to secure sensitive data, especially when it is sent over an insecure network like the internet. The RSA algorithm’s popularity comes from the fact that both the public and private keys can encrypt a message to assure the confidentiality, integrity, authenticity, and non-reputability of electronic communications and data through the use of digital signatures.

1. **Tool & Other Details:**

**Link to Download Tool:** <https://github.com/doancongthang/RSA>

1. **What is the tool about?**

* Using this tool, we can transfer and receive encrypted messages using RSA algorithm between client and server through TCP/IP.
* SERVER sends an encrypted message string with the RSA encryption algorithm.
* The CLIENT receives the encrypted string and. The client can now decrypt it and reply back to the server.

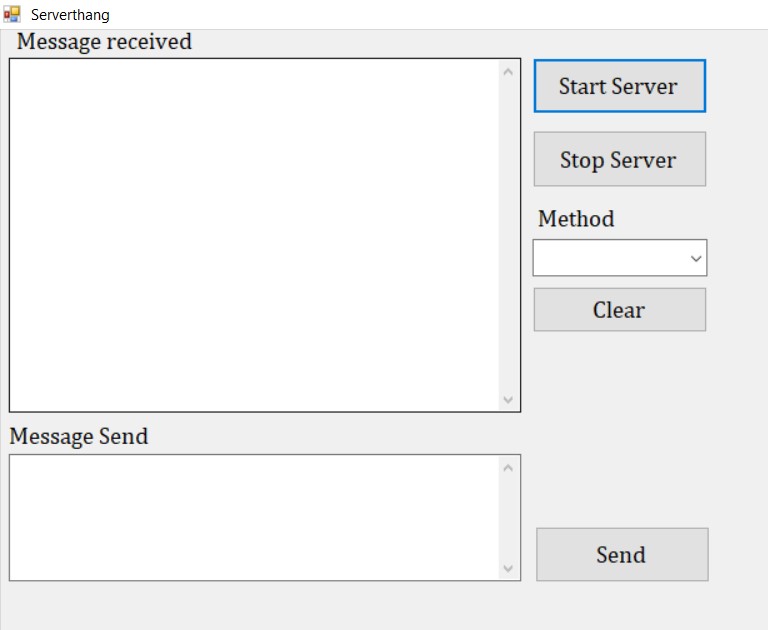
1. **What is RSA Algorithm?**

* RSA (Rivest –Shamir–Adleman) is an [algorithm](https://simple.wikipedia.org/wiki/Algorithm) used by modern computers to [encrypt](https://simple.wikipedia.org/wiki/Encryption) and decrypt messages. It is an asymmetric [cryptographic](https://simple.wikipedia.org/wiki/Cryptography) [algorithm](https://simple.wikipedia.org/wiki/Algorithm)
* Asymmetric means that there are two different [keys](https://simple.wikipedia.org/wiki/Key_(cryptography)). This is also called [public key cryptography](https://simple.wikipedia.org/wiki/Public-key_cryptography), because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the [factors](https://simple.wikipedia.org/wiki/Factorization) of a large [composite number](https://simple.wikipedia.org/wiki/Composite_number) is difficult: when the factors are [prime numbers](https://simple.wikipedia.org/wiki/Prime_number), the problem is called [prime factorization](https://simple.wikipedia.org/wiki/Prime_factorization). It is also a key pair (public and private key) generator.
* RSA involves a public key and private key. The public key can be known to everyone- it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The private key needs to be kept secret. Calculating the private key from the public key is very difficult.

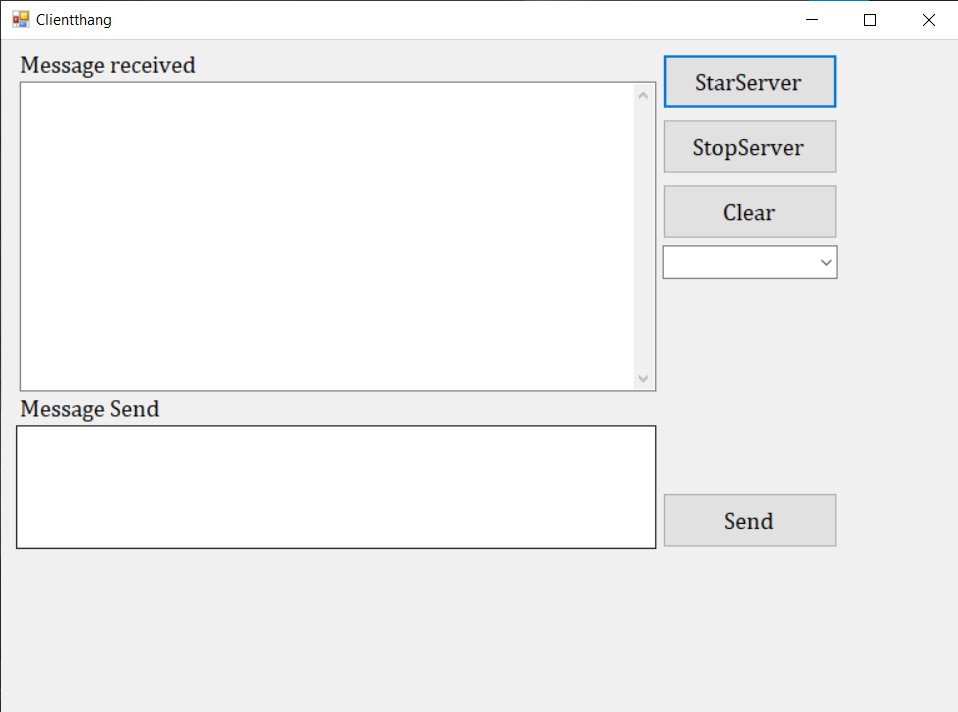
1. **What is TCP/IP?**

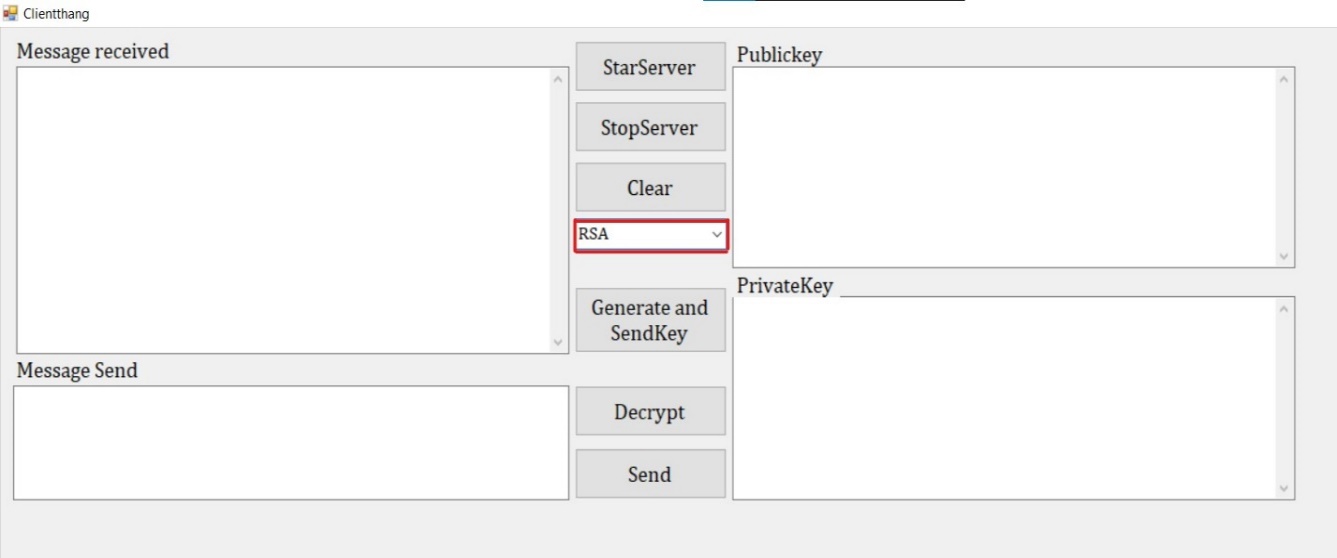
The Transmission Control Protocol (TCP) is one of the main [protocols](https://en.wikipedia.org/wiki/Communications_protocol) of the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite). It originated in the initial network implementation in which it complemented the [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP). Therefore, the entire suite is commonly referred to as *TCP/IP*. TCP provides [reliable](https://en.wikipedia.org/wiki/Reliability_(computer_networking)), ordered, and [error-checked](https://en.wikipedia.org/wiki/Error_detection_and_correction) delivery of a stream of [octets](https://en.wikipedia.org/wiki/Octet_(computing)) (bytes) between applications running on hosts communicating via an IP network.

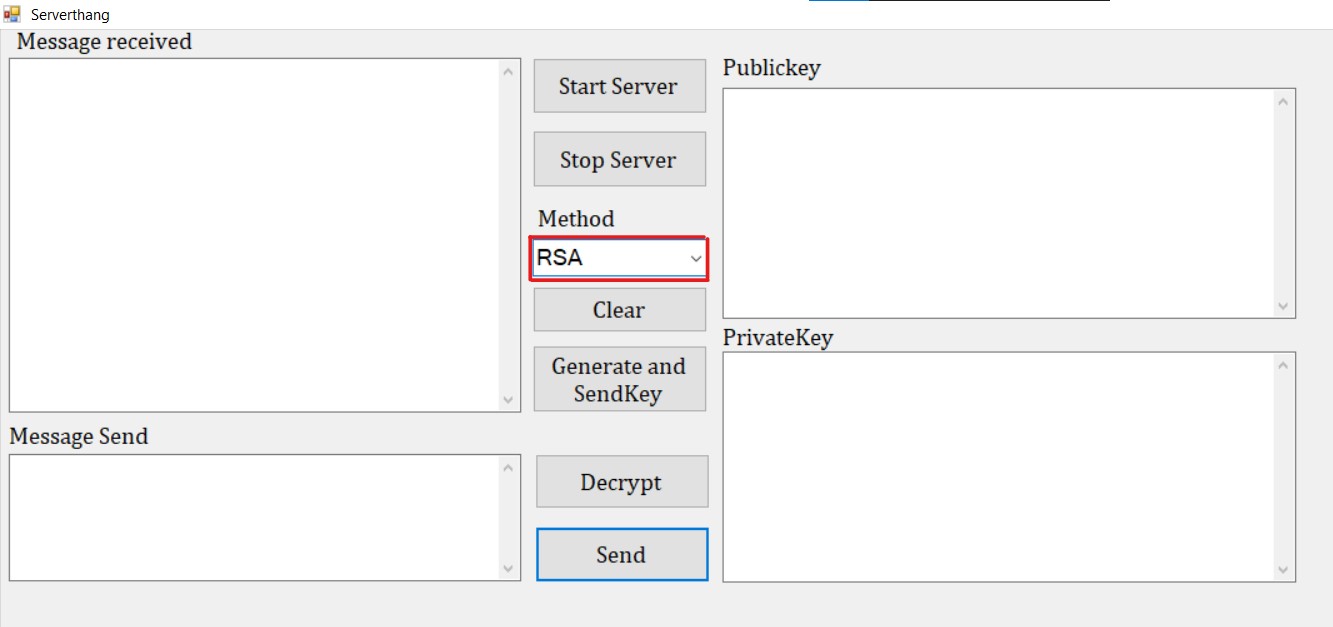
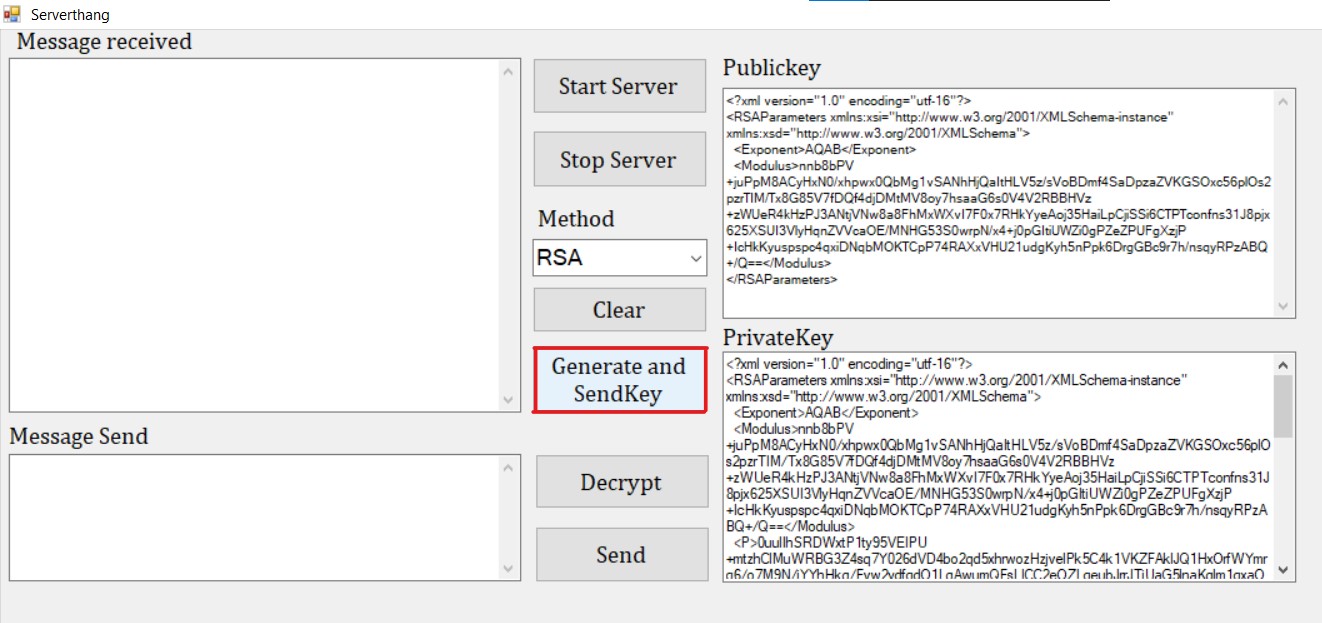
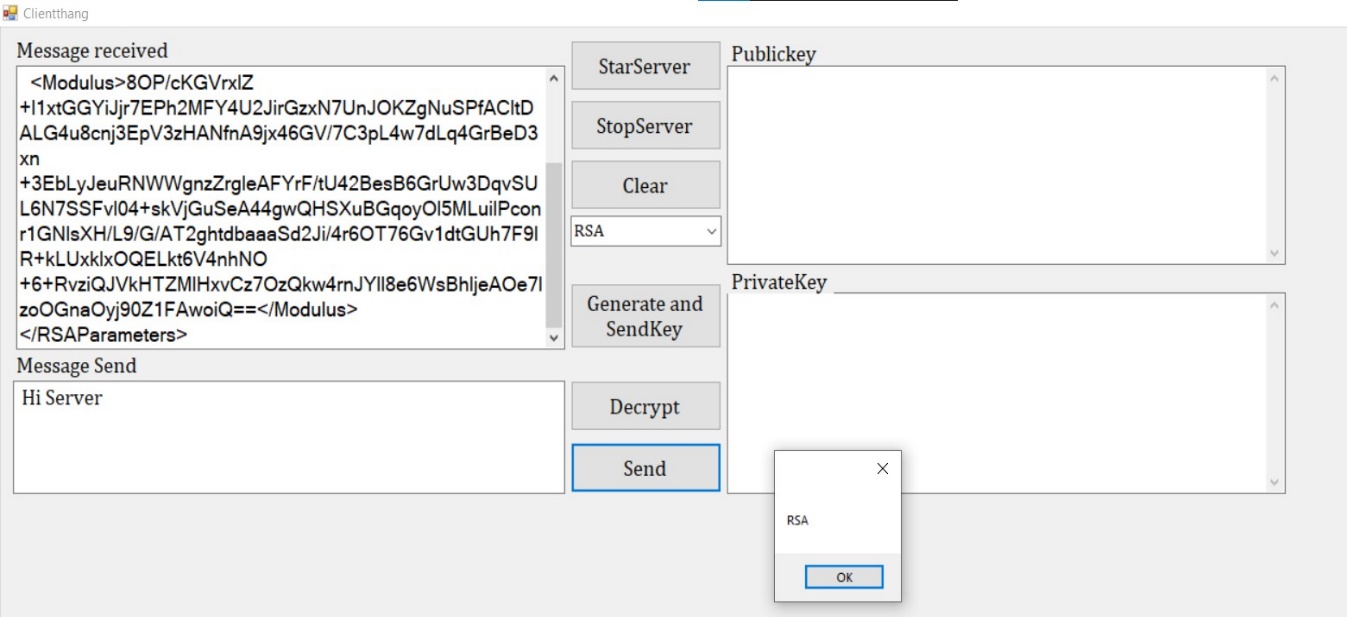
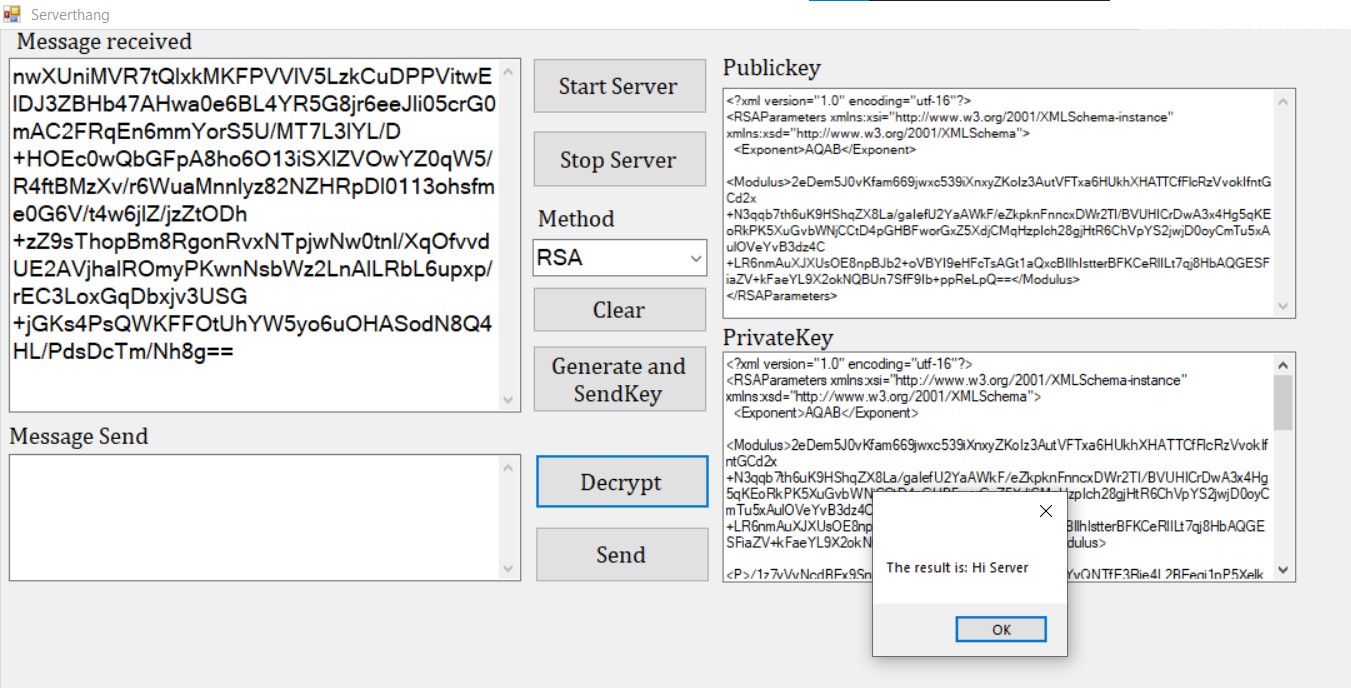
1. **Steps to Initiate Communication:**
2. **Client to Server:**
3. Open file: **ServerThang.exe.**

**Location:** Cokolov\_01\_04\_2020\Cokolov\_01\_04\_2020\_Server\bin\Debug

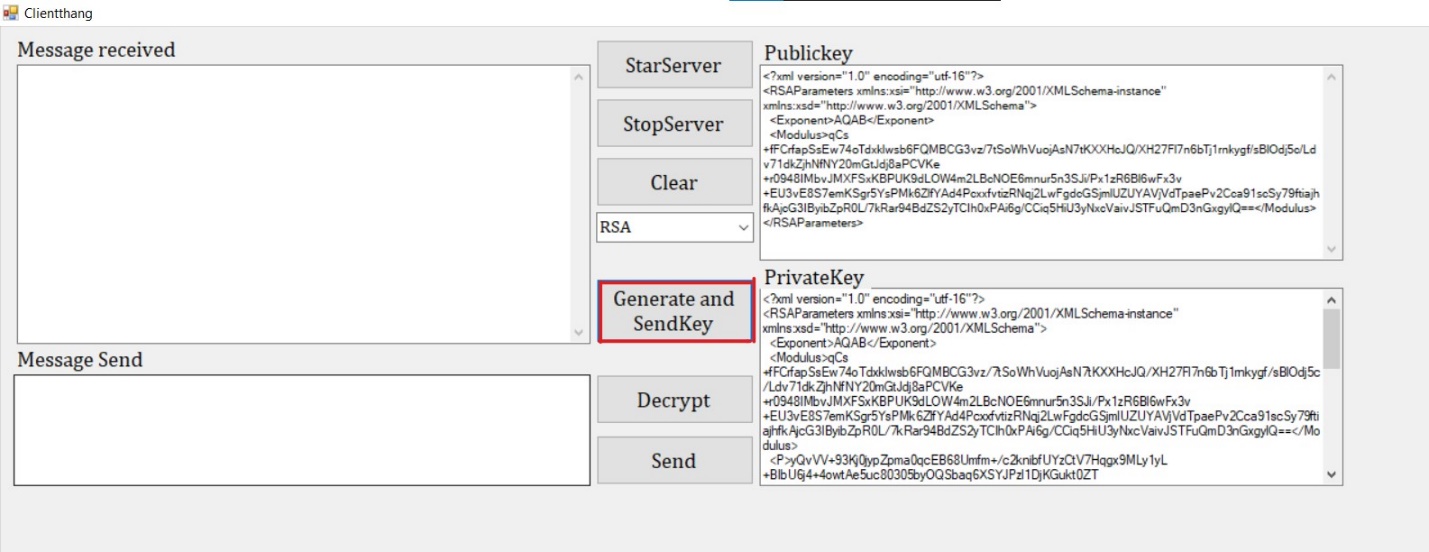
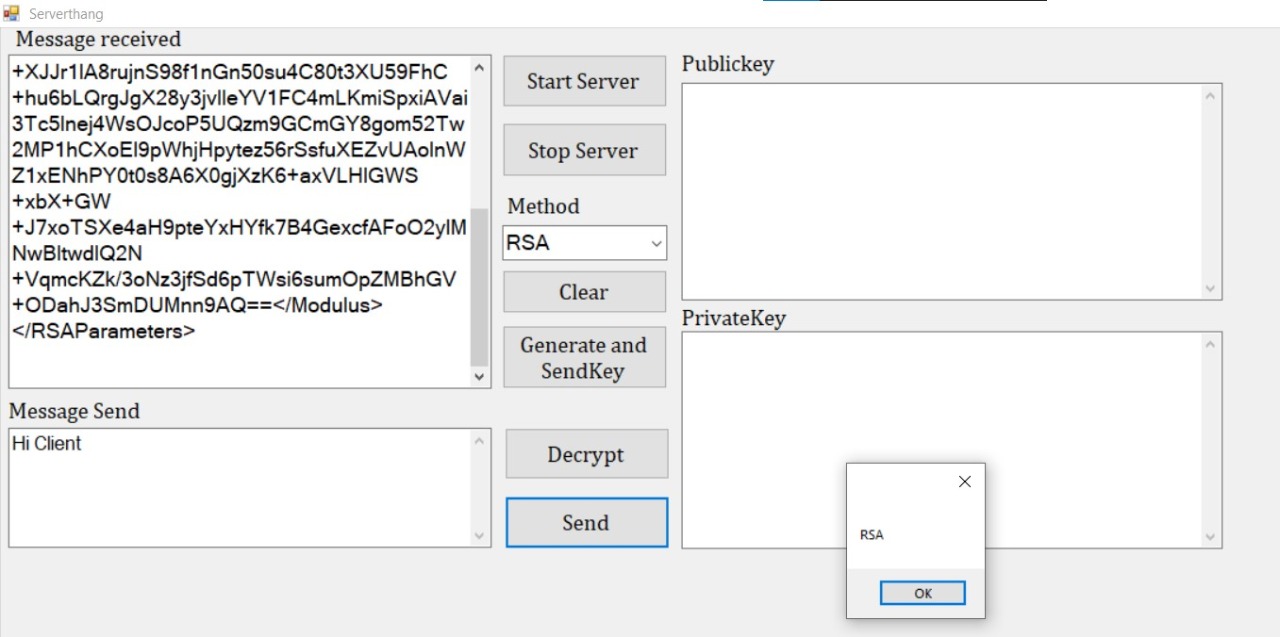
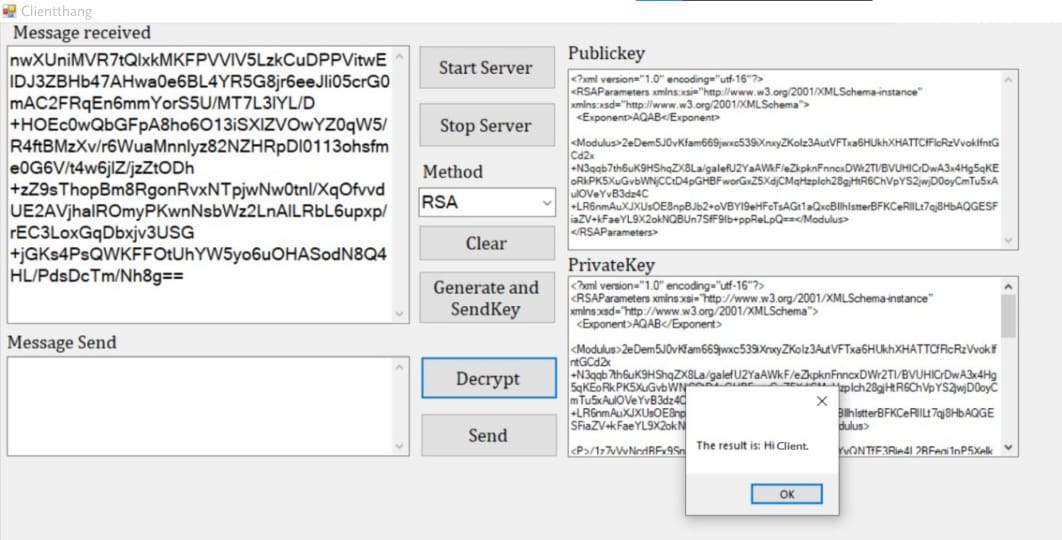
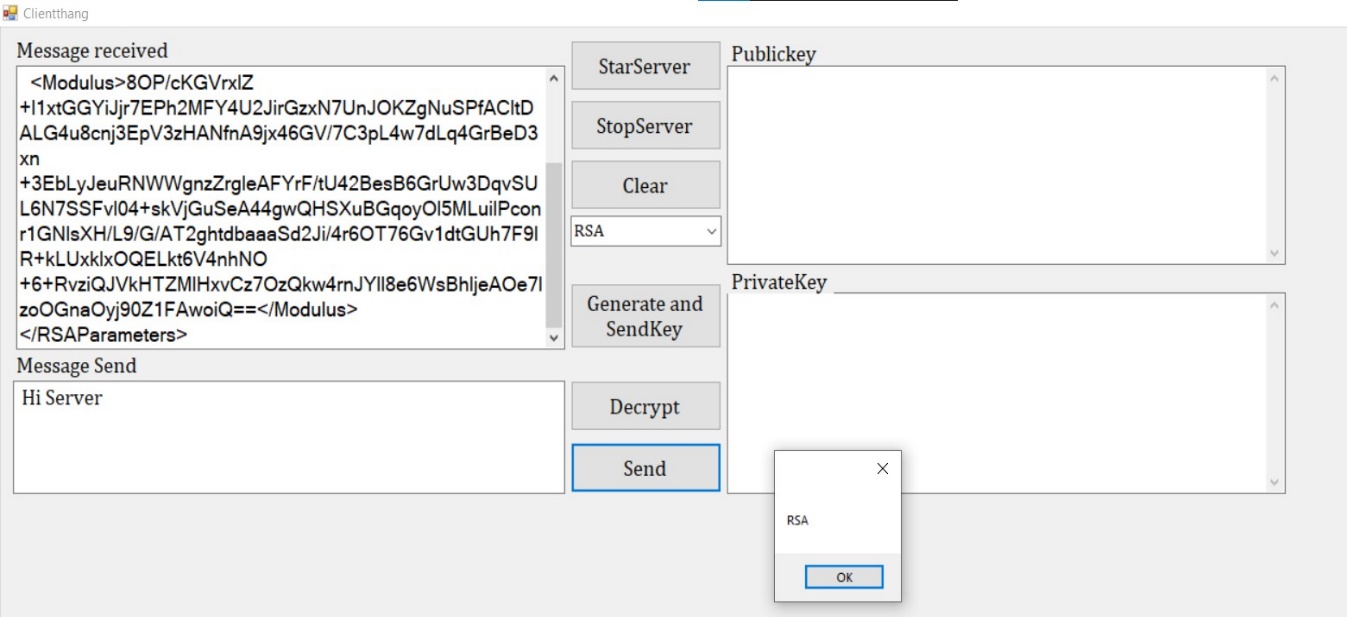
1. Open file: **Client Thang.exe**

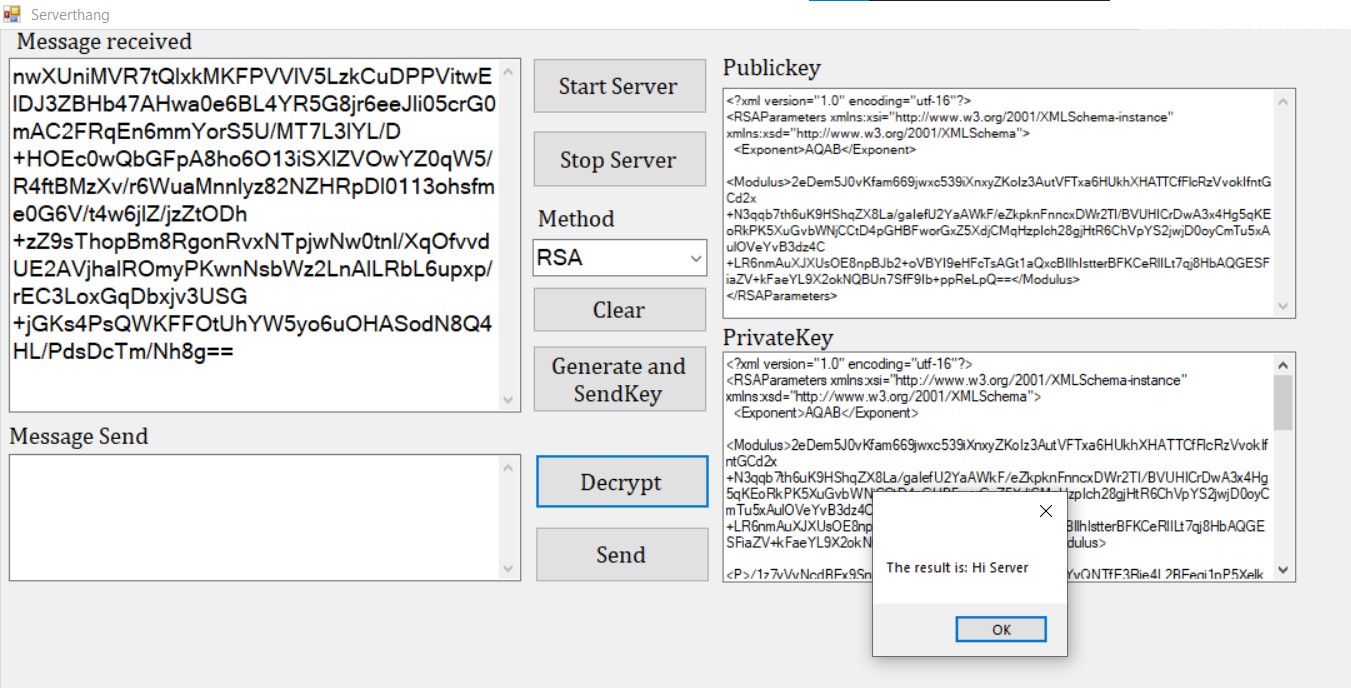
**Location:** Cokolov\_01\_04\_2020\Cokolov\_01\_04\_2020\_Client\bin\Debug

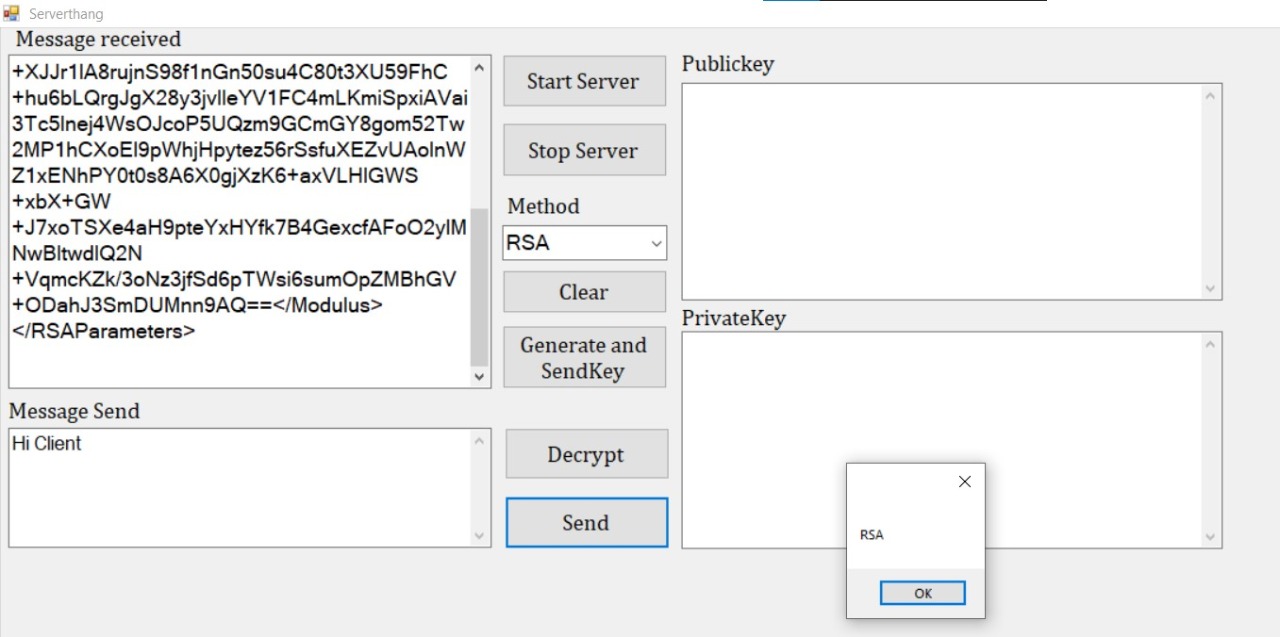
****

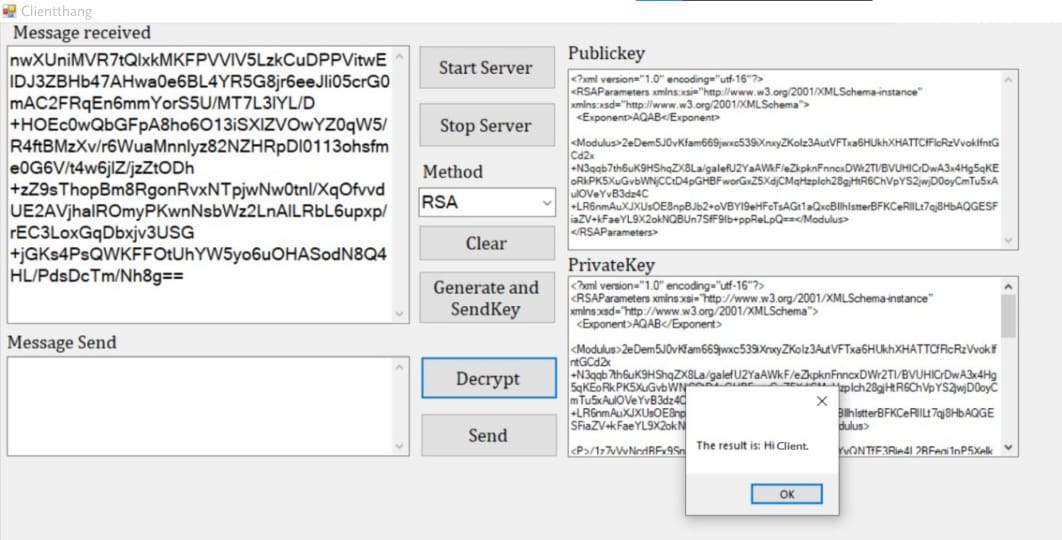
1. Select **RSA** Option in Client.
2. ****Select **RSA** Option in Server
3. Click on **generate and send key** inServer.
4. ****Now Send Message from Client to server.
5. Click on Decrypt Button in server to read message.
6. **Server to Client:**

Repeat the First 4 Steps as Mention in Client to Server Communication. Then Follow The following steps:

1. **** Click on **Generate and send Key** in Client.
2. **** Now send Message from Server to Client
3. **** Click on Decrypt Button in Client to read the message.
4. **Output:**
5. Client -Server Encryption & Decryption



1. ****Server-Client Encryption & Decryption

****

**References:**

We do have used a few references during the process of building our project. The references used are from Websites, Books etc.

The references used are:

* **Websites:**

1: www.github.com

2: [www.en.wikipedia.org](http://www.en.wikipedia.org/wiki/Operating)

3: www.geeksforgeeks.org

* **Reference Books:**

1: Computer security

2: Cryptography and network security

**Skill Developed/Learning Out of This Micro Project:**

* Since we worked in a group, we developed the skill of ‘TEAMWORK’ in us.
* We learnt in brief about client server communication using cryptography tool- COKOLOV.
* We learnt about Data encryption using RSA algorithm.