**MINOR-1**

**Encryption Decryption**

**Project Report**

**BTECH in COMPUTER SCIENCE**

**Specialization in**

**Cloud Computing and Virtualization Technology**

By:

|  |  |  |
| --- | --- | --- |
| **Name** | **Sap ID** | **Roll No.** |
| **Prabal Bansal** | **500068861** | **R110218104** |
| **Prithvi Chauhan** | **500068398** | **R110218109** |
| **Rohit Singh Chauhan** | **500069845** | **R110218128** |
| **Sanjay Singh Chauhan** | **500067645** | **R110218133** |

**Under the guidance of**

**Mr. Amrendra Nath Tripathi**

**Assistant Professor**



**CANDIDATES DECLARATION**

I/We hereby certify that the project work entitled **Encryption Decryption** in partial fulfilment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science And Engineering with Specialization in Cloud Computing and Virtualization Technology and submitted to the Department of Computer Science, University of Petroleum And Energy Studies, Dehradun, is an authentic record of my/ our work carried out during a period from September 2020 under the supervision of Guide Name(s), Designation and Affiliation.

The matter presented in this project has not been submitted by me/ us for the award of any other degree of this or any other University.

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

(Date: 07 December 2020)

Dr. Deepshikha Bhargava

Head

Department of Virtualization

School of Computer Science

University of Petroleum and Energy Studies

Dehradun - 248001 (Uttarakhand)

**ACKNOWLEDGEMENT**

We wish to express our deep gratitude to our guide **Mr Amrendra Nath Tripathi**, for all advice, encouragement and constant support he has given us throughout our project work. This work would not have been possible without his support and valuable suggestions.

We sincerely thank to our Head of the Department, **Dr. Deepshikha**, for his great support in doing our project Encryption Decryption at SoCS.

We are also grateful to **Dr. Manish Prateek** Professor and Director SoCS and **Dr. Kamal Bansal** Dean CoES, UPES for giving us the necessary facilities to carry out our project work successfully.

We would like to thank all our friends for their help and constructive criticism during our project work. Finally, we have no words to express our sincere gratitude to our parents who have shown us this world and for every support they have given us.

**ABSTRACT**

Having prior knowledge about security is helpful to believe some company for security. Our project ie. Implementation of Encryption and decryption algorithms helps user to get to know how much their data is secured. Here we have implemented symmetric algorithms like DES and many less secure primitive encryption and decryption algorithms. And for asymmetric we have implemented RSA. In Client-Server fashion to get user a real time experience.

**Keywords:** Security, Socket, Key, Cipher text.

**TABLE OF CONTENTS**

**Contents**

1. **Introduction**
2. **Literature Review**
3. **Problem Statement**
4. **Objective**
5. **Design Methodology**
6. **Implementation**
   1. **Pseudocode**
   2. **Output Screen**
   3. **Result Analysis**
7. **Conclusion and Future Scope**

# **Introduction**

* Our goal is to implement the working of encryption algorithms by encrypting files and sharing it through socket programming.
* By implementing the encryption algorithms, we have achieved secure transfer of messages from client to server. We have achieved it by using a very complex encryption algorithm which is RSA (Rivest, Shamir and Adelman), DES algorithm and many other less secure algorithms like (Caesar's cipher (Known to everyone) and many more …).

# **Literature Review**

With the advancement of technology, it becomes easy to fall in trap and lost our privacy even trusting some best firms in the business. Through our research with the algorithms we got to find that no algorithm is 100% secure, the security is myth totally depending on any organization for the security of our data is not a good idea, we have to take preventive measures to make it work.

Caesar’s cipher: - this is the simplest algorithm where we just shift characters forward. The message written can easily be decrypted.

At bash cipher: - this is the cipher where we exchange a with z, b with y and so on. Which can be easily decrypted as well.

These both are the most primitive algorithm that we have used at some point, over the time with the revolution there are many algorithms that came up but no one could stay secured properly until the algorithm like Triple DSA and AES algorithm came into game.

DSA is developed by IBM, which is a computer giant for almost 4 decades from now, there are problems like its short key (56 bits). Then they think to applied the same algorithm thrice on the message which makes the key more secured by using three different keys.

But this algo has problems with speed as we are applying the same algo with different keys thrice.

Then the last algo came which we are using till now that is AES which is uses the keys length of 128-bits, 192-bits and 256-bits and involves 4 steps for securing and making of a cipher text.

* Password entropy is based on the character set used (which is expansible by lowercase, uppercase, numbers as well as symbols) as well as password length. Password entropy predicts how difficult a given password would be to crack through guessing, brute force cracking, dictionary attacks or other common methods. We think working on basic concepts of cyber security such as cryptography and password strengthening will help us to represent the knowledge we have gained in the past 2 years of our college academics.
* When we talk about the key length of an RSA key, we are referring to the length of the modulus, n, in bits. The minimum recommended key length for a secure RSA transmission is currently at least ***1024 bits***. A key length of 512 bits is no longer considered secure, although cracking it is still not a trivial task for the likes of you and me. The longer your information needs to be kept secure, the longer the key you should use. Keep up to date with the latest recommendations in the security journals.
* **RSA** is an encryption algorithm, used to securely transmit messages over the internet. It is based on the principle that it is easy to multiply large numbers, but factoring large numbers is very difficult. For example, it is easy to check that 31 and 37 multiply to 1147, but trying to find the factors of 1147 is a much longer process.

File handling in C enables us to create, update, read, and delete the files stored on the local file system through our C program. The following operations can be performed on a file.

* Creation of the new file
* Opening an existing file
* Reading from the file
* Writing to the file
* Deleting the file

In the project the data will be stored in .txt file, when working with .txt files, you need to declare a pointer of type file. This declaration is needed for communication between the file and the program.

FILE \*fptr;

# **Problem Statement**

* As we all are from the IT domain, hence we were highly motivated to work on a concept concerned with the field of cyber security where we have to keep our data safe from malicious intent. Therefore, these algorithms are used to keep the messages just between the client and server and prevent any middleman to have access to them.
* People from non IT background do not know how their personal data is exposed on the internet as of now. All the devices can easily be tampered with that is why these algorithms have been introduced to prevent their data from being leaked as they contain keys which are only available to the sender and receiver which provide end to end encryption.

# **Objective**

Implementing Encryption and Decryption Algorithms through socket programming.

**Sub objective:**

* Implementing DES algorithm.
* Implementing RSA Algorithm.
* Providing layers of security.

# **Design Methodology**

**Phase1:Requirement analysis**

Study concepts of Encryption and Decryption.

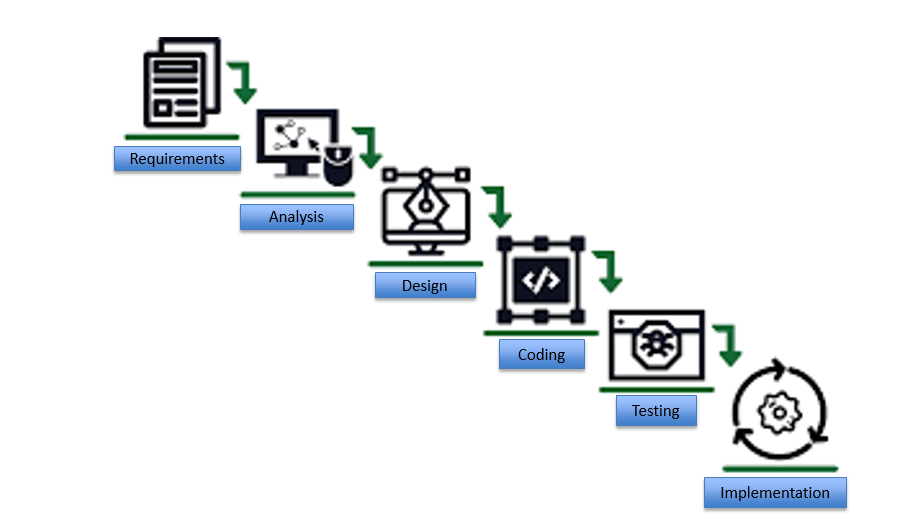
Study of Socket Programming.

**Phase2:Designing and development**Designing and development is further divided into various phases. This phase starts with the input from the Requirement and Analysis phase which will lead this project to the model development phase where a model will be created and further lead to the designing of the algorithm. After completion of the designing of the algorithm phase, the focus will shift on the analysis of the algorithms and their implementation in this project.

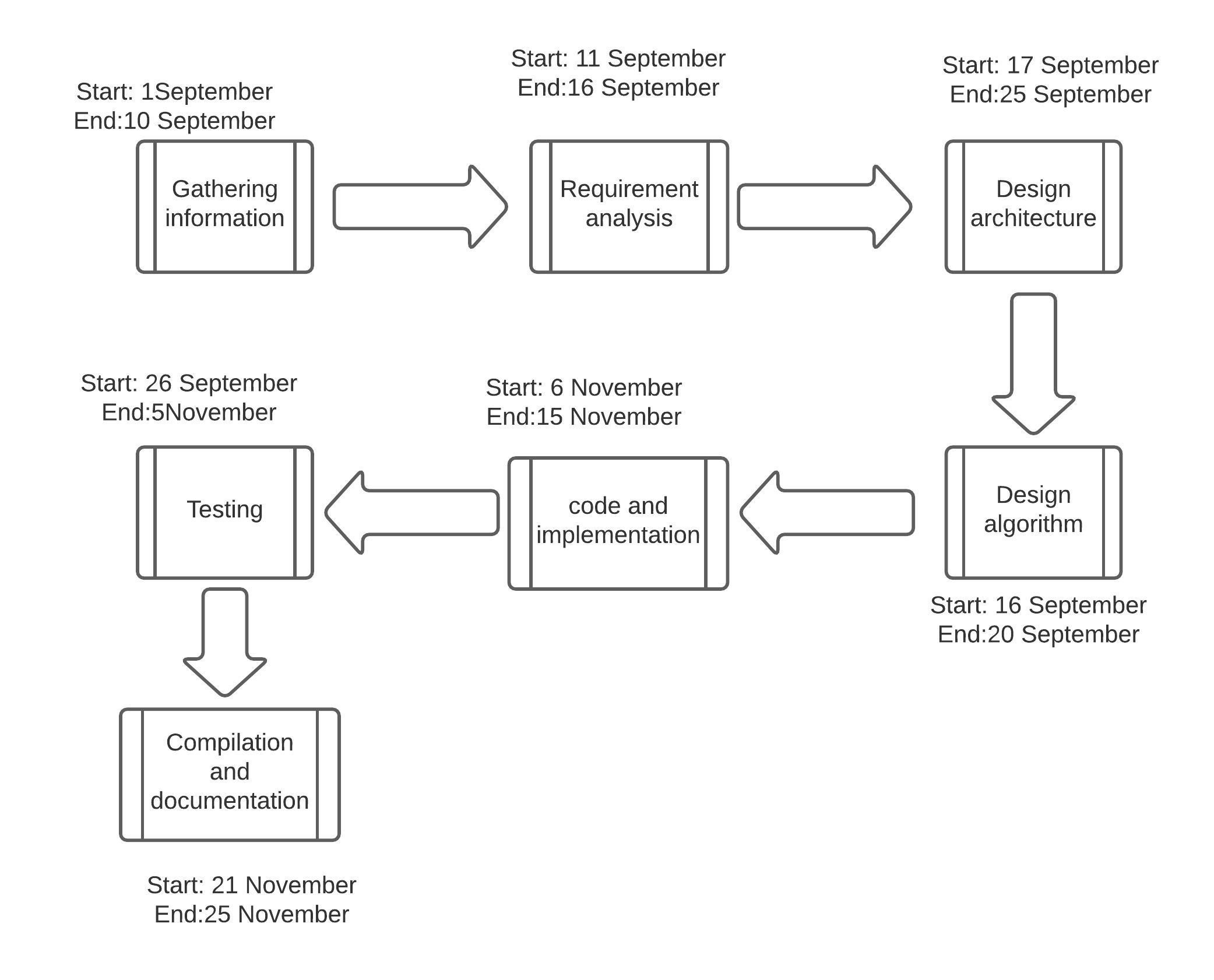
**Phase3:Coding**On receiving system design documents, the work is divided into modules/unit and distributed among the team members and actual coding is started. Since in this phase the code is produced so it is the main focus of the developers. This is going to be the longest phase in this project. The implementation of this project starts in terms of writing program in the suitable programming language and developing error free executable program efficiently.

**Phase4:Testing**Testing will be done with the help of the reserved database in order to find the accuracy of the prediction model.

**Phase5: Integrating and implementing all the above phases.**

****

## **Pert Chart**



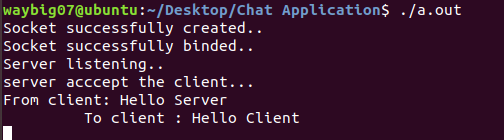
## **Result Analysis**

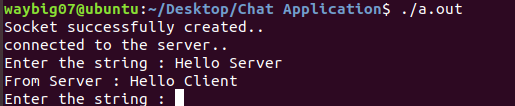
While comparing the two programs through RSA and DES respectively we came to know that DES is much better than RSA in terms of performance and execution. The encryption speed of DES is much more than RSA.

|  |  |  |
| --- | --- | --- |
| Factors | DES | RSA |
| Power consumption | Low | High |
| Key used | Same key used for encrypt & decrypt | Different key used for encrypt & decrypt |
| Key size | 56 bits | >1024 bits |
| Block size | 64 bits | Minimum 512 bits |
| Ciphering & Deciphering Key | same | different |
| Scalability | Scalable due to varying the key size and block size | Not scalable |
| Algorithm | Symmetric algorithm | Asymmetric algorithm |
| Encryption | Moderate | Slower |
| Decryption | Moderate | Slower |

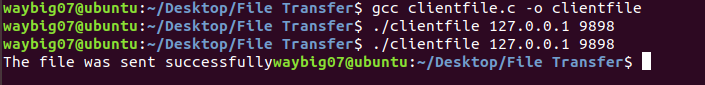
**5.3** **Output**

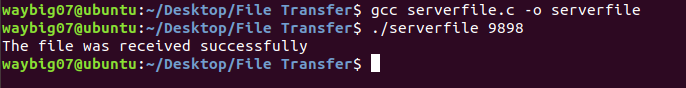
**Connection Established between Server & Client**



****

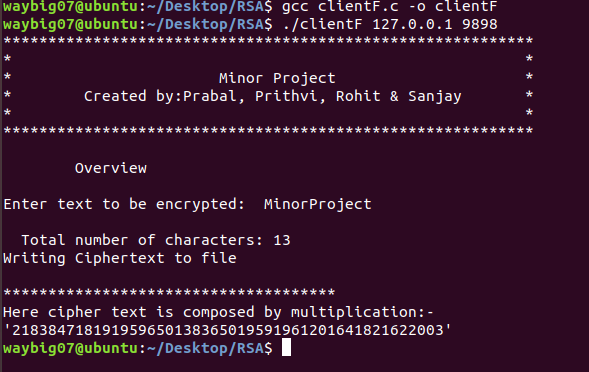
**File Transfer in Socket Programming**



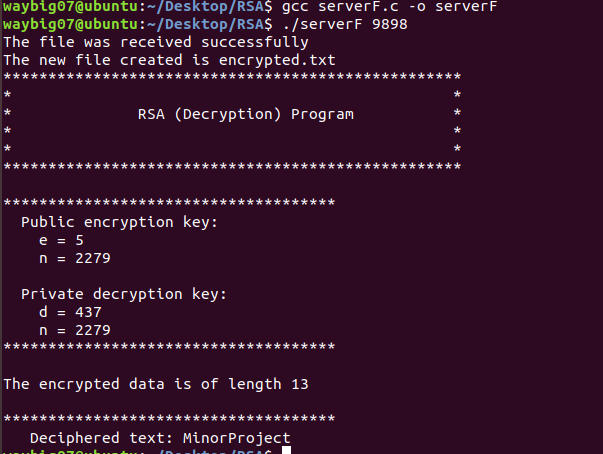


**Socket Programming in RSA Algorithm**

**Client Side**



**Server Side**



# **Conclusion and Future Scope**

Conclusion:

Encryption and decryption algorithms can be applied to almost every device that we used today.

1. In order to avoid any leakage and threat, cryptography should be used in network  security to encrypt and decrypt sensitive information and private messages.

2) It can be achieved by using some of the above-mentioned strategies to

improve the transfer of personal data as well as to protect the transaction.

3) A fair secrecy, verification, integrity, access control and data availability unit is maintained through the use of encryption techniques.

.

Future Scope:

1) It becomes easier to encrypt data with technical development, and it becomes easier to keep data secure with neural networks. Google Brain's neural networks have worked to build encryption without teaching complex encryption algorithms.

Data Science and Cryptographers are figuring out how to block brute force

assault on encryption algorithms and stop any unwanted access to sensitive data.

## 2) We will apply RSA to cryptocurrencies ->

For the development and encryption of blockchain wallets, most blockchains implement a  similar approach to the RSA algorithm. Here's how cryptos are used for asymmetric encryption:

When creating a cryptocurrency wallet, a public address and a private key are generated.

* The public address can be used to obtain cryptocurrency and on the blockchain to  consult the balance.
* The private key, on the other hand, would be used to unlock and invest your crypto in correlation with this public key.

**References**

1. •<https://www.google.co.in/search?q=socket+prgramimg&oq=socket+prgramimg>
2. •[https://c-program-example.com/2012/04/c-program-to-encrypt-and-decrypt-a-password.html](http://https/c-program-example.com/2012/04/c-program-to-encrypt-and-decrypt-a-password.html)
3. •<https://randomnerdtutorials.com/how-to-make-two-esp8266-talk/>
4. •[https://documentation.progress.com/output/ua/OpenEdge\_latest/gscsv/encryption-2fdecryption-algorithms.html#:~:text=Encryption%2Fdecryption%20algorithms&text=The%20AES%20cipher%20is%20the,key%20based%20on%20a%20passphrase.](https://inc-powerpoint.officeapps.live.com/pods/%C2%A0https:/documentation.progress.com/output/ua/OpenEdge_latest/gscsv/encryption-2fdecryption-algorithms.html)
5. •<https://en.wikipedia.org/wiki/Encryption>
6. •<https://patents.google.com/patent/US7013387B2/en>
7. •<https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm>