TRIBHUWAN UNIVERSITY

INSTITUTE OF SCIENCE AND TECHNOLOGY

BIRENDRA MULTIPLE CAMPUS

A PROJECT REPORT ON

“Applied Cryptography in Communication”

This project report is submitted in partial fulfillment of the requirement for the degree of Bachelors of Science in Computer Science and Information Technology.

Submitted by

Bijaya Pokhrel	(TU Roll No 21666/075)
Chetan Rijal	(TU Roll No 21672/075)
Dipesh Bhandari	(TU Roll No 21673/075)

Submitted to

Birendra Multiple Campus

Department of Computer Science and Information Technology

Bharatpur, Chitwan

BIRENDRA MULTIPLE CAMPUS

Bharatpur, Chitwan

SUPERVISOR’S RECOMMENDATION

I hereby recommend that this project prepared under my supervision by team of **Bijaya Pokhrel, Chetan Rijal & Dipesh Bhandari** entitled **“Applied Cryptography in communication”** is accepted as fulfilling in partial requirements for the degree of Bachelor of Science in Computer Science and Information Technology. In my best knowledge, this is an original work in Computer Science by them.

. . . .

Er. Binod Sharma

SUPERVISOR

Department of CSIT

Birendra Multiple Campus

Bharatpur, Chitwan

Tribhuwan University

Institute of Science and technology

BIRENDRA MULTIPLE CAMPUS

Bharatpur, Chitwan

LETTER OF APPROVAL

This is to certify that the project prepared by **Bijaya Pokhrel, Chetan Rijal** and **Dipesh Bhandari** entitled **“Applied Cryptography in Communication”** in partial fulfillment of the requirement for the degree of Bachelors of Science in Computer Science and Information Technology has been well studied and prepared. In our opinion, it is satisfactory in the scope and quality as a project for the required degree. The project was carried out under special supervision and within the time frame prescribed by the syllabus.

Signature of Supervisor **……………………………….** **Er. Binod Sharma**	**Signature of HOD/Coordinator** **……………………………….** **ER. Binod Sharma**
Signature of External Examiner **……………………………….**	**Signature of Internal Examiner** **……………………………….**

ACKNOWLEDGEMENT

First of all we would like to thank our supervisor **Er. Binod Sharma** for his guidance, we couldn't have asked for a better mentor for monitoring and helping us in this project with his knowledge and expertise. We would also like to thank **Mr. Dip Sharma** for his guidelines, his vast knowledge and expertise in Cryptographic Science helped us a lot in this project. This project would not have been success without contribution of each and every one of us, we were always there to cheer and support each other and working together until the end.

We would like to thank **Tribhuwan University** for providing us opportunity to do this project. Finally we would like to thank our family and friends for always being there for us providing constant motivation and support. We would like to thank each and every one of them who were involved indirectly or directly during this journey of creating the project.

ABSTRACT

The project **"Applied cryptography in Communication"** is the practice of using cryptography technique and protocols to secure communication and protect data. This project ensures that our data is only accessible by intended receiver without any alteration or modification of data. Cryptography uses technique to cipher data and make data encrypted and unreadable unless decrypted by algorithms predefined by the sender. Here, at first we register our email and put password for login. After that, we can send an email to other user who is linked to that system. We applied Diffie- Hellman key exchange and the key generated from there will be used in DES for Communication. Receiver convert a unordered message to human readable format using key. In this way, we can secure a message from unauthorized access.

TABLE OF CONTENTS

List of Figures

List of Tables

List of Abbreviation

1. SDLC: System Development Life Cycle
2. SQL: Structured Query Language
3. iOS: iPhone Operating System
4. DFD: Data Flow Diagram
5. OTP: One Time Password
6. GUI: Graphical User Interface
7. DHKE: Diffie-Hellman Key Exchange
8. DES: Data Encryption Standard

Chapter 1: Introduction

1.1 Introduction

Cryptography is a technique of secure communication that deals with developing and analyzing protocols, capable of providing information security[1]. It is an essential aspect of modern communication systems, providing confidentiality, integrity, and authenticity to the information transmitted over networks. In this proposal, we outline our plan to integrate advanced cryptography techniques into an email application, ensuring that user communications are secure and protected from unauthorized access.

Our proposed email application will use a combination of symmetric and asymmetric cryptography, as well as hash functions, to provide strong security for all email communications. In addition, we will implement authentication protocols to verify the identity of users and prevent unauthorized access to their accounts[2].

We believe that our email application, with its cryptography capabilities, will provide users with a high level of security and peace of mind when communicating online.

1.2 Problem Statement

Nowadays, the use of informative data is increasing day by day. Most people have Little knowledge about how to protect their factual data from unauthorized users. Many people just give their credential information in open source where many user can access their data in a easy way. We want to overcome such vulnerability method in important data. We want to give access of data only to the known users. Only cryptography can protect our data from hackers or unknown users. With the help of cryptography we can securely use our password in vast network for online purchase and e-banking. Cryptography is used to secure all transmitted information in the world connected by internet. For example bank transactions wouldn’t be safe without cryptography. Without Cryptography internet traffic would come to halt and we can no longer make phone calls. International organization cannot protect their valuable data and the information, which could be exposed and cause huge loss. Cryptography is one of those areas where a little knowledge goes a long way. Even understanding a few basic terms can really help you in using encryption services, and will mean that you are less likely to get ripped off by over-paid security.

1.3 Objectives

The main objectives of our project to develop a email application, with cryptography capabilities, which will provide users with a high level of security and peace of mind when communicating online. The main objectives of our project focuses on:

- To develop a secure email application that uses cryptography techniques to protect the confidentiality, integrity, and availability of email communications.

- To design an email application that is user-friendly and easy to use, with elegant interfaces and features that make it easy for users to send and receive encrypted emails.

- To promote the need of cryptography techniques among individuals, businesses and organizations that are concerned about the security of their email communications.

- It ensures authentication by verifying the identity of user to sender and client.It ensures receiver that the data received is sent from verified user.

1.4 Scope and Limitation

1.4.1 Scope

- The email application is developed for use on desktop devices including laptops and PC that need minimum hardware requirements.
- The email application will use advanced cryptography techniques, including public key cryptography.
- The email application will be designed to be user-friendly and easy to use.
- Email encryption helps to protect our critical business data and personal information. As our email can contains lot of sensitive information.
- After using encryption program, we don't need to purchase additional software for security. Hence a lot of money can be saved instead of buying a third party service.

1.4.2 Limitation

- It may provide no security if the users devices password is compromised.
- Failure in key management and key leakage can compromise the security of the system.
- When the information is strongly encrypted it can be difficult to access even for genuine user at crucial time.
- The error caused by poor design from human such as weak password and poor implementation cannot be guarded by cryptography.

1.5 Development Methodology

To develop a software product, there must be a clear understanding among team representative about when and what to do. Software development life cycle plays themost important role in developing a software. Software life cycle model is a pictorial and diagrammatic representation of the software life cycle. A life cycle model represents all the methods required to make a software product transit through its life cycle stages. It also captures the structure in which these methods are to be undertaken. There are different software models to implement the SDLC like waterfall model, spiral model, incremental model, iterative model, v-model, agile model, rad model etc.

Among these, we have implemented waterfall model in our project. Waterfall model was introduced by Winston Royce in 1970 which was the first process model to be introduced. Waterfall model is the basic software development life cycle model which is very simple but idealistic. It is a systematic and sequential approach to software development that begins with projects specification of requirements and progresses through planning, modeling, construction and deployment, culminating in ongoing support of the completed software[3]. In this model, each phase must be completed before the beginning of the next phase so that there is no overlapping of the phases. Typically, the output of the one phase acts as the input for the next phase sequentially.

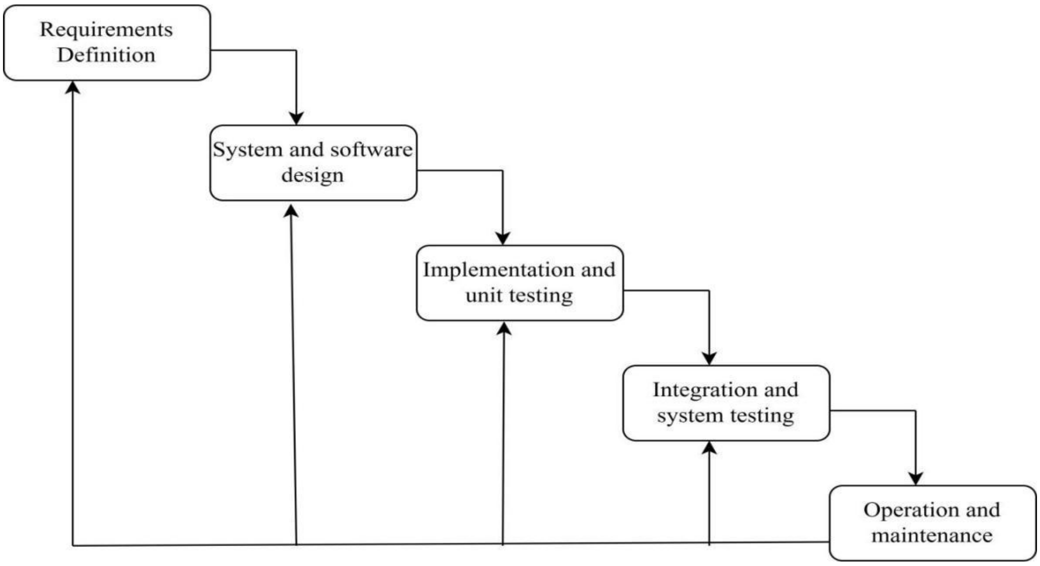

Requirements Definition
System and software design
Implementation and unit testing
Integration and system testing
Operation and maintenance

Fig 1: Waterfall model

1.6 Waterfall Model Phases

The phases of waterfall model are explained below:

A. Requirements definition:

The aim of this phase is to understand the exact requirement of the project and document them properly. Firstly, all the requirements of the customer regarding software are gathered and analyzed which are then documented in a software requirement specification(SRS) document.

B. System and software design:

The system design process allocates the requirements to either hardware or software systems. It establishes an overall system architecture.

C. Implementation and unit testing.

During this stage, software design is converted into a source code using any suitable programming language where each designed module is coded. Unit testing involves verifying that each unit meets its specification.

D. .Integration and system testing:

In this stage, the integration of different designed module in the form of code are integrated and tested as a complete system in order to ensure that the full working system is obtained.

E. Operation and Maintenance

This is the final stage where the system is installed and brought into practical use. Maintenance involves correcting errors that were not discovered in earlier stages of the life cycle in order to enhance and improve the system services. Corrective maintenance, perfective maintenance and adaptive maintenance are carried out in this stage.

1.7 Report Organization

This document is categorized into several chapter and further divided into sub chapter. It is organized as:

- Chapter 1: This chapter is about introduction of our project, which includes problem statement, objectives, scope and limitation, and development methodology.
- Chapter 2: In this chapter background study and literature review is done.
- Chapter 3: This chapter is about system analysis. It also includes requirement analysis and feasibility analysis
- Chapter 4: This chapter includes context diagram of system, it also has data flow diagrams and algorithm details.
- Chapter 5: In this chapter implementation and testing is done. It includes details about the tools used in the project. Unit testing and system testing is also done in this chapter.
- Chapter 6: This chapter consists the conclusion of our project, it also includes future recommendations about changes and possibilities.

Chapter 2: Background Study and Literature Review

2.1 Background Study

In context of Nepal, the need of Cryptography is increasing day by day with growing use of digital technology and internet, which leads to increase in cyber threats such as data theft, identity theft and cyber attacks. With rapid advancement in web technology there is a growing needs to protect sensitive information, and other confidential information from these threats.

Nepal has made significant progress in recent years towards digitization, including the introduction of e-governance and use of digital technology in financial sector. However the lack of proper cryptography measures in communication and the absence of a comprehensive legal framework for cyber security leaves Nepal vulnerable to data and information theft.

Cryptography plays a crucial role in securing digital communication and information systems, and it is essential for protecting sensitive information and preventing cyber attacks. The use of cryptography can help ensure the confidentiality, integrity, authenticity, and non-repudiation of digital communication and information systems, which is essential for protecting the privacy and security of Nepali citizens and business.

The Nepali government has recognized the importance of cyber security and cryptography in communication, and there have been efforts to promote use of cryptography measures and secured communication. However there is still a long way to go in terms of implementing effective cryptography measures and ensuring the security of digital communication and information systems in Nepal.

2.2 Literature Review

Cryptographic communication application are becoming increasing popular as people become more aware of the importance of securing their communication. In this literature review, we will examine some of other cryptographic communication application that are available.

1. Signal - Signal is a free and open source messaging application that provides end to end encryption. It is available for both Android and iOS platforms. Signal uses the same encryption protocol as WhatsApp, but it has more transparent encryption policy.

2. Telegram - Telegram is another messaging application that provides end to end encryption. It is available for Android , iOS and desktop platforms. Telegrams encryption protocol is not as secure as as Signal's, but it does offer more features such as group chat and self-destructing messages.

3. ProtonMail - ProtonMail is a secure email service that provides end-to-end encryption. It is available for both Android and iOS platforms. ProtonMail is based in Switzerland, which has some of the strongest privacy laws in the world.

4. Threema - Threema is a messaging application that provides end-to-end encryption. It is available for both Android and iOS platforms. Threema does not require users to provide their phone number and email address, which makes it more private than other messaging applications.

In conclusion, there are several cryptographic communication application available that provides end-to-end encryption. These application offer varying level of security and features, so it is important to choose the ones that best fits your needs.

Chapter 3: System Analysis

3.1 System Analysis

System analysis is a process of studying and evaluating the security of cryptographic communication system. It involves analyzing the system's architecture, protocols and algorithm to identify potential vulnerabilities and threats to the system's security.

Overall, system analysis is an essential component of an applied cryptography in communication, as it helps to ensure that cryptographic systems are robust, secure and effective in protecting sensitive data and information.

3.1.1 Requirement analysis

Requirement analysis in applied cryptography is the process of identifying and analyzing the security requirement of a cryptographic communication system. It involves identifying needs of system users, security objectives, security threats and evaluating them. After evaluation system must be reviewed and update requirements. By identifying and analyzing the security requirements of the system, developers can ensure that the system is designed to meet the need of its users while providing effective protection against potential security threats.

i. Functional Requirements

The functional requirements for an application of applied cryptography in communication can be divided into several categories, including:

1. Authentication: The system should provide a mechanism for authenticating users and devices involved in the communication. This could include username/password authentication, two-factor authentication, or digital certificates.

2. Key management: The system should generate and manage encryption and decryption keys for secure communication. This could include key generation, key exchange, and key storage.

3. Encryption and decryption: The system should provide the ability to encrypt and decrypt messages to ensure confidentiality of the communication. This could include the use of symmetric or asymmetric encryption algorithms.

4. Digital signatures: The system should provide the ability to create and verify digital signatures to ensure the authenticity and integrity of messages.

Overall, these functional requirements ensure that the application of applied cryptography in communication provides a secure and reliable communication channel for the parties involved.

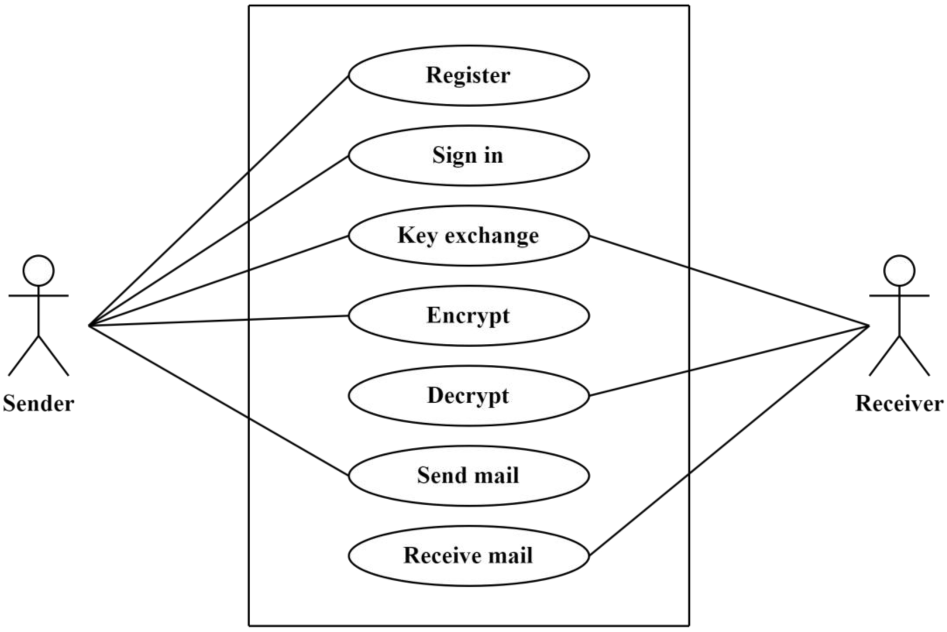


Fig2 : Use case diagram of the system

ii. Non-Functional Requirement

Cryptographic communication has several non functional requirements that are important to consider. Non functional requirements define the overall behaviour, performance, and quality attributes of the system. Some of key non-functional requirements for cryptographic communication application are:

1. Security: The most important requirement of cryptographic application is to to ensure confidentiality, integrity, and authenticity of communicated data. The system should have necessary protocols to protect sensitive information from unauthorized access.

2. Availability and Reliability: The application should be highly applicable and reliable. It should be able to handle system failure and have backup and disaster recovery plan.
3. Scalability: The application should be able to handle increasing number of user without significant impact on performance.
4. Usability: The application should provide user friendly interface that makes it easy for users to communicate securely. The operations should be transparent to users and help user to understand and resolve in case of any issue.
5. Interoperability: The application should be designed to work on different devices and environment. It should be widely accepted across various systems.
6. Maintainability: The update and maintenance should be user friendly, and the system should have proper documentation and version control to support ongoing maintenance.

3.1.2 Feasibility Analysis

Feasibility study is an analysis and evaluation of a proposed project to ensure that it is technically, economically and operationally feasible. It mainly focus on whether the proposed project idea should be proceed or not in terms if various factors.

i. Technical

Technical feasibility evaluates the proposed project can compiles with current technologies, which are needed to accomplish needed requirements. The web application of the project is supported by almost all devices with minimum hardware and software requirements.

ii. Operational

This project provides the application of cryptography in communication process so that the end-to-end encryption is applied during communication. Technically speaking, it’s a web application that provide secure exchange of information and data in this world of the internet.

iii. Economic

We concluded this project to be economically feasible as there was not issue of economic cost and resources as there is only an estimation of cost of effort.

3.2 Schedule

Here we analyzed the the time required to complete the project and identified that the project will fail if it took too long to complete and determine some targeted milestones and time frames for completion as a guideline only.

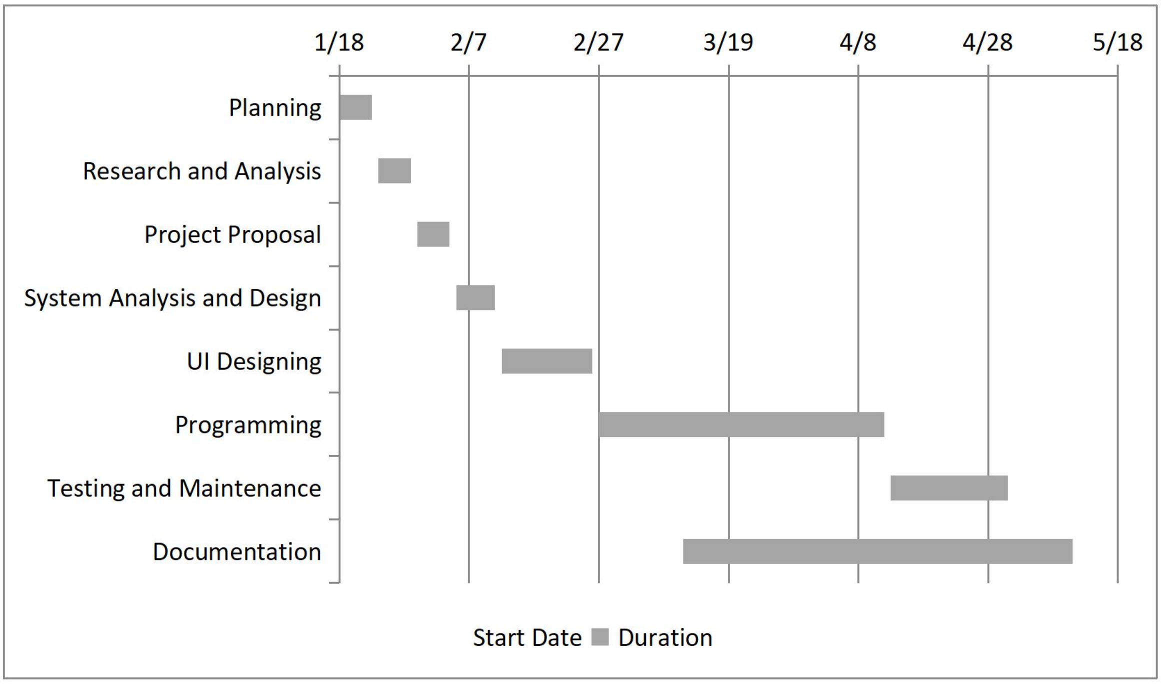
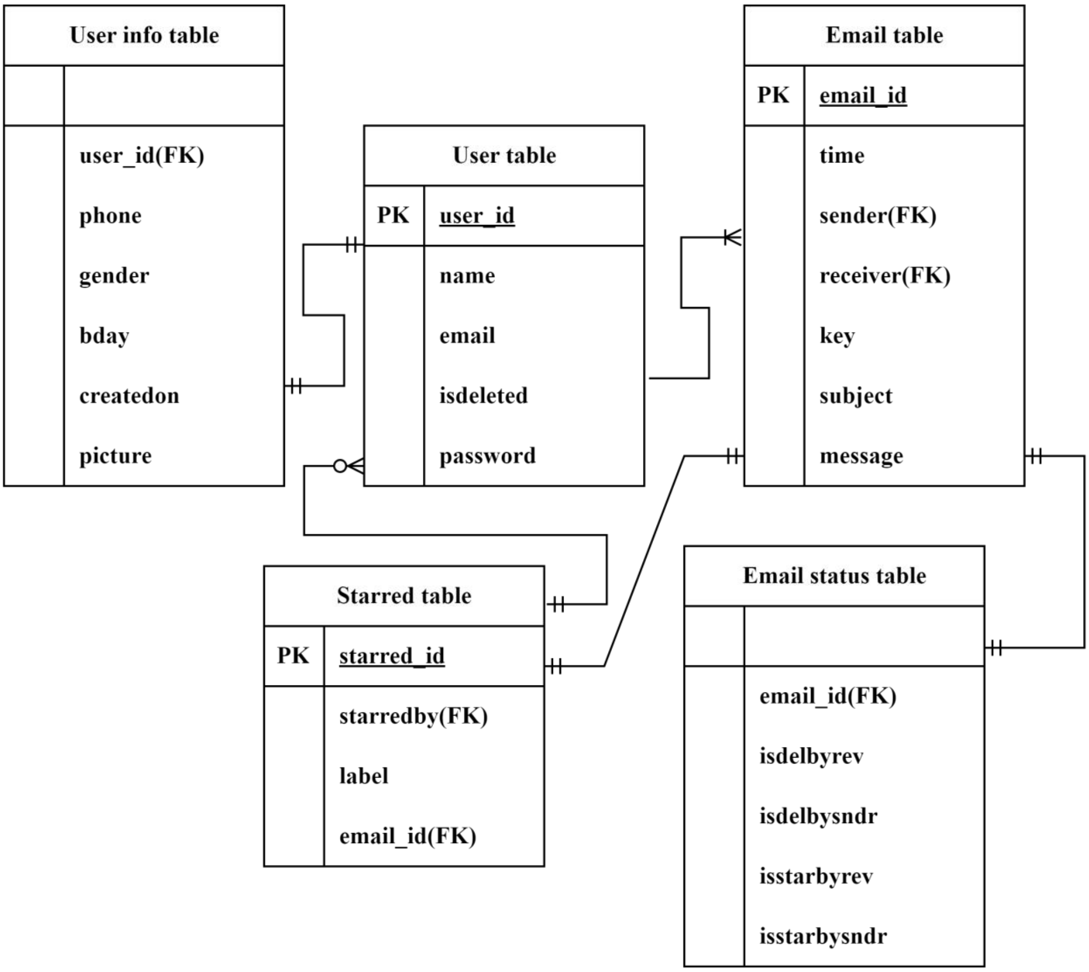


Table 1: Gantt Chart

Chapter 4: System Design

4.1 Database Schema

A database schema is the outline that represents the logical view of the entire database. It defines how the data is structured and how the relations among them are related. It formulates all the constraints that are to be applied to the data.



User info table	
	user_id(FK) phone gender bday createdon picture

User table	
PK	user_id
	name email isdeleted password

Email table	
PK	email_id
	time sender(FK) receiver(FK) key subject message

Starred table	
PK	starred_id

	starredby(FK)
	label
	email_id(FK)

Email status table	
	email_id(FK) isdelbyrev isdelbysndr isstarbyrev isstarbysndr

Table 2: Database Schema

4.2 Context Diagram

In the Design phase of the SDLC, the logical model of the database and the interface of the system is designed. The normalization of the database schema is done in this phase. The context diagram of our proposed system is shown below.

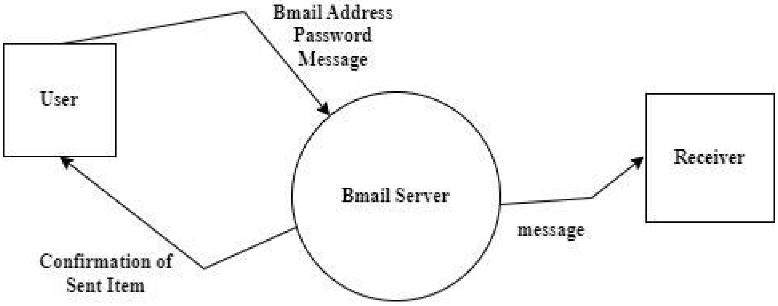


Fig 3: Context diagram of the system

4.3 Data Flow Diagram

A data flow diagram(DFD) is a graphical representation of the flow of data within a system or process. In the context of applied cryptography in communication, a DFD can be used to represent the flow of data through a cryptographic system.

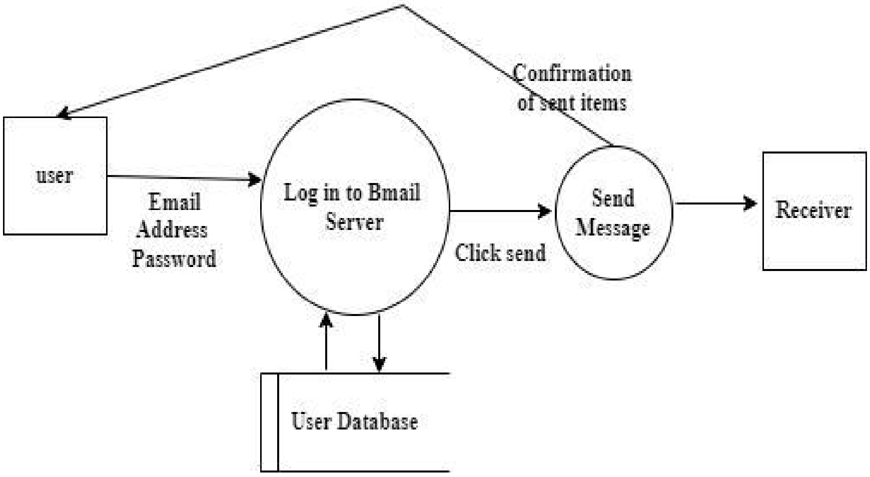


Fig 4: Level 0 DFD of the system

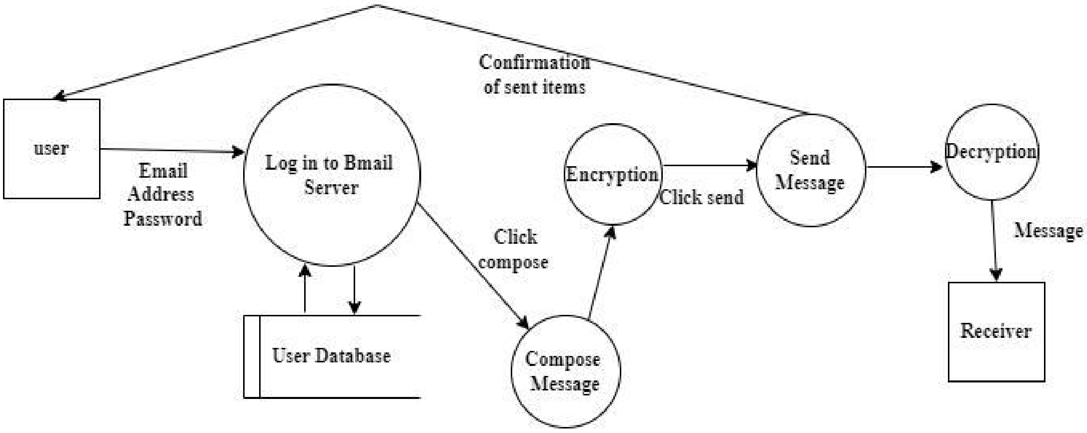


Fig 5: Level 1 DFD of the system

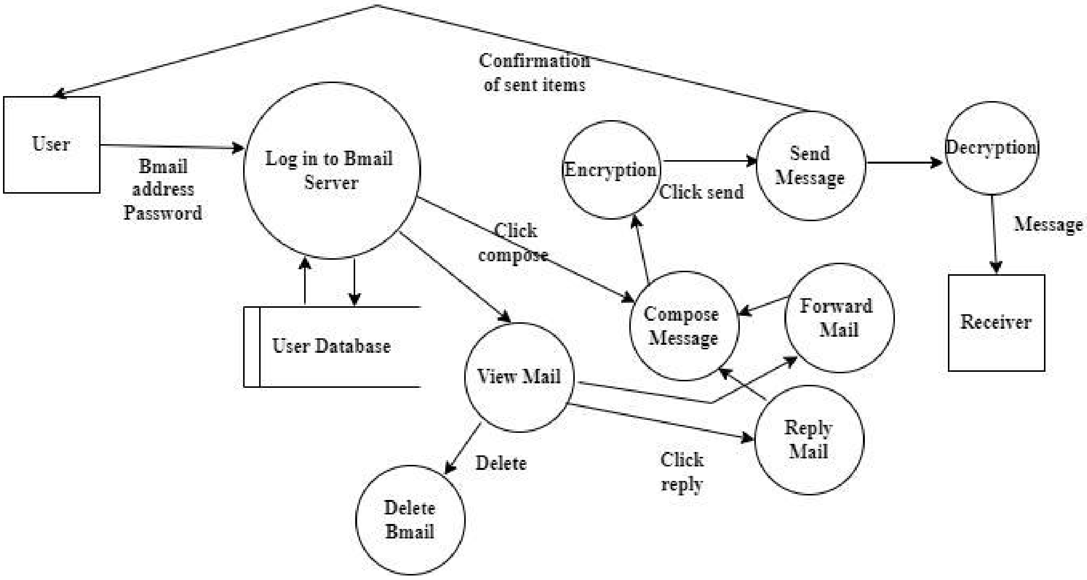


Fig 6: Level 2 DFD of the system

4.4 Algorithm details

4.4.1 Diffie-Hellman key exchange

Diffie-Hellman key exchange is a cryptographic protocol that allows two parties to establish a shared secret over an insecure communication channel[4]. It was developed by Whitfield Diffie and Martin Hellman in 1976 and is widely used in modern encryption process. It is not directly involved in the process of sending an email. However, once a shared secret key is established through Diffie-Hellman, it can be used for encryption and decryption of email messages.

Lets take famous example of Alice and Bob to display Diffie-Hellman key exchange

1. Agreement on parameters:

- Alice and bob both agree on a prime number (p) and a base value (g), which are publicly known. These parameters can be shared through a secure channel or agreed upon in advance.

2. Private key generation:

- Alice chooses a secret integer (a) as her private key.
- Bob chooses a secret integer (b) as his private key.

3. Public key calculation:

- Alice calculates her public key (A) by performing (g^a) mod p
- Bob calculates his public key (B) by performing (g^b) mod p

4. Exchange of public keys:

- Alice shares her public key (A) with Bob.
- Bob shares his public key (B) with Alice.

5. Shared secret key derivation

- Alice calculates the shared secret key (S) by performing (B^a) mod p.
- Bob calculates the shared secret key (S) by performing (A^b) mod p.

After the key derivation step, both Alice and Bob now have the same shared secret key "s." This key can be used for symmetric encryption, using DES to securely communicate over the insecure channel. Since the private keys are never exchanged, the attacker listening to the conversation would find it computationally infeasible to derive the shared secret key from the exchanged public keys.

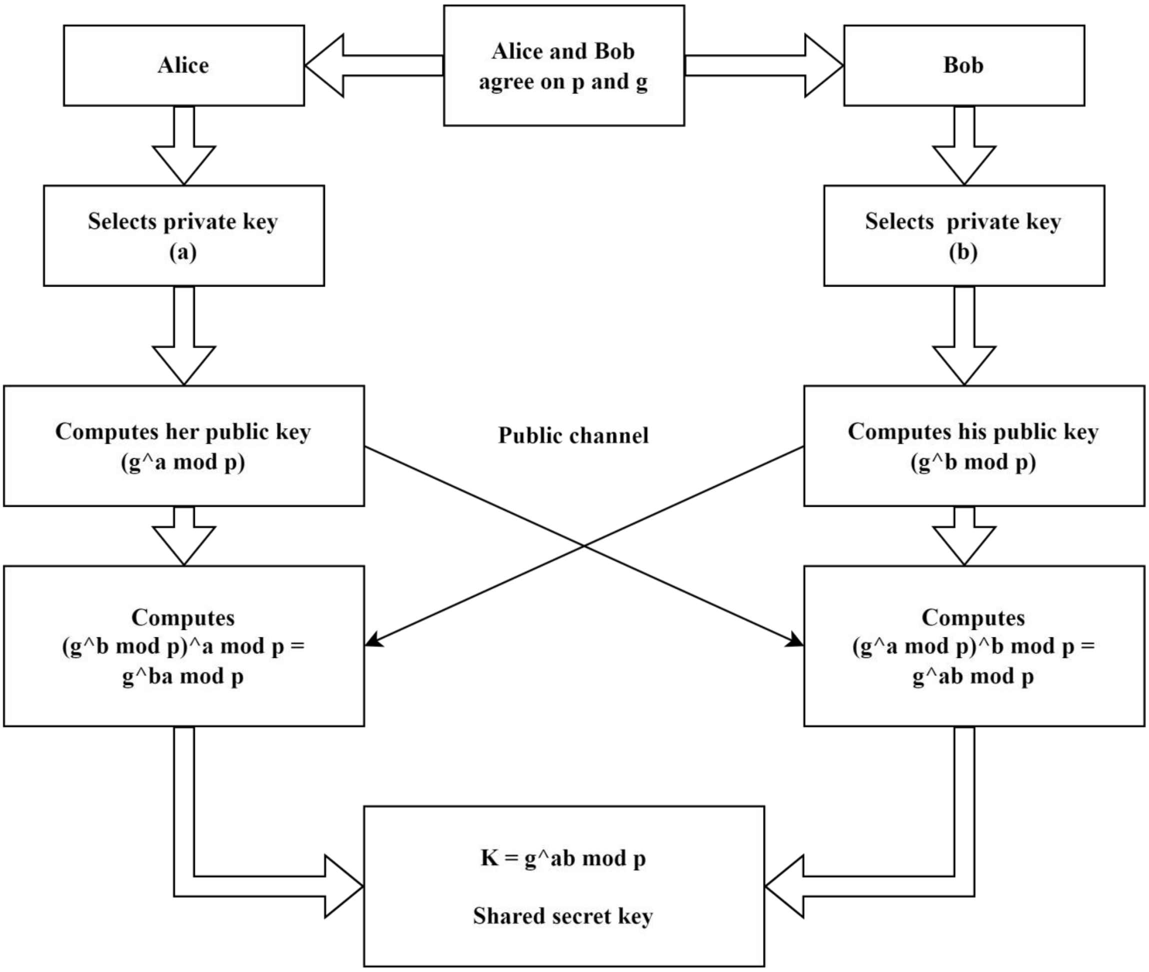

Alice
Alice and Bob agree on p and g
Bob
Selects private key (a)
Selects private key (b)
Computes her public key (g^a mod p)
Public channel
Computes his public key (g^b mod p)
Computes (g^b mod p)^a mod p = g^ba mod p
Computes (g^a mod p)^b mod p = g^ab mod p
K = g^ab mod p
Shared secret key

Fig 7: Diffie-Hellman key exchange

4.4.2 DES Algorithm

The DES (Data Encryption Standard) Algorithm is a block cipher that uses symmetric keys to convert 64-bit plain-text blocks into cipher-text using 48-bit keys. The DES

Algorithm was developed by the IBM team in the 1970s. It has been accepted by the National Institute of Standards and technology(NSIT).

The DES algorithm involves following process

1. Key Generation

- Takes a 64-bit key as input.
- Discards 8 bits for parity, resulting in a 56-bit key.
- Generates 16 48-bit sub-keys through a key schedule process.

2. Initial Permutation(IP):

- Rearrange the positions of the 64-bit plain text block based on a predefined table.

3. Feistal Network:

- Divides the block into two two 32-bit halves (left and right).
- Performs 16 rounds of encryption.

For each round:

a. Expansion:

- Expands the 32-bit right half to 48 bits by duplicating some bits.

b. Key Mixing:

- XORs the expanded right half with a 48-bit sub-key generated from the main key.

c. Substitution:

- Divides the result into eight 6-bit blocks.
- Replaces each block using predefined 4×16 substitution boxes(S-boxes).

d. Permutation:

- Concatenates the output of the S-boxes into 32-bit block.
- Rearrange the bits using a predefined permutation table.

e. Mixing:

- XORs the permuted block with the half of the previous round.

- Result becomes the new right half.

After 16 rounds, the left and right halves are swapped.

4. Final Permutation(FP):

- Applies the inverse of the initial permutation.
- Produces the 64-bit cipher-text block.

The same process can be used for decryption, with the subkeys applied in reverse order.

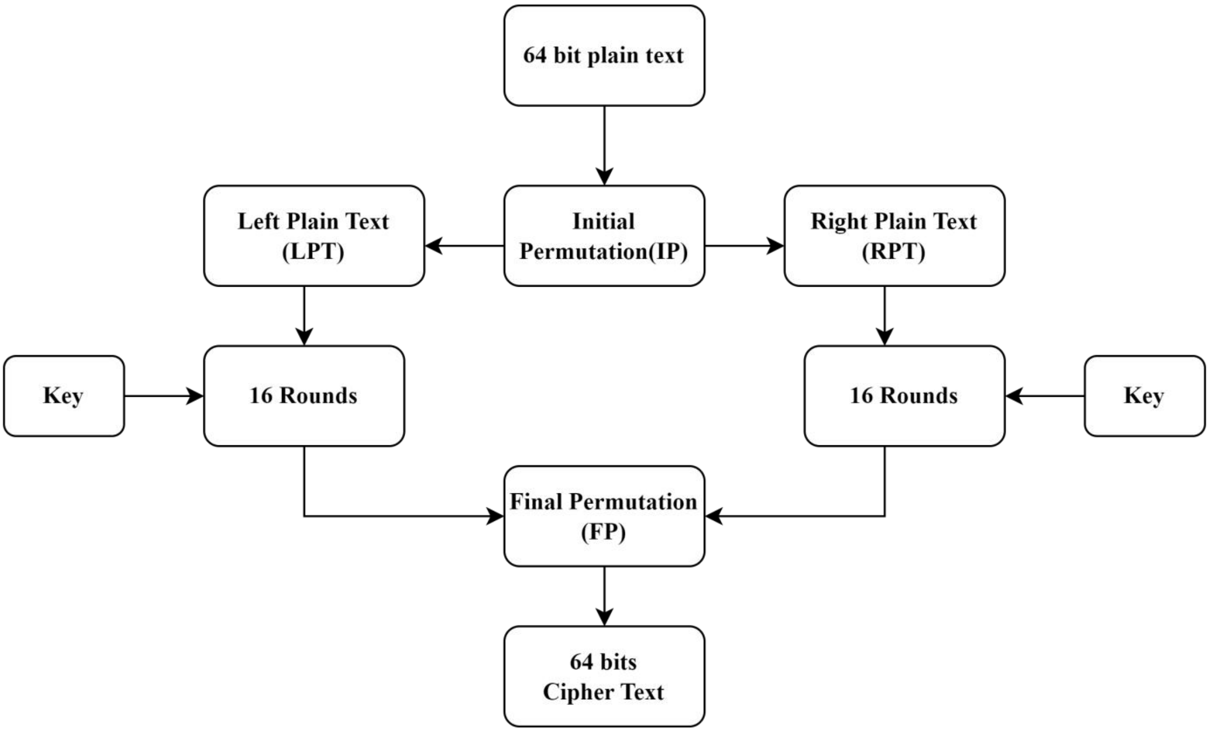


Fig 8: DES Algorithm

Chapter 5: Implementation and Testing

5.1 Implementation

The implementations and testing phase refers to the final stage of moving the solution from development status to production status. In this phase, project developers begin building and coding the software. This phase is followed by software development life cycle models used, tools and the description of major classes/methods.

5.1.1 Tools Used (CASE tools, Programming language, Database platforms)

- **Python**

Python programming language is suitable for our project as it has large standard library that includes modules for a wide range of application such as web development[5]. Python is powerful and versatile language making it good choice for our project work.

- **Tkinter**

Tkinter is python library used which will be used in our project to create graphical user interface of email application. It is simple and easy to use interface for our application. It allows us to customize the appearance and behaviour of GUI component using python code.

- **Socket programming**

Socket programming will be used in our email application as part of our project to send and receive emails over the network. It will be used to establish communication link between server and client.

- **PostgreSQL**

PostgreSQL server will be used to store and manage data for our project, and use SQL to query and manipulate the data. It provides a rich set of SQL commands for working with the data. It also helps to ensure the integrity and security of data in our project.

- **Figma**

Figma is a cloud-based design and cloud-based design and prototyping tool. Figma is used in our project to design user interfaces(UI), designs, and iterative prototypes. It provides a streamlined and collaborative platform for designers, developers, and stakeholders to work together in real time

- **Twilio**

Twilio is a cloud communication platform that provides a set of Application programming interface(API) and tools for developers. We use twilio to integrate messaging functionalities and communication capabilities in our application.

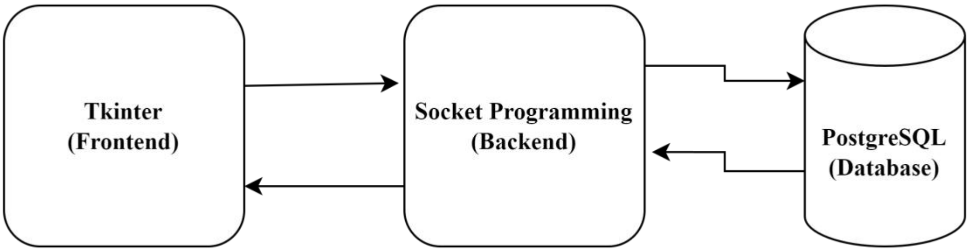


Fig 9: Block diagram of Bmail app

5.2 Testing

Software testing is the process of evaluating and verifying that a software product or application does what it is supposed to do. The benefits of testing include preventing bugs, reducing development costs and improving performance. Test management plan.

5.2.1 Testing case for unit testing

1. Test for sign up;

a) Test case: User fills all the sign up details and valid OTP.

- Expectation: An account created message box should be displayed.
- Result: Successful

b) Test case: User fills all the sign up details and invalid OTP.

- Expectation: An error message box should be displayed.
- Result: Successful

2. Test for sign in;

a) Test case: User fills Verified email and password.

- Expectation: User is successfully signed in to Bmail app and home menu will appear.
- Result: Successful

b) Test case: User fills Unverified email or password.

- Expectation: An error message box should be displayed.
- Result: Successful

3. Test for sending and receiving mail;

a) Test case: User composes a mail with title and body and sends to another email address registered within the system

- Expectation: Mail should be sent to inbox of another email address.
- Result: Successful

b) Test case: User composes a mail with title and body and sends to an unregistered email address.

- Expectation: An error message box should be displayed.
- Result: Successful

c) Test case: User clicks on inbox button.

- Expectation: Detailed history of all received mails should be displayed.
- Result: Successful

d) Test case: User clicks on sent button.

- Expectation: Detailed history of all outgoing mails should be displayed.
- Result: Successful

e) Test case: User replies to a received mail.

- Expectation: Reply mail is send to the email address of the user, whose mail was replied.
- Result: Successful

f) Test case: User forwards a sent or received mail to another registered email address.

- Expectation: Sent or received mail is forwarded to another registered address within the system.
- Result: Successful

4. Test for starred mail;

- Test case: User adds an important mail to starred list.
- Expectation: All the list of starred mail should be displayed.
- Result: Successful

5. Test for delete mail;

- Test case: User deletes a mail from his inbox or sent folder.
- Expectation: A mail is deleted from the inbox or sent folder of user.
- Result: Successful

6. Test for profile management;

- Test case: User wants to change his profile picture.
- Expectation: User can change his desired profile picture from the change picture in profile menu
- Result: Successful

7. Test for delete account from the system;

- Test case: User goes to his profile and clicks delete account.
- Expectation: Users account is deleted from the system.
- Result: Successful

8. Test for logout;

- Test case: User clicks on log out button on the system menu.
- Expectation: User is logged out of the system
- Result: Successful

5.2.2 Test case for system testing

- **Test for user authentication;**

We tested whether the system will detect and differ unregistered user from registered users. The system gave positive response and redirected unregistered user to sign up page while signing in.

- **Testing the entire email sending and receiving process;**

We tested the system for the entire email sending and receiving process, from composing email to receiving it at the recipient inbox. The system gave positive response.

- **Integration of GUI with backend functionality;**

We tested the system for the integration of the GUI with the backend functionality, to ensure that user interactions are handled correctly. The system gave positive response

- **Encryption and Decryption of mails;**

We tested the system for the message encryption and decryption process at the senders and receivers end. The system gave positive response.

Chapter 6: Conclusion and Future Recommendation

6.1 Conclusion

In conclusion the project **“applied cryptography in communication”** plays a crucial role in ensuring the security and privacy of information transmitted over various communication channels. Cryptographic techniques provide a robust framework for protecting sensitive data from unauthorized access, interception and manipulation.

Throughout this project, we explored different aspects of applied cryptography and its significance in communication. We discussed various cryptographic algorithms, such as encryption, decryption and hashing and their application in securing communication channels.

One of the key findings of this project is that applied cryptography enables secure communication by offering confidentiality, integrity, authentication, and non-repudiation of information. Through encryption data can be transferred into an unreadable form, ensuring that only authorized individuals with decryption keys can access and interpret the information.

While applied cryptography provides a strong foundation for secure communication, it is important to note that it is not foolproof. It requires proper key management, secure implementation, and continuous update to address emerging threats and vulnerabilities.

6.2 Future Recommendation

Our project is largely associated with cryptography, in field of cryptography in communication there are several areas that can be explored to enhance security and address emerging challenges. Here are our few recommendation for future

- Quantum resistant cryptography and key exchange
- Homomorphic encryption
- Blockchain-based communication protocols
- Improved usability and user experience

- Continuous monitoring and updates

By exploring these areas and implementing advancements in applied cryptography, we can enhance the security and privacy of communication system, adapt to evolving threats, and promote more secure communication in near future.

References and Bibliography

[1] Douglas R. Stinson, Cryptography: Theory and Practice, Third Edition

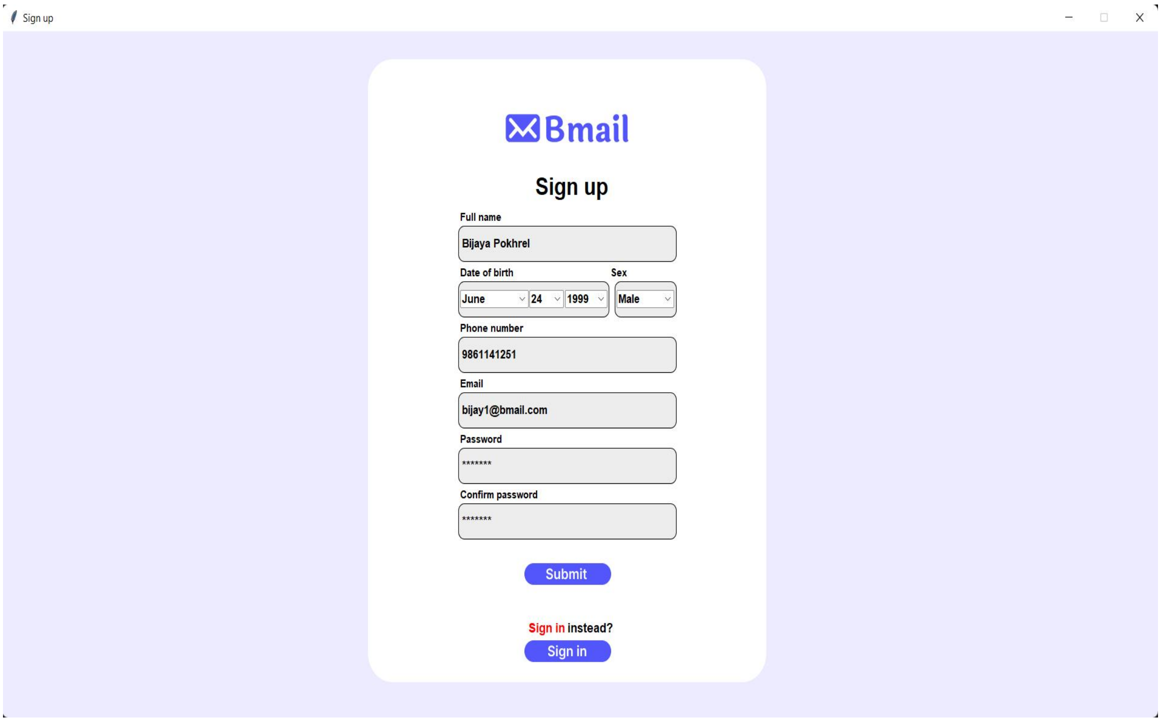
[2] Mark Stamp, Information Security: Principles and Practice, 3rd edition

[3] Winston W. Royce, Managing the Development of Large Software Systems

[4] Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654

[5] Adam Stewart, Python Programming

APPENDIX



Full name: Bijaya Pokhrel

Date of birth: June 24 1999

Sex: Male

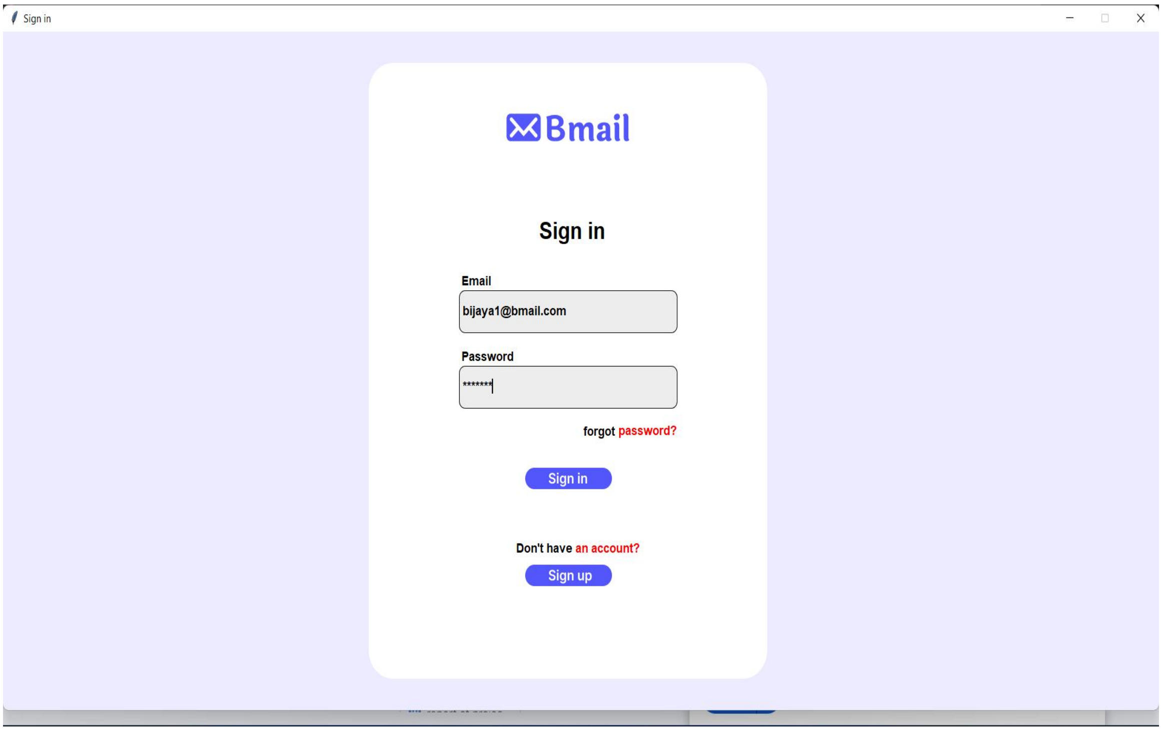
Phone number: 9861141251

Email: bijay1@bmail.com

Password: *******

Confirm password: *******

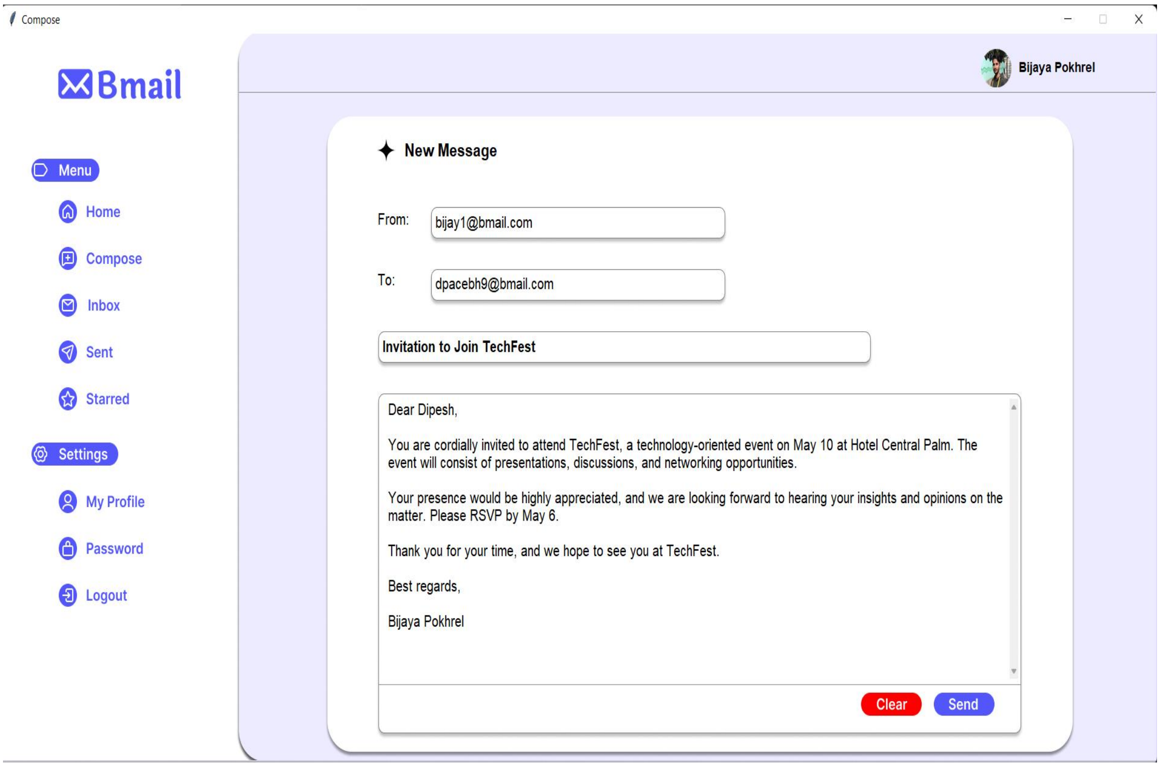
Sign up



Email: bijaya1@bmail.com

Password: *******

Sign in



From: bijay1@bmail.com

To: dpacebh9@bmail.com

Invitation to Join TechFest

Dear Dipesh,

You are cordially invited to attend TechFest, a technology-oriented event on May 10 at Hotel Central Palm. The event will consist of presentations, discussions, and networking opportunities.

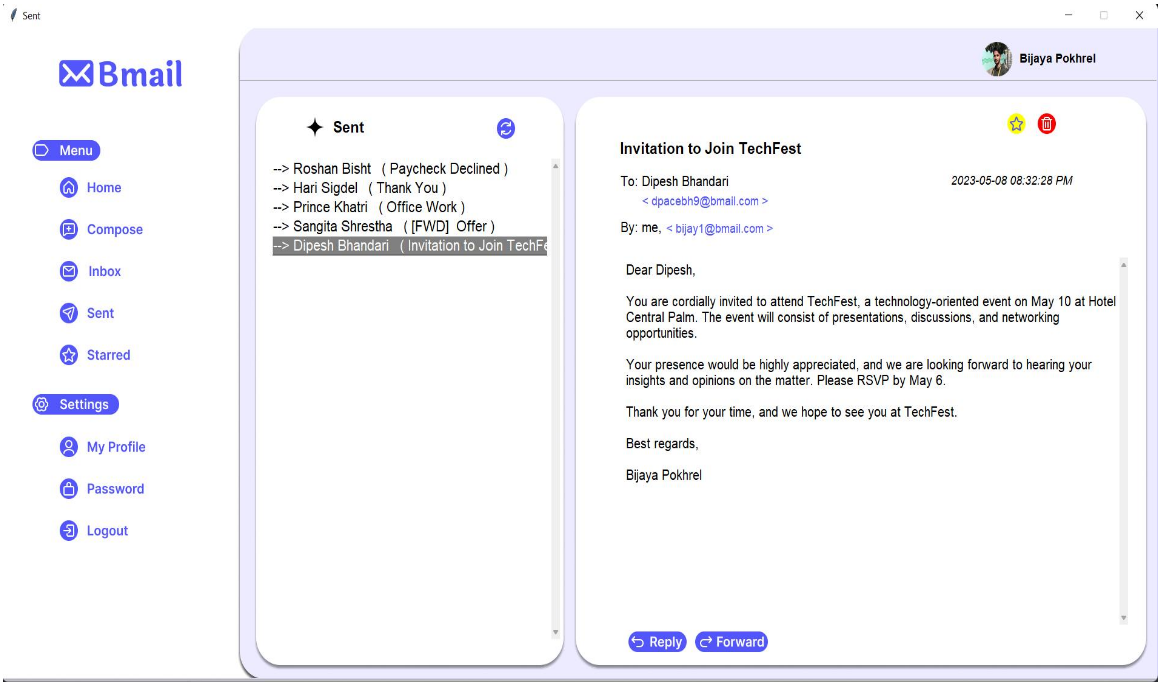
Your presence would be highly appreciated, and we are looking forward to hearing your insights and opinions on the matter. Please RSVP by May 6.

Thank you for your time, and we hope to see you at TechFest.

Best regards,

Bijaya Pokhrel

Compose



```
--> Roshan Bisht   ( Paycheck Declined )
--> Hari Sigdel   ( Thank You )
--> Prince Khatri   ( Office Work )
--> Sangita Shrestha   ( [FWD]  Offer )
--> Dipesh Bhandari    ( Invitation to Join TechFe
```

Invitation to Join TechFest

To: Dipesh Bhandari 2023-05-08 08:32:28 PM
< dpacebh9@bmail.com >

By: me, < bijay1@bmail.com >

Dear Dipesh,

You are cordially invited to attend TechFest, a technology-oriented event on May 10 at Hotel Central Palm. The event will consist of presentations, discussions, and networking opportunities.

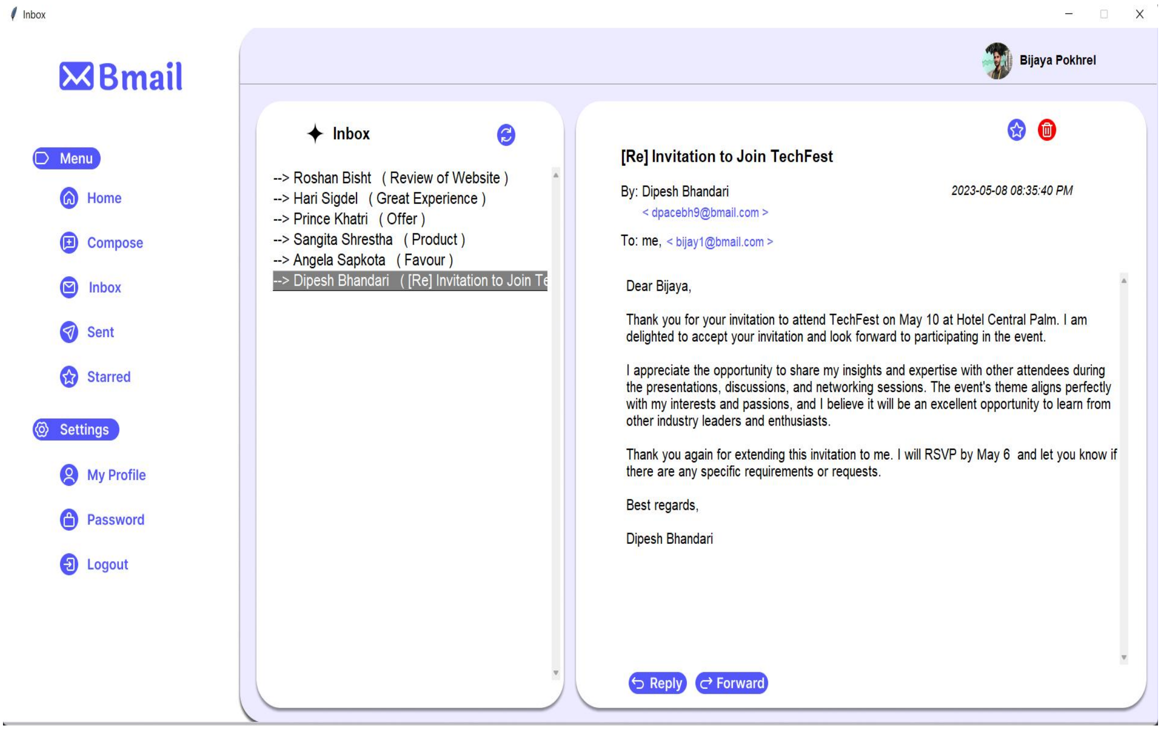
Your presence would be highly appreciated, and we are looking forward to hearing your insights and opinions on the matter. Please RSVP by May 6.

Thank you for your time, and we hope to see you at TechFest.

Best regards,

Bijaya Pokhrel

Sent



--> Roshan Bisht (Review of Website)
--> Hari Sigdel (Great Experience)
--> Prince Khatri (Offer)
--> Sangita Shrestha (Product)
--> Angela Sapkota (Favour)
--> Dipesh Bhandari ([Re] Invitation to Join Te

[Re] Invitation to Join TechFest

By: Dipesh Bhandari 2023-05-08 08:35:40 PM
< dpacebh9@bmail.com >

To: me, < bijay1@bmail.com >

Dear Bijaya,

Thank you for your invitation to attend TechFest on May 10 at Hotel Central Palm. I am delighted to accept your invitation and look forward to participating in the event.

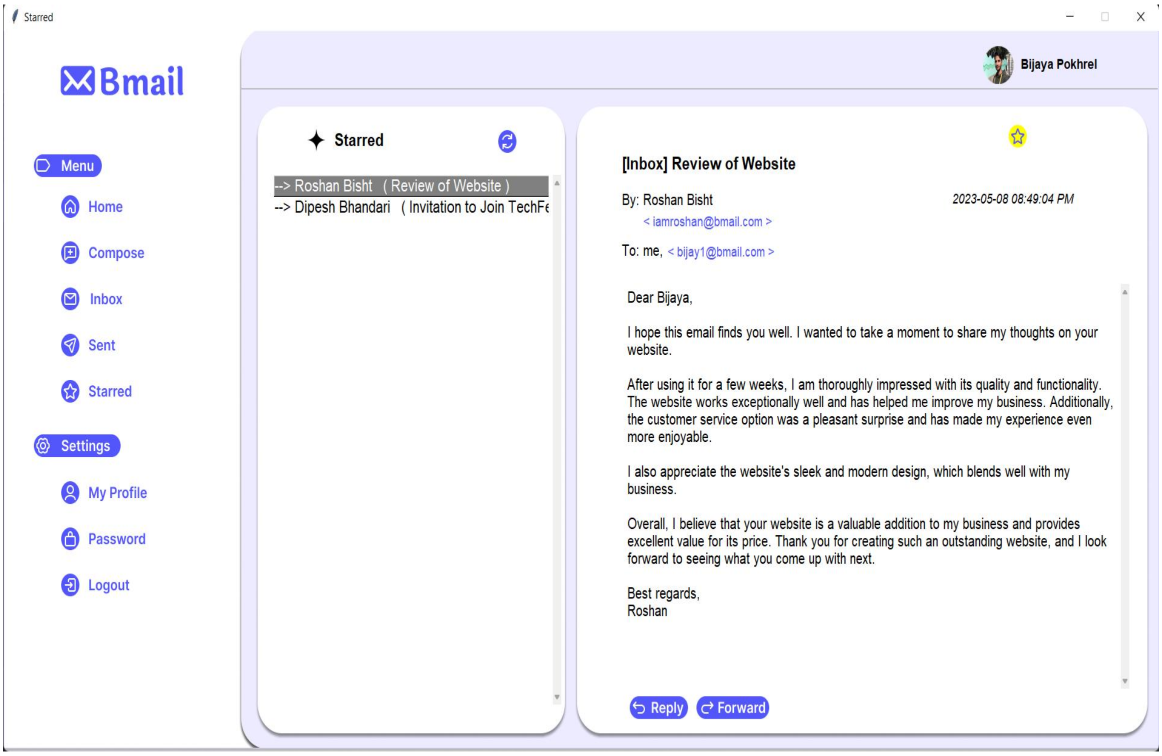
I appreciate the opportunity to share my insights and expertise with other attendees during the presentations, discussions, and networking sessions. The event's theme aligns perfectly with my interests and passions, and I believe it will be an excellent opportunity to learn from other industry leaders and enthusiasts.

Thank you again for extending this invitation to me. I will RSVP by May 6 and let you know if there are any specific requirements or requests.

Best regards,

Dipesh Bhandari

Inbox



--> Roshan Bisht (Review of Website)
--> Dipesh Bhandari (Invitation to Join TechFe

[Inbox] Review of Website

By: Roshan Bisht 2023-05-08 08:49:04 PM
< iamroshan@bmail.com >

To: me, < bijay1@bmail.com >

Dear Bijaya,

I hope this email finds you well. I wanted to take a moment to share my thoughts on your website.

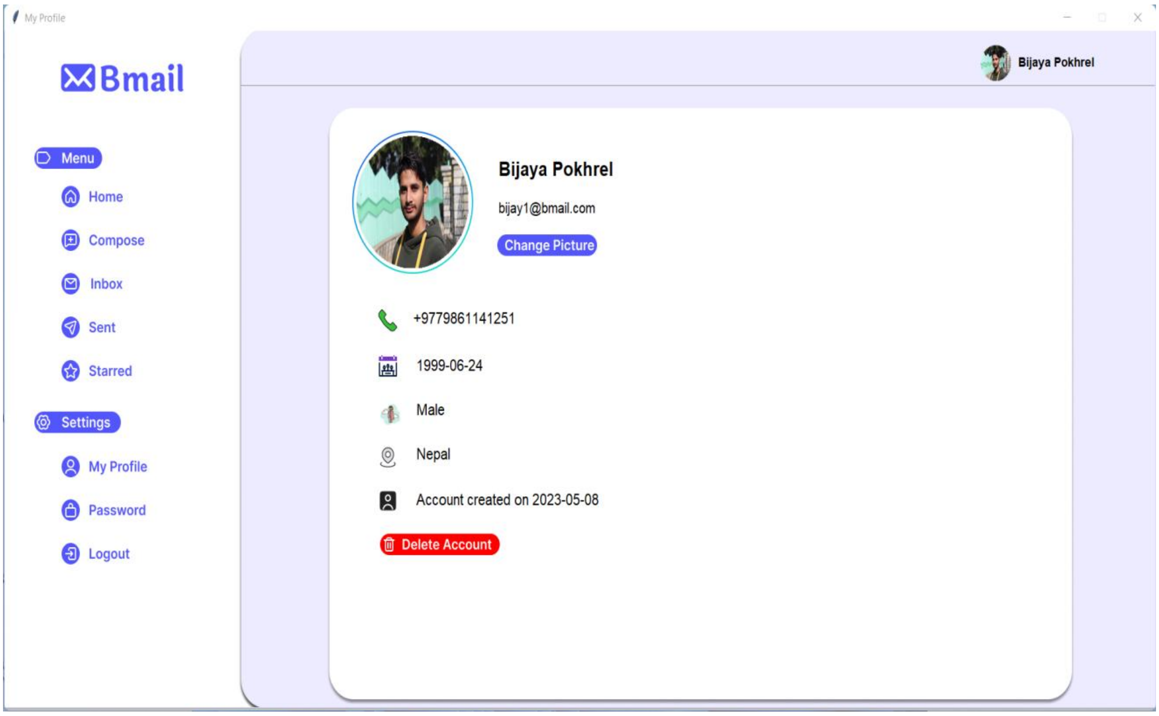
After using it for a few weeks, I am thoroughly impressed with its quality and functionality. The website works exceptionally well and has helped me improve my business. Additionally, the customer service option was a pleasant surprise and has made my experience even more enjoyable.

I also appreciate the website's sleek and modern design, which blends well with my business.

Overall, I believe that your website is a valuable addition to my business and provides excellent value for its price. Thank you for creating such an outstanding website, and I look forward to seeing what you come up with next.

Best regards,
Roshan

Starred



Bijaya Pokhrel

bijay1@bmail.com

☎ +9779861141251

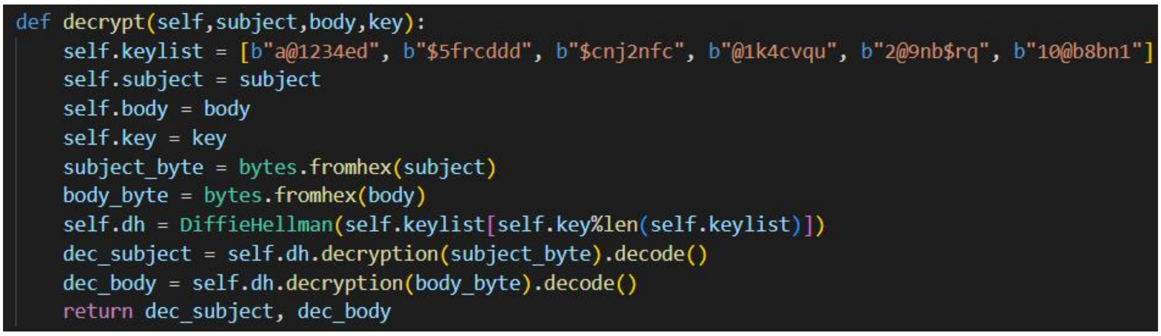
1999-06-24

Male

Nepal

Account created on 2023-05-08

Profile



```
def decrypt(self,subject,body,key):
    self.keylist = [b"a@1234ed", b"$5frcddd", b"$cnj2nfc", b"@1k4cvqu", b"2@9nb$rq", b"10@b8bn1"]
    self.subject = subject
    self.body = body
    self.key = key
    subject_byte = bytes.fromhex(subject)
    body_byte = bytes.fromhex(body)
    self.dh = DiffieHellman(self.keylist[self.key%len(self.keylist)])
    dec_subject = self.dh.decryption(subject_byte).decode()
    dec_body = self.dh.decryption(body_byte).decode()
    return dec_subject, dec_body
```

Code for Decryption