

Efficient Way of Result Publication by Using Cryptography

BY

Masab Hasnain

ID: 172-15-9811

Tanzuma Afroz

ID: 172-15-9764

Saifa Sabrina Mim

ID: 172-15-9853

This Report Presented in Partial Fulfillment of the Requirements for the Degree of
Bachelor of Science in Computer Science in Engineering.

SUPERVISED BY

Mr. Abdus Sattar

Assistant Professor

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

MAY 2021

APPROVAL

This Project/internship titled **EFFICIENT WAY OF RESULT PUBLICATION BY USING CRYPTOGRAPHY**, submitted by **Masab Hasnain, Tanzuma Afroz, Saifa Sabrina Mim** ID No:172-15-9811,172-15-9764,172-15-9853 to the Dept.of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation was held on **02-06-21**.

BOARD OF EXAMINERS

Chairman



Dr. Touhid Bhuiyan

Professor and Head

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner



Md. Sadekur Rahman

Assistant Professor

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner



Dr. Fizar Ahmed

Assistant Professor

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

External Examiner



Dr. Shamim H Ripon

Professor

Department of Computer Science and Engineering

East West University

DECLARATION

We hereby declare that this project base thesis has been done by us under the supervision of **Mr. Abdus Sattar, Assistant Professor of CSE Department**, Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

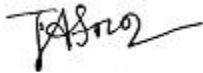


Mr. Abdus Sattar
Assistant Professor
Department of CSE
Daffodil International University

Submitted by:



Masab Hasnain
ID: 172-15-9811
Department of CSE
Daffodil International University



Tanzuma Afroz
ID: 172-15-9764
Department of CSE
Daffodil International University



Saifa Sabrina Mim
ID: 172-15-9853
Department of CSE
Daffodil International University

ACKNOWLEDGMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes it possible to complete the final year project successfully.

We are really grateful and wish our profound indebtedness to **Mr. Abdus Sattar, Assistant Professor of CSE Department, Daffodil International University**. Deep knowledge and keen interest of our supervisor in the field of “**EFFICIENT WAY OF RESULT PUBLISHING BY USING CRYPTOGRAPHY**” to carry out this project. Our project is based on “Web Development” His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all steps have made it possible to complete this project.

We would like to express our heartiest gratitude to Prof. Dr. Touhid Bhuiyan and Head Department of CSE, for his kind help to finish our project and also to other faculty members and staff of CSE department of Daffodil International University.

We would also like to thank our interdependence mate in Daffodil International University, who took part in this discussion while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

Nowadays almost all exam results are published online in Bangladesh. Online publication systems work very well in most cases. But when there is a large number of candidates whose results need to be published, result servers become very slow and unusable. In our project we tried to solve this problem in a cost-effective way. At first, we encrypt the final result and send it to the students by email. On the publication date authority only needs to publish the decryption password. We have also developed an android application by which students can easily decrypt the result. On the client side it is very user friendly. Our approach to solve this problem is very cost effective. We can easily implement this project on existing servers.

TABLE OF CONTENTS

CONTENTS	PAGE
Board of examiners	i
Declaration	ii
Acknowledgements	iii
Abstract	iv
CHAPTER	
CHAPTER 1: INTRODUCTION	1-2
1.1 Introduction	1
1.2 Motivation	1
1.3 Objects	2
1.4 Expected Outcome	2
1.5 Report Layout	2
CHAPTER 2: BACKGROUND	3-5
2.1 Introduction	3
2.2 Current System	3-5
2.3 Research Summary	5
2.4 Scope of the problem	5
2.5 Challenges	5
CHAPTER 3: REQUIREMENT SPECIFICATION	6-9
3.1 Requirement Collection and Analysis	6
3.2 Features	6
3.3 Use Case Modeling and Description	7

3.4	Data Flow Diagram	9
CHAPTER 4: DESIGN SPECIFICATION		10-14
4.1	Introduction	10
4.2	Cryptography	10-11
4.1.1	Themis	10
4.1.2	Secure Cell	10-11
4.1.3	Key Derivation Function	11
4.3	Mail Server	12
4.4	Android Client Application	12-14
CHAPTER 5: IMPLEMENTATION AND TESTING		15-18
5.1	Requirements for Implementation	15
5.2	Implementation of Server	15-16
5.1.1	Testing Implementation	
5.3	Implementation of client	17-18
5.2.2	Testing Implementation	
CHAPTER 6: CONCLUSION AND FUTURE SCOPE		18
6.1	Discussion and Conclusion	18
6.2	Future Work and Further Development	18
REFERENCES		19

LIST OF FIGURES

FIGURES	PAGE NO
Fig: 2.2.1 Result Publication system of Daffodil International University	3
Fig: 2.2.2 Result publication system of education board Bangladesh	4
Fig: 3.3.1 server side	7
Fig: 3.3.2 client side	8
Fig: 3.4.1 data flow diagram	9
Fig: 4.2.1 Secure Cell Seal Mode Encryption	11
Fig: 4.3.1 Mail Server	12
Fig: 4.4.1 Input encrypted result and password	13
Fig: 4.4.2 Display detailed result	14

CHAPTER 1

INTRODUCTION

1.1 Introduction

At the present time, almost every exam result is published through the internet. Students can collect their results by providing registration numbers and other credentials. One of the main problems of this kind of result publication system is, students have to wait for a long time to get their results during the peak hours of publication day. The reason behind this problem is huge traffic on the publishing server for a period of time. As a result, students need to wait in suspense for a long period of time. It is almost impossible for someone who has a poor internet connection to get their result.

In this project, we are going to propose a cost effective and secure solution to this problem.

1.2 Motivation

Our main motivation for this project is to get exam results without any difficulties. We are trying to build a faster and user-friendly platform by using modern technologies in a cost effective way.

- Provide a better solution for the students.
- Lack of modern technologies used in result publications platforms.
- Efficiently handle the server traffic during peak hours.
- Applying cryptography to make a better platform.

1.3 Objectives

The main objective of this project is,

- To reduce the delay of result publication.
- To make a user friendly system.
- To modernize the result publication systems in an efficient way.
- To use the resources of social media and boost our system.
- To ensure a secure platform where the result will not be leaked before specific time

1.4 Expected Outcomes

The outcomes of this project are,

- This technique can be used to improve similar websites.
- People can use the resources of the previous system for our new system.
- People can continue to improve this project.
- It will solve the delay issue of result publication systems.

1.5 Report Layout

Chapter 2, here we will discuss the current systems of online result publications and also provide a brief discussion about our project.

Chapter 3, we provide different diagrams based on the project.

Chapter 4, details about different tools and technologies used in the project.

Chapter 5, We discuss the implementation of our project and also provide test results.

Chapter 6, discuss the update of our project we want to make in future and further developments that are possible.

CHAPTER 2

BACKGROUND

2.1 Introduction

Technology is very much available in Bangladesh these days. Almost everyone owns a smartphone and they also have an email account. Educational Institutions provide unique email accounts for their students. Most of the educational Institutions publish students' academic results through the internet. It is very difficult and costly to deliver every student's result to individuals at the same time of publication. In this chapter we are going to give an overall idea of our project along with discussion about current systems of result publication.

2.2 Current System

Daffodil International University

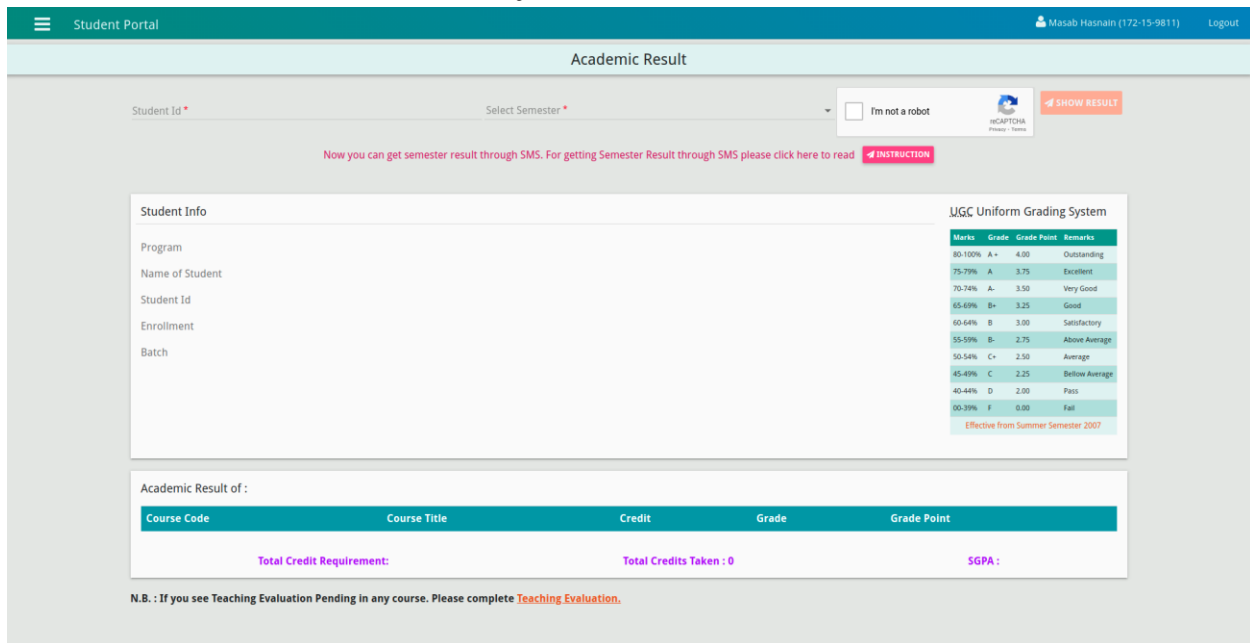


Fig: 2.2.1 Result Publication system of Daffodil International University.

An academic result publication date is announced by the university authority. After that specific time students can visit the student portal and by providing student ID and semester and correct captcha test and view their result of the semester. This process works in normal time. But at the

peak hour of the announced date the server responds very slowly. It takes more than 5 hours for every student to receive their result. The main reason for this delay is because of server traffic at peak hours. Almost every student is trying to get their result by making a request to the server. The server is not able to handle this much request at the same time.

Education Board Results (SSC, HSC)



The screenshot shows the official website of the Ministry of Education, Bangladesh, for the Intermediate and Secondary Education Boards. The page features a green header with the ministry's logo and name. Below the header is a search form with the following fields:

- Examination** : HSC/Alim/Equivalent (dropdown menu)
- Year** : Select One (dropdown menu)
- Board** : Select One (dropdown menu)
- Roll** : (text input field)
- Reg: No** : (text input field)
- 9 + 8** = (text input field)

At the bottom of the form are two buttons: **Reset** and **Submit**. The footer of the page contains the copyright notice: ©2005-2020 Ministry of Education, All rights reserved. and the logo of Teletalk (টেলিটক).

Fig: 2.2.2 Result publication system of education board Bangladesh.

The process is similar to the process mentioned above. But this one requires more user interaction. There is an approximate delay of 10 hours for every student to get their result.

2.3 Research Summary

The above mentioned systems of result publications are not very efficient. These processes are very tedious and time consuming for most of the students and also their parents. The only solution to give a smooth service by using the same system is to increase the server capability. But this is very costly and the server resources will be idle most of the time.

2.4 Scope of the problem

Different servers are designed in various ways. Scope of the problem are given below:

- Some systems do not provide app based solutions.
- Most of the web servers cannot make any improvements.
- Most of them cannot invest more money and efforts to improve the situation.

2.5 Challenges

To develop any project one has to face many challenges. Similarly, in this project we have faced some challenges. We have tried to make a user-friendly system. The

Challenges we have faced are discussed below:

- We cannot check how the system works against bigger datasets.
- Gmail clients have a limit of sending email every day.
- **Android:** No one of our group members was familiar with android. We had to learn and develop the android part of our project.
- **Cryptography:** Our solution is based on cryptography. But there are not many working cross language cryptographic libraries available.
- **Server:** We have developed the server side in linux. And currently we have tested our server in only Ubuntu operating systems.

CHAPTER 3

REQUIREMENT SPECIFICATION

3.1 Requirements Collection and Analysis

There are two parts of our project. Server side and client side.

Server Side:

- Operating System: Linux (Ubuntu)
- GNU compiler for C++
- CSV file containing the result of students.
- An email account to send the emails.
- Mail Server: We have used POCO C++ Library (MailMessage)
- Cryptography: Cross language cryptographic library (Themis)
- IDE: VIM

Client Side:

- Operating System: Android
- Internet connection
- Client email address
- IDE: Android Studio
- Cryptographic library (themis)

3.2 Features:

- Show detail result of students
- User friendly interface for client
- Server program takes input form widely used CSV format dataset
- Server program is very fast

3.3 Use Case Modeling Description

Server Side:

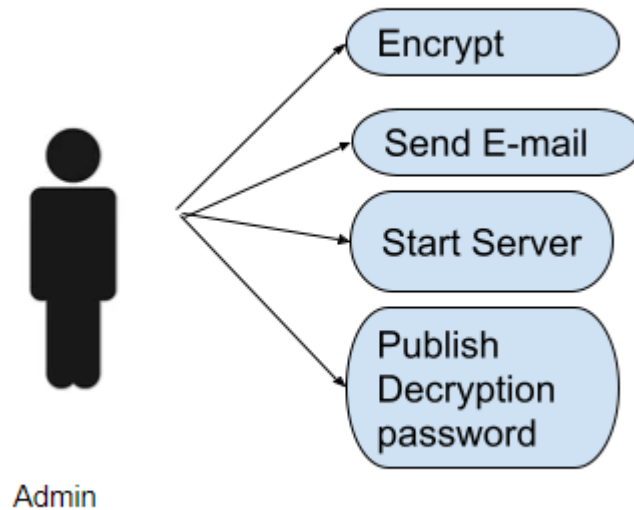


Fig: 3.3.1 server side

In this Use Case Model there is one actor. That is Admin. This use case is the server side of the project. Here we assume that admin already has the raw result dataset. So, admin can encrypt the dataset. Encrypted data will be automatically saved in memory. Admin can send encrypted results to student mails by using the second option. Admin can also start a backup server in case students do not receive emails. Admin will publish the decryption password on the publication date.

Client Side:

Here we also have only one actor. This Use Case Model is much simpler. Here the user only needs to insert the encrypted result and valid password. Detail results will be shown in the next activity.

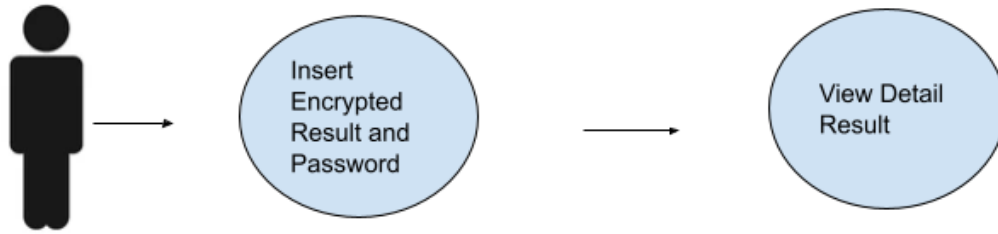


Fig: 3.3.2 client side

3.4 Data Flow Diagram

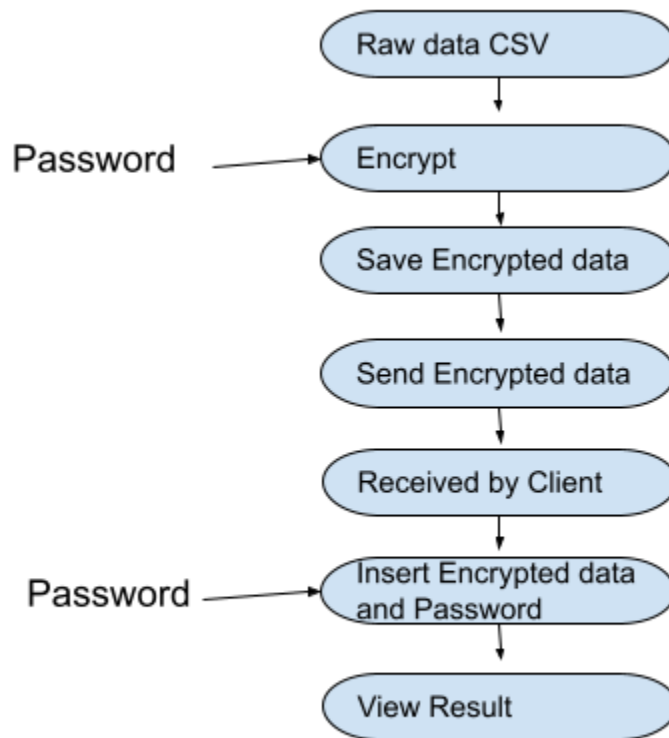


Fig: 3.4.1 data flow diagram

In this diagram we have shown the flow of data. Firstly we have the result of all students stored in a CSV file. In the next step all of the entries in the dataset are encrypted by using a password. Encrypted results are stored in memory. Then the encrypted results are sent to all of the students by using an email server. In the next step students receive the encrypted result through their mail. Finally on the publication date authority or admin only publishes the password. Students need to insert the correct password and encrypted result in the android application. The result is decrypted and formatted and finally displayed to the students.

CHAPTER 4

DESIGN SPECIFICATION

4.1 Introduction

Technology has made human life easier. There is always a way to improve current technologies for better service. In our project we have tried to improve online academic result publication systems. The main parts of our project is described below:

4.2 Cryptography

Our project is mainly based on cryptography. So we had to work a lot to find a suitable cryptographic algorithm. In this project we needed a library that has a framework for both C++ and Java. C++ is a very fast language. As the performance is the main thing we were trying to achieve in this project. So, we have used C++. But it is also possible to use other programming languages on the server side. In our project we will be using the same key to encrypt and decrypt. Therefore we need a symmetric key Cryptographic algorithm. Therefore we have to choose an AES algorithm to encrypt and the key used to encrypt and decrypt should be small and easy to publish. So, we have chosen 'Themis' cryptographic library.

4.1.1 Themis:

Themis is a cross-platform high-level cryptographic library for mobile, web, and server platforms. Themis provides 4 important cryptographic services. Among them we have used the 'Secure Cell' container for our project. Secure Cell is built around AES-256-GCM, AES-256-CTR cryptographic algorithms.

4.1.2 Secure Cell:

Secure Cell is a high-level cryptographic container which provides a simple way of securing data. Secure Cell also has different modes. Here we have used the secure cell in seal mode. Secure Cell in seal mode uses AES-256-GCM cryptographic algorithm. It's a very easy to use framework. User only needs to provide a Password and Data which the user wants to encrypt. Seal mode

automatically uses a strong Key Derivation Function (KDF) to generate the required 256 bit key. Secure Cell in Seal mode will encrypt the data and append an “authentication tag” to it with auxiliary security information

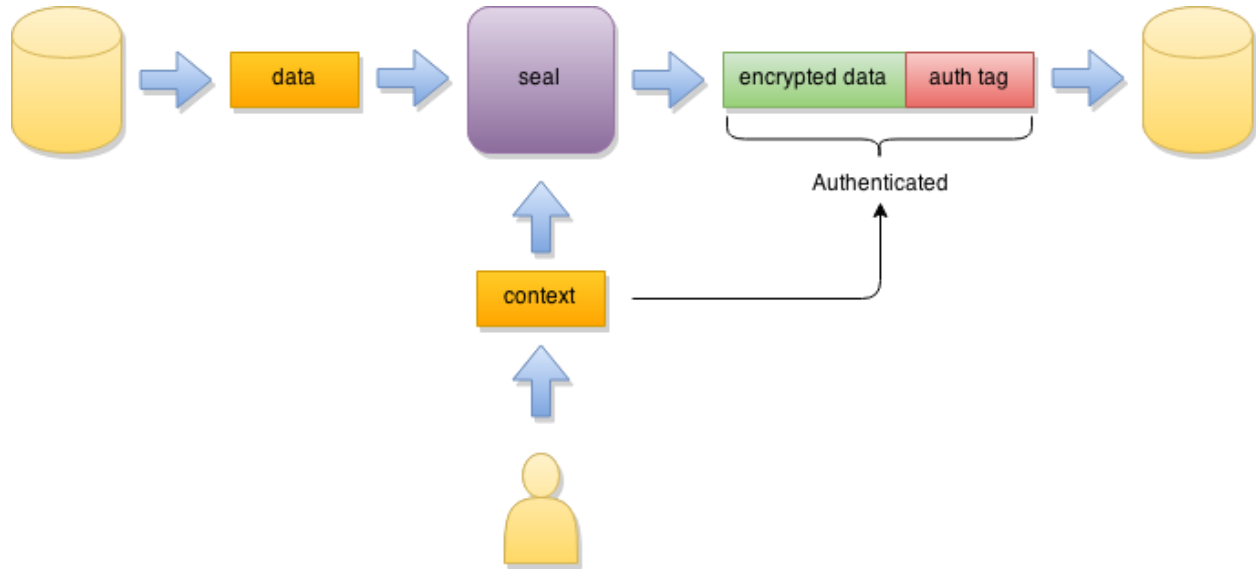


Fig: 4.2.1 Secure Cell Seal Mode Encryption

4.1.3 Key Derivation Function:

A key required to encrypt should be random, unpredictable and fairly long. But these kinds of keys are not very easy to remember for human beings. But humans can remember passphrases or passwords. Passwords cannot be used in encryption in algorithms. Because they may be shorter than required and passwords are also created for limited characters. A key derivation function (KDF) is used to mitigate for deficiencies of passphrases when they are used as keys. KDF augments the input with additional randomness and multiplies the computation complexity by repeated application of hash functions. Cracking a passphrase without KDF requires much less resources than cracking a key. KDF increases resource usage significantly so that cracking a passphrase is not practical. Secure Cell uses a strong password-based KDF (PBKDF2) to convert passphrases into intermediate keys, which are then passed to NIST SP 800-108-based KDF to convert them into the format required by AES.

Finally we have to encode our data to send through email servers. We encode the encrypted data by using base 64 encoding algorithms.

4.3 Mail Server:

A mail server is a server that handles and delivers e-mail over a network, usually over the Internet. A mail server can receive emails from client computers and deliver them to other mail servers. A mail server can also deliver emails to client computers. A client computer is normally the computer where you read your emails, for example your computer at home or in your office. Also an advanced mobile phone or Smartphone, with email capabilities, can be regarded as a client computer in these circumstances.



Fig: 4.3.1 Mail Server

In our project we need to develop a mail server which can send encrypted results to the students through their university email. In our project we have a Gmail mailing service. We also have used the POCO C++ library to send emails.

Here, we have to use an email lookup table. In the cryptographic part of the project all data are saved with email as the primary key. So, we can easily create an email lookup table from that dataset. Then we use the POCO mail library function to create a Gmail session and send the emails to students.

4.4 Android Client Application

Android application is a software developed to run on Android Devices. For our project we need a very simple android application. We have developed the application in Android studio with Java programming language. Themis Cryptographic library has a high level Java interface.

We believe it is better to make simple and easy to use android applications. There are only two activities in our application. One takes the encrypted data and password from the user. And another one is to display detailed results.

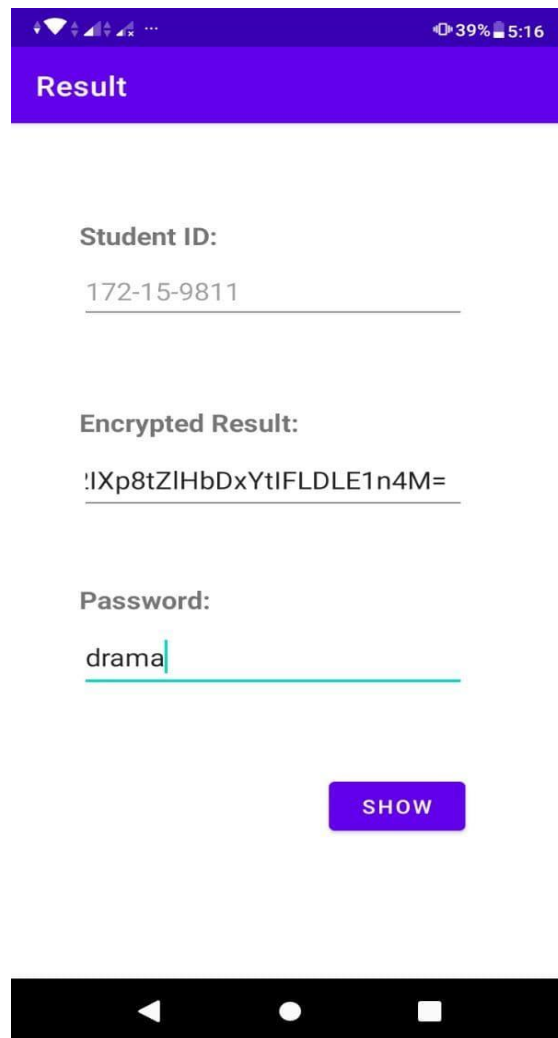


Fig: 4.4.1 Input encrypted result and password.



Fig: 4.4.2 Display detailed result.

CHAPTER 5

IMPLEMENTATION AND TESTING

5.1 Requirements for Implementation

We need some specific tools and operating systems to implement our project. There are two parts of our project. Therefore we have implemented our project both in a computer and in an android device. Details about implementation are described below.

5.2 Implementation of Server

Server was mainly implemented in the Ubuntu linux operating system. We have not tested our server program in other Linux operating systems. The main requirements for server program are:

- Linux operating system (Ubuntu 20.04 LTS)
- Themis cryptographic library installed
- POCO C++ library installed
- An email account
- GNU C++ compiler

We have compiled the source codes of our program in Ubuntu operating system. The email address used to send mails is a personal email address provided by our university i.e. gmail client. All of the necessary libraries and programs were installed from their official websites. Every package used in our program is the latest version.

5.1.1 Testing Implementation

We have tested our program in Ubuntu Linux on an Intel core i3 (2.4 GHz) machine with 8 GB memory installed. The test results are given below:

Table 5.1.1: Test result server

Test no.	Password length	Number of courses (result size)	Encryption successful	SenderEmail login	Email sent	Passed/Failed
01	3	3	Yes	Succeed	Succeed	✓
02	5	2	Yes	Failed	Failed	✗
03	6	3	Yes	Succeed	Succeed	✓
04	8	3	Yes	Succeed	Succeed	✓
05	10	4	Yes	Succeed	Succeed	✓
06	14	5	Yes	Succeed	Succeed	✓
07	16	3	Yes	Succeed	Succeed	✓
08	18	3	Yes	Failed	Failed	✗
09	22	2	Yes	Succeed	Succeed	✓

5.3 Implementation of Client

We need an android application to view our result. The application itself will decrypt the encrypted data and display it to the user. We have used several devices to test our application. The test results are given below:

5.2.2 Testing Implementation

Table 5.2.2: Test result client

Test no.	Password Length	Number of courses (result size)	Email received	Android Version	Decryption Successful	Passed/Failed
01	3	3	Yes	09	Yes	✓
02	5	2	No	-	-	✗
03	6	3	Yes	09	Yes	✓
04	8	3	Yes	09	Yes	✓
05	10	4	Yes	09	Yes	✓
06	14	5	Yes	09	Yes	✓
07	16	3	Yes	10	Yes	✓
08	18	3	No	-	-	✗
09	22	2	Yes	10	Yes	✓

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Discussion and Conclusion

We have tried our best to create a system “An efficient way of result publication by using cryptography”. By using this system universities and other institutions can publish student results within a few minutes. Every student will receive their result as quickly as possible. Another advantage of our system is it will not cost any extra money to set up. It is even possible to set up in existing systems.

6.2 Future work and Further Development

In every system, it is always possible to improve. So, it is also possible to improve our project. First of all, we can check our system to process heavy databases and improve the lacking. It is also possible to set up our system to publish board exam results. We can also send the encrypted data to temporary servers and by this process the whole traffic will be divided among those temporary servers. Though we have tried to keep the client side as simple as possible, the client side of our project can be improved a lot. We have only developed an android application. But we will need to develop client applications for all major platforms e.g. iOS, Windows, Linux etc. The server application can also be developed for other operating systems. Finally with some more optimized cryptographic algorithms it is also possible to reduce the encryption time.

REFERENCES

- [1]. Advanced Encryption Standard (AES). https://en.wikipedia.org/wiki/Advanced_Encryption_Standard/ last accessed on 2/22/21.
- [2]. Galois/Counter Mode (GCM). https://en.wikipedia.org/wiki/Galois/Counter_Mode/ last accessed on 2/22/21.
- [3]. Themis Cryptographic Library. <https://docs.cossacklabs.com/themis/> last accessed on 2/21/21
- [4]. Themis Secure Cell. <https://docs.cossacklabs.com/themis/crypto-theory/cryptosystems/secure-cell/> last accessed on 2/21/21.
- [5]. Themis JAVA Library. <https://docs.cossacklabs.com/themis/languages/java/features/#secure-cell> last accessed on 2/21/21.
- [6]. Themis C++ Library. <https://docs.cossacklabs.com/themis/languages/cpp/features/#secure-cell> last accessed on 2/21/21.
- [7]. POCO C++ libraries. <https://pocoproject.org/> last accessed on 2/23/21
- [8]. Sending an email using POCO library. <https://www.daniweb.com/programming/software-development/threads/472361/sending-a-email-using-poco-library> last accessed on 1/10/21.
- [9]. Daffodil International University Result Page. <http://studentportal.diu.edu.bd/#/result> last accessed on 2/26/21.
- [10]. Education Board Results. <http://www.educationboardresults.gov.bd/> last accessed on 2/26/21

Plagiarism Checked by
Abdus Sattar, Assistant Professor, Department of CSE

02-05-2021

CRYPTOGRAPHY

ORIGINALITY REPORT

4%

SIMILARITY INDEX

4%

INTERNET SOURCES

0%

PUBLICATIONS

4%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to Rider University

Student Paper

3%

2

Submitted to Daffodil International University

Student Paper

<1%

3

github.com

Internet Source

<1%

4

assignmenttutoronline.com

Internet Source

<1%

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off