DEPARTMENT OF COMPUTER SCIENCE

The Mango Messenger

DIPLOMA PROJECT

Poznan, 2021

Contents

1 Project Assumptions **2**
- 1.1 Project description . . . 2
- 1.2 Project objectives . . . 2

2 Impelentation **4**
- 2.1 Project tasks . . . 4
- 2.2 Project implementation . . . 5
  - 2.2.1 System Requirements . . . 5
- 2.3 Project outcomes . . . 10
- 2.4 Usefulness of project . . . 10
- 2.5 Project self-evaluation . . . 10
- 2.6 Material and bibliography used to carry out the project . . . 11
- 2.7 List of annexes . . . 11

Bibliography **12**

A RSA Algorithm comments **13**
- A.1 Details . . . 13
  - A.1.1 One way functions . . . 13
  - A.1.2 Euler's totient theorem . . . 13
- A.2 RSA Encryption algorithm . . . 14

Partner Details

Mentor's details

First name and surname	Szymon Murawski
Degree	Dr. Inz.
Date and signature	

Team members' details

First name and surname	Petro Kolosov
Course of study	Computer Science
Type of study program	Daytime
Date and signature	

First name and surname	Serhii Holishevskyi
Course of study	Computer Science
Type of study program	Daytime
Date and signature	

First name and surname	Illia Zubachov
Course of study	Computer Science
Type of study program	Daytime
Date and signature	

First name and surname	Arslanbek Temirbekov
Course of study	Computer Science
Type of study program	Daytime
Date and signature	

Chapter 1

Project Assumptions

1.1 Project description

Please provide an abbreviated description of the project, in line with the following structure. The description should not be more than 10,000 characters long (including spaces). Please use Times New Roman font, 12 pts, 1.5 spacing.

1. Research project
2. Justification for selecting the subject
3. Project's scope in terms of subject matter, object of research, time and space
4. Work methodology research (method and techniques)

Nowadays, instant messaging systems achieve a great success and became the main mean of communication between people via an internet. Thanks to the simplicity and quickness of the message exchanging more and more people over the world start to use instant messengers on daily basis. However, such a great attention forces us to discuss another aspect of these systems, an aspect of the information security and user privacy. The main aim of this thesis is to design and implement an instant messaging system that copes with the required functionalities and satisfies the defined security requirements.

1.2 Project objectives

1. To provide the system requirements for instant messaging system, both functional and non-functional.
2. To analyze and propose mitigations for security and user privacy vulnerabilities of the instant messaging system.
3. To propose web service (API's) architecture that fits the requirements.

4. To discuss an authorization mechanism that fits the requirements.
5. To discuss and apply E2E Encryption to the system, if necessary.
6. To implement web service.
7. To implement web client.
8. To implement mobile client.
9. To implement desktop client.

Chapter 2

Impelentation

2.1 Project tasks

Task 1.

Task name	
Entities involved to solve the task	
Task completion outcomes	
Star date of task execution	
End date of task execution	

Task 2.

Task name	
Entities involved to solve the task	
Task completion outcomes	
Star date of task execution	
End date of task execution	

Task 3.

Task name	
Entities involved to solve the task	
Task completion outcomes	
Star date of task execution	
End date of task execution	

Task 4.

Task name	
Entities involved to solve the task	
Task completion outcomes	
Star date of task execution	
End date of task execution	

2.2 Project implementation

[Please develop the theoretical assumptions of the project, including notes; present the empirical part of the project – research results and conclusions,as well as subject-matter description, etc. Please present computations and calculations, if any, in annexes. Please do not change the names of the points below. There is no predefined structure within individual points. Also, additional parts, forming individual points, can be enumerated according to your own concept. The theoretical and empirical part should not exceed 50,000 characters. Please use Times New Roman font, 12 pts, 1.5 spacing.]

1. Theoretical assumptions
2. Description of facts
3. Empirical research

2.2.1 System Requirements

Prior to software module implementation, it is essentially important to define the functionality module will obtain. In this section we discuss functional and non-functional requirements of secure instant messaging system from customer's prospective. Generally, there are three forms of software product requirements: business, functional, and non-functional. Business requirements [Dilworth and Kochhar, 2007] typically answer how the product will address the needs of your company and its users. They also reveal the business model of the app and what problems it can solve. Functional requirements [Malan, Bredemeyer, et al., 2001] are about functionalities that will be implemented in the application. Non-functional requirements [Chung et al., 2012] describe how these functionalities will be implemented.

Mostly common and simple way to define software product's functional requirements is User Stories. User stories [Cohn, 2004] should be understandable both to developers and to you as the client, and should be written in simple words. The most popular way of writing a user story is with the following formula:

```
"As a <user type>, I want <goal> so that <reason>."
```

Now, let's group the main features of the application as follows

- Registration
- Authentication
- Managing contacts

- Sending messages and media to individuals
- Creating and managing groups
- Sending messages and media to groups
- Viewing messages history
- Managing profile settings

Registration user stories

- As an unregistered user, I want to tap “Register” so that I see the registration form and register myself.
- As an unregistered user, I want to use my phone number to register so that my account is tied to my phone number.
- As an unregistered user, I want to use my e-mail address to register so that my account is tied to my e-mail address.
- As an unregistered user, I want to add a display name during registration so that other users can find me using it.
- As an unregistered user, I want to choose how to receive the registration confirmation via SMS or e-mail so that notification is sent to me via SMS or e-email.
- As an unregistered user, I want to receive the registration confirmation via SMS or Email so that I can activate my account.
- As a registered user, I want to confirm my email address so that I get confirmation link via email I provided.
- As a registered user, I want to confirm my phone number so that I use specified form to do it.

Authentication user stories

- As a registered user, I want to authenticate myself using both combinations email-password and phone-password so that I use the specified form with two inputs.
- As a registered user, I want to restore my password if I forget it so that I use specified form and restore my password.
- As an authenticated user, I want my session on each device to least 7 days so that after 7 days of inactivity device will be logged out automatically.

Managing contacts user stories

- As an authorized user, I want to see my contact list so that there is a list of users who are my contacts.
- As an authorized user, I want to search users so that I write user display name or phone number of e-mail address to specified input, click "Search user" button and see results.
- As an authorized user, I want to add other user to my contact list so that I click "Add contact" button on user profile and add him to my contact list.
- As an authorized user, I want user search input to accept empty or whitespace queries so that all users displayed as search result.
- As an authorized user, I want to remove the user from my contact list so that I click "Remove contact" button on user profile and remove him from my contact list.
- As an authorized user, I want to navigate to private chat with the user from my contact list so that I click "Message" button at user profile and get navigated to the private chat with him.

Sending messages and media to individuals user stories

- As an authorized user, I want to send a text message so that another user sees my message.
- As an authorized user, I want to add an attachment to the message so that another user sees the message with attachment.
- As an authorized user, I want to add an emoji to the message so that another user sees the message with emoji.
- As an authorized user, I want to tap "Edit" on my message so that message I edited is changed immediately in the chat.
- As an authorized user, I want to tap "Delete" on my message so that message immediately disappears from the chat.
- As an authorized user, I want to share secret messages with users from my contact list so that our are messages encrypted for anyone else including system administrators.
- As an authorized user, I want each new message in private chats I participate to be displayed immediately in real-time so that I do not reload page.

Creating and managing groups user stories

- As a registered user, I want to tap "Create channel" so that I create a new channel of the one of the types: Private channel, Public channel, Readonly channel.
- As a registered user, I want to tap "Start direct chat" so that I create a new direct chat with specified user.
- As a registered user, I want to tap "Start secret chat" so that I create a new secret chat with specified user.
- As a registered user, I want to join public groups so that I click button "Join group" to join the group.
- As a registered user, I want to tap "Archive" so that I archive the specified chat or channel.
- As a registered user, I want to tap "Un-archive" so that I un-archive the specified archived chat or channel.
- As a registered user, I want my secret chats to be device-specific so that I can see a secret chat only on the device that I used to start this chat.

Sending messages and media to groups user stories

- As an authorized user, I want to send a text message so that other members of the group see the message I sent.
- As an authorized user, I want to add an attachment to the message so that other members of the group see the message with attachment I sent.
- As an authorized user, I want to add an emoji to the message so that other members of the group see the message with emoji I sent.
- As an authorized user, I want to tap "Edit" on my message so that other members of the group see the message I edited.
- As an authorized user, I want to tap "Delete" on my message so that my message is deleted for all members of the group.
- As an authorized user, I want to search public groups by title so that I enter display name to specified field, click button "Search chats" and see results.
- As an authorized user, I want each new message in groups I participate to be displayed immediately in real-time so that I do not reload page.

Viewing messages history user stories

- As an authorized user, I want to view a message history of particular chat or group so that I see a list of my active chats on the UI.
- As an authorized user, I want to search messages in particular chat so that I see the results in messages window of the chat.

Managing profile settings user stories

- As an authorized user, I want to update my personal information in profile settings so that other users my updated personal information.
- As an authorized user, I want to update my social network links in profile settings so that other users my updated social media.
- As an authorized user, I want to change my profile picture so that all other users will see updated one.
- As an authorized user, I want reset password, so that my password will change.
- As an authorized user, I want to tap "Logout" button so that current device will be logged out from the system.
- As an authorized user, I want to tap "Logout all" button so that all my authorized devices will be logged out from the system.

Non-functional requirements

- **NFR01.** Graphic user interface of the system should be well organized. To fulfill this requirement, we follow an ISO 9241–161:2010 (en) Ergonomics of human-system interaction standard [ISO and STANDARD, 2010].
- **NFR02.** The system should have well performance, which meant to respond it at least 1 second. User should have a device with at least 6 GB RAM and CPU with 1.8 GHZ, 100 Mbps internet connection. Server must have the following hardware: Intel 2.4 GHz 8 Cores server processor, 64GB DDR4 (4x16GB) memory, NVME or SAS server disk with a minimum capacity of 1.6 TB.
- **NFR03.** The unique, unambiguous identifier of users in the system is the username. It is set in the profile settings.
- **NFR04.** The UI must be well displayed with the following browsers, in the versions current at the date of receipt of the system or, depending on technical possibilities, with the latest versions that support correct operation of the system:
  - Google Chrome 72.0.36.

  - Mozilla Firefox 64.0.2.
  - Microsoft Edge 17.17134.

- **NFR05.** The system shall force users to use passwords with a minimum length of 8 characters and using at least one capital letter and one number and one special symbol.
- **NFR06.** The UI must be compatible to use on mobile device screens with a minimum width of 600 pixels.
- **NFR07.** The UI must be compatible to use on desktop or laptop device screens with a minimum display width of 1024 pixels.

2.3 Project outcomes

Please describe the achieved outcomes of the project. If possible, please provide figures showing the described outcomes. Please confront them with the objectives of the project. This part should be between 2000 and 10,000 characters long. Please use Times New Roman font, 12 pts, 1.5 spacing. Full description of solutions that were worked out and project outcomes, if any, should be presented in annexes.

2.4 Usefulness of project

Please justify how this project is useful (how the project can be used in practice). The description should not exceed 6000 characters. Please use Times New Roman font, 12 pts, 1.5 spacing.

2.5 Project self-evaluation

Each of the project's Authors describes his or her skills and competencies that were developed while working on the project and identifies issues encountered while working on the project. If during the work on the project the team had not completed any tasks planned earlier, or omitted them altogether, please specify what were these tasks and why they had not been completed. This part should not exceed 6000 characters. Please use Times New Roman font, 12 pts, 1.5 spacing.

2.6 Material and bibliography used to carry out the project

Please enumerate sources used by the team during the work on the project (as per the applying layout, Times New Roman font, 12 pts., 1.5 spacing).

2.7 List of annexes

In this place you should list all additional documents, e.g. preprinted forms, data sets, financial statements, survey templates, diagrams, concepts, strategies, studies, analyses, procedures, regulations, technical documents, plans, models, etc. which significantly contributed to the project. Please prepare all annexes in accordance with the template in place. Please use Times New Roman font, 12 pts, 1.5 spacing. All annexes form an integral part of the project.

Bibliography

Chung, Lawrence et al. (2012). *Non-functional requirements in software engineering*. Vol. 5. Springer Science & Business Media.

Cocks, Clifford C (1973). "A note on non-secret encryption". In: *CESG Memo*.

Cohn, Mike (2004). *User stories applied: For agile software development*. Addison-Wesley Professional.

Dilworth, John and AK Kochhar (2007). "Creation of an e-business requirements specification model". In: *Journal of Manufacturing Technology Management*.

ISO, BSEN and BRITISH STANDARD (2010). "Ergonomics of human-system interaction". In.

Malan, Ruth, Dana Bredemeyer, et al. (2001). "Functional requirements and use cases". In: *Bredemeyer Consulting*.

Rivest, Ronald L, Adi Shamir, and Leonard Adleman (1978). "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2, pp. 120–126.

Appendix A

RSA Algorithm comments

A.1 Details

A.1.1 One way functions

One way function – is a function that is easy to compute on every input, but hard to invert given the image of a random input. For instance, the function

$$f(m) = m^e \bmod N \equiv C$$

where e, N are public constants is one-awy function, because it is easy to compute C given m, however it is hard to compute m given C.

A.1.2 Euler's totient theorem

Given a number N and its prime factorization $p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, then Euler's totient function $\phi(N)$ is defined as

$$\phi(N) = (p_1^{e_1} - p_1^{e_1-1}) \cdot (p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

In particular, for positive number M such that its factorization is $p1 \cdot p2$, the $\phi(M)$ is

$$\phi(M) = (p_1 - 1) \cdot (p_2 - 1)$$

Euler's theorem relates the modular division and exponent as follows, given number m, then

$$m^{\phi(N)} = 1 \bmod N$$

It means that reminder of division $m^{\phi(N)}$ by N is always 1. By the equality $1^K = 1$

$$M^{K \cdot \phi(N)} = 1 \bmod N$$

If we multiply both parts by M, we get

$$M \cdot M^{K \cdot \phi(N)} = M^{K \cdot \phi(N)+1} = M \bmod N$$

A.2 RSA Encryption algorithm

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977 [Rivest, Shamir, and Adleman, 1978]. The basic technique was first discovered in 1973 by Clifford Cocks [Cocks, 1973] of CESG (part of the British GCHQ) but this was a secret until 1997. The patent taken out by RSA Labs has expired.

Historically, the process of encryption is considered to be symmetric one. That means that prior the communication, the sides conclude on the common key to be used in encryption. This process is similar to the first sharing keys and only after that the locked chest with the message. Such approach is highly cost since it requires to share the defined keys between each actor if the number of actors is greater than 2. Much more simpler is to think about secured communication channel that in terms of asymmetric encryption. The real life example would be if Alice shares with all actors an opened lock having key. So that Bob receives an opened lock, writes letter to Alice, puts letter to the chest, locks this chest with received from Alice lock. This way, only Alice will be able to open the chest and to read the letter. This is an idea of the asymmetric encryption. However, such a simple from first glance idea requires complex number theory approach. A concept of opened lock may be interpreted in terms of one-way functions. One way function – is a function that is easy to compute on every input, but hard to invert given the image of a random input. Thus, it is much simpler to close the lock without key, but very difficult to open lock trying the combinations of the key. For instance, the function

$$f(m) = m^e \bmod N = C$$

where e, N are public constants is one-awy function, because it is easy to compute C given m, however it is hard to compute m given C. So, assume that Alice defines two positive integer constants e, N and sends it to Bob. Bob encrypts the secret message m using $f(m)$

$$f(m) = m^e \bmod N = C$$

Then Bob sends encrypted message C to the Alice. Given C Alice must fetch the Bob's message m. In order to decrypt C, Alice has to compute

$$C^d \bmod N = m^{ed} \bmod N \equiv m,$$

where e for encryption and d for decryption. Now the problem is to define such d that it is hard to the listener to fetch it. In order to define the secret d, Alice chooses two enough big prime numbers: P, Q, let's say around 150 digits both. Then Alice multiplies these two prime numbers in order to get N

$$N = P \cdot Q$$

The N is around 300 digits. Now Alice can share N with anyone, since it takes decades to find its prime factorization by the fundamental problem of prime factorization. Next, it is very important to know such a function, which depends on the knowledge of factorization of N. Such function is an Euler's totient function. Given a number N and its prime factorization $p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, the Euler's totient function $\phi(N)$ is defined as

$$\phi(N) = (p_1^{e_1} - p_1^{e_1-1}) \cdot (p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

In particular, for positive number M such that its factorization is $p1 \cdot p2$, the $\phi(M)$ is

$$\phi(M) = (p_1 - 1) \cdot (p_2 - 1)$$

Euler's theorem relates the modular division and exponent as follows, given number m, then

$$m^{\phi(N)} = 1 \bmod N$$

It means that reminder of division $m^{\phi(N)}$ by N is always 1. By the equality $1^K = 1$

$$M^{K \cdot \phi(N)} = 1 \bmod N$$

If we multiply both parts by M, we get

$$M \cdot M^{K \cdot \phi(N)} = M^{K \cdot \phi(N)+1} = M \bmod N$$

It follows that Alice is able to define the secret d as follows

$$e \cdot d = K \cdot \phi(N) + 1$$
$$d = \frac{K \cdot \phi(N) + 1}{e}$$

The following image demonstrates the concept of RSA approach

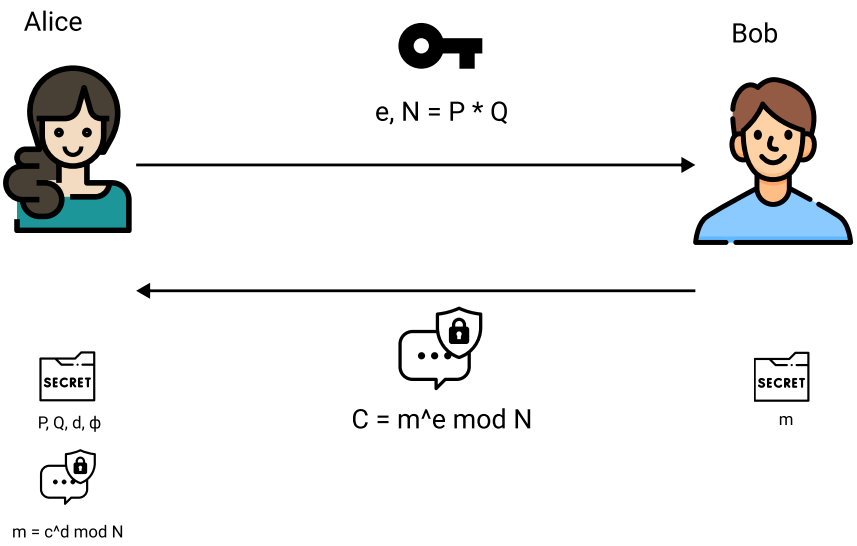

FIGURE A.1: Secret chat encryption concept diagram. Source:

To summarize, the process by the steps is as follows

- Alice defines the large secret prime numbers $P,\ Q$.
- Alice computes $N = P \cdot Q$ and $\phi = (P-1)(Q-1)$
- Alice chooses an integer e, $1 < e < \phi$ such that $\gcd(e, \phi) = 1$.
- Alice computes secret exponent d, $1 < d < \phi$ such that $ed \equiv 1 \bmod \phi$.
- Alice shares public key (N, e) with Bob and keeps private key (d, p, q) is secret.
- Bob defines the message m, encrypts it as $C = m^e \bmod N$.
- Bob sends C to Alice.
- Alice decrypts C using her secret d, so she gets m

$$m = C^d \bmod N$$

Security of the RSA approach is based on the complexity of fundamental problem of prime factorization, which takes decades to solve having enough large number.