Daniel Wait| Candidate No.

[school] | Centre No.

Messenger App

Unit 3: programming project

For OCR Specification H446

Contents

[1 Analysis 2](#_Toc71703020)

[1.1 Problem Identification 2](#_Toc71703021)

[1.1.1 Problem outline 2](#_Toc71703022)

[1.1.2 How can the problem be solved by computational methods? 2](#_Toc71703023)

[1.1.3 Computational methods 2](#_Toc71703024)

[1.1.4 Stakeholder Identification 3](#_Toc71703025)

[1.2 Research 4](#_Toc71703026)

[1.2.1 Existing program – Discord 4](#_Toc71703027)

[1.2.2 Existing solution – Internet Relay Chat (IRC) 7](#_Toc71703028)

[1.3 Stakeholders 9](#_Toc71703029)

[1.3.1 Interview with Ethan Sandy 9](#_Toc71703030)

[1.3.2 Survey Aims 11](#_Toc71703031)

[1.3.3 Survey Results 11](#_Toc71703032)

[1.4 Requirements 16](#_Toc71703033)

[1.4.1 Stakeholder requirements 16](#_Toc71703034)

[1.4.2 Limitations 16](#_Toc71703035)

[1.4.3 Software requirements 16](#_Toc71703036)

[1.5 Success Criteria 17](#_Toc71703037)

[2 Design 19](#_Toc71703038)

[2.1 System decomposition 19](#_Toc71703039)

[2.2 Algorithms 23](#_Toc71703040)

[3 Development 26](#_Toc71703041)

[4 Evaluation 26](#_Toc71703042)

[5 References 27](#_Toc71703043)

# Analysis

## Problem Identification

### Problem outline

Currently, the encryption in-transit system is widely used in instant messaging apps. This means that a user’s messages will be in plaintext in the service provider’s server, which allows the service provider to read users’ conversations breaching their privacy. These companies are then also susceptible to potential attackers accessing confidential information through this potential backdoor. Therefore, I will be making a solution to this problem of user privacy by making an end-to-end encrypted instant messaging program.

For this solution to work, the following features are required: only the endpoint users have the key for the symmetric encryption algorithm to qualify the system as end-to-end encryption; an easy-to-use GUI so that anyone can navigate and use the program; a login/sign-up system to authenticate users’ identities to the server to facilitate historic message viewing; networking capabilities in order send and receive messages from different networks with a low enough latency to be a viable ‘instant’ messaging platform.

### How can the problem be solved by computational methods?

This problem is well suited to a computational approach as it can be solved using computational methods. This is because the processes of encrypting, sending then decrypting messages over a network can be greatly abstracted for the user so that they do not need any prior technical knowledge to use the program. The solution will also have many algorithms to carry out processes without the need for complex input from the user.

### Computational methods

**Problem recognition** – The general problem is creating a program where sensitive information is not ever in plaintext whilst passing through the server. However, the more specific problems are creating a system of generating two symmetric private keys over a network connection that people monitoring the network are unable to recreate and sending and receiving the messages over that network. Once this is overcome the rest of the solution is using those keys to do the encryption/decryption and presenting the messages to the user in an intuitive form.

**Abstraction** – It is not necessary (or feasible) for the user to have hands-on control over every single process that happens when sending their messages. Therefore, abstraction will be used to hide most of the processes from the user to streamline their experience by only showing relevant detail. Some of these processes will be the following: encrypting and decrypting their message; segmenting their messages into packets; sending the packets to the server.

**Thinking ahead** – I have thought ahead by choosing C# to write the program is since I expect the backend to require a lot more focus than the frontend; the GUI capabilities in C# are much greater than Python for example (the language I am most familiar with), due to its support for WYSIWYG GUI builders in Visual Studio. I made this decision so that I can spend more time focusing on the development of the backend.

**Procedural thinking & decomposition** – The problem can be decomposed into a set of much smaller problems, using procedural thinking I will develop a solution to each of these in turn. This set of problems will allow me to possibly use test harnesses during development to isolate certain parts of the program during the development process. This structure will make the overall solution easier to work with and will make the entire process more efficient.

**Thinking concurrently** – Through the use of concurrent processing, I will make the server-side program more efficient by processing each user’s requests on a virtual thread. This will mean that the program can deal with requests from multiple users and the same time, which is important as if they were acted on procedurally the bandwidth of the system would be dramatically reduced leading to very high latency.

**Performance modelling** – I will make heavy use of performance modelling to ensure that the program functions efficiently. On the smaller scale, I will use performance modelling to profile my encryption algorithms to make sure that they properly balance processing time and security since for this application an algorithm that sufficiently encrypted data in a few milliseconds is vastly superior to an algorithm that more complexly encrypts data in a few minutes. On a larger scale, I will use performance modelling to ensure that my server-side program has properly utilised threads to have a suitable bandwidth to support both average and peak throughput.

### Stakeholder Identification

The first group of potential stakeholders are the users who will prioritise privacy and security. The needs of this group are that all communications are encrypted so they cannot be read while passing through the server and that their sensitive information (e.g., passwords and keys) are protected while they are being stored. This group will most likely use the solution for everyday use as their main communication platform; for this reason, the solution must be robust enough for that use case. I have selected a user to represent this group of stakeholders: Ethan S. He is a student who believes that privacy is very important, especially online where he makes a conscious effort to minimise his digital footprint by limiting any personally identifiable information about himself. For these reasons, I believe that he will be a fair representative for this group’s needs.

The second group of potential stakeholders are the users who want a messenger app that is lightweight and easy to use. The needs of this group are that all components of the user interface are intuitive and clearly labelled and that the program requires no prior setup or configuration so the program can easily be installed and immediately used. This group will most likely only infrequently use the solution to keep in touch with friends and family; for this reason, the solution must have an easy system for finding contacts and have a low barrier of use as to not discourage them. I have selected a user to represent this group of stakeholders: [to be added]

## Research

### Existing program – Discord

Discord is a free instant messaging and VoIP platform created in 2015 centred around enabling communities to connect through guilds: collections of chat rooms and voice channels. In 2019 the platform saw 250 million users with a total of 25 billion messages being sent per month [1] making it one of the largest gaming-focused communications platforms available.



**Features:**

Each guild is managed by users with varying levels of permissions which can be as general or customised as desired by the guild owner. In the text channels, you can send files, links, and text with basic mark-up. In voice channels, as well as streaming audio you can also use webcams and stream your desktop. The purpose and scope of a guild very flexible as there is no predefined structure: they can be created for a small group of friends or as large official game hubs.

**Differences:**

Discord is not a privacy-focused platform and users are expected to forfeit their privacy in exchange for ease of use and versatility. Discord uses the encryption in-transit system meaning that all traffic is decrypted on the server-side; for non-audio/video data, the HTTPS protocol is used which is encrypted using TLS or SSL. It is also known that Discord inspects all user traffic whilst it passes through their server. However, the reason why is unknown.

**Parts I can apply to my solution:**

1. The idea of having a central area consisting of multiple ‘channels’ for different conversations or topics would potentially be worth including in my solution. This is because it would be an intuitive structure for larger chat rooms, where having a singular area for everyone to talk in would not be feasible.
2. I also think that Discord’s feature of activity statuses for each user would be a good addition to my solution. This would not be an essential feature but, if I have enough time to add it, it will improve the overall experience of the user by enabling them to see who is also online while they are using the program.

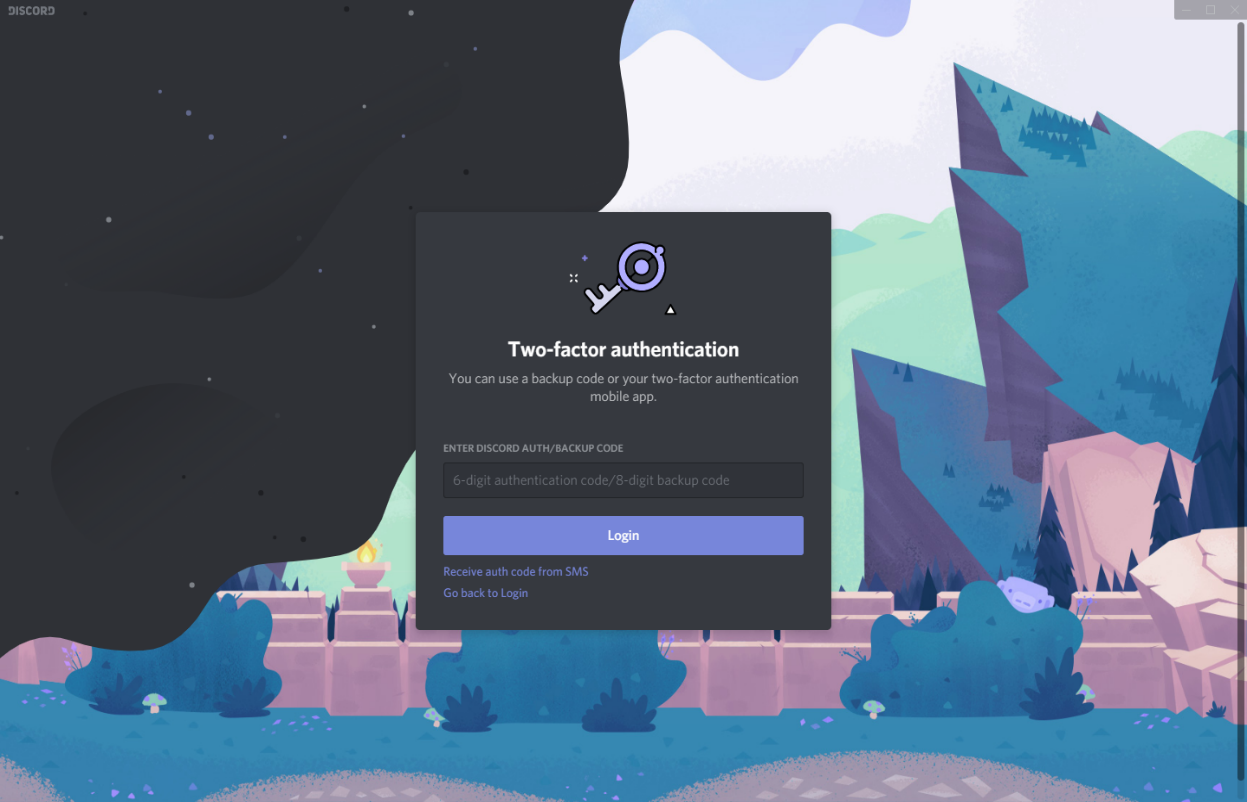
**Splash Screen:**

When starting Discord, a splash screen appears showing the user that processes are occurring behind the scenes. This is useful as it gives visual feedback to the user and gives the program time to connect to the server and load all the required resources into the RAM.

I will consider this feature for my solution as it will give my program time to establish a server connection before the user can try to log in without appearing to the user as the program has frozen.

**Logging In**

To use Discord, users must first log in. This can be done with an email and password or by scanning a QR code from the Discord mobile app. In my solution, I will also require the user to log into an account before they can use the program. This is because protecting messages behind a password improves privacy which is one of the requirements for the program. A login system will also be useful as it provides each user with a unique identifier that can be used when addressing messages and viewing contacts.

**Two-factor authentication**

Discord has the option to enable two-factor authentication. This means that when logging in to your account you need both the correct credentials and access to another method of proving your identity. Common methods are SMS message, email or a dedicated authenticator app, Discord chose the latter.

I will consider this feature for my program as it will add more security to the login process which would further satisfy the stakeholders’ requirements.

**Creating an account**

When creating a Discord account, usernames are case sensitive and are automatically postfixed with a number after a ‘#’ called a discriminator. This robust naming system is done to allow up to ten thousand people to have the same username. I will consider implementing this feature in my solution as preventing username collisions improves the experience for the user by allowing them to continue using their username from any other service.

Discord’s password requirements are on the other hand very lenient: “Must be between 6 and 128 characters long” [2]. Therefore, it is up to the user to choose a sufficiently broad character pool for their password which many users will forgo in exchange for convenience. So, for my solution, I will consider implementing some further requirements for the strength of passwords. This is since the privacy given by the end-to-end encryption will be undermined by an easily guessed password.

**Adding friends**

To add a friend (contact), you enter their complete Discord Tag (username) and send them a Friend Request. A complete username is needed as there are many users of Discord who have the same username so the only thing that differentiates these users is their discriminator. The recipient of this request can then accept or decline this request.

In my solution, I will consider a similar method of adding contacts by searching their username. However, since my user base will be much smaller than that of Discord, I may give the user feedback to similar names to what they entered by pattern matching the string they want to search and a list of all registered accounts.



**Home page**

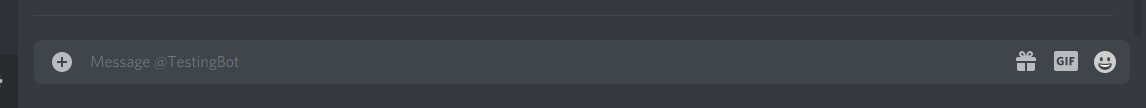
The default home page for Discord is a list of the user’s online friends. This page consists of four tabs: “Online” the default; “All” which includes offline friends; “Pending” which are accounts that the user has sent friend requests to and “Blocked”. Upon clicking on a friend in either of the first two tabs, a DM (direct message) thread is opened. This gives users quick access to all their DM threads as well as giving them a helpful overview of who is currently online.

I will consider having a similar homepage in my solution as immediate, easy access to conversations will greatly improve the flow of the program for the user. The online statuses and overview of online friends will also be a helpful addition to the program.

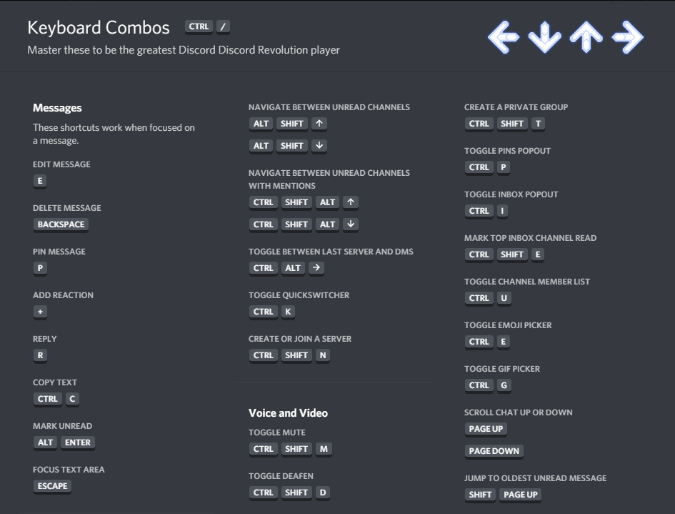
**Direct Messages**

DM threads on Discord are the conversations between users. These can show historic conversations if the users have sent each other messages in the past or empty when beginning a conversation. The messages that users send each other can be generalised as one of two formats:

1. Text, up to 2000 characters
   * Emojis
   * Embeds
   * Colouring
   * Code blocks with syntax highlighting
   * All the other Markdown formatting features
2. Files, up to 8MB (100MB with subscription)
   * Images (including GIFs) with previews
   * Playable audio files and videos with picture-in-picture
   * All other file types must be downloaded
     + Executable files cannot be sent for security reasons



In my solution, I will consider including the feature of viewing historic messages since if messages were lost after being viewed this would not make the program very helpful for the user. Secondly, I will consider including the ability to send multiple types of messages. This is because limiting the program to only text would be restrictive for the users when compared to alternative programs.

**Navigation**

Discord has many shortcuts which are helpfully listed on a dedicated help screen in the program. This streamlines the experience for power-users of the program while allowing regular users to continue using their normal cursor orientated navigation.

Many parts of the Discord UI are divided into groups of tabs: servers, DM threads and channels are all formatted as such. This makes the program very friendly for most users as tab-based navigation is a common UI style in websites, mobile apps, and desktop applications.

For my solution, I will consider also using tab-based navigation as it is well established and fits well with messaging apps and their lists of contacts/conversations. I may also consider giving the user the option to operate some features in my program via keyboard shortcuts, albeit on a smaller scale to Discord as complete keyboard navigation is not a requirement.

### Existing solution – Internet Relay Chat (IRC)

Internet Relay Chat is an internet protocol created in 1988 to allow group plaintext conversations with channels working on a client-server model or to individuals with private messages using the Direct Client-to-Client protocol (DCC). In February 2005, at the height of IRC the largest network – QuakeNet – saw a peak user count of almost a quarter of a million users [3]. This has dramatically reduced since then and is now at an average of 10 thousand users [4]. However, the protocol is still used by some services today as a means of lightweight communication typically attached to a larger service: The Twitch IRC network is responsible for the live chat in a Twitch stream and some games such as Tabletop Simulator, StarCraft, and Unreal Tournament use IRC for their in-game chat.



*Image via* [*WeeChat.org*](https://weechat.org/about/screenshots/)

**Networking:**

The structure of an IRC network is a spanning tree, in which clients will connect to one of the multiple servers that all share the same state. This introduces the first limitation of IRC: the fact that the networks are distributed becomes extremely inefficient with large networks as all the servers need to know about all the other servers, clients and channels every time something happens. The second limitation is that if one of the server-server connections was to go down, the network would split in half and many users will appear to have disconnected in what is called a netsplit.

**Difference:**

In my solution, I will use a centralised network. This means that I will not have to constantly share state information between servers like in an IRC network so the configuration and maintenance will be easier. However, the solution will be limited with scalability as the maximum throughput of the network is limited to the bandwidth of the one machine and the only way to scale up the network is to upgrade the parts in that machine.

**Group Messaging:**

To access IRC channels, users must first install an IRC client and select the domain name for the network they want to connect to. Once connected they will have to choose a display name. This is because users do not need to register to use IRC, only supply a short identifier in the form of a nickname. Finally, once they join a network’s channel, the network’s server they are connected to will relay all the messages they send to all the other users connected to the channel, and vice versa.

**Difference:**

In my solution, I will require users to register before they can use the program. This will help to prevent the nickname collisions which occurred with IRC where multiple people had/wanted the same nickname. This will ensure the all the messages are sent to the correct users and data validation can be used to make sure no two people accidentally share an identifier.

**Offline Messages:**

Some IRC networks support bouncers that enable offline messages, these are daemons on a server that act as a proxy for the client. When a client connects to a bouncer, the bouncer simply relays all the traffic to and from the server. However, in the event the client disconnects, the bouncer can store the messages that the client would have received if they were still connected. These will then be sent to the client once they reconnect. A similar implementation for offline messages is having a client run on an always-on server to which users connect to via SSH for their session. This also allows users who do not have an IRC client installed to connect.

**Part I can add to my solution:**

In my solution, I could include a way of archiving messages for users when they are not online. This could be implemented in a similar way to the bouncer where if the server detects that the client is no longer connected it will reroute the messages to a daemon. However, I will need to find a way of securely storing the user’s messages as security is a focus point of the solution.

**Typical Client User Interface:**

The layout of the UI for many IRC clients is the following: channels on the left, a nickname list on the right and the chat in the middle (this has become a common chat program layout as can be seen in Discord’s GUI in the section prior). In the past and in addition to standalone programs, Opera came with an IRC client attached to Opera Mail and there was an IRC client for Firefox called ChatZilla. This proved that IRC was a very lightweight protocol with not many needs besides a socket to run off.

**Part I can include in my solution:**

In my solution, I will also try to create a lightweight protocol that only requires a single socket as it is a requirement for my solution to create a lightweight program. I also think that sticking to the tried and tested chat program layout shown in many IRC clients will be a good inclusion into my program; since it will make using the program a lot easier for users who have used other chat programs in the past and it seems like an intuitive design for new users.

## Stakeholders

### Interview with Ethan Sandy

This interview is being conducted to investigate the following: the opinion of the stakeholder on common features in messages apps; comments on some of the findings from the research into Discord and opinions on some decisions for features in my solution.

**Topic: Discord research**

1. Do you use Discord?

Yes, often

1. Which features from Discord would you like to see in my program?

The ability to send different types of messages

1. Are there any message types in Discord that are not important?

They all have their uses, but files are sent the least

1. Can you rank the message types in Discord in descending order of importance?

Text, media, emojis, files

1. Which features from Discord would you like changed?

The Nitro[[1]](#footnote-1) exclusive features (animated emojis and bigger file size limits)

From question 1, it was established that Ethan has a lot of experience with messaging apps. Because of this, I know that his answers and opinions are based on previous experience rather than preconceptions.

In question 2, he said that including a range of message types would benefit my solution. This agrees with what I found during the Discord research.

Question 3 told me that all the types of messages found in Discord are important. This surprised me as I expected some formats to be neglected. However, by asking question 4 I was able to find out that there is a hierarchy of importance that I can investigate further.

Lastly, in question 5, Ethan identified a shortcoming in Discord that I can consider implementing a solution for in my program: since there is no need for exclusive content in my solution as it will be completely free.

**Topic: Program controls**

1. Do you use the keyboard shortcuts in apps?

No, I was not even aware Discord had shortcuts until now

1. Would you like to see keyboard shortcuts in my program?

No, they would likely not be used

1. Should messages be sent by pressing a send button or by pressing “Enter”?

“Enter” as it is the most common and intuitive

Question 1 and 2 showed me that users often do not utilise keyboard shortcuts in programs and it will therefore be an unnecessary feature to include in my solution.

For question 3, Ethan said that the pressing Enter method of sending messages is the most common and intuitive. Since being easy to use is important for the solution I make this the way users send messages.

**Topic: Messages and conversations**

1. Do you want to be able to view old messages you have sent somebody?

Yes

1. How far back should the old messages go back?

All messages. If you are storing messages, it should be all or nothing

1. Should multiple conversations be tabs (like Discord) or individual pop-out windows (like Steam)?

A tab per conversation

1. Should messages be on both the left and right (like WhatsApp) or all on the left with usernames (like Discord)?

Along the left with usernames

For question 1 and 2, Ethan said that having all past messages between two users visible would be a good feature to include in my program. I especially agree with his comment on including past messages being “all or nothing”.

Next, the answers to question 3 and 4 gave me an idea of the design that he wants to see for the program. I will use these as the basis for my UI mock-up in the design section.

**Topic: Accounts**

1. Should accounts be needed to use the program?

Yes

1. Should you have to be friends with someone to send them a message?

No, a friend system is not needed with so few users

1. Should usernames have a common structure or be completely custom?

Custom

1. Should there be requirements on the strength of account passwords?

Yes

1. Should the login process include two-factor authentication?

Yes, although it should be optional

In question 1, Ethan says that accounts should be required for the program. This confirmed my expectations that accounts, and therefore accountability, are important for security-focused applications.

For question 2, he said that – due to the small user base of the program – a friend system is not needed. For this reason, I will not prioritise this feature but will rather deem it a feature that could be added to the feature.

Questions 3 and 4 showed me that no restrictions on usernames and restrictions on passwords are preferred. This is a common pair of rules for usernames and passwords and will be the rules I include in my program.

Lastly, question 5 was about two-factor authentication. Ethan said that it should be included but not be forced upon the user. This is the industry standard when it comes to 2FA as many people forgo the security in exchange for convenience.

### Survey Aims

To help me better understand the requirements of the stakeholders, I have created a survey to send to them (since in-person interviews are not possible at this time).

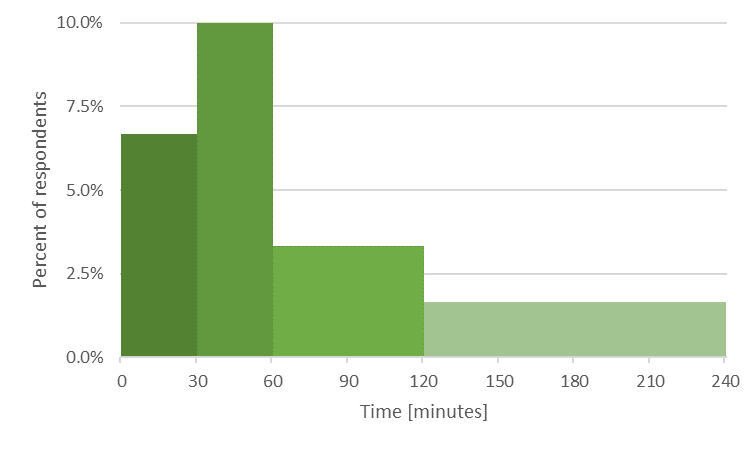
**Aims for the survey:**

Firstly, I want to investigate the stakeholders’ current use patterns with messaging apps. I believe this will give me a good insight into standards and expectations. This is especially relevant for my stakeholders whose needs involve an easy-to-use platform as I will research some of the most used platforms and see what makes their user interface so accessible.

Secondly, I wanted to hear the stakeholders’ opinions on some common features of messaging apps. This information from the stakeholders will be crucial as I will use it to inform my decision of whether a feature is worth including in my final solution.

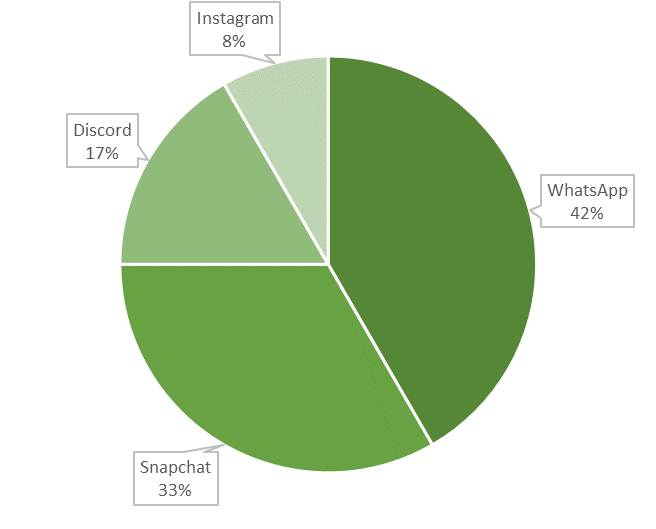
### Survey Results

**Question 1 – “How much time do you spend on messaging apps each day?”**

****

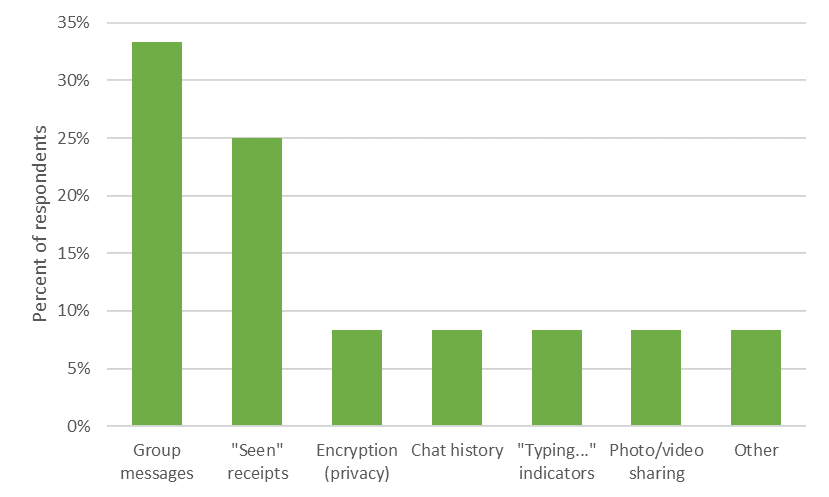
**Question 1 told me that the respondents to this survey had an above average messaging app usage. The respondents had a modal class of 30-60 minutes and a (linearly interpolated) median of 55 minutes: these are much greater than the UK’s average of 28 minutes** [5]**. This is the best case for a group of respondents as it means that the survey was almost guaranteed to be completed using respondents’ experiences of features rather than their preconceptions.**

**Question 2 – “What is your most used messaging app?”**

****

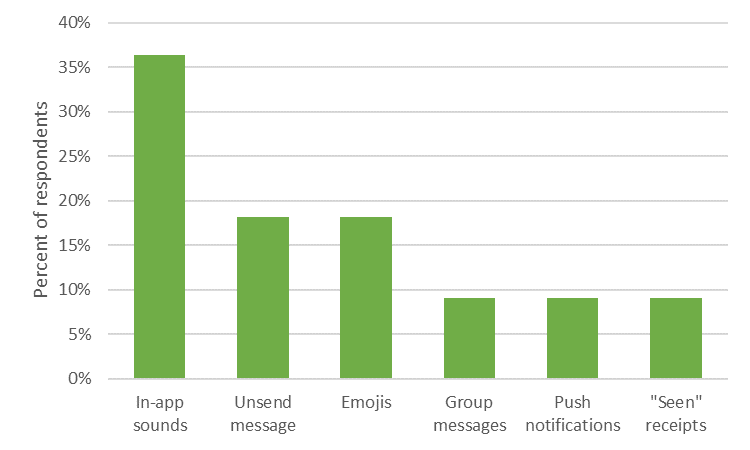
**The results from this question showed me that the most used messaging app among the respondents was WhatsApp, a privacy focused end-to-end encrypted messaging app. This, along with the results from question 1, confirm to me that the respondents were suitable stakeholders for this program and therefore their opinions and decisions should be trusted.**

**Question 3 – “What is your favourite feature of messaging apps?”**



This data showed me that the stakeholders deemed group messages and “Seen” receipts to be their favourite features. For this that reason I should consider these as features to prioritise in my solution.

**Question 4 – “What is your least favourite feature of messaging apps?”**

****

This question was the direct inverse of question 4. It showed me that in-app sounds, un-sending messages and emojis are the three most disliked features of messages apps. Therefore, I will not be considering these to be included in my solution. The appearance of emojis is not a surprise here since it was also identified as the 2nd least used message type on Discord.

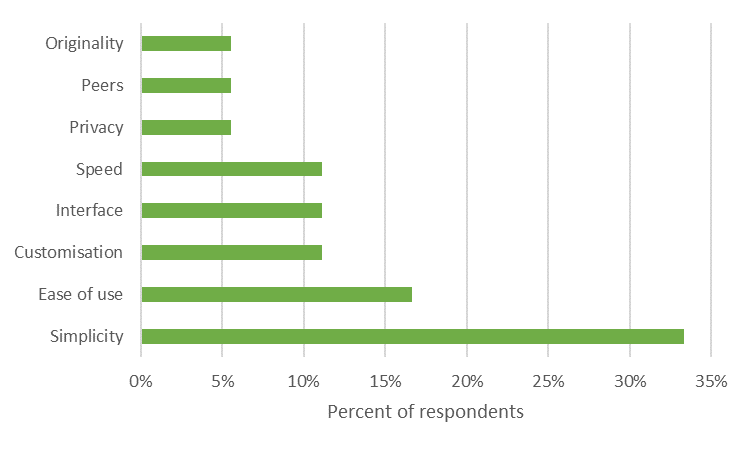
**Question 5 – “How important are the following features?”**



The data from this question showed me that the stakeholders do not think that the following features make a significant impact in a messaging app: in-app sounds, emojis, “typing…” indicators, and un-sending messages. From this, along with the results from question 4, I can see that these features are non-essential so I will not consider these for the list of necessary features for my solution.

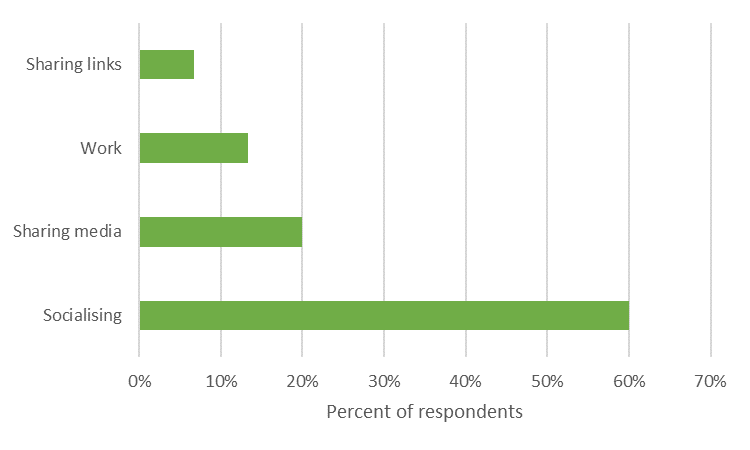
The data also showed me that four features are generally deemed core features: group messages, individual messages, encryption, and media sharing. As these are important for the stakeholders, I will consider these for the list of features that must be in the final solution. These findings are supported by the results from question 3 as well as the interview with Ethan Sandy.

**Question 6 – “What do you look for in a messaging app?”**



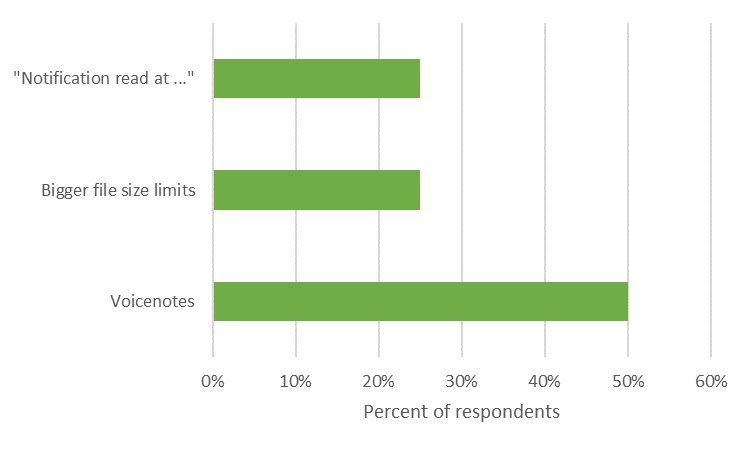
The top qualities for messaging apps were simplicity and ease of use. I will consider these when designing my UI.

**Question 7 – “What do you mainly use messaging apps for?”**



The fact socialising and sharing media appeared at the top was not a surprise. However, two of the answers were: sharing links and work. To accommodate for the respondents who put down sharing links, I will investigate automatically hyperlinking text and opening browsers. I am unsure of how to accommodate the working users so may consider adding profanity filters unless any other features arise.

**Question 8 – “What feature might you want to see added to messaging apps?”**



**Question 9 – “How important is privacy for you?”**



## Requirements

### Stakeholder requirements

### Limitations

**Hardcoded server IP:**

When a client tries to connect to the server, it will use a hardcoded IP address as its target. This means that the IP address of the server must be static and cannot be moved onto another network. For this limitation to be fixed the server would have to be added to a DNS server so that the domain can dynamically point to the server. However, this is beyond the scope of the project.

**Group messaging:**

Group messaging – the most chosen “favourite feature” and rated the third most important feature from the stakeholders’ survey – will not be implemented in the solution. This is down to the vast increase in complexity from individual end-to-end encrypted messaging to group end-to-end encrypted messaging; implementing such a feature will take up too much time and would require the redesign of many of the procedures of the solution. For these reasons, I will be unable to implement the feature.

### Software requirements

For simplicity, I will only be building a Windows x86 version of the solution for development and the final evaluation. However, using the dotnet compiler, executables for all the following operating systems can be built from the source.

|  |  |  |
| --- | --- | --- |
| OS | Version | Architectures |
| Windows | 7 SP1+, 8.1 | x64, x86 |
| Windows 10 | 1607+ | x64, x86 |
| Mac OS X | 10.13+ | x64 |
| Fedora | 32+ | x64 |
| Debian | 9+ | x64, ARM32, ARM64 |
| Ubuntu | 20.10, 20.04, 18.04, 16.04 | x64, ARM32, ARM64 |

Information from the .NET Core GitHub repository [6]

The final user of the program will not be required to install the .NET runtime as the solution will be published self-contained. This means that the download will be larger as it will contain the .NET libraries, runtime and dependencies needed.

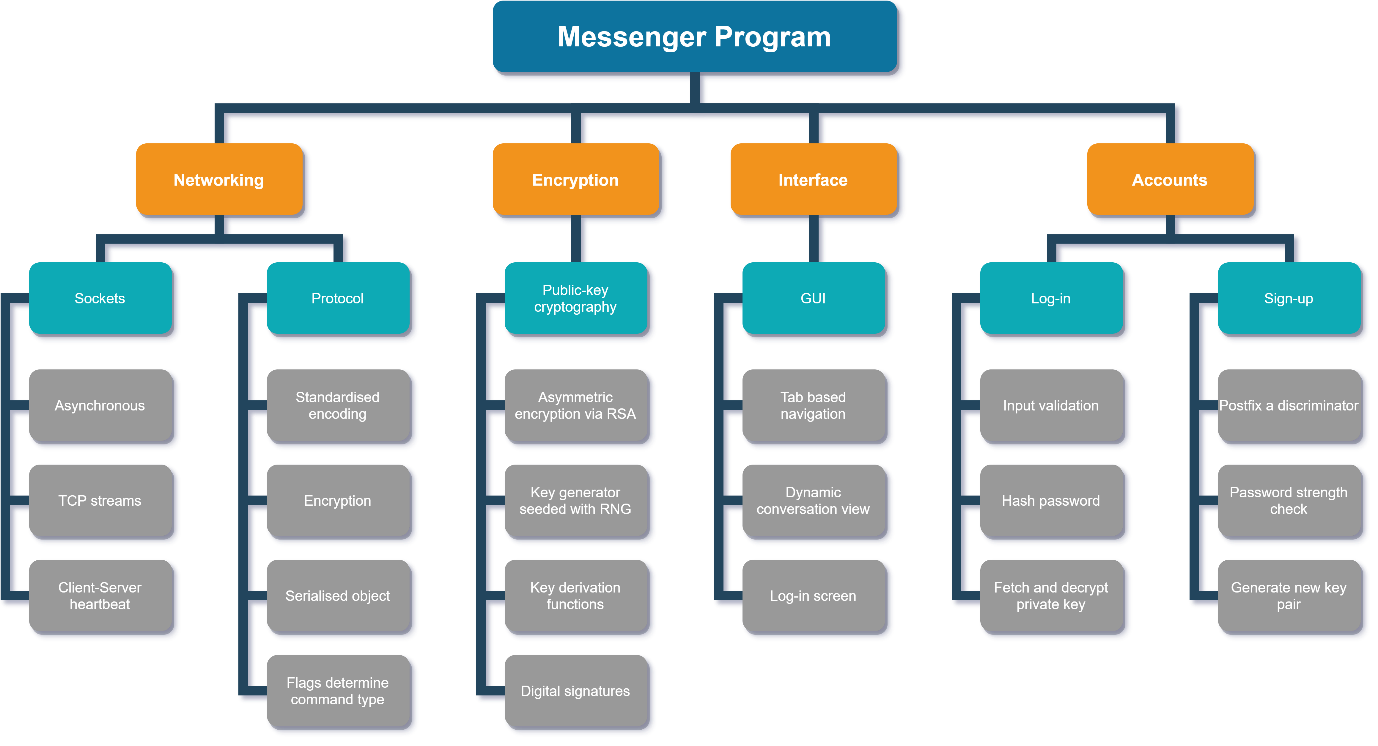
Internet access will be required to run the program as the client program needs to communicate with the server.

## Success Criteria

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Requirement | Justification | Reference |
| 1 | Client sockets connect to server at start-up of the program | The app needs a connection to the server so it should connect while the app starts to minimise waiting time | Discord (splash screen) |
| 2 | Client socket tells the server it is closing before the app is closed | Prevents any errors from occurring and begins the client disconnect procedure |  |
| 3 | The socket sends heartbeats to the server to show that it is still open | Stops the possibility that a client has disconnected without the server realising which will lead to errors | IRC (PING) |
| 4 | User must log in to their account to access the program | Ensures that only people with valid credentials can view an account’s messages | IRC (?) or Stakeholders |
| 5 | New users can create an account | New users need a way of accessing the app | IRC (?) or Stakeholders |
| 6 | Users are not allowed to try to log in if the socket cannot connect | With no connection, logins cannot be authorised so the login process cannot be done |  |
| 7 | Usernames must be unique | Prevents situations where two people can accidentally share credentials | Existing solution - Internet Relay Chat (IRC) |
| 8 | Password must be of a minimum strength (upper, lower, digits, special characters) | Makes sure the password is not a security flaw for the user | Discord (account creation) |
| 9 | Users can type out a message and send it with a "Send" button | Intuitive button to send the message | Discord (UI) |
| 10 | Users can type out a message and send it with the Enter key | Enter is a common key to press to send a message | Discord (controls) |
| 11 | Users can see a list of their contacts | Users can easily see whom they are sending the message to | Existing program - Discord |
| 12 | Users can click on a contact to message with them | No need to manually address each message they send like an email | Discord (UI) |
| 13 | Users can see past conversations with a contact | Users do not have to worry that old messages will be lost | Stakeholder survey |
| 14 | Users can be added to contacts by searching their username | Usernames are easier for a user to remember than an IP address | Discord (add friend) |
| 15 | Messages are encrypted with the recipient's public key | The recipients public and private keys are a keypair as it is asymmetric encryption |  |
| 16 | Messages are decrypted with the recipient's private key | Only the intended recipient can view the message as the decryption key is private |  |
| 17 | Messages are signed with the sender's private key | The sender can prove their identity by using a key that only they know |  |
| 18 | Signatures are checked with the sender's public key | The recipient must be able to prove that a message came from the user it claims to be from |  |
| 19 | Messages cannot be read while in the server | End-to-end encryption requires messages to not be able to be read during transit |  |
| 20 | Key pairs can be generated | Public and private keys are needed for the encryption of all messages |  |
| 21 | Public keys can be accessed by anyone | Public keys are used to check signatures and encrypt messages so they must be visible to everyone |  |
| 22 | The server can accept incoming client connections | Allows clients to connect to the server when they are opening the app |  |
| 23 | Each connected client is handled a separate thread | Concurrency allows for greater scalability in the number of clients and reduces their response time |  |
| 24 | The server authorises logins against its database | Only clients supplying valid credentials can view a user's messages |  |
| 25 | The server can create new accounts | New clients must be issued an account to start using the app |  |
| 26 | Messages are routed to the intended recipient | Users must only receive messages addressed to them | Existing solution – Internet Relay Chat (IRC) |
| 27 | Messages are held in the server if the recipient is not connected | Users may not be connected when a message is being sent so that must be accounted for | Existing solution – Internet Relay Chat (IRC) |
| 28 | Undelivered messages are sent the next time the recipient connects | Users should no miss out on messages because they were not online | Existing solution – Internet Relay Chat (IRC) |

# Design

## System decomposition



Networking – Sockets

**Asynchronous:** Using sockets, I will be able to do asynchronous operations as to not block the program’s GUI for the user. This is paramount for the networking as if the operations are synchronous the IO will almost always be blocked for the user due to the constant communication with the server. To implement this part of the program I will need to implement callback functions and threading.

**TCP streams:** By using TCP, a connection orientated protocol, the server and client will have a dedicated stream to communicate via. The retransmission of lost packets is also important for the user as waiting longer for a message is better than receiving a malformed or incomplete message. In comparison, using UDP does have faster speeds but that is not necessary for this application and the unreliability is too significant to ignore. To implement this part of the program I will need to bind a socket to a port on the server and infinitely listen, I will then need to bind a socket to the same port on the server’s IP on the client.

**Client-server heartbeat:** A constant heartbeat message that will be pinged between the client and server will be used to give both parties up-to-date information about whether either party has ungracefully disconnected. This needs to be in the program as either socket may not get the opportunity to send a proper close message (such as in the event of the ethernet cable being pulled out) so the client/server will only find out when they try to send a transmission and never get a reply. To implement this part of the program I will need to send a message at a constant interval between the client and server, then if one of the parties does not get the message after a certain time it can be assumed that the other party has ungracefully closed.

Networking – Protocol

**Standardised encoding:** Using a standardised character encoding across all my transmissions will ensure that any text that is entered into one client will be displayed the same way in another client. This is included in response to the problems faced in IRC where character encoding was client determined and so some characters were different when viewed from a different client. To implement this part of the program I will pass all text inputs through the same encoder as part of the data validation process and the same decoder as part of the transmission receiving procedure.

**Encryption:** Since the program requires end-to-end encryption, making sure that no messages can be read during transit is important. Therefore, all transmission data will be encrypted with the recipient’s public key and signed with the sender’s private key. This will be implemented as a part of the transmission creation and receiving procedure so that it is done to all messages.

**Serialised object:** For easier sending and receiving of transmission, a common format that will be easy to read values from is needed. Since the transmission will be an object before its sent, I will create an object that will be serialised when sent. When the recipient gets the transmission, it can de-serialised and immediately used by the receiver. This part of the program will possibly be implemented by using JObjects, this is a JSON object that contains many tokens that will be used to transfer information between the client and server.

**Flags determine command type:** Creating a general format for all transmission and then giving more information and specifying the purpose of the message via flags gives consistency to the transmission while not sacrificing functionality. These flags will declare the purpose of a request as, due to the structure of the transmission, I am unable to prefix messages with a command name so will need to integrate the request’s purpose into the object that will be sent. This part of the solution will most likely be done with Boolean values in the JObject or a token dedicated to holding a command name.

Encryption – Public-key Cryptography

**Asymmetric encryption vis RSA:** To encrypt the transmission, there are two routes to go down. Firstly, there is symmetric encryption which will require a Diffie-Helman key exchange to establish a shared secret key between two parties while the messages are being sent in plaintext through the server and then AES could be used once the secret key is established. The other is asymmetric encryption, this involves each party generating a random public key which is sent to the server to be available to all clients, and a private key which decrypts messages encrypted by the public key (the key is only known by the owner). I will implement the latter as symmetric encryption will require each time two clients communicate each client will need to fetch the key specifically for that pair whereas with asymmetric encryption the same key pair is used for all communications. I will implement this part of my solution by fetching or generating a key pair immediately after the login process.

**Key generator seeded with RNG:** To generate an effective private key, it must use truly random data rather than pseudorandom (from a PRNG). This is because using non-random data can open the possibility for keys to be guessed easier which undermines all the program’s security. This part of the solution will be implemented by using an RNG to generate as close to a truly random seed for the key generator.

**Key derivation functions:** To allow users to sign in to their account from any computer, their private keys must be stored on the server. However, this would be very poor practice if the key is stored in plaintext so it must be encrypted. However, the question of how you store the key to that encryption then arises. The solution is using a symmetric encryption algorithm that derives the key using the user’s password via a key derivation function (KDF). Using a KDF means that the key to decrypt a user’s password never makes its way out of a client’s memory let alone stored anywhere so the clients are not restricted to where they can log in from. This part of the program will be implemented by putting the user’s password through a KDF (possibly PBKDF2) after the log-in process, then fetching the encrypted private key from the server and decrypting it for use.

**Digital signatures:** By storing all users’ public keys in a centralised server that also handles all the traffic, there is the possibility of man-in-the-middle (MITM) attacks. One way to prevent this is to authenticate all messages. This will involve encrypting a small bit of data with the sender’s private key and appending it to the message; this extra data is called the signature. The recipient can then decrypt this signature with the sender’s public key, if the resulting plaintext matches an agreed-upon value the message has successfully be authenticated, else it has not come from the sender it claims to have been from and is most likely the result of an attempted MITM attack. To implement this part of the program I will use RSA once again as it is asymmetrical and the generated key pair from message encryption can be used.

Interface – GUI

**Tab based navigation:** To move about the program, windows will be organised into tabs which the user can click on to view. This will mean that when a conversation is opened with another user the conversation view is opened in the same window as the contact list. To implement this part of the solution I will need to have a TabControl in the main view and a UserControl for each conversation.

**Dynamic conversation view:** Since the nature of a messaging app means that messages will appear while the user is looking at a certain conversation, I will need to dynamically add controls to the UserControl in which the conversation is being displayed in. This part of the program will likely be implemented by creating a template for a message – time, content, shape to hold text, sender/recipient – which can then be filled out with the data of each incoming message and added to the view.

**Login screen:** Upon opening the program, users will be required to sign in to an account or create an account. This means that a login screen will need to open first before the user can get access to the main part of the program. This will need to be done after connecting to the server since the login request will need to be sent from the socket. This part of the solution will be implemented by triggering a window to open only once the connection has been established, which will then lead to the main view being opened once a successful login has occurred.

Accounts – Log-in

**Input validation:** When the user inputs their username and password, a request will be sent off to the server to check the credentials against the database. This request should only go through when the form has been properly completed will valid data. Therefore, there must be checks in place to make sure inputs are completed and properly validated before being sent to the server. To implement this part of the program I will be doing some simple checks on the presence of data, the length of data and cleaning out whitespace and non-permitted characters from the input.

**Hash password:** Since the communication channel between the client and server is insecure until the client logs into an account. There is the possibility of using an ephemeral key to temporarily encrypt these communications, but I do not think this added complexity will be necessary for this use case. Therefore, to protect the user’s credentials the password will be hashed before being sent. This will then be checked against the hash in the server’s database to make sure the password is correct. By hashing the password, the plaintext is unknown, but it can still be used to compare against other hashed values. This part of the program will be implemented using the SHA-256 hashing algorithm.

**Fetch and decrypt private key:** As mentioned in the sections about KDFs, the user’s private key is stored on the server. Therefore, upon a successful log-in, the fetched encrypted private key must be decrypted. This part of the program will be implemented by putting the user’s plaintext password through the KDF and using the output as the decryption key. The private key will then only be stored in memory which will be wiped when the program is closed.

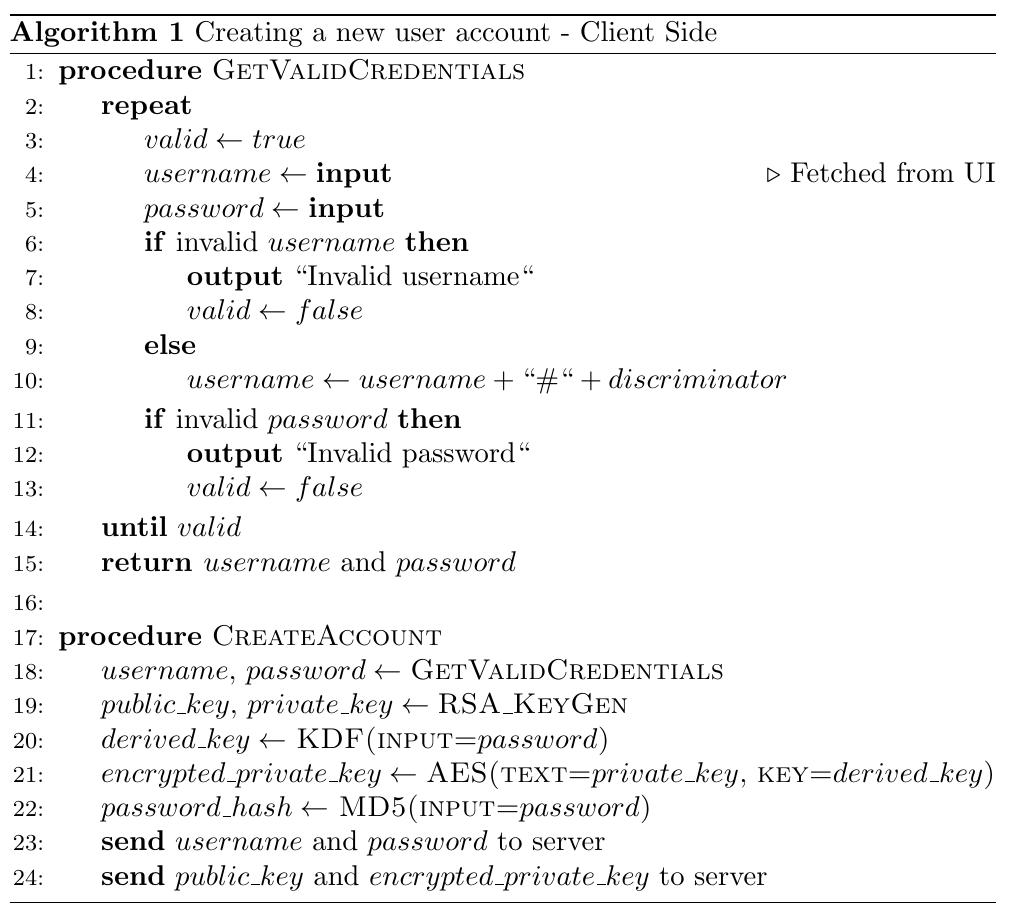
Accounts – Sign-in

**Postfix a discriminator:** Addressing the issue encountered in IRC and solved in Discord, username collisions will be prevented by postfixing a new user’s username with a two-digit number which Discord called the discriminator. This number will be automatically assigned so can add “uniqueness” to two otherwise identical usernames. This part of the solution will be implemented as a random number or as an automatically incrementing value (the latter being more likely) that will be in the format username#discriminator.

**Password strength check:** The weakest link in a system’s security chain is typically the endpoints and more specifically the user’s password. Therefore, to prevent all the encryption behind the scenes from being undermined I will force the user to have a strong password. This part of the solution will be implemented by only accepting new accounts with passwords that have both upper-case and lower-case letters, at least one letter, digit and special character and be at least 8 characters long.

**Generate new key pair:** Before any encrypted messages are sent between users, the new user must generate a key pair for RSA. The public key will then need to be sent to the server so that it can be accessed by any other client. The public key on the other hand should not be accessible to any other client but should be accessible to the user when they sign in on another machine: so, will be encrypted and stored in the server. The user’s password will be passed through a KDF (possibly PBKDF2) to generate the key for a symmetric encryption algorithm (possible AES) which the private key will be passed through before being sent off to the server for storage.

## Algorithms



**Summary** – This algorithm will be executed when a new user wants to create an account. This is because all users will require an RSA key pair to facilitate encrypted communications and a pair of credentials to allow them to log in from any device.

**Line 3 to 4** – The username and password will be fetched from text boxes in the UI. The submit button that will call the subroutine CreateAccount() will only be enabled when both fields because enabling it right away will lead to the possibility of empty strings being used in the function and the visual aid will guide the user.

**Line 7 to 12** – The input validation for the username will require the username’s length to be between 3 and 128 characters long and does not contain any non-encodable characters. Due to the requirement of eliminating nickname collisions, a discriminator needs to be postfixed to prevent nickname collisions, this will be done on line 8 if the username is valid.

**Line 13 to 17** – Due to the success criterion “strong minimum password strength”, the input validation for the password will require the following criteria to be satisfied:

* Both uppercase and lowercase characters
* A mix of letters and numbers
* At least one special characters
* Between 8 and 128 characters

**Line 18** – To allow users to amend their credentials if they are not accepted, a “repeat…until” (or “do…while”) loop is used to continue requesting usernames and passwords until a valid pair is supplied. This will appear in the UI in the form of the invalid text box(es) being highlighted.

**Line 26** – As addressed in 2.1 System decomposition, a key derivation function will be required to generate a symmetric key for AES to decrypt and encrypt the user’s private key that will be stored on the server. There are a few possible functions that the KDF in the pseudocode can be: KDF1, PBKDF2 or KBKDFVS. The final implementation will be chosen based on .NET implementation, security, and computation time.

**Line 28** – Since all passwords need to be store securely, the password must be hashed first. This will be done via MD5 with the possibility of an added salt. The salt will be different for each user and will mean that even if two users have the same password, their password hashes will not be the same. This also has the benefit of helping to reduce the effectiveness of hash table attacks.

**Line 29 to 30** – Lastly, all the new information to make the user’s account must be sent to the server. Even though this will be transmitted over an insecure channel, all the sensitive information has been either hashed or encrypted. Although, man-in-the-middle attacks are (very much) possible at this point, addressing this vulnerability is beyond the scope of this program so will have to remain in the program.

# Development

# Evaluation

# References

|  |  |
| --- | --- |
| [1] | C. Corberly, “Discord has surpassed 250 million registered users,” TechSpot, 13 May 2019. [Online]. Available: www.techspot.com/news/80064-discord-has-surpassed-250-million-registered-users.html. [Accessed 12 February 2021]. |
| [2] | A. Schmelyun, “Password requirements for Discord,” [Online]. Available: passhints.co/discord/. [Accessed 13 April 2021]. |
| [3] | A. Gelhausen, “IRC Networks - Top 10 in the annual comparison,” Netsplit, 2005. [Online]. Available: netsplit.de/networks/top10.php?year=2005. [Accessed 19 February 2021]. |
| [4] | A. Gelhausen, “IRC Network QuakeNet,” Netsplit, [Online]. Available: netsplit.de/networks/QuakeNet/. [Accessed 19 February 2021]. |
| [5] | J. Schwartz, “Messaging Apps: Average Usage Time Around the World,” SimilarWeb, 30 June 2016. [Online]. Available: www.similarweb.com/corp/blog/messaging-apps/. [Accessed 18 April 2021]. |
| [6] | Collaborative, “.NET Core 3.1 - Supported OS Versions,” 15 October 2019. [Online]. Available: github.com/dotnet/core/blob/main/release-notes/3.1/3.1-supported-os.md. [Accessed 18 March 2021]. |
| [7] | C. Kalt, *Internet Relay Chat: Architecture,* RFC 2810 ed., 2000. |
| [8] | J. Oikarinen and D. Reed, *Internet Relay Chat Protocol,* RFC 1459 ed., 1993. |

1. Nitro is Discord’s paid subscription service [↑](#footnote-ref-1)