

Czech University of Life Science Prague
Faculty of Economics and Management
Department of Information Engineering



Bachelor thesis

**User Interface Specification of Mobile Application
Supporting Encrypted Communication**

Author: Valeriya Sasina

Supervisor: Ing. Josef Pavlíček, Ph.D.

© 2017 CULS Prague

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Valeriya Sasina

Informatics

Thesis title

User Interface Specification of Mobile Application Supporting Encrypted Communication

Objectives of thesis

To design mobile application which follows next use cases:

- automatically encryption of messages (by send button press)
- automatically decryption of messages after receiving the password
- enter password into key store for encrypt mechanisms

To choose type of encryption (SSL, SSH – RSA)

To prepare Paper prototype of these application

Methodology

- Analyze current state of instant messaging mobile applications as WhatsApp, Viber etc.
- Study suitable literature for searching current state of encryption mechanisms.
- From the result of study define current state of mobile application and their ability to support encryption mechanisms.
- Define typical Use Cases and prepare UI Specification for suitable mobile application.
- Prepare paper prototype according to the UI Specification and test it.

Describe conclusions for gained results.

The proposed extent of the thesis

45

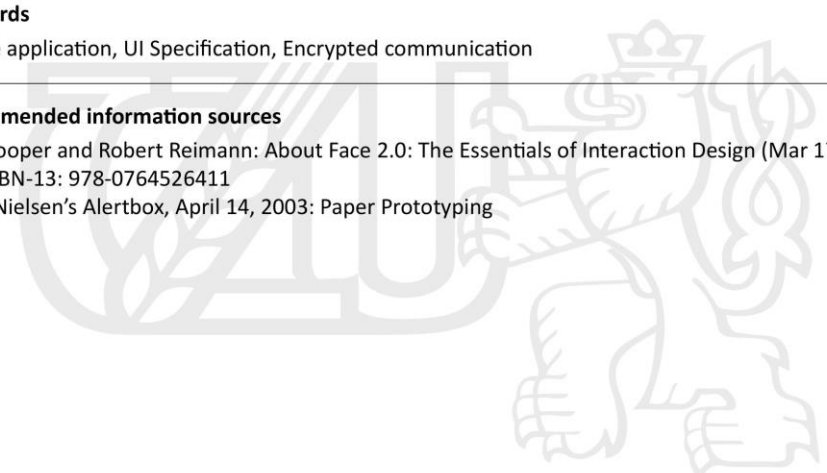
Keywords

Mobile application, UI Specification, Encrypted communication

Recommended information sources

Alan Cooper and Robert Reimann: About Face 2.0: The Essentials of Interaction Design (Mar 17, 2003), ISBN-13: 978-0764526411

Jakob Nielsen's Alertbox, April 14, 2003: Paper Prototyping



Expected date of thesis defence

2016/17 SS – FEM

The Bachelor Thesis Supervisor

Ing. Josef Pavlíček, Ph.D.

Supervising department

Department of Information Engineering

Electronic approval: 1. 11. 2016

Ing. Martin Pelikán, Ph.D.

Head of department

Electronic approval: 1. 11. 2016

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 14. 03. 2017

Declaration

I hereby declare to have compiled this final thesis “User Interface Specification of Mobile Application Supporting Encrypted Communication” entirely myself and in accordance with recommendations of my supervisor, that I indicate all the literature and other supporting materials used in the index of bibliography.

In Prague 15th of March, _____ Valeriya Sasina

Acknowledgements

Therefore, I would like to thank my supervisor Ing. Josef Pavlíček, Ph.D. for Your time, instructions and advice that were very helpful and essential during writing of this thesis.

User Interface Specification of Mobile Application Supporting Encrypted Communication

Specifikace Uživatelské rozhraní mobilní aplikace pro podporu šifrované komunikace

Summary

Aim of this bachelor thesis is to prepare a User Interface specification for mobile application with encrypted communication function. In order to let the User send encrypted messages to other users of this application from his list of contacts, as well as, to decrypt the correspondence by pressing one button and inserting passcode.

During the research will be observed and defined the current state of messaging applications on the market, analyzed possible encryption mechanisms and chosen the suitable one. Based on these observations will be designed, prototyped and tested interface of instant messaging mobile application according to the UI Specification.

Key words

Mobile application, UI Specification, Encrypted communication, Instant Messenger

Souhrn

Cílem této práce je připravit specifikaci uživatelského rozhraní pro mobilní aplikace s šifrovanou komunikační funkcí. Aby bylo možné nechat uživatele odesílat šifrované zprávy ostatním uživatelům této aplikace ze svého seznamu kontaktů, jakož i pro dešifrování korespondenci stiskem jednoho tlačítka a vložení přístupového kódu.

Během výzkumu budou sledovány a definovány současný stav messaging aplikace na trhu, analyzovány možné mechanismy šifrování a vybrán vhodný. Na základě těchto výzkumu budou navrženy a testovány rozhraní mobilní aplikace v závislosti na UI specifikace.

Klíčová slova

Mobilní aplikace, UI specifikace, šifrované komunikace, Instant Messenger

Contents

1. Introduction.....	8
2. Objectives and Methodology.....	9
3. Literature overview.....	10
3.1 Overview.....	10
3.2 History and early development.....	10
3.3 Top 5 Instant messaging apps.....	15
3.3.1 WhatsApp Messenger.....	15
3.3.2 Viber.....	16
3.3.3 Skype.....	16
3.3.4 Line.....	17
3.3.5 WeChat.....	17
3.4 App for business.....	19
3.5 Security risks.....	19
4. Encryption methods.....	21
4.1 Symmetric encryption.....	21
DES.....	22
AES.....	24
4.2 Asymmetric encryption.....	25
Diffie-Hellman.....	26
RSA.....	27
4.3 Hashing.....	28
SHA-1.....	28
MD5.....	29

4.4 The combination of encryption methods	31
4.5 End-to-end encryption	32
5. Practical part	33
5.1 SWOT analysis	33
5.2 Results from research	35
5.3 Goals.....	35
5.4 Personas	36
5.5 Use cases and scenarios	38
5.5.1 Log in use case	38
5.5.2 Settings use case.....	40
5.5.3 Chat use case	42
5.5.4 Group chat use case.....	47
6. Test in Usability Study	49
7. Changes in UI Specification	50
8. Conclusion	51
9. Bibliography	52
Table of Figures	56

1. Introduction

In previous years, people have made a big step in developing the sphere of information technologies. Nowadays it is already difficult to imagine life without internet, its importance increases from year to year.

Every day we surf the sites, read news, and which is more important - we communicate with other people. Moreover, for this we use mobile messengers. Today, their variety is greater than ever before, and there appears more and more applications.

It is possible to concern differently to the virtual communication, but deny it is pointless. Modern life requires to be in touch all the time, and technical devices only help at this aim. So many people use different messengers on their devices: desktops, laptops, tablets and smartphones.

On the one hand, it is not that good that people are increasing online communication, and decrease personal communication, but on the other hand, this saves a lot of time.

Nowadays applications become more and more secured, but these security methods are mostly headed to avoid stealing data while transferring. Also nowadays exists applications where messages are deleted. In addition, we should not forget about entering passcodes and Touch ID functions. However, what if someone will somehow bypass security. It would be much better to have one more level of security in the means of making personal data save. What I suggest is a messenger that will encrypt the messages not only inside the device, but also "outside", so the users will actually see that their messages are encrypted and unreadable. The mechanism of such encryption idea is simple: when user opens an application he sees all his chats and messages encrypted, and to decrypt his messages the system asks for the passcode, saved by the user at the registration.

This simple mechanism will ensure user that his messages are really encrypted, and will guarantee the protection of data from the stranger.

2. Objectives and Methodology

Objectives

The aim of this bachelor thesis is to prepare paper prototype of fully completed design of instant messaging mobile application that follows next use cases:

- automatically encryption of messages (by send button press)
- automatically decryption of messages after receiving the password
- entering password into key store for encrypt mechanism

and to choose type of encryption method based on the results of research in the form SWOT analysis applied on the instant messaging mobile applications.

Methodology

This survey will walk through several stages:

- Analyze current state of instant messaging mobile applications as WhatsApp, Viber etc.
- Study suitable literature for searching current state of encryption mechanisms.
- From the result of study define current state of mobile application and their ability to support encryption mechanisms.
- Define typical Use Cases and prepare UI Specification for suitable mobile application.
- Prepare paper prototype according to the UI Specification and test it.
- Describe conclusions for gained results.

The practical value of this thesis will consist in the fully completed design of instant messaging mobile application usable for implementation and development of physical application of this type.

3. Literature overview

3.1 Overview

It is hard to imagine more popular software category for smartphones than messengers. They used a huge amount of users both for personal use and for business. If 10 years ago the mobile Internet speed was not always enough for instant messaging, then now it is more than enough even for group video conferencing. Together with the increase in bandwidth of communication channels changed, an idea of what features should have a messenger. Now it can be used not only for writing messages, but also for making free calls to other users anywhere in the world.¹

3.2 History and early development

The history of online instant messengers started in 1988, when a Finnish developer Jarkko Oikarinen invented IRC protocol (Internet Relay Chat). There were main elements of modern chat: the ability to see the users online, send and receive messages and files.

Instant messaging has been growing field for many years, so it is quite difficult to accurately determine the time of occurrence of the first messengers. Nevertheless, easy enough to keep track of when instant messaging services have made a quantum leap and become really popular.

In the 90s, at the dawn of the era of instant messengers, most of the people who had access to the Internet, use the phone Dial-Up Modem. It was very slow (only 56 kbit/sec compare with the current 100 Mbit/sec), expensive and unstable way of connecting. Nobody connected to the Internet for more than one or two hours a day, as it was blocking phone and was paid for every minute. No one even dreamed about Internet access from mobile phones at those times. In addition, the idea of smartphones then seemed simply fantastic. The screens of mobile phones were black and white and can hold a maximum of two lines of text. However, only few people could afford mobile phones. Therefore, it is obvious that the first generation of instant messengers have been created mainly for the PC.

¹ How Instant Messaging Works. How Stuff Works [online]. [cit. 2016-06-14]. Available from: <http://computer.howstuffworks.com/e-mail-messaging/instant-messaging.htm>

The first messenger very well known today was ICQ (from English I SEEK YOU), which appeared in 1996. It all started with the four students from Israel, who created a company Mirabilis and began working on a program to communicate on the Internet and local networks. When create a program, they sent it for their friends and acquaintances. Those invited in "ICQ" their friends and acquaintances. The number of users has grown exponentially. After a while the talented foursome released a corporate version of ICQ. "ICQ" pioneered instant messengers market. Following the "ICQ" appeared AIM and MSN / WLM, and Gadu-Gadu, QQ, NateOn, Google Talk, Miranda, QIP, Skype and many others, including the only open standard - XMPP or Jabber.²

Despite the diversity of messengers, there was something that united them: "presence status". When you opened the app, the first thing you saw was a list of all your contacts and their status indicating if they are "Online".

You could discuss something with a friend only when both of you were online. There were also group chats, but their use has also been associated with a variety of problems and limitations. You could join a group chat just went into the net, but the participants of the chat are not necessarily able to be online at the same time with you. Anyone could be suddenly disconnected for any reason (instability of the compound, or a phone call). You missed all the conversations that took place at the time when you were offline. In addition, group chats are constantly inundated with automated messaging to change the status of contacts: Matt joined the chat; Jane disconnected.³

Little by little, many problems of the first series of messengers have been fixed or disappeared by themselves. The DSL modems provide high-speed and much more stable connection; there were developed offline messages and logs of conversations in which the story of chats was recorded.

² The History of Messengers: The First Wave. Grovety Inc. [online]. [cit. 2016-06-14]. Available from: <https://grovety.com/the-history-of-messengers-the-first-wave>

³ The history of the instant messengers, from IRC to Pidgin. Eioba [online]. [cit. 2016-06-14]. Available from: <http://www.eioba.com/a/119m/the-story-and-the-protocols-behind-instant-messengers>

With the development of mobile gadgets and cheaper Internet more and more people have become more actively using smartphones. In 2009 came the era of WhatsApp, which today is the most popular instant messenger in the world. Its developers have taken a strategically correct decision - they first tied user account to a phone number. As a result, the volume of SMS-traffic began to fall with catastrophic rate.

Initially WhatsApp was not a messenger. Jan Koum has created a service that showed the status of the contacts in the phonebook. The service also allowed to put your status manually.

WhatsApp was not in demand until in June 2009 Apple has created a push-notification option. Application began to resemble itself, even when the iPhone owner was not use it. Now every time a WhatsApp user changed his status, service alerted the whole list of his contacts. People began responding to each other statuses, and the application has become a means of communication itself.⁴

While its' own messenger with reference to the phone number was only at BlackBerry, it allows to communicate only to the owners of this smartphone. The iPhone does not have iMessage. Google Talk, Skype and ICQ was not that good as WhatsApp, because the list of contacts in these services was not attached to the phone numbers. By the way, when Koum created WhatsApp, it took him few months to manually synchronize it with all the prefixes that were used in phone numbers around the world.⁵

In August 2009 was announced the second version of WhatsApp, now with the messaging function. Followers of service for a few weeks rose to 250 thousand users. In December of the same year application was able send photos. By early 2011 WhatsApp has become the most popular app in the US App Store.⁶

⁴ MailOnline [online]. [cit. 2016-06-18]. Available from: <http://www.dailymail.co.uk/news/article-2563513/From-food-stamps-billionaire-How-WhatsApp-founder-went-struggling-immigrant-founder-19bn-messaging-service.html>

⁵ WhatsApp: The inside story. Wired [online]. [cit. 2016-06-18]. Available from: <http://www.wired.co.uk/article/whatsapp-exclusive>

⁶ WatsApp is the most popular chat app in more than half the world. Business Insider [online]. [cit. 2016-06-18]. Available from: <http://www.businessinsider.com/whatsapp-is-the-most-popular-chat-app-in-more-than-half-the-world-2016-5>

Today there are a huge number of messaging applications that are very similar to each other. The standard feature set includes not only text messages, but also file transfer, audio and video. The differences mainly lie in the interface and method of creating an account: with reference to the telephone number, to the page in the social network or, it is necessary to register a new account.

In almost every country with a developed IT-industry already exists its own service for free messaging. They are especially popular in Asia. This is due to the high usage of mobile internet - almost every resident of Japan, South Korea and China has a smartphone. This also applies to the poor, for them phone often replaces the computer. Therefore, messengers to them more convenient than e-mail and social networks.

In each of the countries listed above exists their leader in instant messengers. In China it is WeChat, Japan - Line, South Korea - KakaoTalk. There are also a free messaging services of Canadian, Israeli and Russian origin. To stand out from the rest, they come up with more and more new features.

If WhatsApp is considered a "killer" of ICQ, Viber is called a threat to Skype. In the three years since Viber come in sight, almost without investing in advertising, it has attracted 100 million active users. The audience of a Skype service, existing for more than 10 years, is three times bigger. Viber secret of rapid growth is the same as of WhatsApp - bounding contacts to the phone book of the user. In addition, when a person uploads Viber to his smartphone everyone in his list of contacts gets notification of it.

The rest of the function of this messenger differ slightly from the Skype features. The main purpose of Viber is free calls, but it is also possible to send messages, files, and stickers.

Stickers are something between emoticons and Japanese cartoon characters. They are images for expressing emotions or actions. Unlike emoticons, stickers more detailed and give information not only through facial expressions, but also through body language.

Stickers has been invented by the Japanese messenger Line in 2011. Initially, they were all free, but later it became possible to purchase additional sets of pictures.

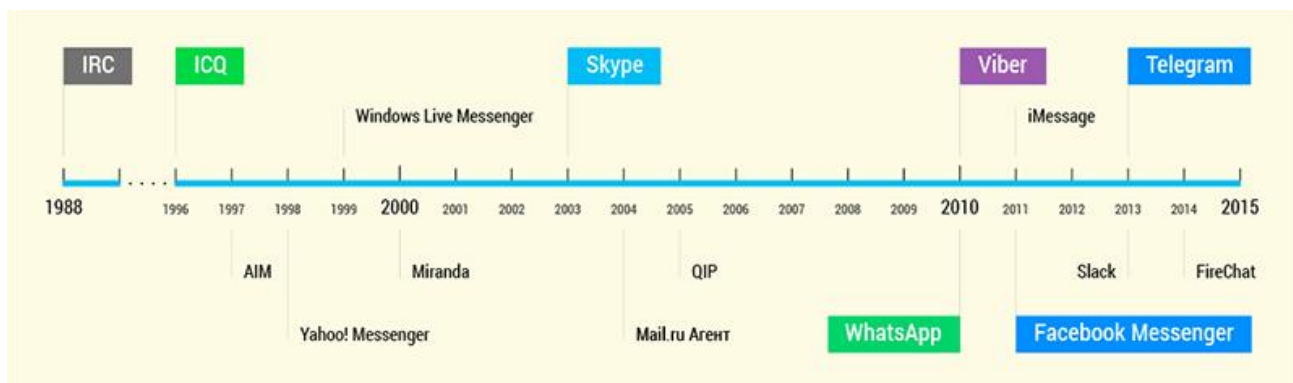
Messengers do not want to be just messaging services. Many of them have already entered the market of social networks. The pioneers in this, again, are the Asian services. Over the past three years, they have turned from SMS alternative to full social platforms.

Japanese messenger Line aims to be an alternative to Facebook, while maintaining the function of individual communication. At the same time director of marketing believes that the messengers and social networks have different social roles, and they are not direct competitors.

After the revelations of Edward Snowden in 2013, there on the market appeared a category of messengers, who's main function is data security.

For example, the most famous service of this kind in Russia is a Telegram, a project of former CEO "VKontakte" Pavel Durov. Posts in this messenger are not encrypted on remote servers, but on mobile devices themselves. This means that even the administration itself can not decrypt the messages of its users. Also Telegram has a function of self-destruction of messages after sending.⁷

Figure 1: Development of messengers timescale



Source: The History of Messengers: The First Wave. Grovetz Inc. [online]. [cit. 2016-06-20]. Available from: <https://grovety.com/the-history-of-messengers-the-first-wave>

⁷ The State of Social Media and Messaging in Asia: How Brands Use Messaging Apps to Engage Users. Nexmo [online]. [cit. 2016-06-20]. Available from: <https://www.nexmo.com/blog/2016/03/15/state-of-social-media-and-messaging-in-asia/>

3.3 Top 5 Instant messaging apps

Traditional SMS messages gradually fade into the background, while easy-to-use instant messaging applications go to the front. Functionality of messengers develops, transforming them from simple programs for messaging in a serious communication tool. Messengers compete with social networks and each other.

3.3.1 WhatsApp Messenger

WhatsApp is very easy to use and is currently the most popular application for correspondence and phone calls.

WhatsApp operating principle is very simple - the program syncs the data from the phonebook and automatically adds to contacts those users whose numbers were found on the device. If you want to contact a person on a certain number, it must first be added to the contacts list on your phone and then it will be available in the application.

In terms of messages WhatsApp gives all necessary possibilities as Stickers, voice notes, geotagging, etc. also it is possible to share files, photos and contacts.

Regarding the voice calls, can be said that the application does not allow to call on the landline and mobile phones. Voice calls can only be made to other users of the service. The connection quality is high enough, and bandwidth consumption is negligible. Calls as messages are completely free, the user only pays for Internet access on the mobile operator tariffs.

In the means of security, it should be noticed that on April 5, 2016 developers have announced that in all new versions of the application was included end-to-end encryption. The program is available on the leading mobile platforms and has Web-client.⁸

⁸ WhatsApp features. WhatsApp [online]. [cit. 2016-06-20]. Available from: <https://www.whatsapp.com/features/>

3.3.2 Viber

Messenger appeared in 2010 and was created as an alternative to Skype. Functional is almost the same, but Viber is integrated with the contact list of the user. Also Viber is very similar to WhatsApp, but has a number of advantages in the form of calls to regular numbers.

The first time user starts the application it requires to log in using the mobile phone number. Then numbers from the phonebook of the device will be added in Viber contacts list.

Viber provides chat, calls to other users, and calls to landlines and mobile numbers. Chat allows user not only to save on sms, but also to share the various content such as photos, video, geotagging and so on. It is also possible to record an audio message or use stickers.

User can contact with anyone from contact list in various ways, by free calls or messages, or video conference call directly on the phone number, which is listed as Viber Out.

In Viber benefits may also be included group chats of maximum 20 members, and Public chats where are participating millions of users from around the world. They are grouped by themes, dedicated to some events, famous personalities and so on. Viber is translated into more than 20 different languages, and in the list of supported platforms are Windows and Android, as well as iOS, Mac OS X and even Linux. According to the developers, all data is protected by end-to-end encryption.⁹

3.3.3 Skype

One of the oldest services for communication, initially focused on voice and video calls, but also allows to share and text messages. The service supports all existing mobile platforms.

This application has entered the market in 2003. At the first, it was positioned as a service for voice calls. Popularity did not come to it at once, as the calls over the Internet required a sufficiently wide channel, which not many people had at that time. Today the audience of Skype is more than 300 million people. Skype can be used to call any phone worldwide.

⁹ Messaging app Viber names Boston its US headquarters. BetaBoston [online]. [cit. 2016-06-25]. Available from: <http://www.betaboston.com/news/2015/10/16/messaging-app-viber-names-boston-its-us-headquarters/>

Application purchased by Microsoft, has already become a standard for fast messaging and phone calls, it allows to exchange instant messages, calls, and make the video chat. It is also possible to send SMS-messages or make calls to landlines at low rates. The app is absolutely free and works on all platforms, as well as on PCs and even TVs.

As an identifier Skype uses an e-mail. The method of ather old, but very reliable. Optionally user can attach a phone number, but not in the sense in which this is done in Viber and WhatsApp. There is no synchronization with the list of contacts of the device, and the added number will only be displayed on the display of the recipient in an outgoing call with Skype. Otherwise, it will often show the message "number is not defined."

Chats in Skype are very convenient. User can use stickers, download files, share locations or create group chat, inside which he can make both audio and video calls, with up to 25 people at a time.¹⁰

3.3.4 Line

Another popular messenger with hundreds of millions of users is mostly popular in Asia.

The mechanism is the same as in WhatsApp or Viber, wherein the identifier is a telephone number. In chat mode, LINE allows users to add stickers, pictures, voice messages, and other content. By this means, it is not much different from its competitors. The main advantage of LINE are calls both to application users and to mobile phones. The audio conference can simultaneously engage up to 200 people.¹¹

3.3.5 WeChat

The subscriber base currently consists of 600 million people, it provides sending text and voice messages, share files, including video. From the name is obvious that it was created with an aim of group chats. Among the interesting features are a built-in photo editor, automatic translation from major languages, as well as integration in the QQ and Facebook.

¹⁰ Everything you need to know about Skype. Softonic [online]. [cit. 2016-06-28]. Available from: <https://features.en.softonic.com/everything-you-need-to-know-about-skype>

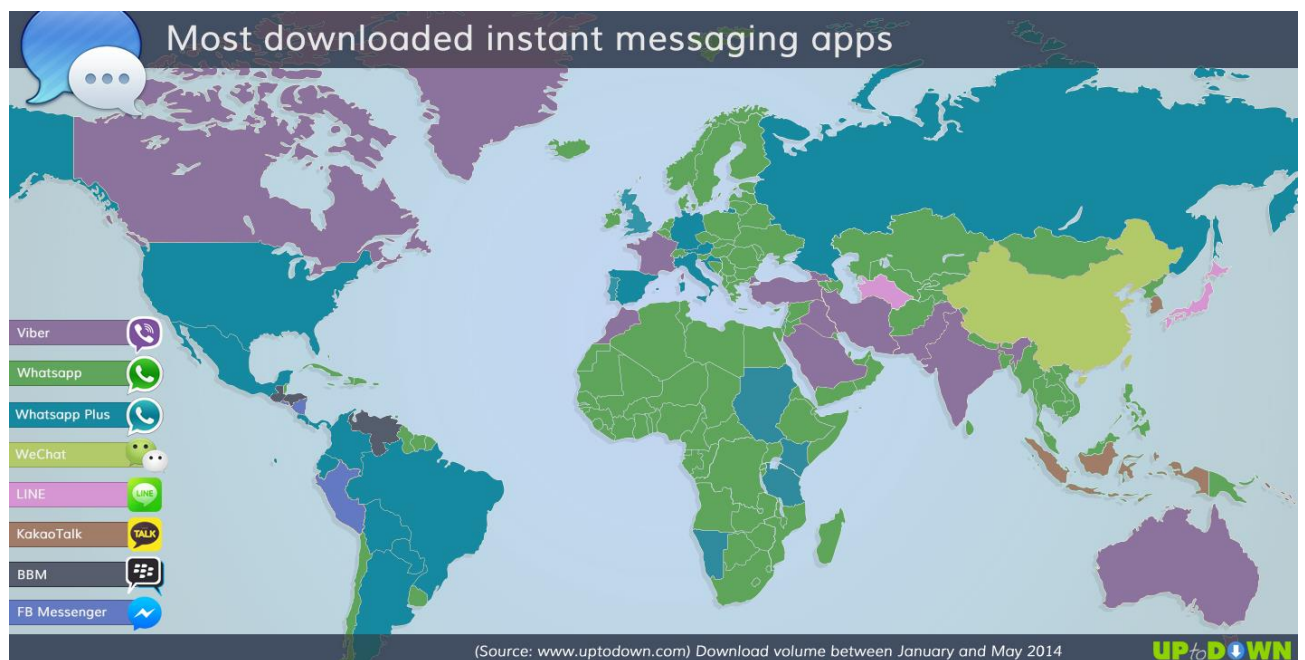
¹¹ Line: Free Calls & Messages [online]. [cit. 2016-06-28]. Available from: <https://line.me/en/>

This is just a small number of the whole variety of existing messengers. Different sources will give different ratings.

There is no leader among the messengers. WhatsApp is better for those who can not live without the constant exchange of text messages, Viber will help to save on the long phone calls and Skype is perfect in making video conference connecting to the caller on the other side of the globe. A little more specific are ICQ and Hangouts. The first service has long stalled in development, but it boasts a large user base, the second is ideal for those who constantly uses Google services. The functionality of messengers somehow intersects and is constantly expands.

Of course, if mobile Internet was not that cheap, instant messengers would never gain such popularity. Today, almost every mobile operator offers mobile Internet, so users can significantly save on communication via instant messengers.¹²

Figure 2: Most downloaded instant messaging apps



Source: Infographic: Instant Messaging Apps - Regional Preferences. *One Europe* [online]. [cit. 2016-06-28]. Available from: <http://one-europe.net/eurographics/infographic-instant-messaging-apps-regional-preferences>

¹² WeChat Help Center [online]. [cit. 2016-06-28]. Available from: http://help.wechat.com/cgi-bin/newreadtemplate?t=help_center/topic_list&plat=android&lang=en&Channel=helpcenter&detail=1003598

3.4 App for business

As well as for personal communication messengers are very suitable for business purposes.

Thus, Viber added the ability to create public accounts for companies and brands. Until now, for communication between business and customers they use public chats Viber, where a company representative could write messages, and subscribers could only read, or a company and a customer should have added each other to contacts.

Business account will allow to organize a two-way communication with subscribers. While now creating a business account is only on request, as well as public chats, but this service is absolutely free.

The number of mobile messengers increase rapidly and they entice more and more users from social networks. In the near future the same situation will take place in the business area, and instead of corporate Facebook will corporate Vibers.¹³

3.5 Security risks

With the spread and portability of mobile devices a set of security issues has arisen. Many people carry mobile phones. As soon as the devices become more skillful, offering access to corporate e-mail, databases and other corporate information, the question of how to protect this information becomes a priority.

If the device is stolen or lost, there will be the risk of compromising confidential data. This applies not only to the data residing on the device, but also to applications that provide access to data on a remote server.

Additionally, interaction with the wireless network using the mobile device creates its own set of risks inherent to it. With certain knowledge and equipment one can steal data from almost every moment between your device and the end point of your interaction.

¹³ WhatsApp rival Viber launches branded accounts for companies and public figures. Geektime [online]. [cit. 2016-07-05]. Available from: <http://www.geektime.com/2016/11/09/whatsapp-rival-viber-launches-branded-accounts-for-companies-and-public-figures/>

Users share a lot of personal moments in messengers, so developers try to create better encryption in the latest versions of their applications to secure messages and calls. Thus, only user and the person with whom he is communicating can read or listen to the content, and no one else.¹⁴

Figure 3: Data stored in instant messages apps



Source: *The Best Encrypted Messaging Apps You Can (and Should) Use Today*. *Heimdall Security* [online]. [cit. 2016-07-09]. Available from: <https://heimdalsecurity.com/blog/the-best-encrypted-messaging-apps/>

¹⁴ What does security mean? [online]. [cit. 2016-07-09]. Available from: <http://ccss.usc.edu/499/lecture1.html>

4. Encryption methods

Encryption is essential for protecting the confidentiality. There are different types and methods of encryption used to protect data today.

4.1 Symmetric encryption

With symmetric encryption normal human readable data, known as plaintext, is encrypted in the way that it becomes unreadable. This data scrambling is performed with the key. Once the data is encrypted, it can be safely transmitted to the receiver. At recipient the encrypted data is decoded using the same key which was used to encode. Thus it is clear that the key is the most important part of a symmetric encryption. It must be hidden from outsiders, since each one has access to it will be able to decrypt the private data. That is why this type of encryption is also known as the "secret key". In modern systems, the key is usually a line of data, which is derived from a strong password, or completely random source. It is put in the symmetric encryption software which uses it to scramble the input data. Data scrambling is achieved using a symmetric encryption algorithm such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), or the International Data Encryption Algorithm (IDEA). The weakest part in this type of security is encryption key, in terms of storage, as well as the transfer of the authenticated user. If a hacker is able to get the key, he can easily decrypt the encrypted data, destroying the whole point of encryption. Another disadvantage results from the fact that the software that processes the data may not work with the encrypted data. Therefore, to be able to use this software, the data must first be decoded. If the software itself is compromised, an attacker can easily obtain data.^{15 16}

¹⁵ What are the Different Techniques of Encryption? Buzzle [online]. [cit. 2016-09-03]. Available from: <http://www.buzzle.com/articles/what-are-the-different-techniques-of-encryption.html>

¹⁶ Understanding the 3 Main Types of Encryption. Atomic Object [online]. [cit. 2016-09-03]. Available from: <https://spin.atomicobject.com/2014/11/20/encryption-symmetric-asymmetric-hashing/>

Symmetric encryption algorithms

DES (Data Encryption Standard) is a symmetric encryption algorithm in which one key is used both for encrypting and decrypting data. DES was developed by IBM and approved in 1977 as the official standard (FIPS 46-3). DES has blocks of 64 bits and 16 frame structure of Feistel network, and uses a key with a length of 56 bits for encryption.

The input data for a block cipher is a block of n size bits and a k -bit key. At the output, after applying the encrypting transformation, an n -bit encrypted block is received. An insignificant difference in the input data lead to a significant change in the output. Block ciphers are implemented by repeatedly applying some basic transformations to the blocks of the source code.¹⁷

There are two basic transformations:

- Complex conversion on one local part of the block.
- Simple conversion between parts of a block.

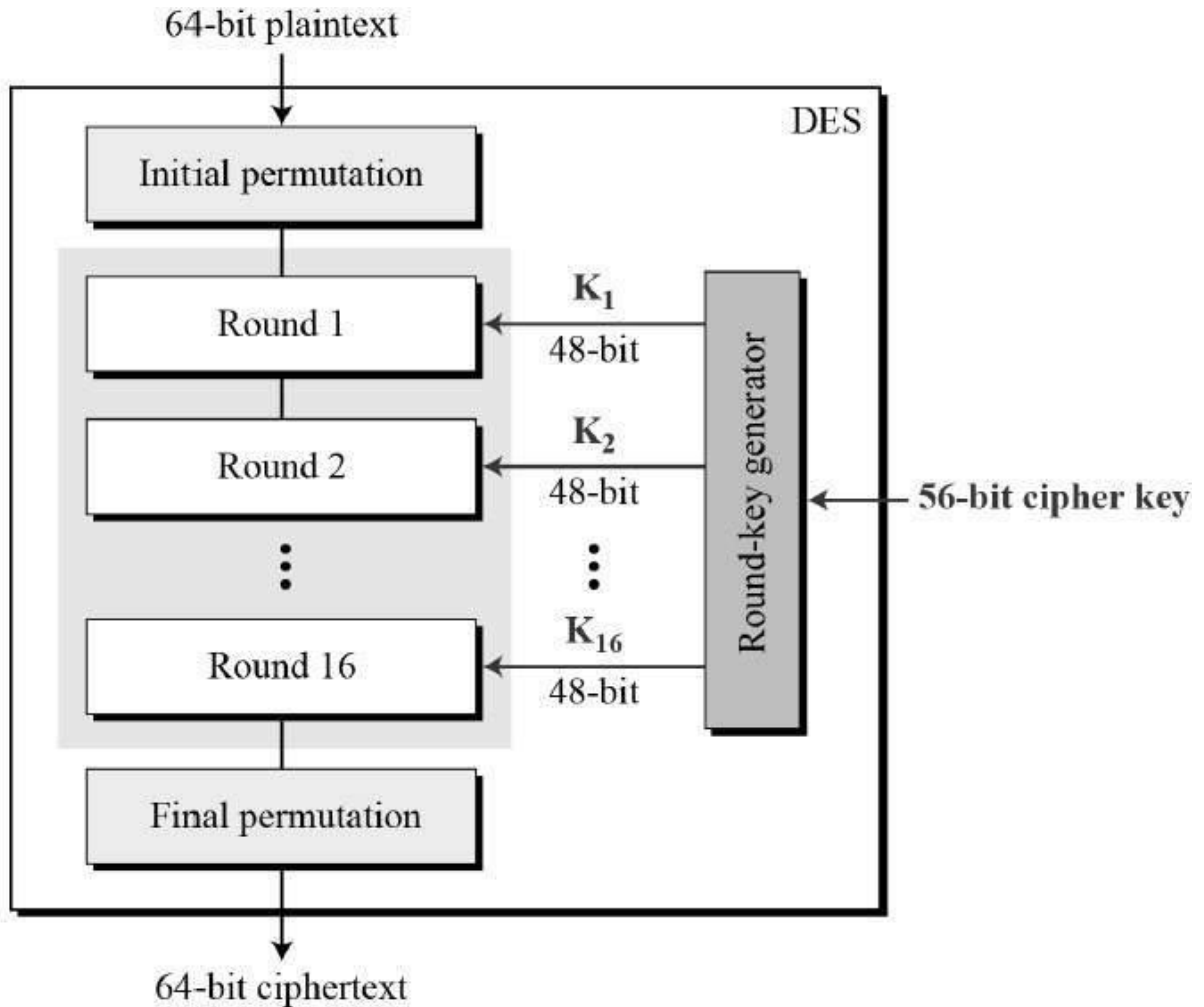
Since the conversion is done block-wise, at first the source data should be separated into blocks of the required size. In this case, regardless of the format of the source data, it could be text documents, images or other files, they should be interpreted in a binary form and only then divided into blocks.

In the DES algorithm, a direct conversion by the Feistel network in encryption and the reverse transformation by the Feistel network in decryption are used.

The encryption process consists of an initial permutation, 16 encryption cycles using a 56-bit key and the final permutation.

¹⁷ Data Encryption Standard (DES) [online]. [cit. 2016-09-15]. Available from: <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

Figure 4: DES algorithm



Source: Data Encryption Standard. *TutorialsPoint* [online]. [cit. 2016-09-15]. Available from: https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm

When decrypting data, all actions are performed in the reverse order. In 16 cycles of decryption, unlike encryption using a direct transformation of the Feistel network, the reverse transformation by the Feistel network is used here.

Due to the small number of possible keys (only 2^{56}), it becomes possible to go through all possible options of the key. In 1998, the Electronic Frontier Foundation using a special DES-Cracker computer, managed to crack DES in 3 days.¹⁸

Currently, DES with a 56-bit key is used only for outdated systems, and most often is used more crypto-stable forms as 3DES, DESX. 3DES is a simple effective replacement for DES, and now it is considered as a standard.¹⁹

AES (Advanced Encryption Standard) is also known as Rijndael, is a symmetric block cipher algorithm adopted by the US government as a standard as a result of a competition held between technology institutes. It replaced the outdated Data Encryption Standard, which no longer met the requirements of network security, which became more complex in the 21st century.²⁰

AES and Rijndael are not exactly the same, since AES has a fixed block size of 128 bits and key sizes of 128, 192 and 256 bits, while for Rijndael any block and key sizes can be specified, from a minimum of 32 Bit to a maximum of 256 bits.²¹

It is believed that the 128-bit key used in Advanced Encryption Standard is quite reliable protection against frontal attack, that is, from a purely mathematical point of view, to pick one correct password out of all possible is an impossible task. Due to the statistics, the data protected by this algorithm has never been hacked. However, all this works with a key size of at least 128 bits, since earlier cryptographic algorithms still did not withstand the strength test.²²

¹⁸ How long does it take to crack DES and AES? Gryptography [online]. [cit. 2016-09-15]. Available from: <http://crypto.stackexchange.com/questions/752/how-long-does-it-take-to-crack-des-and-aes>

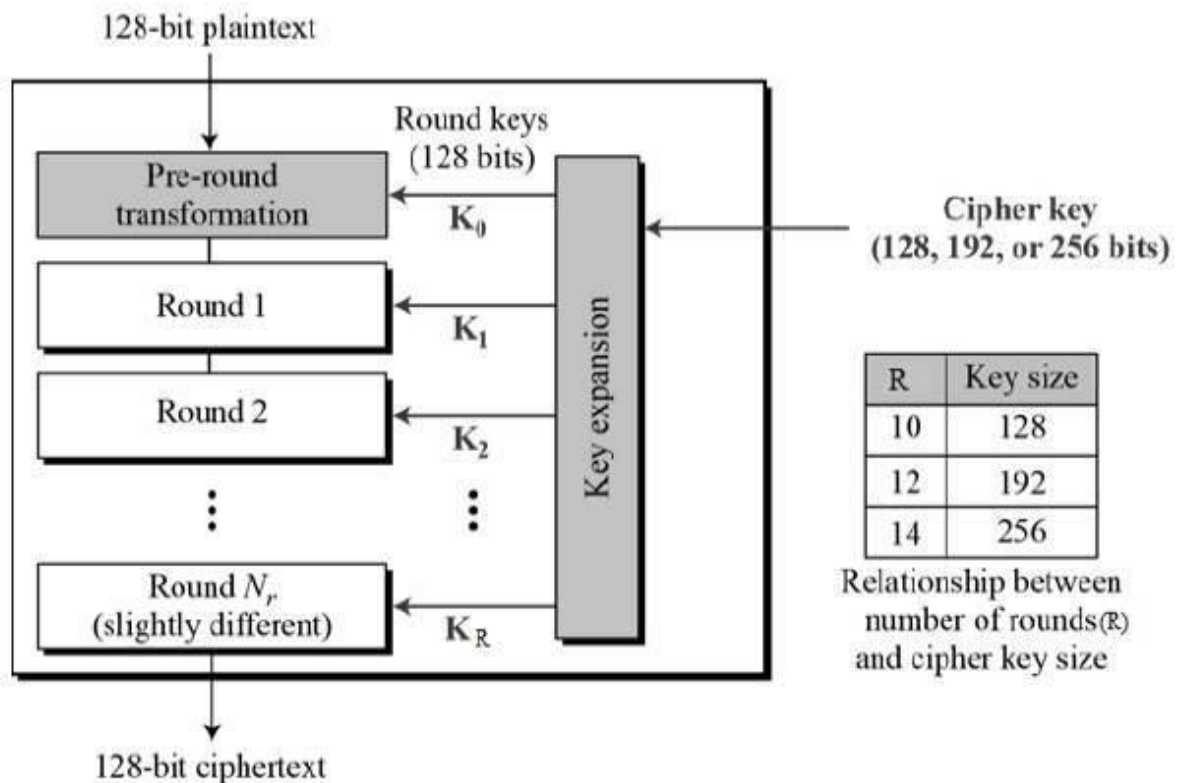
¹⁹ Is DES or 3DES still being used today? Stack Overflow [online]. [cit. 2016-09-18]. Available from: <http://stackoverflow.com/questions/1619212/is-des-or-3des-still-being-used-today>

²⁰ Advanced Encryption Standard (AES). TechTarget [online]. [cit. 2016-09-20]. Available from: <http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>

²¹ The Differences Between Rijndael and AES. Microsoft Developer [online]. [cit. 2016-09-20]. Available from: <https://blogs.msdn.microsoft.com/shawnfa/2006/10/09/the-differences-between-rijndael-and-aes/>

²² How secure is AES against brute force attacks? EE Times [online]. [cit. 2016-09-20]. Available from: http://www.eetimes.com/document.asp?doc_id=1279619

Figure 5: AES algorithm



Source: Advanced Encryption Standard. *TutorialsPoint* [online]. [cit. 2016-09-20]. Available from: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

4.2 Asymmetric encryption

Asymmetric key encryption works similarly as symmetric key; it uses a key for encryption of transmitted messages. However, instead of using the same key, it uses completely different one to decrypt the message. The key used for encryption is available to anyone of all network users. As such, it is known as the "public" key. On the other hand, the key used for decryption is stored in secret, and is intended for use in private by the user. Therefore, it is known as "private" key. Asymmetric encryption is also known as public key encryption. Since, in this method, the secret key needed to decrypt the message should not be transmitted every time, and it is usually known

only to the user (receiver), the probability that an attacker can decrypt the message considerably lower. Diffie-Hellman and RSA algorithms are examples of using public key encryption.^{15 16}

Asymmetric encryption algorithms

Diffie-Hellman key exchange is an algorithm that allows two parties to get the secret key using non-secure communication channel. The scheme of open distribution of keys proposed by Diffie and Hellman made a real revolution in the world of encryption, as it removed the main problem of classical cryptography - the problem of key distribution.

The Diffie-Hellman algorithm itself was introduced to the world back in the year 1976. Its creators were Whitfried Diffie and Martin Hellman, who in their search for safe and reliable methods of data encryption relied on the work of Ralph Merkle, who developed the so-called system of distribution of public keys. But if Merkel developed an exclusively theoretical framework, Diffie and Hellman presented the public with a practical solution to this question.²³

The algorithm itself was created in such a way as to ensure not only the confidentiality of data transferred by one side to the other, but also to safely extract them on receipt. Roughly speaking, such a transmission system should provide full protection in all possible channels of communication. In its pure form, the Diffie-Hellman algorithm is vulnerable to modification of data in the communication channel, including the "Man in the Middle" attack, so the schemes using it use additional methods of one-way or two-way authentication.

Using this algorithm each side generates a random natural number a - private key, then Together with the remote party, sets the open parameters p and g (usually the values of p and g are generated on one side and transmitted to the other), where p is a random prime number and g is a primitive root mod p . After that first side computes the public key A using the conversion over the private key a , by the formula $A=g^a \text{ mod } p$ and exchanges public keys with the remote side. On the next step it calculates the shared secret key K using the public key of the remote side B and its private key a , by formula $K=B^a \text{ mod } p$. This key is equal on both sides, as

²³ WHAT IS DIFFIE-HELLMAN? DELL EMC [online]. [cit. 2016-10-04]. Available from: <http://www.centera.bz/emc-plus/rsa-labs/standards-initiatives/what-is-diffie-hellman.htm>

$$B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p$$
²⁴

In practical implementations, for a and b are used numbers of the order of 10^4 and p of the order of 10^300 . The number g should not be large and usually has the value 2 or 5.

It should be noted again that the Diffie-Hellman algorithm works only on communication lines reliably protected from modification. If it were applicable to any open channels, it would have long ago removed the problem of key distribution and, perhaps, replaced all asymmetric cryptography. However, in cases where the data can be modified in the channel, there is an obvious possibility of wedging in the process of generating the keys "Man in the middle" using the same scheme as for asymmetric cryptography.²⁵

RSA (an abbreviation for the names Rivest, Shamir and Adleman) is a cryptographic algorithm with a public key, based on the computational complexity of the factorization problem for large integers.

Cryptographic systems with a public key use so-called one-way functions. One-sidedness is understood not as a theoretical directionality, but as a practical impossibility to calculate the inverse value using modern computational means for a foreseeable time interval.²⁶

RSA is a relatively slow algorithm, which is why it is not widely used to directly encrypt user data. Most often this method is used to send encrypted shared keys for a symmetric encryption key, which in turn can perform mass encryption and decryption operations at a much higher speed.

Generation of keys in RSA is carried out as follows:

1. Two prime numbers p and q are chosen (such that p is not equal to q).
2. The module $N = p * q$ is calculated.

²⁴ «Diffie-Hellman Key Exchange» in plain English. StackExchange [online]. [cit. 2016-10-05]. Available from: <https://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english>

²⁵ Diffie-Hellman key exchange (exponential key exchange). TechTarget [online]. [cit. 2016-10-05]. Available from: <http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange>

²⁶ RSA algorithm (Rivest-Shamir-Adleman). TechTarget [online]. [cit. 2016-10-05]. Available from: <http://searchsecurity.techtarget.com/definition/RSA>

3. The value of the Euler function from the module N is calculated: $\phi(N) = (p-1)(q-1)$.
4. We choose a number e , called an open exponent, the number e must lie in the interval $1 < e < \phi(N)$, and also be relatively prime to the value of the function $\phi(N)$.
5. The number d , called the secret exponent, is calculated such that $d * e = 1 \pmod{\phi(N)}$, that is, it is multiplicatively inverse to the number e modulo $\phi(N)$.²⁷

This scheme is not used in practice for the reason that it is not practically reliable or semantically secured. Indeed, the one-way function $E(m)$ is deterministic, which means that for the same values of the input parameters produces the same result, which means that the necessary condition of practical reliability of the cipher is not met.

4.3 Hashing

The technique uses a hashing algorithm known as a hash function to generate a special line from the data known as a hash. This hash has the following properties: the same data is always produces the same. It is inadvisable to try different combinations of input data to generate the same hash. Thus, the main difference between the hash and the other two methods of data encryption is that once the data is encrypted (hashed), it can not be made back in its original form. This fact ensures that even if a hacker gets hash, it will be useless for him, since he can not decrypt the message content.¹⁵ Message Digest 5 (MD5) and Secure Hashing Algorithm (SHA) are two widely used hash algorithms. As mentioned previously, it is almost impossible to decrypt the data from a given hash. However, this is true only if strong hashing is implemented. In the case of weak implementation of the hashing technique, a persistent hacker using a sufficient amount of resources, and brute force attacks can find data that match the hash.¹⁶

SHA-1 implements a hash function built on the idea of a compression function. The inputs of the compression function are the 512-bit message block and the output of the previous message block. The output is the value of all hash blocks until this point. In other words, the hash of the

²⁷ RSA Algorithm [online]. [cit. 2016-10-07]. Available from: http://www.di-mgt.com.au/rsa_alg.html

block M_i is $h_i = f(M_i, h_{i-1})$. The Hash value of the entire message is the output of the last block.²⁸

The original message is divided into blocks of 512 bits each. The last block is padded to a length that is a multiple of 512 bits. First, add 1 (bit), and then zeros, so that the block length becomes $(512 - 64 = 448)$ bits. The remaining 64 bits write the length of the original message in bits (in big-endian format). If the last block has a length of more than 448, but less than 512 bits, the addition is performed as follows: first 1 bit is added, then zeros up to the end of the 512-bit block; After that, another 512-bit block is created, which is filled up to 448 bits with zeros, after which in the remaining 64 bits the length of the original message in bits (in little-endian format) is written. The last block is always added, even if the message already has the required length. The main loop iteratively processes each 512-bit block. The iteration consists of four stages of twenty operations in each. The message block is converted from 16 32-bit words to 80 32-bit words. The final value is the union of five 32-bit words into one 160-bit hash value.²⁹

SHA-1 has vulnerability to various types of attacks. The main ones:

- Finding collisions is a situation where two different initial messages correspond to the same hash value.
- Finding the prototype - the original message by its hash.

MD5 (Message Digest 5) is a 128-bit hash algorithm developed by Professor Ronald L. Rivest of the Massachusetts Institute of Technology (MIT) in 1991. It is intended for creation of "prints" or digests of the message of any length and the subsequent check of their authenticity. It was widely used to verify the integrity of information and store passwords in a closed form.³⁰

The hash algorithm looks like this. The input stream is aligned so that its length becomes comparable to 448 modulo 512. First, a single bit is added to the end of the stream, then the required number of zero bits. Then a 64-bit representation of the length of the input stream is

²⁸ Secure Hashing Algorithms. Brilliant [online]. [cit. 2016-10-17]. Available from: <https://brilliant.org/wiki/secure-hashing-algorithms/>

²⁹ How Hash Algorithms Work [online]. [cit. 2016-10-19]. Available from: <http://www.metamorphosite.com/one-way-hash-encryption-sha1-data-software>

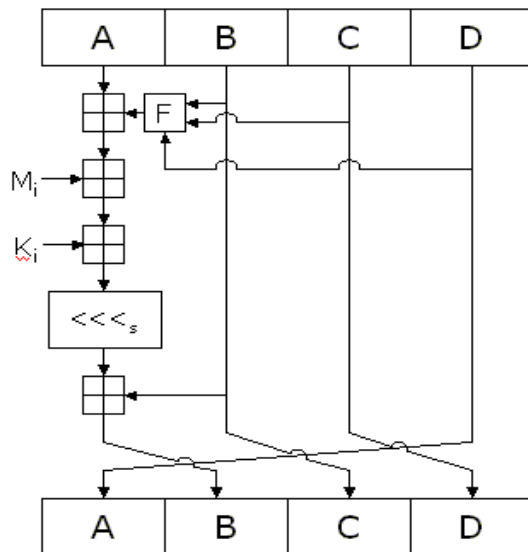
³⁰ Message Digest 5 (MD5). Techopedia [online]. [cit. 2016-10-22]. Available from: <https://www.techopedia.com/definition/31700/message-digest-5-md5>

added to the result of the previous step. Thus, in this step, the stream length becomes a multiple of 512 bits or 16 32-bit words. Further, the buffer is initialized, it consists of four constants (A, B, C, D), designed to collect the hash. After that, 4 auxiliary logic functions are defined that convert the input 32-bit words.

- $F(X,Y,Z) = (X \text{ and } Y) \text{ or } (\text{not}(X) \text{ and } Z)$
- $G(X,Y,Z) = (X \text{ and } Z) \text{ or } (Y \text{ and } \text{not}(Z))$
- $H(X,Y,Z) = (X \text{ xor } Y \text{ xor } Z)$
- $I(X,Y,Z) = (Y \text{ xor } (X \text{ or } \text{not}(Z)))$

Then there are four rounds of transformation. Each round consists of 16 elementary transformations, using functions and sequentially storing the hash in the buffer. At the end, the result of the calculations stored in the buffer is a hash. And when it is printed in the reverse order, it is MD5 hash. The hash contains 128 bits (16 bytes) and is usually represented as a sequence of 32 hexadecimal digits.³¹

Figure 6: MD5 algorithm



Source: The MD5 cryptographic hash function. *Ius Mentis* [online]. [cit. 2016-09-22]. Available from: <http://www.iusmentis.com/technology/hashfunctions/md5/>

³¹ The MD5 cryptographic hash function. *Ius Mentis* [online]. [cit. 2016-10-22]. Available from: <http://www.iusmentis.com/technology/hashfunctions/md5/>

Earlier it was thought that MD5 allows to obtain a relatively reliable identifier for a data block. Since 1993, studies have appeared regularly that reveal new vulnerabilities in the MD5 algorithm. At the moment, the MD5 algorithm is considered vulnerable ³² and is gradually replaced by the SHA algorithm.

4.4 The combination of encryption methods

As discussed above, each of these three encryption techniques suffer from some drawbacks. However, when using a combination of these methods, they form a highly reliable and efficient encryption system. Most often, the methods of the public key and secret combined and used together. Secret key method enables quick decoding, while the public key method offers a safer and more convenient way to transfer the secret key. This combination of methods is known as the "digital envelope".³³ PGP e-mail encryption program is based on the technique of "digital envelope". Hashing is used as a means to test password strength. If the system stores the hash of the password, instead of a password, it will be safer, because even if a hacker gets the hash, he can not understand or read it. During the test, the system checks the hash of the incoming password, and see if the result is the same as what is stored. Thus, the actual password will be visible only in brief moments when it should be changed or checked, which will significantly reduce the chances of getting it into the wrong hands. Hashing is also used for data authentication using the secret key. The hash is generated using the data and the key. Consequently, only visible data and a hash and the key itself is not transferred. Thus, if any changes are made to the data or the hash, they will be readily detected.³⁴

It should be mentioned that these methods can be used to effectively encode data into an unreadable format, which can ensure that they stay safe. Most of the current systems generally use a combination of these methods of encryption, along with a strong implementation of

³² Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms [online]. [cit. 2016-10-23]. Available from: <https://tools.ietf.org/html/rfc6151>

³³ Digital Envelope. Techopedia [online]. [cit. 2016-11-02]. Available from: <https://www.techopedia.com/definition/18859/digital-envelope>

³⁴ Multiple encryption. A Few Thoughts on Cryptographic Engineering [online]. [cit. 2016-11-03]. Available from: <https://blog.cryptographyengineering.com/2012/02/02/multiple-encryption/>

security algorithms. In addition to safety, the system also provides many other procedures, such as checking the identity of the user and to ensure that the data can not be falsified.

4.5 End-to-end encryption

End-to-end encryption is a system in which encrypted information is sent from sender's device to receiver's device directly, without a middleman. The rule of private key do not allow to decrypt the information to anyone other than its recipient. Thus, encryption of messages and decryption take place without the participation of the server. Currently, E2E encryption reliability is not in doubt. However, every person who wants to use the services of encryption, it is necessary to get acquainted with some of its shortcomings.

Since all received messages together with their decryption keys are stored in the device memory, its loss or theft will lead to a loss of all the correspondence that can not be restored.

Imagine a classic E2E conversation "one to one". In this case, only two devices are involved: device "A" and device "B". Device "A" encrypts data so that only the device "B" could read it. This conversion does not use a lot of bandwidth and takes a second.

Now imagine a conversation in a group chat of twenty members. The sender's device will have to encrypt a message for each participating device in a dialog. In this case - twenty times. Now add to this the ability to register two or more devices on one account, such as phone and tablet. The number of required encryptions will increase.

Although the technology is not new and has existed for several decades, end-to-end encryption is not widely spread. Even so, the importance of the end-to-end encryption will only grow as the Internet and digital technologies evolve.³⁵

³⁵ End-to-end encryption (E2EE). TechTarget [online]. [cit. 2016-11-08]. Available from: <http://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE>

5. Practical part

5.1 SWOT analysis

Table 1: SWOT analysis

Strengths	Weaknesses
1. High security level of messages 2. Include all main features of standard instant messaging app	1. Large number of instant messaging apps 2. New and unknown in the market
Opportunities	Threats
1. High interest among users due to the uncommon features 2. Cooperation with big corporations	1. Low interest to the new/unknown app among users 2. Requirement to enter passcode

Source: Author

Strengths

1. High security level of application

As was already said, security is very important aspect of any correspondence and high level of protection of data is one of the strongest sides of this application.

2. Include all main features of standard instant messaging app

All needed features in one app will positively affect the number of users.

Weaknesses

1. High competition level

Great number of similar applications in the market can affect the interest to this application.

2. New and unknown in the market

Users may have low confidence level in the new and unknown application, which can negatively affect the number of downloads and future of this app.

Opportunities

1. High interest among users due to the uncommon features

There is an opportunity that new feature will catch an interest among very big number of users due to its unusualness.

2. Cooperation with big corporations

Corporations are always care much about leak of data through private conversations. Using this application may prevent such situations.

Threats

1. Low interest to the new/unknown app among users

Big amount of similar applications on the market may cause a low interest between users, who are already get used to the other applications.

2. Requirement to enter passcode

User may be bored of entering the passcode every time he/she wants to reread the conversation or answer the newly receiver message.

5.2 Results from research

After the research, several main areas were identified, which should be noted when developing this application.

Firstly, users expect the basic functions of an application of this type, such as messaging, sending stickers, photos, audio and video files, the ability to send sound messages and location tags. Also, users prefer applications with the ability to make free audio and video calls. A great advantage is the creation of an account by means of a mobile phone number, where the synchronization with the phonebook automatically takes place.

Another important aspect is the encryption method used in the application. In this case, end-to-end encryption is most suitable, as this technique is already successfully used in applications of this type and is relatively familiar among common users, which will certainly help to locate potential users to the new application.

There also is a need to pay attention to the design of the application. Although the presence of a new interesting and useful function should theoretically attract users, the wrong design can scare them away. Therefore, it was decided to follow the standard design for this type of applications. The user should feel comfortable using this application, which is why the familiar layout of the elements on the screen will help the user to quickly get used to the new application.

5.3 Goals

1. Log in to the application using phone number
2. List of contacts from phonebook
3. Set passcode for encryption/decryption of messages
4. Send encrypted message
5. Decrypt messages in chat
6. Create a group chat
7. Make voice/video call

8. Send sticker/photo/video/file/location
9. Last calls list
10. Delete a chat
11. Latest online status
12. Modify personal account

5.4 Personas

Name: Timothy White

Age: 35

Gender: Male

Hobby: Plays bowling

Background: Timothy has MBA and works in big IT company. He organizes the work of the teams on different projects. Clients are big and small companies. Due to the many meetings Timothy not always has access to the laptop to answer work emails, but there is always his smartphone in his pocket for work issues solution.

Typical day: Every morning he takes coffee on the way to the office, where briefing with the teams working on the projects. At lunch time he has some meetings with the clients at which they discuss further cooperation. During the day he receives reports about flow of the current projects. At the end of the day he meets with his friends at the bar or in bowling.

Additional info:

Occupation: Chief project manager

Marital Status: Single

Name: Jake Winters

Age: 28

Gender: Male

Hobby:

Background: Jake has a Bachelor Degree and works in the company, which has many offices through the whole country. As a head of regional office from time to time he goes to business trips for the purpose of training or for report in head office. He recently got married and the feelings are still very strong, therefor during these trips he has intimate correspondence with his wife.

Typical day: In the morning he is having breakfast with his wife and goes to work. At work he conducts business correspondence with colleague from other regional offices and follows the work of his managers. After work he drives along the way to the flower shop or pastry-shop to buy something that will please his wife. After that he heads to his home for dinner.

Additional info:

Occupation: Head of regional office

Marital Status: Married

Name: Amy Spenser

Age: 16

Gender: Female

Hobby: Watching movies

Background: Amy is a high school student and after the graduation she plans to go to college. She is very popular and has a lot of friends. She chats a lot with her friends about girlish things and also about boys. As most of teenagers she is afraid that somebody will know her secrets.

Typical day: In the morning she wakes up, has breakfast and go to school. During the lunch she gossips with her friends in the canteen. After school she goes to the theater class to the rehearsal for the spring theatrical performance. After it she arranges a meeting with friends to go to cinema.

Additional info:

Occupation: High School Student

5.5 Use cases and scenarios

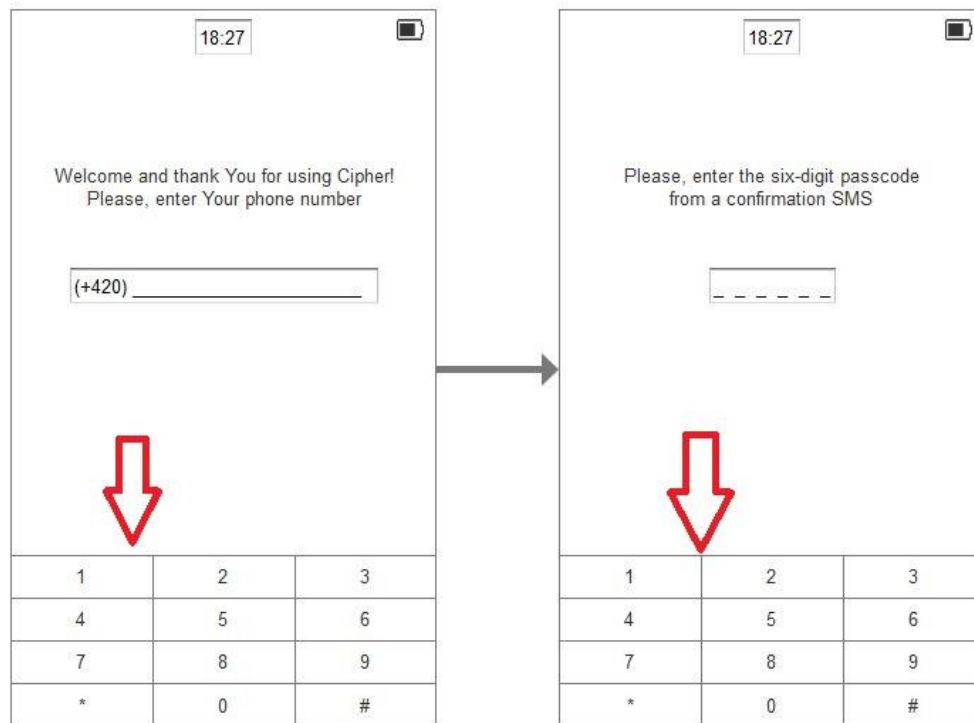
5.5.1 Log in use case

After uploading this application to the device, User expects to log in to it using phone number. As well User wants to see the list of contacts with whom he/she can communicate by this application.

Log in Scenario

Application asks for Users' current phone number, after receiving it, application sends an SMS with confirmation code for this number. Service expects to receive this code in the special field.

Figure 7: Log in Scenario



Source: Author

Synchronization of contacts Scenario

Application asks User for allowance in order to use phonebook, as soon as it obtains the permission, it adds all contacts, who are using this app to the contact list.

Figure 8: Synchronization of contacts Scenario



Source: Author

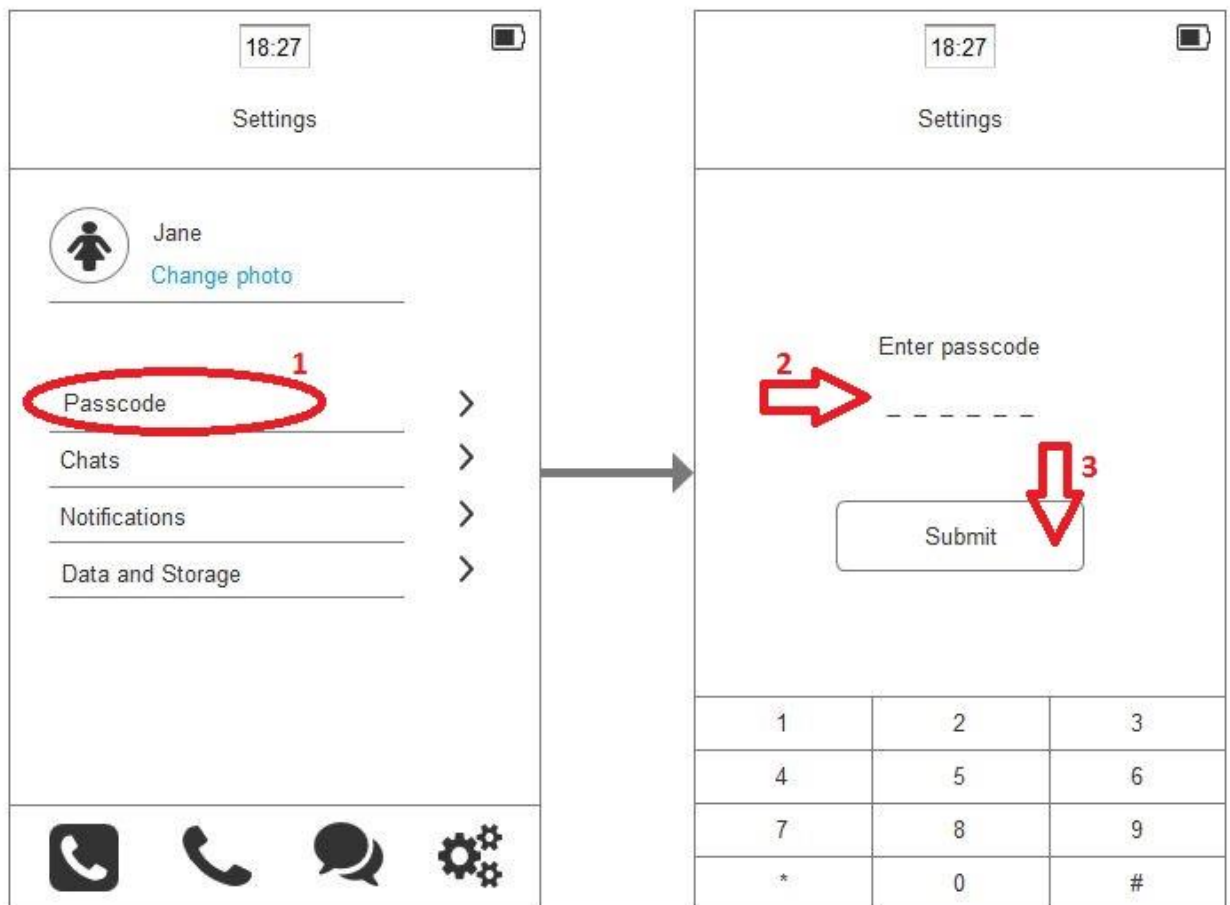
5.5.2 Settings use case

User expects to modify settings of his/her personal account. The main User demand is to set passcode for encrypting/decrypting messages, in order to protect personal or business correspondence.

Set passcode Scenario

Application allows User to set passcode for further encryption and decryption of messages. After User sets the code, system automatically encrypts all existed chats and asks User to enter code every time User decides to decrypt the chat.

Figure 9: Set passcode Scenario

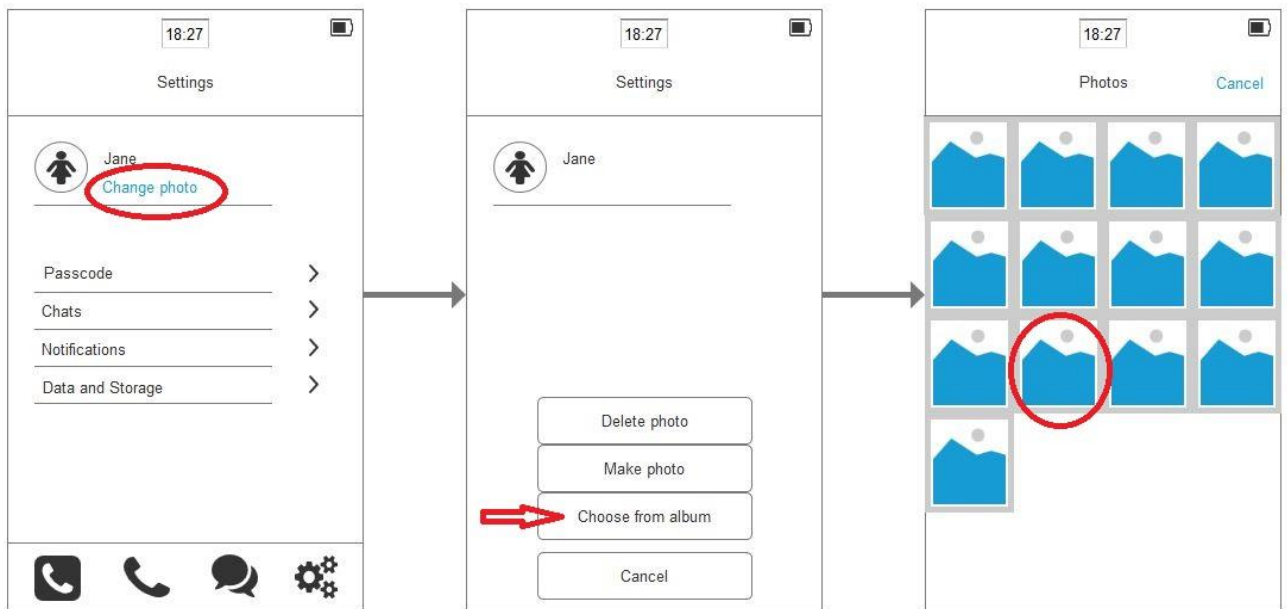


Source: Author

Change profile photo Scenario

Application gives User possibility to change profile photo, by selecting photo from photo album of the device or by making a new photo.

Figure 10: Change profile photo Scenario



Source: Author

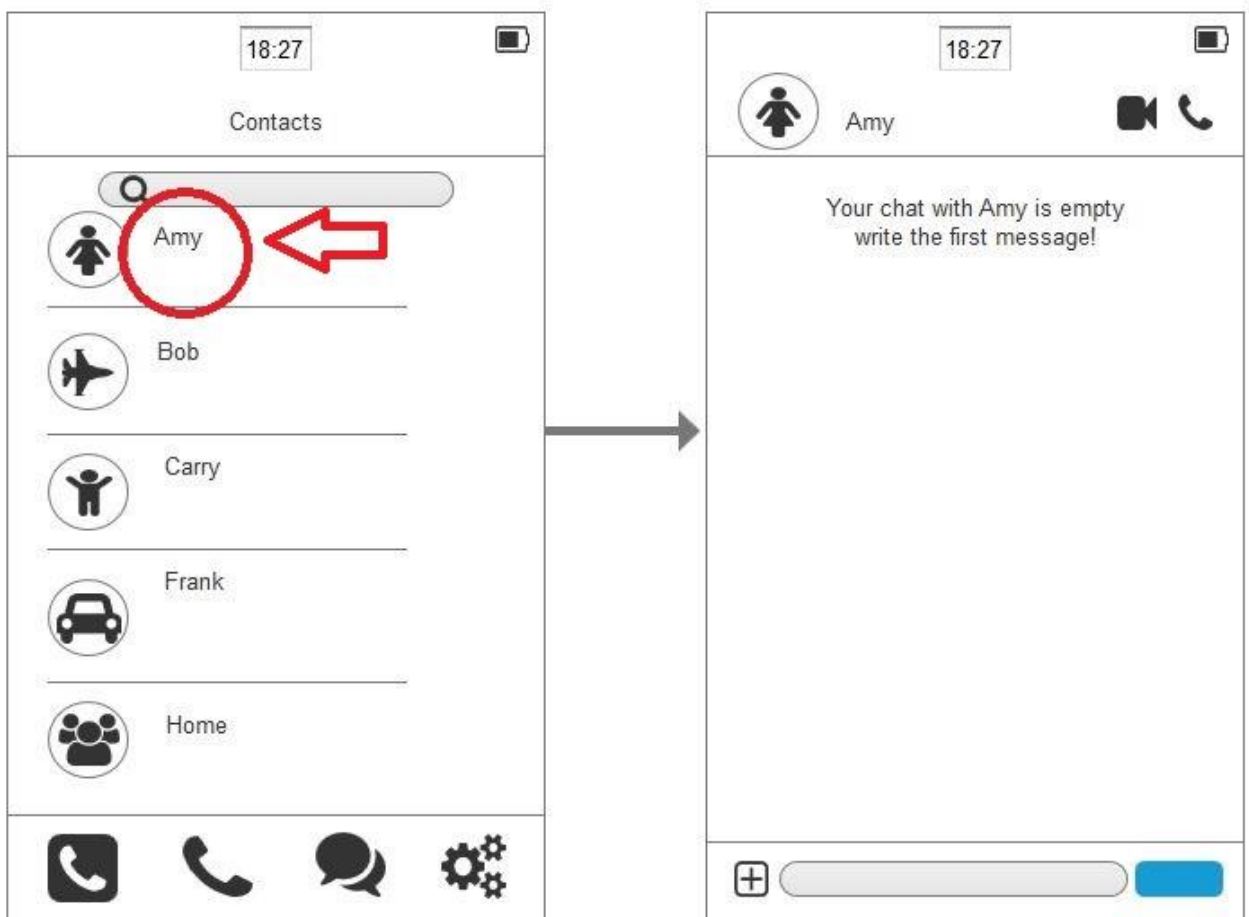
5.5.3 Chat use case

User expects to communicate with other users by sending encrypted messages, sending photos, videos, files etc. making voice and video calls.

New chat Scenario

Application allows User to contact anyone in the contact list who also uses this application, and opens new screen with empty chat.

Figure 11: New chat Scenario

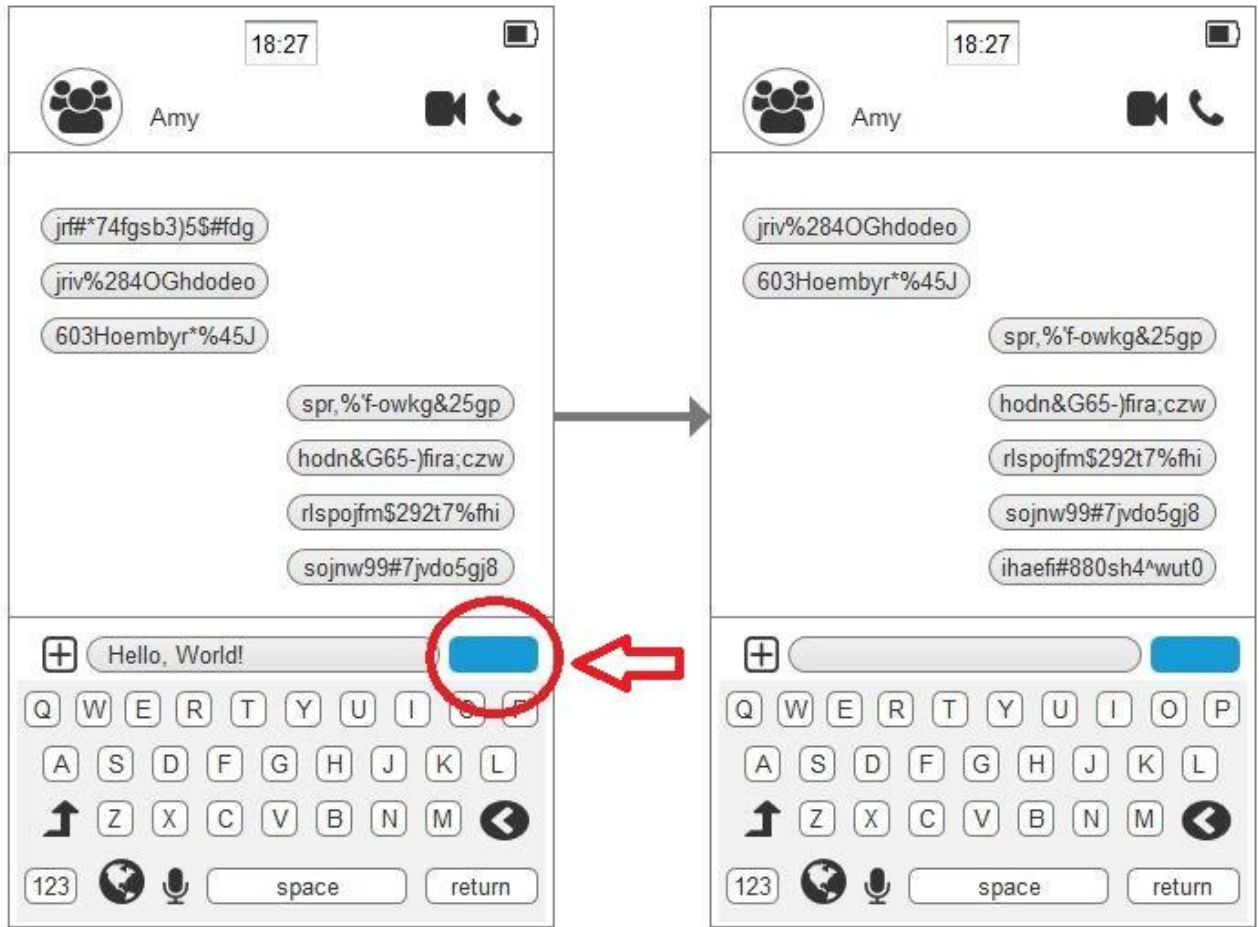


Source: Author

Send encrypted message Scenario

Application allows User to send encrypted messages. As soon as "Send" button pressed, system encrypts the message and sends it to the recipient.

Figure 12: Send encrypted message Scenario

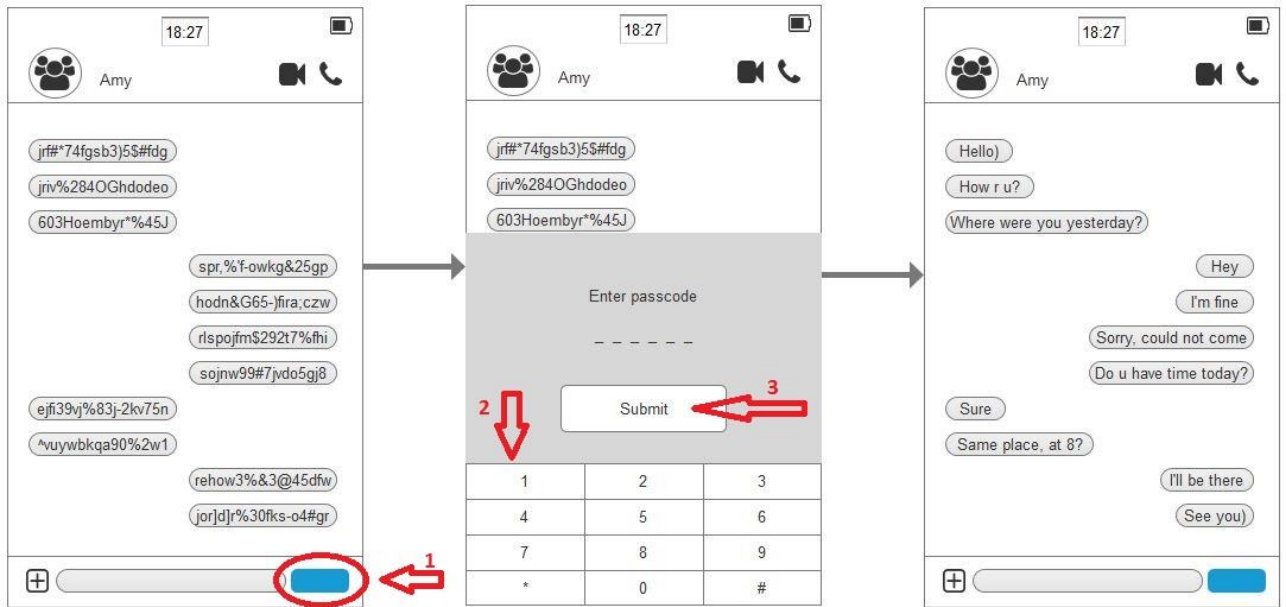


Source: Author

Decrypt chat Scenario

Application allows User to decrypt messages in chat. After the "Decrypt" button is pressed, system asks for the passcode, set by the User. As soon as the correct passcode received, application decrypts messages, which stay visually decrypted until the application runs.

Figure 13: Decrypt chat Scenario

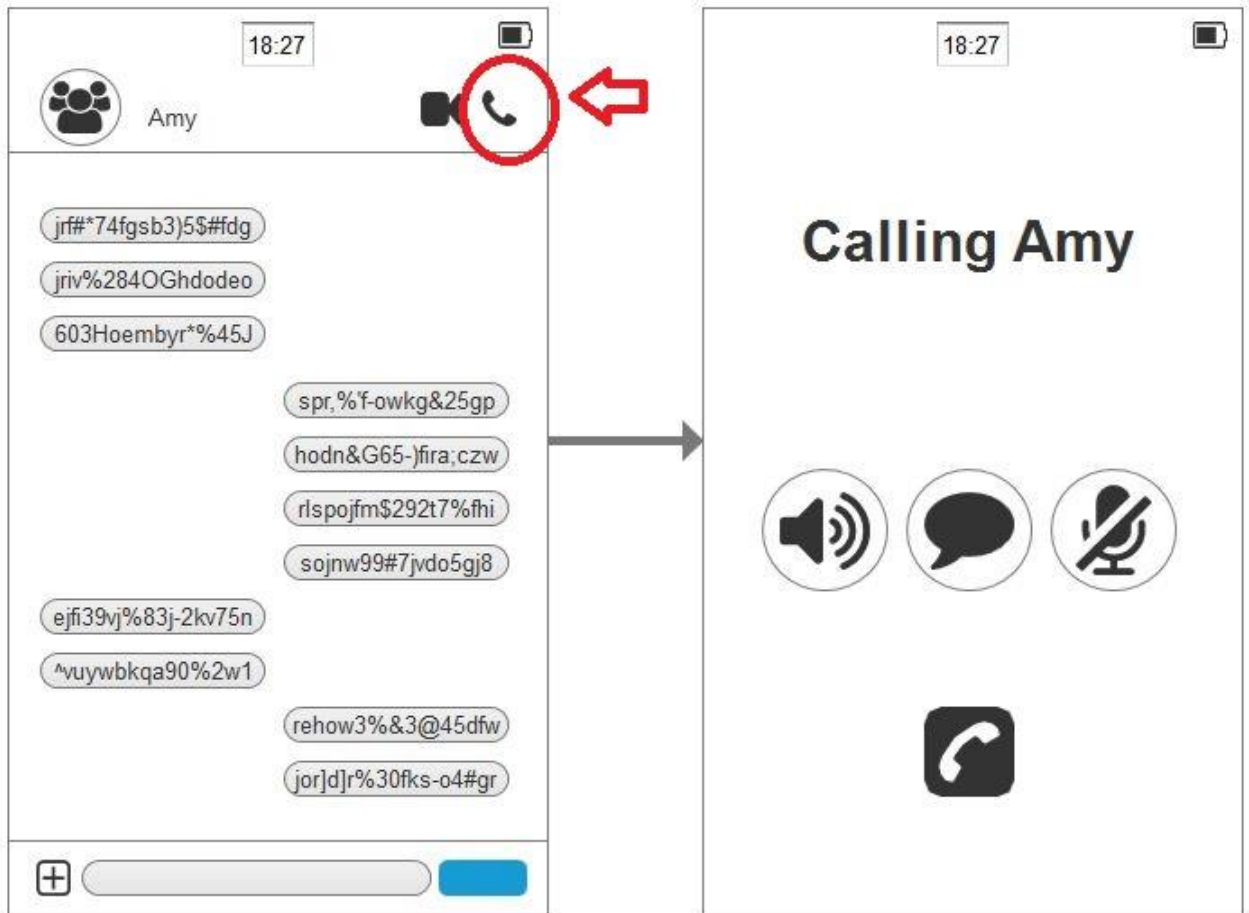


Source: Author

Make voice call Scenario

Application allows User to make free voice calls to the other User inside the application. The recipient will receive the call to his/her device with the note that call is made from the app.

Figure 14: Make voice call Scenario

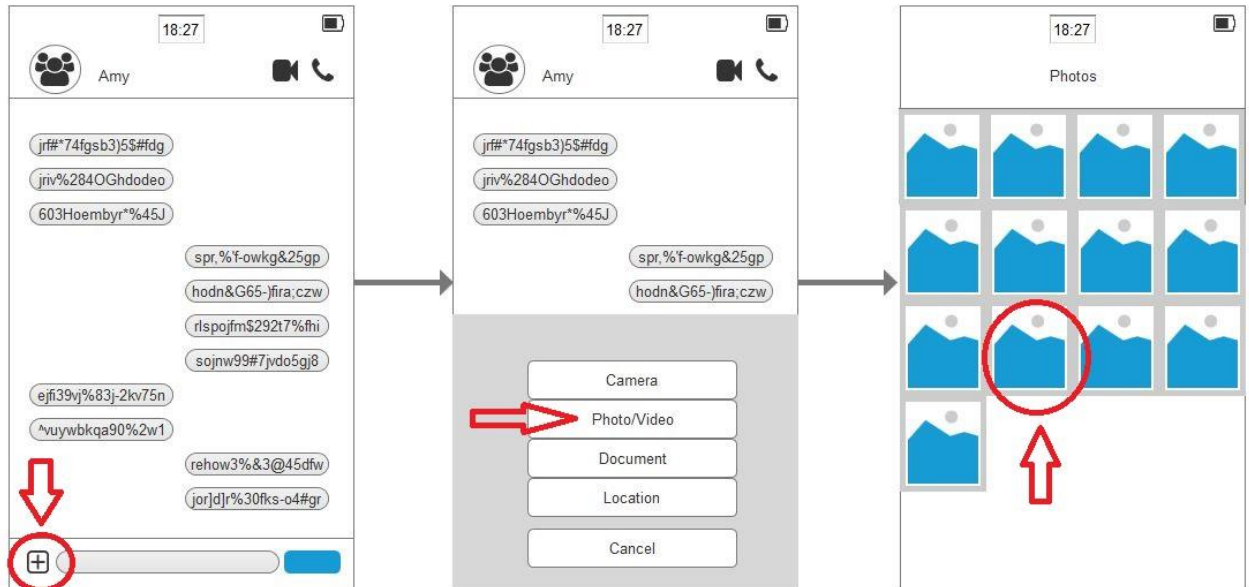


Source: Author

Send photo Scenario

Application allows User to attach photo to the message or send photo itself. Photo can be from the photo album of the device or taken in that moment. System also asks for the permission to use photo album or camera.

Figure 15: Send photo Scenario



Source: Author

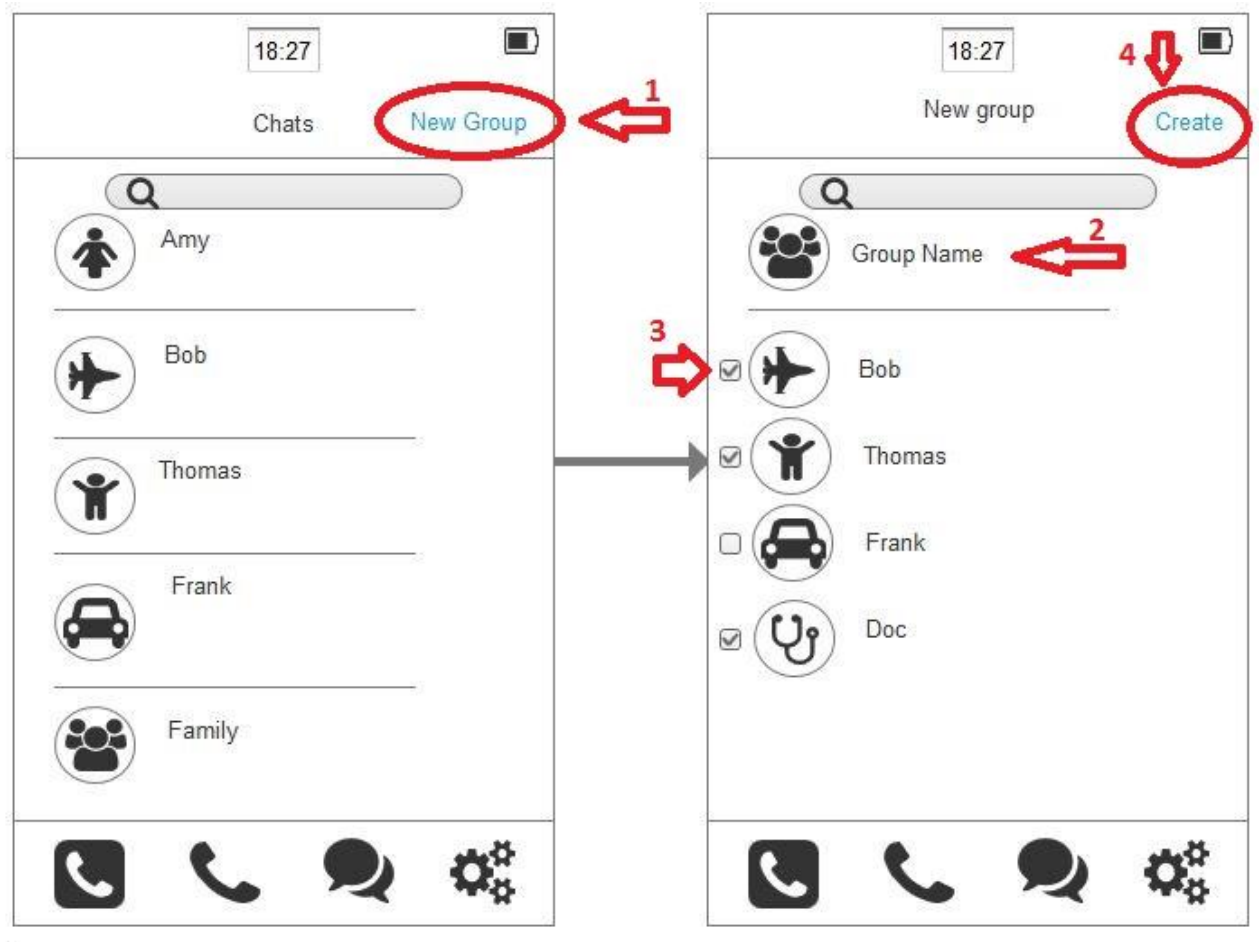
5.5.4 Group chat use case

User expects to have possibility to create group chats, in order to communicate with several persons in one chat, make groups by interest, business, family or other reasons.

Create group chat Scenario

Application allows User to create group chat of maximum 20 members. System offers list of contacts from which members of chat can be selected. Also there is a possibility to name the chat and select picture of a chat.

Figure 16: Create group chat Scenario

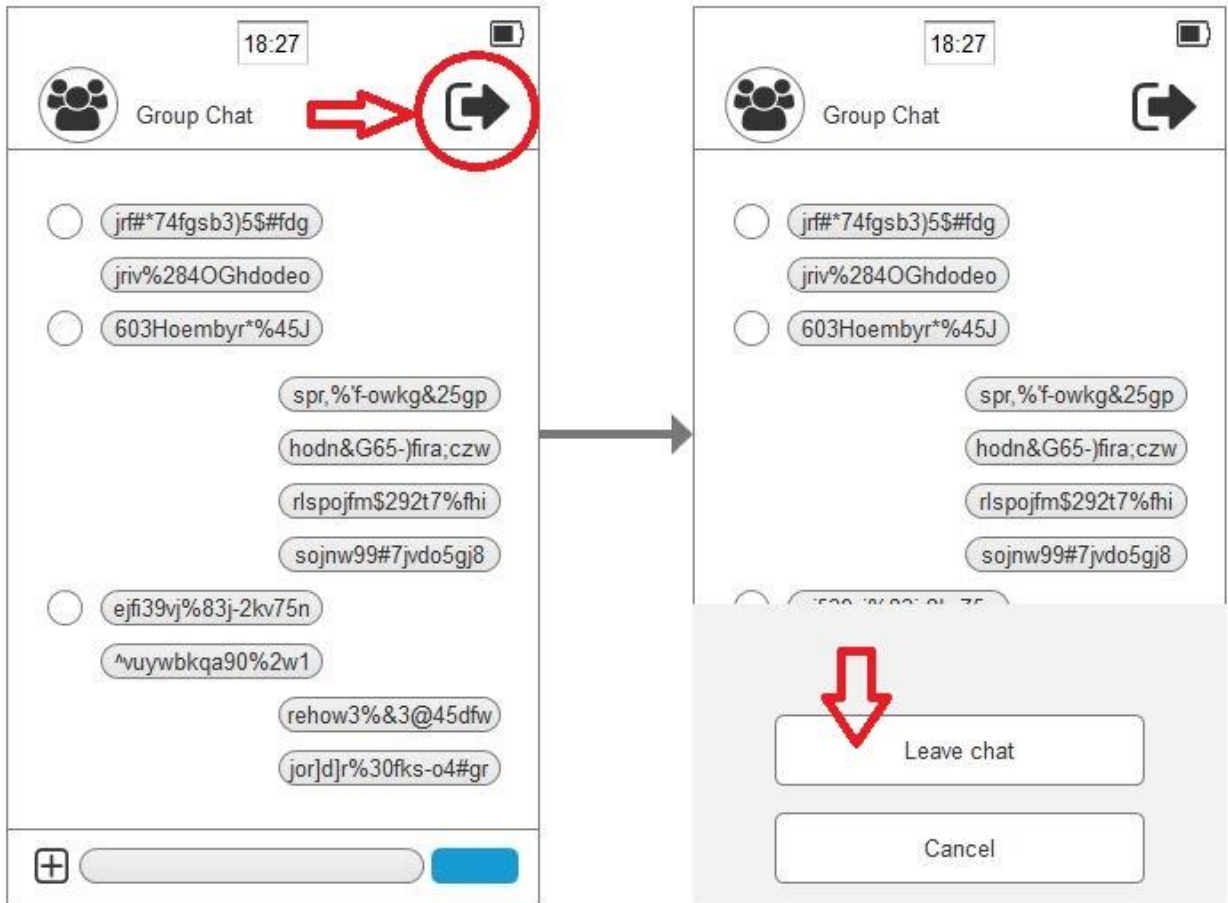


Source: Author

Leave group chat Scenario

Application allows User to leave group chat in any moment. The chat will be removed from the chat list, when User left it.

Figure 17: Leave group chat Scenario



Source: Author

6. Test in Usability Study

After the discussion with my supervisor it was decided to use electronic clickable prototype in usability testing instead of paper prototype. This prototype was developed by myself in Axure RP a software for creating prototypes, layouts, website specifications and applications.

Usability heuristic testing took place in the Usability Lab of Faculty of Economics and Management CULS in Prague by the group of 5 testers. Due to the Jacob Nielsen's research in the field of Usability Studying, it was settled to run several small tests in group of 5 Users.³⁶

At the discussion with testing group I was able to identify several main likes. First of all, testing group was pleasantly surprised about encryption function, how it was applied and they confirmed that there was no chance to identify the content of correspondence before the decryption. Secondly, testing group mentioned the clearness and simplicity of the interface. As regular Users they also identified rather big size of buttons, which is very convenient while using mobile application. As well testing group marked their satisfaction with the expected functionality of this application, such as sending photos, making calls, changing profile photo etc.

The main difficulties were with identifying the purpose of two icons with handset: the phonebook and last calls. So this made me think of signing the names of main buttons. Also one of the testers considered to be better to make some profile logo on the top of the pages to help user identify that he/she is currently logged in. This statement can be argued as if user registers once he/she cannot log out, but can only delete the current account and then create a new one.

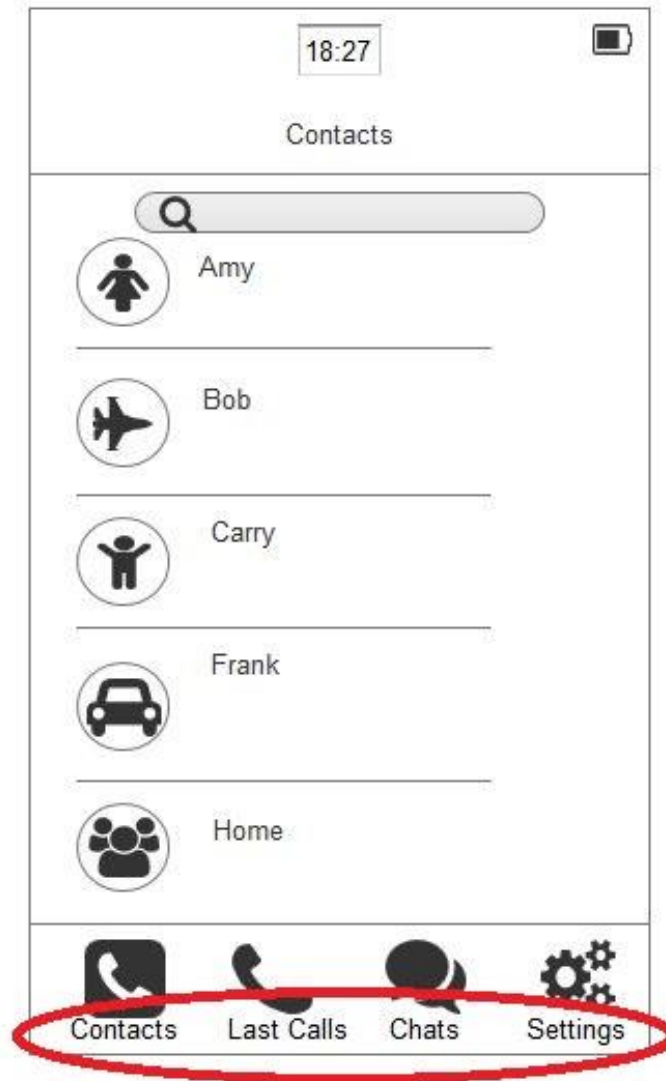
To sum up the testing, there were identified many positive aspects, however there was decided to add button names for more comfortable using.

³⁶ Why You Only Need to Test with 5 Users. *Nielsen Norman Group* [online]. [cit. 2017-02-22]. Available from: <https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/>

7. Changes in UI Specification

Basing on the reviews of the testing group, there was decided to make changes in UI design.

Figure 18: Changes in User Interface



8. Conclusion

To sum up, it should be said that those aims which were set are fully fulfilled. The User Interface for the mobile application supporting encrypted communication was created and has been tested under suitable conditions in laboratory specifically designed for this kind of testing.

This Interface satisfies the requirements described above: User is able to send and receive encrypted messages, decrypt these messages by pressing button and entering passcode, as well as availability of basic instant messaging application functions.

During the research the current state of messaging applications on the market has been observed and it can be said with confidence that instant messaging apps will become dominant platform to create a new computing interface that will change how people interact with each other. And as these applications deeply permeates into humans lives, the level of protecting personal data stored in applications should grow.

After the carried research, now it is possible to predict the future of the idea of developing instant messaging application supporting encrypted communication.

9. Bibliography

1. How Instant Messaging Works. How Stuff Works [online]. [cit. 2016-06-14]. Available from: <http://computer.howstuffworks.com/e-mail-messaging/instant-messaging.htm>
2. The History of Messengers: The First Wave. Groverty Inc. [online]. [cit. 2016-06-14]. Available from: <https://groverty.com/the-history-of-messengers-the-first-wave>
3. The history of the instant messengers, from IRC to Pidgin. Eioba [online]. [cit. 2016-06-14]. Available from: <http://www.eioba.com/a/119m/the-story-and-the-protocols-behind-instant-messengers>
4. MailOnline [online]. [cit. 2016-06-18]. Available from: <http://www.dailymail.co.uk/news/article-2563513/From-food-stamps-billionaire-How-WhatsApp-founder-went-struggling-immigrant-founder-19bn-messaging-service.html>
5. WhatsApp: The inside story. Wired [online]. [cit. 2016-06-18]. Available from: <http://www.wired.co.uk/article/whatsapp-exclusive>
6. WhatsApp is the most popular chat app in more than half the world. Business Insider [online]. [cit. 2016-06-18]. Available from: <http://www.businessinsider.com/whatsapp-is-the-most-popular-chat-app-in-more-than-half-the-world-2016-5>
7. The State of Social Media and Messaging in Asia: How Brands Use Messaging Apps to Engage Users. Nexmo [online]. [cit. 2016-06-20]. Available from: <https://www.nexmo.com/blog/2016/03/15/state-of-social-media-and-messaging-in-asia/>
8. WhatsApp features. WhatsApp [online]. [cit. 2016-06-20]. Available from: <https://www.whatsapp.com/features/>
9. Messaging app Viber names Boston its US headquarters. BetaBoston [online]. [cit. 2016-06-25]. Available from: <http://www.betaboston.com/news/2015/10/16/messaging-app-viber-names-boston-its-us-headquarters/>
10. Everything you need to know about Skype. Softonic [online]. [cit. 2016-06-28]. Available from: <https://features.en.softonic.com/everything-you-need-to-know-about-skype>

11. Line: Free Calls & Messages [online]. [cit. 2016-06-28]. Available from:
<https://line.me/en/>
12. WeChat Help Center [online]. [cit. 2016-06-28]. Available from:
http://help.wechat.com/cgi-bin/newreadtemplate?t=help_center/topic_list&plat=android&lang=en&Channel=helpcenter&detail=100359
13. WhatsApp rival Viber launches branded accounts for companies and public figures. Geektime [online]. [cit. 2016-07-05]. Available from:
<http://www.geektime.com/2016/11/09/whatsapp-rival-viber-launches-branded-accounts-for-companies-and-public-figures/>
14. What does security mean? [online]. [cit. 2016-07-09]. Available from:
<http://ccss.usc.edu/499/lecture1.html>
15. What are the Different Techniques of Encryption? Buzzle [online]. [cit. 2016-09-03]. Available from: <http://www.buzzle.com/articles/what-are-the-different-techniques-of-encryption.html>
16. Understanding the 3 Main Types of Encryption. Atomic Object [online]. [cit. 2016-09-03]. Available from: <https://spin.atomicobject.com/2014/11/20/encryption-symmetric-asymmetric-hashing/>
17. Data Encryption Standard (DES) [online]. [cit. 2016-09-15]. Available from:
<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>
18. How long does it take to crack DES and AES? Gryptography [online]. [cit. 2016-09-15]. Available from: <http://crypto.stackexchange.com/questions/752/how-long-does-it-take-to-crack-des-and-aes>
19. Is DES or 3DES still being used today? Stack Overflow [online]. [cit. 2016-09-18]. Available from: <http://stackoverflow.com/questions/1619212/is-des-or-3des-still-being-used-today>
20. Advanced Encryption Standard (AES). TechTarget [online]. [cit. 2016-09-20]. Available

- from: <http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>
21. The Differences Between Rijndael and AES. Microsoft Developer [online]. [cit. 2016-09-20]. Available from: <https://blogs.msdn.microsoft.com/shawnfa/2006/10/09/the-differences-between-rijndael-and-aes/>
 22. How secure is AES against brute force attacks? EE Times [online]. [cit. 2016-09-20]. Available from: http://www.eetimes.com/document.asp?doc_id=1279619
 23. WHAT IS DIFFIE-HELLMAN? DELL EMC [online]. [cit. 2016-10-04]. Available from: <http://www.centera.bz/emc-plus/rsa-labs/standards-initiatives/what-is-diffie-hellman.htm>
 24. ¹ «Diffie-Hellman Key Exchange» in plain English. StackExchange [online]. [cit. 2016-10-05]. Available from: <https://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english>
 25. Diffie-Hellman key exchange (exponential key exchange). TechTarget [online]. [cit. 2016-10-05]. Available from: <http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange>
 26. RSA algorithm (Rivest-Shamir-Adleman). TechTarget [online]. [cit. 2016-10-05]. Available from: <http://searchsecurity.techtarget.com/definition/RSA>
 27. RSA Algorithm [online]. [cit. 2016-10-07]. Available from: http://www.dimgt.com.au/rsa_alg.html
 28. Secure Hashing Algorithms. Brilliant [online]. [cit. 2016-10-17]. Available from: <https://brilliant.org/wiki/secure-hashing-algorithms/>
 29. How Hash Algorithms Work [online]. [cit. 2016-10-19]. Available from: <http://www.metamorphosite.com/one-way-hash-encryption-sha1-data-software>
 30. Message Digest 5 (MD5). Techopedia [online]. [cit. 2016-10-22]. Available from: <https://www.techopedia.com/definition/31700/message-digest-5-md5>
 31. The MD5 cryptographic hash function. Ius Mentis [online]. [cit. 2016-10-22]. Available from: <http://www.iusmentis.com/technology/hashfunctions/md5/>

32. Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms [online]. [cit. 2016-10-23]. Available from: <https://tools.ietf.org/html/rfc6151>
33. Digital Envelope. Techopedia [online]. [cit. 2016-11-02]. Available from: <https://www.techopedia.com/definition/18859/digital-envelope>
34. Multiple encryption. A Few Thoughts on Cryptographic Engineering [online]. [cit. 2016-11-03]. Available from: <https://blog.cryptographyengineering.com/2012/02/02/multiple-encryption/>
35. End-to-end encryption (E2EE). TechTarget [online]. [cit. 2016-11-08]. Available from: <http://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE>
36. Why You Only Need to Test with 5 Users. *Nielsen Norman Group* [online]. [cit. 2017-02-22]. Available from: <https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/>

List of Figures

Figure 1: Development of messengers timescale	14
Figure 2: Most downloaded instant messaging apps	18
Figure 3: Data stored in instant messages apps	20
Figure 4: DES algorithm	23
Figure 5: AES algorithm	25
Figure 6: MD5 algorithm	30
Figure 7: Log in Scenario	38
Figure 8: Synchronization of contacts Scenario	39
Figure 9: Set passcode Scenario	40
Figure 10: Change profile photo Scenario	41
Figure 11: New chat Scenario	42
Figure 12: Send encrypted message Scenario	43
Figure 13: Decrypt chat Scenario	44
Figure 14: Make voice call Scenario	45
Figure 15: Send photo Scenario	46
Figure 16: Create group chat Scenario	47
Figure 17: Leave group chat Scenario	48
Figure 18: Changes in User Interface	50

List of Tables

Table 1: SWOT analysis	33
-------------------------------------	----