

WROCLAW UNIVERSITY OF SCIENCE AND TECHNOLOGY  
FACULTY OF FUNDAMENTAL PROBLEMS OF TECHNOLOGY

## CRYPTOGRAPHY PROJECT

### TINDERELLA

#### AUTHORS

GRZEGORZ ZABOROWSKI 236447, MIKOŁAJ GRZEGRZÓŁKA 241073,  
PAULINA JAŁOSIŃSKA 232892

WROCLAW 2021

# Contents

<b>1</b>	<b>Crucial Information about the project</b>	<b>2</b>
1.1	General Information . . . . .	2
1.1.1	Used technology . . . . .	2
1.1.2	Firebase . . . . .	2
<b>2</b>	<b>Main goals</b>	<b>4</b>
<b>3</b>	<b>Technicals and instructions</b>	<b>5</b>
3.1	Classes . . . . .	5
3.1.1	SplashScreen Class . . . . .	5
3.1.2	MainActivity Class . . . . .	5
3.1.3	Login and Login_Register_Class Classes . . . . .	5
3.1.4	SettingsActivity Class . . . . .	5
3.1.5	Chat class . . . . .	5
<b>4</b>	<b>Summary and future development</b>	<b>11</b>
4.1	Summary . . . . .	11

# Chapter 1

## Crucial Information about the project

### 1.1 General Information

#### 1.1.1 Used technology

The Tinderella application layout was created with usage of the Android Studio Layout Editor that enables you to quickly build layouts by dragging UI elements into a visual design editor instead of writing layout XML by hand. The design editor can preview your layout on different Android devices and versions, and you can dynamically resize the layout to be sure it works well on different screen sizes.

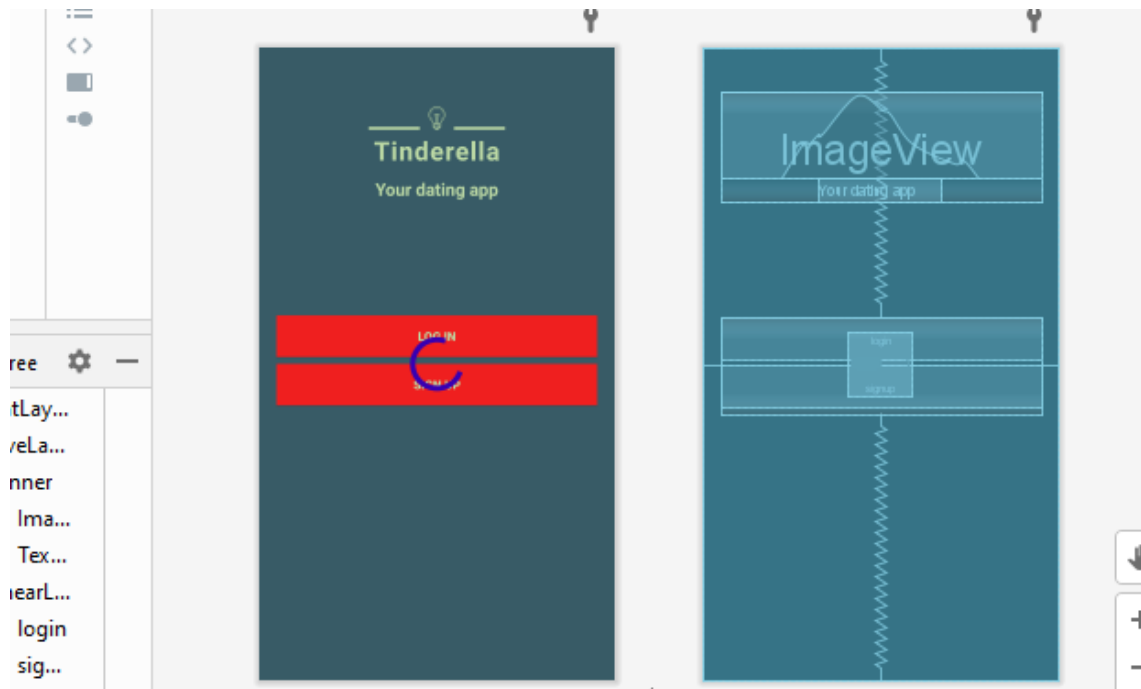


Figure 1.1: Application layout creation

#### 1.1.2 Firebase

Firebase is a platform developed by Google for creating mobile and web applications. It is a tool that offers a number of services related to application programming, their analysis, quality and stability monitoring and the

achievement of specific business goals. In the project, we use three modules available in Firebase: Authentication, Realtime Database, Storage. Storage serves as storage for media (photos), while Realtime Database is used to store user data such as chat messages, record of the protocol performed, etc.

## Chapter 2

# Main goals

The basic assumptions of the implemented project was to create a mobile application as a clone of the popular Tinder application. The basic assumption was the implementation of an appropriate protocol between the two users  $P_i$  and  $P_2$ , with input values  $x_i$  and  $x_2$ . As a calculation of the  $F_i$  protocol  $(x_i, x_2) = F_2(x_1, x_2) = b$ , assuming that  $b = x_1 \wedge x_2$ . The visual layer of the application was to reflect the basic functionalities present in Tinder as much as possible and thus allow for a protocol-protected chat between selected couples in terms of their matches.

### Base of the application

The base form of the application presents the basic functionalities in the field of registration, supplemented with standard verification methods. Consecutive personalization of the account, along with the characteristics of the potential services of the platforms used, the same as in the original Tinder. After that, the selection service in the field of standard selection of people in accordance with the assumptions of the user, to the chat secured by a Yao's garbled circuit protocol for matching appropriate people. In addition, there are aesthetic and advertising issues that complement the entire application

### Yao protocol

In a standard two-party computation, we deal with two parties, each of which has input values  $x$  and  $y$ , and their standard assumption is to calculate the functionality of  $F(x, y) = (F_1(x, y), F_2(x, y))$ , assuming the first party gets  $F_1(x, y)$  and the second gets  $F_2(x, y)$ . The presented functionality may be probabilistic, in which  $F(x, y)$  is a random generated variable. By default, assuming that nothing is obtained in the security protocol except the value of the output, assuming that the output is distributed in accordance with the presented functionality. In the case of the functionality of the Yao protocol, assume that  $F$  is a functionality with a given polynomial-time, and that the values of  $x$  and  $y$  are the input values for parties, respectively. The first step is to set up the  $F$  functionality as a boolean circuit  $C$ . The detailed description of how such a circuit is computed is helpful in the general principle of operation of the Yao protocol. So we know that  $x$  and  $y$  are the input values of parties, then circuit  $C(x, y)$  is computed gate-by-gate, sequentially from the input wires to the output wires. When the incoming wires to gate  $G$  receive successively the values of  $\alpha, \beta \in \{0, 1\}$ , we obtain the possibility of giving the following wires coming out of gate the values  $G(\alpha, \beta)$ . The output value of such a circuit is obtained from the input values of the circuit wires.

## Chapter 3

# Technicals and instructions

The application was created and teasted on the Pixel 3a emulator available from Android Studio and the Xiaomi Mi 10 lite Model: M2002J9G smartphone using the Android system.

### 3.1 Classes

#### 3.1.1 SplashScreen Class

In the SplashScreen class, the Tinderella startup screen is initiated in the onCreate function.

#### 3.1.2 MainActivity Class

In the MainActivity class authorization is checked. Also Cards i.e. objects contaning informations about proposed users, the LikeBtn and DislikeBtn buttons are displayed. Clicking one of these buttons will execute the corresponding classes. At the top of the display there are buttons that lead to SettingsActivity or ChatActivity. At the top of the display there are buttons that lead to SettingActivity or Chat(activity).

#### 3.1.3 Login and Login\_Register\_Class Classes

These classes initialize activities that allow to user to log in to the application or register account if the account is not already created. Confirmation of the email address is necessarily. There is also a possibility of logging out.

#### 3.1.4 SettingsActivity Class

These class initialize activity responsible for putting basic information about a user to the application. There is also possibility of choosing profile photo from the gallery.

#### 3.1.5 Chat class

These class initialize Chat layout that makes a possible to chat with matched users.

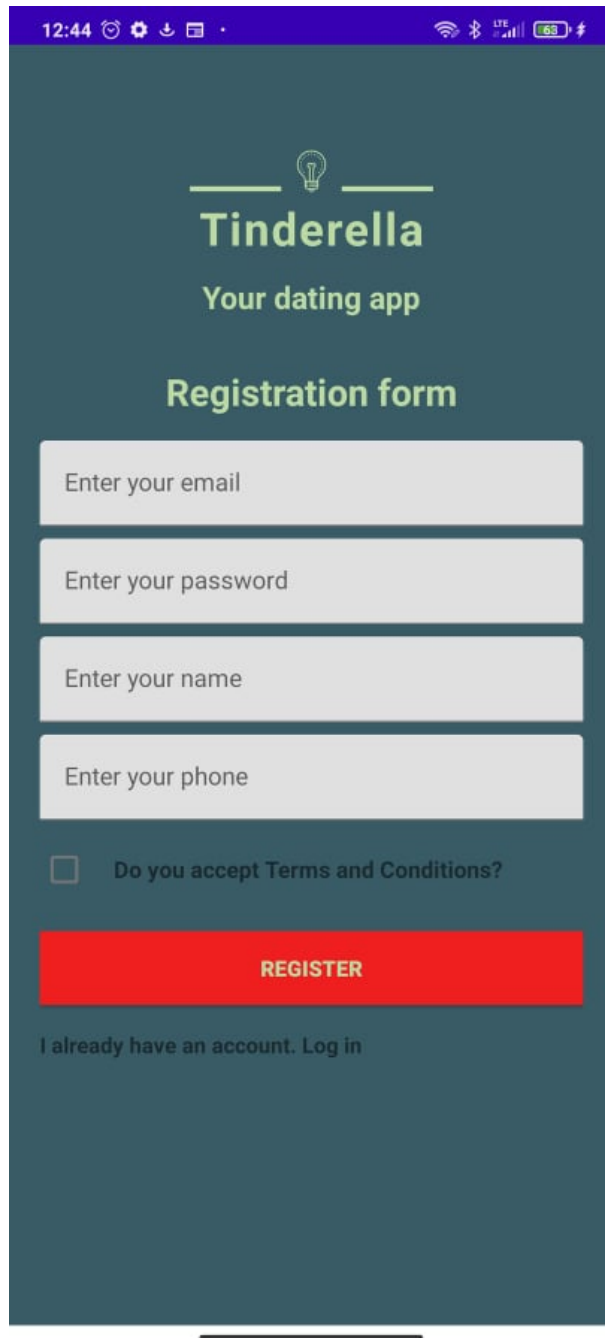


Figure 3.1: Splash screen



Figure 3.2: Card and buttons





The image shows a mobile app registration screen for 'Tinderella'. At the top, there's a status bar with the time 12:44 and various icons. Below it, the app's logo 'Tinderella' is displayed in a light blue font, with a lightbulb icon above it. The tagline 'Your dating app' is centered below the logo. The main heading 'Registration form' is in a bold, light blue font. The form consists of four light gray input fields stacked vertically, each with a placeholder text: 'Enter your email', 'Enter your password', 'Enter your name', and 'Enter your phone'. Below these fields is a checkbox with the text 'Do you accept Terms and Conditions?'. A prominent red button with the text 'REGISTER' in white is positioned below the checkbox. At the bottom of the form, there is a link that says 'I already have an account. Log in'. The entire form is set against a dark teal background.

12:44

Tinderella

Your dating app

Registration form

Enter your email

Enter your password

Enter your name

Enter your phone

☐ Do you accept Terms and Conditions?

REGISTER

I already have an account. Log in

Figure 3.3: Register layout

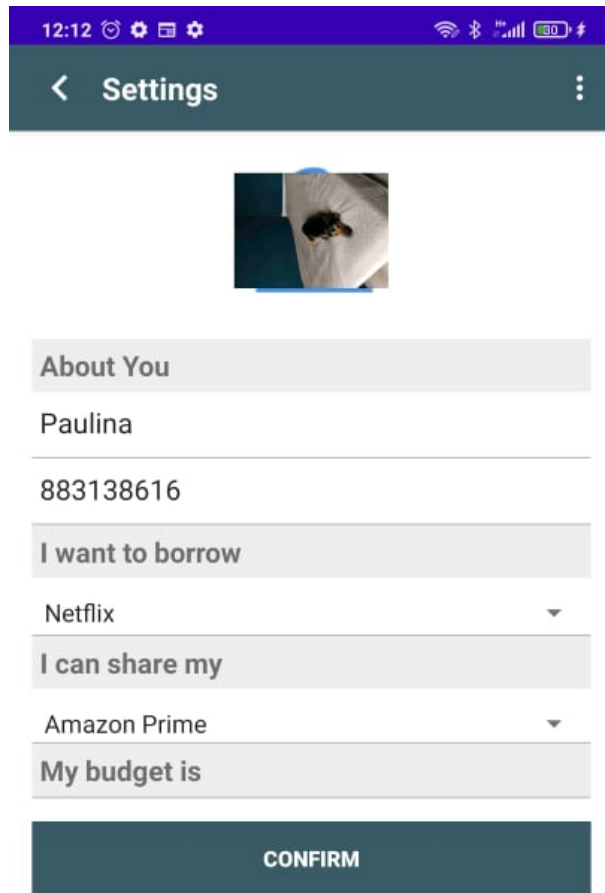


Figure 3.4: Settings layout



Figure 3.5: Chat layout

## Chapter 4

# Summary and future development

### 4.1 Summary

The Cinderella application has been fully designed, implemented, installed on the device and tested. All elements of the application are working properly. There are many possibilities to develop this application like improving the security of typing and keeping passwords, making matching algorithms better, giving a possibility to add more photos or to use some safer and more professional database storage systems than Firebase Realtime Database (Firebase has been claimed to be used by Google to track users without their knowledge).