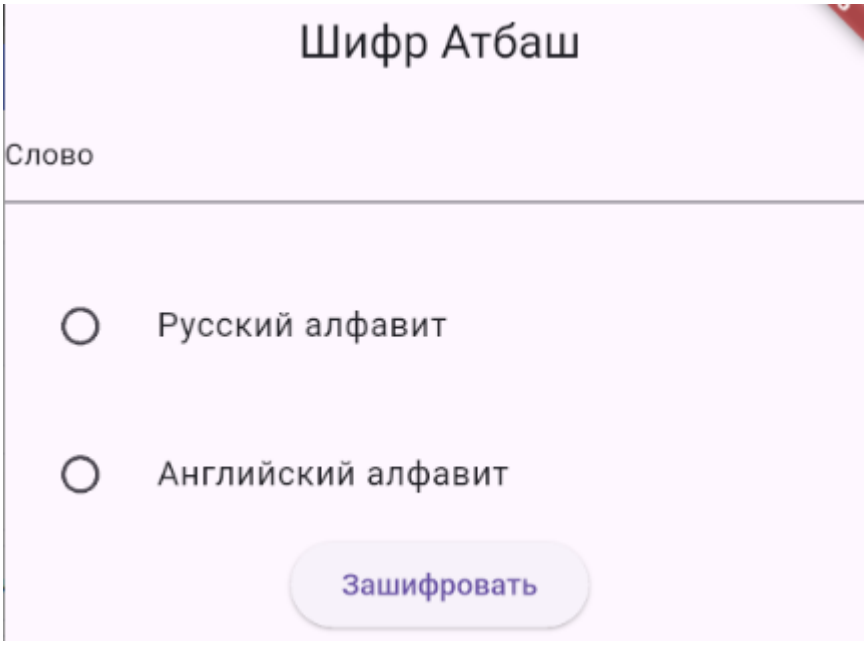
Лабораторная работа №1. Шифр Атбаш.

Суть алгоритма очень проста - первая буква алфавита заменяется на последнюю букву алфавита, вторая – на предпоследнюю и так далее.

Реализовать алгоритм, создав мобильное приложение. В качестве элементов пользовательского интерфейса использовать стандартные виджеты Flutter. Возможно разместить поле ввода текста для шифрования, радиокнопки для выбора алфавита (русский, английский), кнопку для выполнения функции шифрования, а также поле вывода результата.

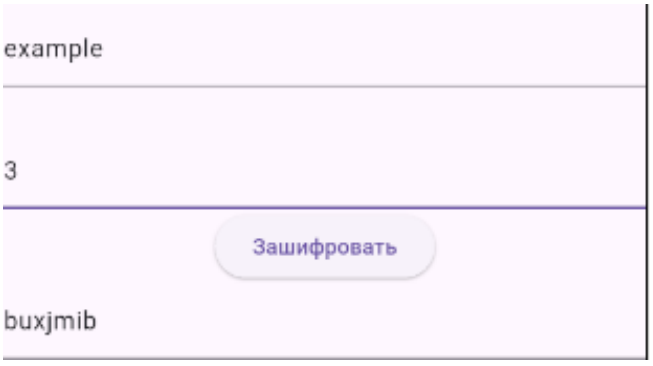


Лабораторная работа №2: Шифр Цезаря

Реализовать приложение для зашифровки-дешифровки текста шифром Цезаря.

Схема работы следующая: каждая буква слова изменяется в зависимости от сдвига. Например, если указать сдвиг 3, буква А изменится на Г, И – на Л и так далее.

На макете разместить текстовые поля для ввода слова и сдвига, а также кнопки для выполнения действий. Результат можно выводить в третье текстовое поле, либо в виджет типа Text. Выполнять шифрование для двух алфавитов – русского, английского. Реализовать алгоритм дешифровки.



Лабораторная работа №3. OAuth 2.0. Интеграция авторизации с помощью сторонних сервисов.

Внедрить в приложение авторизацию с помощью стороннего сервиса. Разрешается использовать любой отечественный сервис (ВК, Яндекс и т. д). **Создание учётных записей** через Google и сторонние зарубежные сервисы запрещено согласно № 406-ФЗ.

http://publication.pravo.gov.ru/document/0001202307310022?index=1

Лабораторная работа №4: Аутентификация пользователя

Реализовать защиту критически важных разделов приложения (например, экран профиля пользователя) с помощью биометрии или код-пароля. При попытке доступа к защищенному разделу приложения программа должна попросить пользователя подтвердить личность (например, с помощью отпечатка пальца).

Разрешается использовать соответствующие библиотеки (найти их можно в pub.dev). Проверить работу приложения на устройстве.

Лабораторная работа №5. Создание интерфейса авторизации-регистрации пользователя.

Создать интерфейс мобильного приложения. На главном экране возможно спрашивать у пользователя, в какой раздел он собирается попасть – авторизации или регистрации. Экраны должны быть реализованы отдельно.

В процессе регистрации уделять внимание полям с паролем – основному полю, а также полю для подтверждения пароля. Добавить надписи (hint) каждому полю. Скрывать чувствительную информацию при вводе (например, закрывать пароль символами *****).

Реализовать обработку исключительных ситуаций:

- Проверять, что при регистрации пользователь использует пароль не менее 8 символов, как минимум 1 спецсимвол и 1 цифру;
- все поля в процессе регистрации пользователем были заполнены;
- пароли в двух (пароль, подтверждение пароля) полях совпадают.

Использовать регулярные выражения. СТОРОННИЕ БИБЛИОТЕКИ И ПЛАГИНЫ ПРИМЕНЯТЬ ЗАПРЕЩЕНО.

Лабораторная работа №6. Создание безопасной архитектуры хранения паролей. Реализовать регистрацию, авторизацию пользователей, применяя шифрование

паролей с использованием современных алгоритмов (bcrypt, scrypt, argon2). Возможно использовать локальную БД (SQLite, PostgreSQL).

Лабораторная работа №7: Аудит разрешений мобильного приложения

Изучить перечень разрешений, запрашиваемых приложением. Определить необходимость каждого запрашиваемого разрешения. Выявить возможность злоупотребления доступом к чувствительным данным в приложении (местоположение, контакты, микрофон и др.).

Мобильное приложение можно выбрать самостоятельно. Подготовить отчёт по выполненной работе.