**Министерство образования Иркутской области**

Государственное бюджетное профессиональное

образовательное учреждение Иркутской области

«Иркутский авиационный техникум»

(ГБПОУИО «ИАТ»)

|  |  |
| --- | --- |
| КР. 09.02.03.18.16-2.19.ПЗ |  |

Приложение «Шифровка данных»

|  |  |  |
| --- | --- | --- |
| Председатель ВЦК: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, дата) | (М.А. Кудрявцева) |
| Руководитель: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, дата) | (А.С. Некипелова) |
| Студент: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, дата) | (Д.М.Овинов) |

Иркутск 2018

**Содержание**

[**Введение** 3](#_Toc531559357)

[**1** **Общая часть** 4](#_Toc531559358)

[**1.1** **Обзор программного обеспечения для разработки** 4](#_Toc531559359)

[**1.2** **Обоснование необходимости использования выбранных методов** 5](#_Toc531559360)

[**2** **Специальная часть** 6](#_Toc531559361)

[**2.1** **Постановка задач** 6](#_Toc531559362)

[**2.2** **Описание теоретической части** 6](#_Toc531559363)

[**2.3** **Алгоритм работы программы** 10](#_Toc531559364)

[**3** **Технологическая часть** 11](#_Toc531559365)

[**3.1** **Руководство пользователя** 11](#_Toc531559366)

[**3.2** **Системно – технические требования** 12](#_Toc531559367)

[**Заключение** 13](#_Toc531559368)

[**Список используемых источников** 14](#_Toc531559369)

[**Приложение** А 15](#_Toc531559370)

# **Введение**

В истории было много криптографических приложений, начиная от простых шифров, используемых Юлием Цезарем для отправления военных приказов своим генералам, до более сложных средневековых шифров, и знаменитых кодов Энигма во Второй Мировой войне.

Развитие компьютеров в 20-м веке позволило создать более сложные средства шифрования.

Цель курсовой работы заключается в разработке мобильного приложения, для шифрования данных. Задачи, направленные на достижение цели:

1. Изучение теории криптографии;
2. Выбор используемых шифров;
3. Разработка алгоритмов выбранных шифров;
4. Разработка дизайна (интерфейса) приложения;
5. Разработка основной логики приложения;
6. Отладка приложения;

# **Общая часть**

# **Обзор программного обеспечения для разработки**

Android Studio — интегрированная среда разработки производства Google, с помощью которой разработчикам становятся доступны инструменты для создания приложений на платформе Android OS. Android Studio можно установить на Windows, Mac и Linux. Создана на базе IntelliJ IDEA.

Среда Android Studio предназначена как для небольших команд [разработчиков мобильных приложений](http://wnfx.ru/) (даже в количестве одного человека), или же крупных международных организаций с GIT или другими подобными системами управления версиями. Опытные разработчики смогут выбрать инструменты, которые больше подходят для масштабных проектов. [Решения для Android](http://wnfx.ru/android-razrabotka-mobilnyih-prilozheniy/) разрабатываются в Android Studio с использованием Java или C++. В основе рабочего процесса Android Studio заложен концепт непрерывной интеграции, позволяющий сразу же обнаруживать имеющиеся проблемы. Продолжительная проверка кода обеспечивает возможность эффективной обратной связи с разработчиками. Такая опция позволяет быстрее опубликовать версию мобильного приложения в Google Play App Store. Для этого присутствует также поддержка инструментов LINT, Pro-Guard и App Signing.

С помощью средств оценки производительности определяется состояние файла с пакетом прикладных программ. Визуализация графики дает возможность узнать, соответствует ли приложение ориентиру Google в 16 миллисекунд. С помощью инструмента для визуализации памяти разработчик узнает, когда его приложение будет использовать слишком много оперативной памяти и когда произойдет «сборка мусора». Инструменты для анализа батареи показывают, какая нагрузка приходится на устройство.

Разработчики приложений для Android предпочитают именно эту программу. Согласно отзывам, которые оставляют пользователи IDE, софт дает больше возможностей, предоставляет более гибкую среду разработки, нежели конкуренты. О чем только говорит наличие такого многофункционального эмулятора и еще нескольких инструментов, которые включены в пакет Android Studio! Видно, что с каждым обновлением IDE становится только лучше, в него интегрируют новый функционал, не забывая про старый.

# **Обоснование необходимости использования выбранных методов**

Разработка приложения с помощью среды разработки Android studio и языка программирования Java обоснуется следующими причинами:

* Н­­­­е малые теоретические и практические знания языка Java;
* Имеющийся опыт работы в Android studio;
* Большое количество функциональных интегрированных в среду инструментов;

# **Специальная часть**

# **Постановка задач**

Приложение должно шифровать введенные данные по одному из выбранных шифров. После ввода информации, указания пароля и по желанию выбора дополнительных параметров, приложение должно будет зашифровать её.

# **Описание теоретической части**

Блочный шифр (block cipher) — это функция шифрования, которая применяется к блокам текста фиксированной длины. Текущее поколение блочных шифров работает с блоками текста длиной 128 бит (16 байт). Такой шифр принимает на вход 128-битовый открытый текст и выдает 128-битовый шифрованный текст. Блочный шифр является обратимым: существует функция дешифрования, которая принимает на вход 128-битовый шифрованный текст и выдает исходный 128-битовый открытый текст. Открытый и шифрованный текст всегда имеет один и тот же размер, который называется размером блока (block size).

Чтобы зашифровать сообщение, нужен секретный ключ. Невозможно скрыть сообщение, не сохраняя что-нибудь в секрете. Подобно открытому и шифрованному тексту, ключ шифрования также представляет собой строку битов. Наиболее распространены ключи размером 128 и 256 бит. Шифрование открытого текста p при помощи ключа K принято обозначать как E(K, p) или EK(p), а расшифровку шифрованного текста c при помощи ключа K — D(K, c) или DK(c).

Иногда блочный шифр было бы удобно представить в виде большой таблицы, построенной на основе конкретного ключа. Для каждого фиксированного ключа можно построить таблицу соответствий, которая бы отображала все варианты открытого текста в соответствующий шифрованный текст. Разумеется, это была бы очень большая таблица. Для блочного шифра с размером блока 32 бит понадобилась бы таблица размером 16 Гбайт, для шифра с размером блока 64 бит — 150 млн. Тбайт, а для шифра с размером блока 128 бит — 5·1039 байт. В таблице содержится ровно по одному экземпляру всех возможных вариантов шифрованного текста. Набор элементов шифрованного текста совпадает с набором элементов открытого текста, порядок расположения которых изменен. В математике это называется перестановкой (permutation). Блочный шифр с размером блока k бит задает перестановку k-битовых элементов для каждого из заданных значений ключа.

Блочные шифры применяются только к блокам текста фиксированного размера. Чтобы зашифровать какой-нибудь текст, размер которого не совпадает с размером блока, необходимо воспользоваться одним из режимов работы блочных шифров (block cipher modes).

Наиболее популярным режимом работы блочных шифров является сцепление шифрованных блоков (cipher block chaining — CBC). Каждый блок открытого текста складывается с помощью операции XOR с предыдущим блоком шифрованного текста. Стандартная формулировка режима CBC выглядит следующим образом:

Ci = E(K, Pi ⊕ Ci−1) для i = 1, . . . , k.

(1)

В открытый текст вносится “элемент случайности” путем его прибавления к предыдущему блоку шифрованного текста. В режиме CBC одинаковые блоки открытого текста преобразуются в разные блоки шифрованного текста, что значительно сокращает объем информации об открытом тексте, доступной злоумышленнику.

Следует заметить, что в качестве C0 используется значение, называемое вектором инициализации (initialization vector — IV). Использовать фиксированный вектор инициализации не следует. В противном случае в первом блоке каждого сообщения могут возникнуть проблемы. Если два разных сообщения начинаются с одного и того же блока открытого текста, соответствующие шифрованные сообщения будут начинаться с одинаковых блоков шифрованного текста. На практике сообщения часто начинаются с одинаковых или похожих блоков шифрованного текста, поэтому не стоит помогать злоумышленнику.

AES (Advanced Encryption Standard — улучшенный стандарт шифрования)

Алгоритм AES не относится к шифрам Файстеля. Ниже показан один раунд алгоритма AES (Рисунок 1).

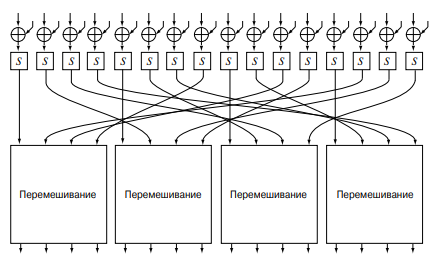


Рисунок 1 – Структура одного раунда AES

Последующие раунды имеют аналогичную структуру. На вход алгоритма подается блок открытого текста длиной 16 байт. Вначале открытый текст складывается с помощью операции XOR с 16-байтовым (128-битовым) подключом. На рисунке этот процесс обозначен операторами ⊕ (каждый байт подключа складывается с соответствующим байтом открытого текста). Затем каждый из 16 байт полученного результата подается на вход таблицы S матриц, которая отображает 8-битовые входные значения в 8-битовые выходные значения. Все S-матрицы одинаковы. Полученные байты переставляются в некотором заданном порядке. И наконец, каждая группа из 4 байт подвергается перемешиванию, которое осуществляется с помощью линейной функции перемешивания. Термин “линейная” означает лишь то, что каждый бит выходных данных функции перемешивания получен в результате применения операции XOR к нескольким входным битам. Применение функции перемешивания завершает раунд. Полный процесс шифрования состоит из 10-14 раундов, в зависимости от размера ключа. Подключи AES, генерируются на основе некоторого ключа шифрования. Для расшифровки текста необходимо использовать обратные S матрицы, да и функция, обратная перемешиванию, существенно отличается от самой функции перемешивания.

В алгоритме AES можно выделить несколько функциональных блоков, каждый из которых имеет свое назначение. Операции XOR складывают значение ключа с данными, S-матрицы обеспечивают нелинейность, а функции перестановки и перемешивания гарантируют наличие диффузии. Шифр AES имеет очень четкую структуру, каждая часть которой выполняет строго определенную задачу.

# **Алгоритм работы программы**

# **Технологическая часть**

# **Руководство пользователя**

# **Системно – технические требования**

Минимальные системные требования устройства:

1. Архитектура на базе операционной системы Android 4.4 “KitKat” и выше;
2. Оперативная память от 512 Мб;
3. 12 Мб свободного пространства;
4. Наличие камеры (Не обязательно);
5. Наличие GPS (Не обязательно);

# 

# **Заключение**

# **Список используемых источников**

# **Приложение** А

**Листинг приложения**

public class MainActivity extends AppCompatActivity implements LinearViewHolder.ActionListener {  
  
 private RecyclerView itemresviews;  
 private ResAdapter linearAdapter;  
  
 @Override  
 protected void onCreate(Bundle savedInstanceState) {  
 super.onCreate(savedInstanceState);  
 setContentView(R.layout.*activity\_main*);  
 Toolbar toolbar = findViewById(R.id.*toolbar*);  
 setSupportActionBar(toolbar);  
  
 SharedPreferences preferences = PreferenceManager.*getDefaultSharedPreferences*(this);  
// MyLocation.SetUpLocationListener(this);  
 String lang = preferences.getString("lang", "default");  
 if (lang.equals("default")) {  
 lang =getResources().getConfiguration().locale.getCountry();}  
 Locale locale = new Locale(lang);  
 Resources res = getResources();  
 DisplayMetrics dm = res.getDisplayMetrics();  
 Configuration conf = res.getConfiguration();  
 conf.locale = locale;  
 res.updateConfiguration(conf, dm);  
 List<EncryptedClass> cryptoList;  
 DataBase database = App.*getInstance*().getDatabase();  
 EncryptedDAO encryptedDAO = database.encryptedDAO();  
 cryptoList = encryptedDAO.getAll();  
 itemresviews = findViewById(R.id.*itemresview*);  
 LinearLayoutManager layoutManager = new LinearLayoutManager(this);  
 itemresviews.setLayoutManager(layoutManager);  
 itemresviews.setItemAnimator(new DefaultItemAnimator());  
 linearAdapter = new ResAdapter();  
 if (cryptoList.size() != 0)  
 linearAdapter.addAll(cryptoList);  
 linearAdapter.addHeader(inflateHeader());  
 linearAdapter.setActionListener(this);  
 itemresviews.setAdapter(linearAdapter);  
 }  
  
 private View inflateHeader() {  
 CardView Header = (CardView) getLayoutInflater().inflate(  
 R.layout.*header*, itemresviews, false);  
 Header.setUseCompatPadding(true);  
 return Header;  
 }  
  
 public void onCipherClick(View view) {  
 Intent intent = null;  
 switch (view.getId()) {  
 case (R.id.*btn\_text*):  
 intent = new Intent(MainActivity.this, MessageActivity.class);  
 break;  
 case (R.id.*btn\_file*):  
 intent = new Intent(MainActivity.this, FileActivity.class);  
 break;  
 case (R.id.*btn\_image*):  
 intent = new Intent(MainActivity.this, ImageActivity.class);  
 break;  
 case (R.id.*btn\_open*):  
 intent = new Intent(MainActivity.this, TestedActivity.class);  
 break;  
 }  
 startActivityForResult(intent, 1);  
 overridePendingTransition(R.anim.*slide\_right*, R.anim.*alpha*);  
 }  
  
  
 @Override  
 public boolean onCreateOptionsMenu(Menu menu) {  
 getMenuInflater().inflate(R.menu.*menu\_main*, menu);  
 return true;  
 }  
  
 @Override  
 public boolean onOptionsItemSelected(MenuItem item) {  
 int id = item.getItemId();  
 if (id == R.id.*action\_settings*) {  
 Intent intent = new Intent(this, SettingsActivity.class);  
 startActivityForResult(intent, 1);  
 overridePendingTransition(R.anim.*slide\_up*, R.anim.*alpha*);  
 return true;  
 }  
  
 return super.onOptionsItemSelected(item);  
 }  
  
 @Override  
 public void OnItemClick(long id) {  
 Intent intent = new Intent(MainActivity.this, ViewItemActivity.class);  
 // intent.putExtra(EncryptedClass.class.getSimpleName(), linearAdapter.getItem(position));  
 intent.putExtra("Position",id);  
 startActivityForResult(intent, 1);  
 overridePendingTransition(R.anim.*slide\_right*, R.anim.*alpha*);  
 }  
}