УДК 004.056.55

КРИПТОГРАФІЧНИ МЕТОДИ:ПЕРЕСТАНОВКИ

Тихомиров Богдан

Науковий керівник: канд. ф.-м. наук, доцент Лисенко І.М.

Ніжинський державний університет імені Миколи Гоголя, Україна

Дана стаття присвячена розробці мобільного програмного забезпечення для пристроїв з операційною системою Android, яке дозволяє шифрувати та розшифровувати повідомлення методом маршрутної перестановки. У статті розглянуто суть методу маршрутної перестановки, наведено приклад шифрування. Розроблений мобільний застосунок, містить коротку теоретичну інформацію про метод маршрутної перестановки та дозволяє зашифрувати та розшифрувати довільне повідомлення, вказавши розмірність таблиці самостійно.

Ключові слова:криптографічні методи, метод маршрутної перестановки, мобільний застосунок.

CRYPTOGRAPHIC METHODS:PERMUTATIONS

Tykhomyrov B.

Scientific supervisor: Candidate of Physical and Mathematical Sciences, I. M. Lysenko

Nizhyn Gogol State University, Ukraine

This article is dedicated to the development of mobile software for devices with the Android operating system. This software allows to encrypt and decrypt messages using the Route Cipher. The method of Route cipher is considered, an example of encryption is given. Developed mobile application, contains brief theoretical information about the Route Cipher and allows you to encrypt and decrypt any message, specifying the dimension of the table yourself.

Keywords: cryptography, the Route Cipher, mobile app.

Постановка проблеми. Безпека інформації є досить актуальною проблемою в наш час. Серед різних методів захисту інформації центральне місце займають криптографічні методи.

Перші шифри з’явилися ще на початку нашої ери. Наприклад, римський імператор Гай Юлій Цезар використовував в своєму листуванні шифр, який згодом було названо його ім’ям. Збільшення об'ємів інформації сприяло швидкому розвитку шифрувальної техніки і її впровадженню замість ручних шифрсистем. З появою ЕОМ змінилися принципи і підходи до шифрування даних, але володіння основними криптографічними методами захисту

інформації дослідження та розуміння принципів історичних шифрів необхідні будь якому фахівцю, що займається створенням систем захисту інформації.

Оскільки дана робота присвячена програмній реалізації криптографічних методів перестановки, було проведено аналіз публікацій з даної теми [1-4]. Встановлено, що широкого застосування отримали методи маршрутної перестановки, які ґрунтуються на записі відкритого тексту (тобто тексту, що потрібно зашифрувати) у прямокутну таблицю певної розмірності по горизонталі зліва на право.

Повідомлення при цьому виписують по вертикалях, починаючи з верхнього правого кута, по черзі зверху вниз.

Наприклад зашифруємо зазначеним вище способом фразу КРИПТОГРАФІЯ, використовуючи прямокутну таблицю розміром 4х3 (див. Табл. 1).

Таблиця 1

Шифрування методом маршрутної перестановки

К	Р	И	П
Р	Г	О	Т
А	Ф	І	Я

Зашифрована фраза виглядає наступним чином:

ПТЯІОИФГРАРК

Мета статті полягає у розробці мобільного застосунку, який реалізує метод маршрутної перестановки

Виклад основного матеріалу (результатів) дослідження. Створений програмний застосунок «Cryptography», дозволяє зашифрувати та розшифрувати повідомлення методом маршрутної перестановки. Це мобільний за стосунок, розроблений засобами Android Studio.

Розглянемо приклад додатку по виконанню маршрутних перестановок

Зайшовши в за стосунок, користувач потрапляє на головну сторінку, де можна переглянути Інформацію про метод та конкретно застосувати метод Маршрутної перестановки (див. Рис. 1).

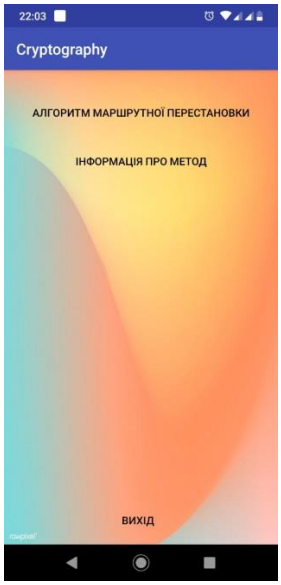

Рис.1 Головна сторінка

Далі представлено частину коду для ініціалізації кнопок головної сторінки:

```
public class MainActivity extends AppCompatActivity {
//метод завантаження активіті
void load(int name)
{
//Ініціалізація повідомлення зміни поточного активіті на активіті алгоритму маршрутної перестановки
Intent PermutationIntent = new Intent(this, Permutation.class);
if (name == 1){
// перехід на активіті алгоритму маршрутної перестановки
startActivity(PermutationIntent);
}
else
// виведення повідомлення у разі невдачі
Toast.makeText(this, "Error: not load activity!", Toast.LENGTH_SHORT).show();
}
// метод закриття додатку
private void closeActivity() {
this.finish();
}
```

```
@Override
protected void onCreate(Bundle savedInstanceState) {
super.onCreate(savedInstanceState);
setContentView(R.layout.activity_main);
// ініціалізація кнопки "Вихід"
final Button exits = (Button) findViewById(R.id.exits);
// ініціалізація кнопки "Алгоритм маршрутної перестановки"
final Button Bpermutation = (Button) findViewById(R.id.Permutation);
// обробка натискання на кнопку "Алгоритм маршрутної перестановки"
Bpermutation.setOnClickListener(new View.OnClickListener() {
@Override
public void onClick(View v) {
load(1);
}
});
// обробка натискання на кнопку "Вихід"
exits.setOnClickListener(new View.OnClickListener() {
@Override
public void onClick(View v) {
// виклик методу закриття додатку
closeActivity();
}
});
}
}
```

Зайшовши на сторінку Алгоритм Маршрутної перестановки користувач побачить Activity подане на рис. 2.

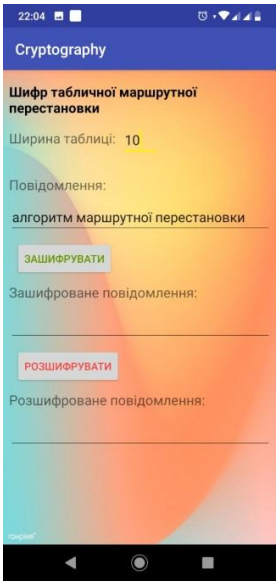

Рис.2 Алгоритм Маршрутної перестановки

Ввівши потрібне повідомлення та ширину таблиці, користувачу потрібно натиснути кнопку «Зашифрувати». Результат з’явиться в полі Зашифроване повідомлення (див. Рис. 3).

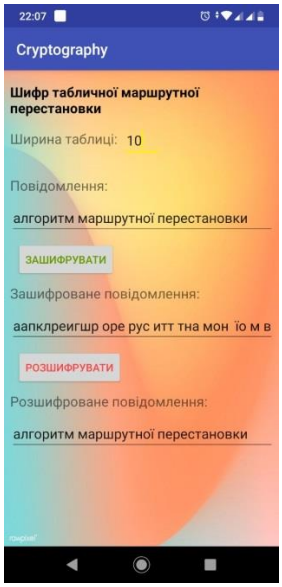

Рис.3 Шифрування та розшифрування повідомлення

Висновки та перспективи подальших пошуків у напрямі дослідження. Отже, у роботі представлено розроблений мобільний за стосунок, який дозволяє зашифровувати та розшифровувати повідомлення. Надалі даний застосунок планується удосконалювати та оновлювати. Зокрема, він буде доповнений й іншими методами перестановок такими як шифр вертикальної перестановки, шифр «поворотна решітка», шифр двійної перестановки.

Список літератури

1. Алферов А. П., А. Ю. Зубов, А. С. Кузьмин, А. В. Черёмушкин. Основы криптографии / Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин А. В. – Гелиос АРВ, 2002.

2. Бабаш А. В., Криптография / Бабаш А. В., Шанкин Г. П. – М. СОЛОН-ПРЕСС, 2007.

3. Риксон Ф. Б. Коды, шифры, сигналы и тайная передача информации / Риксон Ф.Б. – Астрель, 2011.

4. Дориченко С. А. 25 этюдов о шифрах: Популярно о современной криптографии / Дориченко С. А., Ященко В. – Теис, 1994.