сится к проекту. Так же указывается лидер проекта. Лидером может выступать любой активированный пользователь.

После тогда как в системе появились проекты, можно добавлять задачи. Задачи может добавлять любой зарегистрированный пользователь, которого активировал администратор. При добавлении задачи, название задачи генерируется как уникальная последовательность символов. В задаче указывается кто ее назначил, выбирается текущий пользователь и следует указать кому задача назначается.Так же указывается тип ошибки («Bug», «Support», «Task», «Improvoment», «NewFeature») и статус с которым следует рассматривать поставленную задачу.Среди особенностей реализованной системы следует отметить возможность работы с окнами приложения как с отдельными вкладками. Пользователь может одновременно следить за изменениями в проектах и задачах.

Заключение

Система управления проектами строится на основе плана управления проектом, который описывает то, как будет использоваться система. Содержание системы управления проектом изменяется в зависимости от области приложения, особенностей организации, сложности проекта и доступности необходимых ресурсов. Система строится так, чтобы максимально соответствовать стратегическим целям и производственным ресурсам клиентской организации.

УДК 004.021

Студ. О.Д. Гуцев, В.В. Хорхалёв
Науч. рук. доц., канд. физ.-мат. наук Н. Н. Буснюк
(кафедра информационных систем и технологий, БГТУ)

АЛГОРИТМ ШИФРОВАНИЯ A3

Цель данной работы: Изучить реализацию алгоритма шифрования A3 COMP128, используемого при авторизации мобильной станции в сети GSM.

Задачи:

1. Изучить структуру сети GSM.
2. Изучить алгоритм работы A3.
3. Изучить алгоритм реализации A3 COMP128.
4. Реализовать алгоритм A3 COMP128 на языке C++.

GSM (отназваниягруппы*Groupe Spécial Mobile*, позжепереименованв Global System for Mobile Communications) (*русск.*СПС-900) — глобальный стандарт цифровой мобильной сотовой связи, с разделением каналов по времени (TDMA) и частоте (FDMA). Разработан под

эгидой Европейского института стандартизации электросвязи (ETSI) в конце 1980-х годов. (1)

Суть аутентификации в GSM — избежание клонирования мобильного телефона пользователя.

Рисунок 1 – Структура сотовой сети стандарта GSM

На рисунке 2 схематично представлены шаги работы сети GSM (2).

1. Телефон оператора подключается к сети.

2. Для подтверждения своей подлинности телефон посылает специальный идентификационный код, называемый TMSI.

3. Центр Аутентификации(ЦА) генерирует 128-битное случайное число RAND и посылает его на Мобильную Станцию(МС).

4. МС зашифровывает полученное число RAND, используя свой секретный ключ K_i и алгоритм аутентификации A3.

5. МС берет первые 32 бита из последовательности, полученной на предыдущем шаге(назовем их SRES(signed response)) и отправляет их обратно на ЦА.

6. ЦА проделывает ту же операцию и получает 32 битную последовательность XRES(expected response).

7. После чего ЦА сравнивает SRES и XRES. В случае, если оба значения равны, телефон считается аутентифицированным.

8. МС и ЦА вычисляют сессионный ключ шифрования, используя секретный ключ K_i и алгоритм формирования ключа A8 $K_c=A8_{ki}(RAND)$.

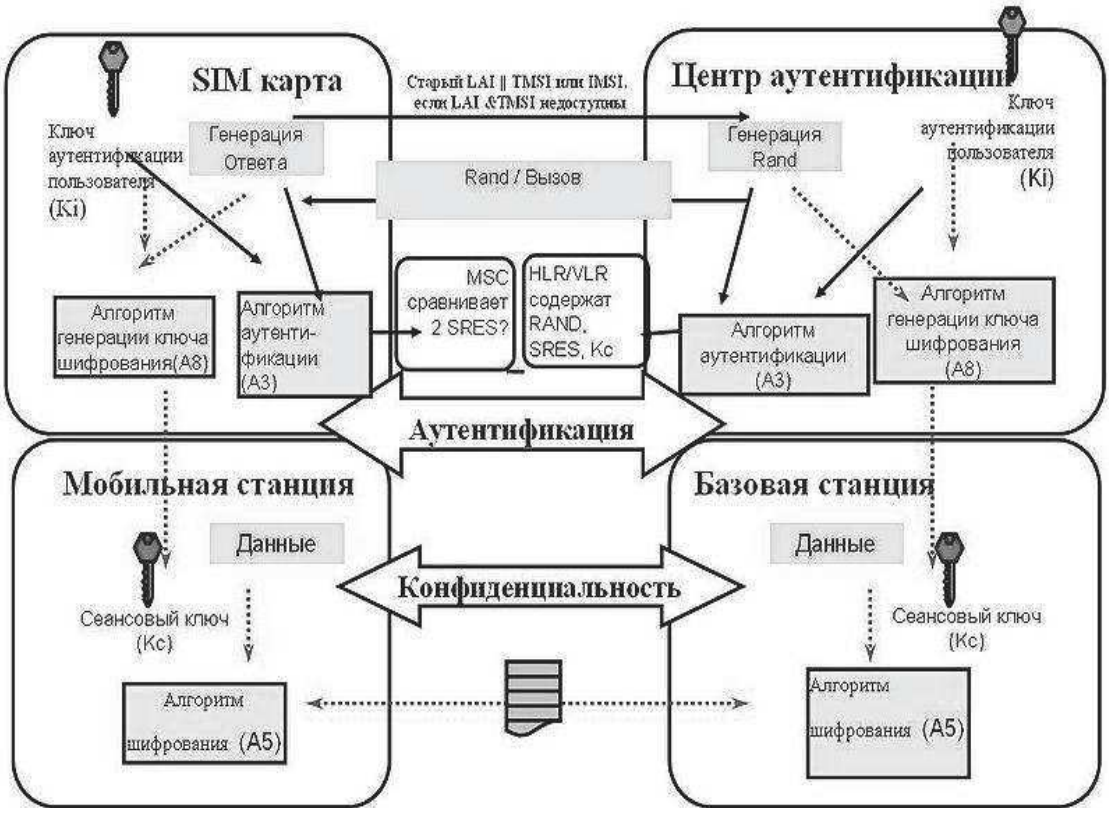

Рисунок 2 - Принцип работы участка Центр аутентификации – Базовая станция – Мобильная станция

Алгоритм программы

1. Получить входные данные (ключ, пароль) в 16-ном виде;
2. Преобразовать введённые данные в 2-ую систему счисления;
3. Загрузка 16 последних байт из случайного пароля;
4. Выполнить пункты от 5 до 7 9 раз, пункт 8 8 раз с увеличением счётчика;
5. Загрузка 16 первых байт из ключа;
6. Выполнение перестановок с использованием константных массивов;
7. Формирование битов из байтов;
8. Выполнить перестановки с использованием сформированных битов;
9. Объединить байты в числа;
10. Вывести пользователю полученный результат в 16-ной системе счисления;

Один из важных этапов разработки – написание кода программы. На рисунке 3 представлен фрагмент кода, выполняющий перестановки с использованием константных массивов.

```
for (int j = 0; j<5; j++)
for (int k = 0; k<(1 << j); k++)
for (int l = 0; l<(1 << (4 - j)); l++) {
m = l + k*(1 << (5 - j));
n = m + (1 << (4 - j));
y = (x[m] + 2 * x[n]) % (1 << (9 - j));
z = (2 * x[m] + x[n]) % (1 << (9 - j));
x[m] = table[j][y];
x[n] = table[j][z]; }
```

Рисунок 3 - Фрагмент кода алгоритма на языке C++

Главной особенностью алгоритма является обеспечение безопасности за счёт неизвестности. На данный момент надёжность данного механизма защиты сведена к минимуму из-за утечки данных массивов.

ЛИТЕРАТУРА

1 Бабков В.Ю., Вознюк М.А. Михайлов П.А. Сети мобильной связи. Частотно-территориальное планирование. - СПб, ГУТ. - 2000.

2 Бабков В.Ю., Вознюк М.А., Дмитриев В.И. Системы мобильной связи.– СПб: Изд. СПбГУТ.– 1998.

УДК621.679

Студ. В. С. Лёля
Науч. рук. ассист. Л. С. Мороз
(кафедра информационных технологий, БГТУ)

РАЗРАБОТКА БРАУЗЕРНЫХ ИГР НА ОСНОВЕ ТЕХНОЛОГИЙ HTML5, JAVASCRIPT И PHASER FRAMEWORK

Целью данной работы является изучение и использование технологий разработки браузерных игр без применения Flashанимации. В работе продемонстрированы две созданные браузерные игры, а также представлен сайт по обучению всех желающих работе с рассматриваемыми технологиями.

Основными базовыми знаниями, которые нам потребуются, являются знания HTML5, CSS, JavaScript(TypeScript). Стоит отметить, что для работы так же нужны знания английского языка, так как большая часть вспомогательных материалов по разработке не переведена на русский язык.

Используем технологию HTML5 CANVAS.

CANVAS — это элемент HTML5, предназначенный для создания растрового двухмерного изображения при помощи скриптов, обычно на языке JavaScript. Может быть использован для отображения диа-