**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ   
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

Факультет компьютерных наук

Департамент программной инженерии

|  |  |
| --- | --- |
| СОГЛАСОВАНО  Доцент департамента программной инженерии факультета компьютерных наук, канд. физ.-мат. наук.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А.Набебин  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2015 г. | УТВЕРЖДАЮ  Академический руководитель образовательной программы «Программная инженерия»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.В. Шилов  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_2015 г. |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. Инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл.*** | RU.17701729.501430-01 81 01-1-ЛУ | | **Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи**  **Пояснительная записка**  **ЛИСТ УТВЕРЖДЕНИЯ**  **RU.17701729.501430-01 81 01-1-ЛУ**  Исполнитель  студент группы 102 ПИ  \_\_\_\_\_\_\_\_\_\_\_/Берюхов А.С./  «\_\_\_»\_\_\_\_\_\_\_\_\_\_2015 г.  **2015** | | |  |

УТВЕРЖДЕНО

RU.17701729.501430-01 81 01-1-ЛУ

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. Инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл.*** | RU.17701729.501430-01 81 01-1 | | **Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи**  Пояснительная записка  RU.17701729.501430-01 81 01-1  **Листов 18**  **2015** |  |

**СОДЕРЖАНИЕ**

[1. Введение 3](#_Toc419892938)

[1.1. Наименование программы 3](#_Toc419892939)

[1.2. Документы, на основании которых ведется разработка 3](#_Toc419892940)

[2. Назначение и область применения 4](#_Toc419892941)

[2.1. Функциональное назначение 4](#_Toc419892942)

[2.2. Эксплуатационное назначение 4](#_Toc419892943)

[2.3. Краткая характеристика области применения 4](#_Toc419892944)

[3. Технические характеристики 5](#_Toc419892945)

[3.1. Постановка задачи на разработку программы 5](#_Toc419892946)

[3.2. Описание алгоритма и функционирования программы 5](#_Toc419892947)

[3.2.1. Регистры сдвига 6](#_Toc419892948)

[3.2.2. Полиномы обратной связи 6](#_Toc419892949)

[3.2.3. Управление тактированием 7](#_Toc419892950)

[3.2.4. Подготовка последовательности для шифрования в течение кадра 7](#_Toc419892951)

[3.2.5. Шифрование 8](#_Toc419892952)

[3.3. Описание и обоснование выбора метода организации входных и выходных данных 9](#_Toc419892953)

[3.4. Описание и обоснование выбора состава технических и программных средств 9](#_Toc419892954)

[3.4.1. Описание выбора состава технических средств 9](#_Toc419892955)

[3.4.2. Обоснование выбора состава технических средств 10](#_Toc419892956)

[3.4.3. Описание выбора состава программных средств 10](#_Toc419892957)

[3.4.4. Обоснование выбора состава программных средств 10](#_Toc419892958)

[4. Ожидаемые технико-экономические показатели 11](#_Toc419892959)

[4.1. Предполагаемая востребованность 11](#_Toc419892960)

[4.2. Экономические преимущества разработки по сравнению с аналогами 11](#_Toc419892961)

[5. Источники, использованные при разработке 12](#_Toc419892962)

[6. Приложения 14](#_Toc419892963)

[6.1. Описание и функциональное назначение классов 14](#_Toc419892964)

[6.2. Описание и функциональное назначение полей, методов и свойств 14](#_Toc419892965)

# 1. Введение

## 1.1. Наименование программы

Наименование программы – «Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи».

Условное обозначение для программы – А5КоДек.

## 1.2. Документы, на основании которых ведется разработка

* 1. Приказ Национального исследовательского университета «Высшая школа экономики» № 6.18.1-02/1912-10 от 19.12.2014.

# 2. Назначение и область применения

## 2.1. Функциональное назначение

Программа предназначена для осуществления потокового шифрования и дешифрования любых файлов, представленных в двоичном виде; реализованного алгоритмом А5-1, схожим с используемым для шифрования мобильной связи. Программа должна скрывать информацию от неавторизованных лиц (не имеющих аутентичного ключа) и давать доступ к ней авторизованным (имеющим ключ).

## 2.2. Эксплуатационное назначение

Программа предназначена для защиты информации от несанкционированного использования. Она позволяет решать проблемы создания защищенного канала связи и хранения информации в виде, недоступном третьим (неавторизованным) лицам.

## 2.3. Краткая характеристика области применения

«Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи» – программа, реализующая шифрование цифровых данных с помощью алгоритма А5-1.

Задача программы заключается в обеспечении возможности обратимого преобразования информации в целях сокрытия от неавторизованных лиц, с предоставлением, в то же время, авторизованным пользователям доступа к ней. [11].

Решение данной задачи имеет потенциальное приложение в разных областях:

1. Передача голосовых данных по каналам мобильной связи – обеспечение конфиденциальности передаваемых данных между абонентом и базовой станцией.
2. Передача информации от адресанта к адресату без возможности доступа к ней третьими лицами.
3. Хранение информации в зашифрованном виде.

# 3. Технические характеристики

## 3.1. Постановка задачи на разработку программы

Разрабатываемая программа должна обеспечивать выполнение перечисленных ниже функций:

1. Выбор файла для шифрования / дешифрования.
2. Выбор файла, в который будет записан результат работы программы.
3. Ввод ключа.
4. Получение результата в виде шифрованного / дешифрованного файла с помощью алгоритма A5-1 в указанном пользователем директории под указанным именем.

## 3.2. Описание алгоритма и функционирования программы

В программе используется алгоритм, описанный в статье «A5 – The GSM Encryption Algorithm» [1].

В силу особенностей алгоритма, для шифрования и дешифрования информации используется одна и та же программа.

Стоит заметить, что A5 – это семейство шифров: A5/0, A5/1, A5/2 и A5/3. Когда говорят об A5 как об отдельном шифре, подразумевают A5/1, как первый из семейства.

Весь процесс шифрования можно условно разделить на следующие части: сбор и подготовка данных для шифрования, создание новой сессии шифрования, разбивка данных на кадры (фреймы).

Далее для каждого кадра последовательно выполняется инициализация регистров сдвига: 64 такта для установки ключа, 22 такта для установки номера фрейма, 100 тактов с управлением сдвигами без генерации последовательности, наконец 228 тактов с генерацией выходной последовательности.

Рассмотрим каждую из частей подробнее.

### 3.2.1. Регистры сдвига

Регистры сдвига или линейные регистры сдвига с обратной связью – основа этого алгоритма. Сами по себе они легко поддаются криптоанализу, а, следовательно, не являются криптостойкими. Поэтому применяется система из трёх регистров сдвига, длины 19, 22 и 23 бита.

### 3.2.2. Полиномы обратной связи

Полиномы (или многочлены) обратной связи задают выходные биты регистров. Для работы необходим бинарный примитивный полином заданной длины (18, 21 или 22 степени соответственно). Степень слагаемых с коэффициентом, равным 1 определяет биты, сумма которых по модулю два (операция xor) является выходным битом регистра.

В целях криптостойкости алгоритма необходимо, чтобы каждый регистр сдвига имел максимально возможный период – минимальная длина получаемой последовательности до начала её повторения. Максимальный период T=2L-1, где L – длина регистра, достигается использованием примитивного полинома.

Используемые полиномы являются секретными, их вычисление злоумышленниками равносильно вскрытию алгоритма. Поэтому для промышленного применения необходимо в каждой отдельной копии продукта (для отдельной категории пользователей) использовать свой набор полиномов. Подобрать такие полиномы помогает второй программный продукт, разработанный в рамках этой темы курсовой работы – «Программа проверки полиномов на примитивность».

Для учебных целей использовался набор примитивных полиномов, используемый Россом Андерсоном в статье «A5 – The GSM Encryption Algorithm» [1]:

* X19 + X18 + X17 + X14 + 1 для R1,
* X22 + X21 + 1 для R2,
* X23 + X22 + X21 + X8 + 1 для R3.

### 3.2.3. Управление тактированием

Для повышения криптостойкости используется переменное тактирование регистров. Управление тактированием осуществляется следующим образом.

Каждый регистр имеет определенные биты синхронизации. Для регистра 1 (R1) – это бит с номером 8, для регистров R2 и R3 – бит с номеров 10.

На каждом такте вычисляется major значений этих битов по формуле F = x & y | x & z | y & z, где & – булево И, | – булево ИЛИ, x, y, z– биты синхронизации регистров.

В данном такте сдвигаются только те регистры, бит синхронизации которых равен major (таким образом сдвигаются два или все три из трёх регистров).

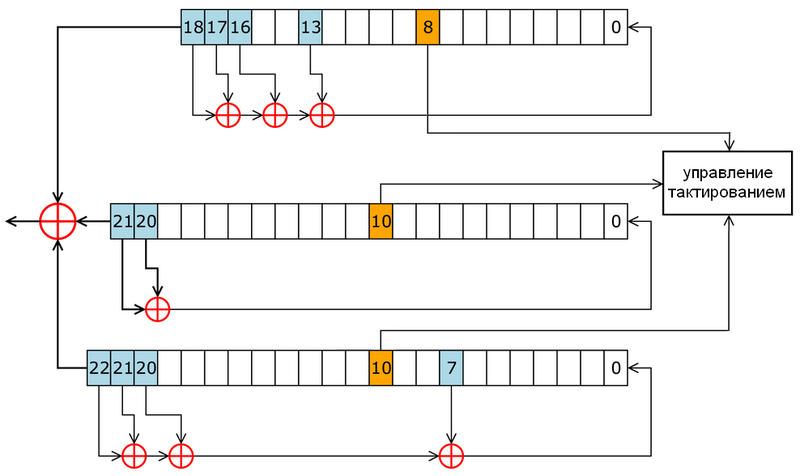
### 3.2.4. Подготовка последовательности для шифрования в течение кадра

Рассмотрим непосредственно, что происходит для генерации 228 бит последовательности шифрования.

Каждая сессия имеет свой сеансовый ключ – последовательность из 64 бит, сформированный алгоритмом А8 в случае мобильной передачи данных, и введенный пользователем в данной программе.

Вся сессия делится на кадры (фреймы) по 114 бит в случае двустороннего шифрования / дешифрования, как в мобильной связи или по 228 бит, в случае одностороннего шифрования (используется в данной программе).

Для каждого такого кадра инициализируются заново регистры. Сначала регистры обнуляются. Затем происходит 64 такта, при которых очередной бит ключа складывается по модулю два с младшим битом каждого регистра, затем регистры сдвигаются на бит. После выполняется 22 аналогичных такта с номером фрейма. Далее следуют 100 тактов с управлением тактированием без генерации последовательности. Наконец идут 228 тактов с управлением тактированием и генерацией последовательности (рис.1). Первые 114 тактов могут использоваться для шифрования, последние 114 – для дешифрования, либо все 228 для шифрования или дешифрования.



Рисунок

### 3.2.5. Шифрование

Входной файл считывается побайтно. Каждый раз отсчитывается 228 бит, инициализируются регистры ключом и номером кадра. Получается 228 бит последовательности для шифрования. Биты входного файла складываются по модулю два с битами последовательности и сохраняются побайтно в выходной файл с использованием буфера (так как 228 бит составляют 28 целых байта и 4 бита). По окончании входного файла сохраняются данные из буфера, входной и выходной файлы сохраняются, алгоритм заканчивает свою работу.

Класс A5\_1, методы которого осуществляют работу с регистрами и генерацию последовательности для шифрования, содержит методы для получения одной 228-битной последовательности, либо двух 114 битной последовательности, что позволяет использовать эту библиотеку для двустороннего потокового шифрования.

## 3.3. Описание и обоснование выбора метода организации входных и выходных данных

Входные данные должны быть получены из файла любого размера, с любым расширением, выбранного пользователем.

Выходные данные сохраняются в файл, указанный пользователем.

Выбор метода организации входных и выходных данных обоснован требованиями технического задания.

## 3.4. Описание и обоснование выбора состава технических и программных средств

### 3.4.1. Описание выбора состава технических средств

Для запуска и работы программы требуется компьютер, со следующими свойствами:

1. Процессор Pentium с частотой 233 МГц или более быстрый (рекомендуется не менее 300 МГц).
2. Не менее 64 МБ оперативной памяти (рекомендуется не менее 128 МБ).
3. Не менее 1,5 ГБ свободного места на жестком диске.
4. Дисковод для компакт- или DVD-дисков.
5. Клавиатура, мышь Microsoft Mouse или совместимое указывающее устройство.
6. Видеокарта и монитор, поддерживающие режим Super VGA с разрешением не менее чем 800x600 точек. [10]

### 3.4.2. Обоснование выбора состава технических средств

Выбор состава технических средств обусловлен использованием ОС Microsoft Windows XP и новее.

### 3.4.3. Описание выбора состава программных средств

Для запуска и работы программы требуется компьютер, со следующим предустановленным программным обеспечением:

1. операционная система Microsoft Windows XP и новее;
2. установленный Microsoft .NET Framework 2.0.

### 3.4.4. Обоснование выбора состава программных средств

Версия Microsoft .NET Framework 2.0 выбрана как минимальная из предлагаемых средой Microsoft Visual Studio.

Microsoft Windows XP выбрана как минимальная из предлагаемых приложением Install Shield.

# 4. Ожидаемые технико-экономические показатели

## 4.1. Предполагаемая востребованность

Программа может применяться для коммерческого и некоммерческого использования, связанного с шифрованием данных, подлежащих защите от несанкционированного доступа. Может использоваться для передачи данных в зашифрованном виде, с передачей ключа по надежному каналу связи, либо вычислением ключа сторонними программами и алгоритмами.

## 4.2. Экономические преимущества разработки по сравнению с аналогами

В ходе быстрого поиска в сети Интернет аналогов, использующих этот же алгоритм выявлено не было.

Представленное приложение имеет ряд преимуществ:

1. Распространяется свободно (бесплатно).
2. Не имеет необходимости обслуживания.
3. Срок эксплуатации не ограничен.

# 5. Источники, использованные при разработке

1. Росс Андерсон. А5 – алгоритм шифрования GSM [Электронный ресурс] / URL: <http://www.ussrback.com/crypto/source/algorithms/A5-GSM-Algorithm.txt> (Дата обращения: 12.01.2015, режим доступа: свободный, на англ. языке).

2. А.А. Набебин. Проблема оптимизации шифрования информации [Электронный ресурс], 2009.

3. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography [Электронный ресурс]. – CRC Press, 2005.

4. A5/1. From Wikipedia, the free encyclopedia. [Электронный ресурс] / URL: <http://en.wikipedia.org/wiki/A5/1> (Дата обращения 16.02.2015, режим доступа: свободный, на англ. языке).

5. A5. Материал из Википедии — свободной энциклопедии [Электронный ресурс] / URL: <https://ru.wikipedia.org/wiki/A5> (Дата обращения 4.02.2015, режим доступа: свободный).

6. Регистр сдвига с линейной обратной связью. Материал из Википедии — свободной энциклопедии [Электронный ресурс] / URL: <https://ru.wikipedia.org/wiki/Регистр_сдвига_с_линейной_обратной_связью> (Дата обращения 4.03.2015, режим доступа: свободный).

7. Единая система программной документации – М.: ИПК Издательство стандартов, 2000.

8. В.В. Побельский. Язык Си #. Базовый курс: учеб.пособие / В.В. Подбельский. – М.: Финансы и статистика., 2011. – 384 с.: ил.

9. Герберт Шилдт, C# 4.0: полное руководство.: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2011.

10. Системные требования для операционных систем Windows ХР [Электронный ресурс] / URL: <https://support.microsoft.com/ru-ru/kb/314865> (Дата обращения 20.02.2015, режим доступа: свободный).

11. Шифрование. Материал из Википедии — свободной энциклопедии [Электронный ресурс] / URL: <https://ru.wikipedia.org/wiki/Шифрование> (Дата обращения 14.02.2015, режим доступа: свободный).

# 6. Приложения

## 6.1. Описание и функциональное назначение классов

Таблица 1. Описание и функциональное назначение классов

|  |  |
| --- | --- |
| Класс | Назначение |
| MainForm | Определяет внешний вид главного окна программы MainForm. Содержит код обработчиков событий. |
| Program | Осуществляет работу с файлами и подготовку данных для шифрования – использования методов класса A5\_1. |
| A5\_1 | Шаблон для создания объектов-сессий шифрования. Содержит методы, необходимые для задания ключа шифрования, номера сессии, формирования и вывода шифровальной последовательности. |

## 6.2. Описание и функциональное назначение полей, методов и свойств

Таблица 2. Описание и функциональное назначение полей класса MainForm

|  |  |  |  |
| --- | --- | --- | --- |
| Имя | Тип | Модификаторы | Назначение |
| AboutToolStripMenuItem | System.Windows.Forms.ToolStripMenuItem | private | Пункт меню «О программе» |
| buttonDestin | System.Windows.Forms.Button | private | Кнопка «Выбрать расположение файла-результата» |
| buttonOpen | System.Windows.Forms.Button | private | Кнопка «Открыть файл» |
| buttonRun | System.Windows.Forms.Button | private | Кнопка «Запустить» |
| components | System.ComponentModel.IContainer | private | Логический контейнер |
| groupBox | System.Windows.Forms.GroupBox | private | Рамка и заголовок вокруг группы элементов управления |
| HelpToolStripMenuItem | System.Windows.Forms.ToolStripMenuItem | private | Пункт меню «Справка» |
| InName | string | private | Строка для хранения пути входного файла |
| key | string | private | Строка для хранения пути ключа |
| labelKey | System.Windows.Forms.Label | private | Надпись «Введите восьмисимвольный ключ» |
| menuStrip | System.Windows.Forms.MenuStrip | private | Строка меню |
| openFileDialog | System.Windows.Forms.OpenFileDialog | private | Запрашивает пользователя об открытии входного файла данных |
| OutName | string | private | Строка для хранения пути выходного файла |
| progressBar | System.Windows.Forms.ProgressBar | private | Представляет индикатор выполнения процесса шифрования |
| saveFileDialog | System.Windows.Forms.SaveFileDialog | private | Запрашивает пользователя об выборе входного файла данных |
| textBoxKey | System.Windows.Forms.TextBox | private | Текстовое поле для ввода ключа |

Таблица 3. Описание и функциональное назначение методов класса MainForm

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Имя | Модификаторы | Тип возвращаемого значения | Аргументы | Назначение |
| AboutToolStripMenuItem\_Click | private | void | object sender, EventArgs e | Обработчик события Click |
| buttonDestin\_Click | private | void | object sender, EventArgs e | Обработчик события Click |
| buttonOpen\_Click | private | void | object sender, EventArgs e | Обработчик события Click |
| buttonRun\_Click | private | void | object sender, EventArgs e | Обработчик события Click |
| Clean | private | void | – | Задает начальные параметры формы |
| HelpToolStripMenuItem\_Click | private | void | object sender, EventArgs e | Обработчик события Click |
| MainForm | public | MainForm (конструктор) | – | Конструктор для формы |

Таблица 4. Описание и функциональное назначение методов класса Program

(примечание: в классе Program полей нет)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Имя | Модификаторы | Тип возвращаемого значения | Аргументы | Назначение |
| create | internal static | void | string InName, string OutName, string Key, ref ProgressBar pr | Осуществляет работу с файлами и подготовку данных для шифрования – использования методов класса A5\_1 |

Таблица 5. Описание и функциональное назначение полей класса A5\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Имя | Тип | Модификаторы | Назначение |
| R1 | uint | private | Хранение текущего состояния регистра сдвига R1 |
| R2 | uint | private | Хранение текущего состояния регистра сдвига R2 |
| R3 | uint | private | Хранение текущего состояния регистра сдвига R3 |
| R1MASK | uint | private static | Хранение маски длины регистра сдвига R1 |
| R2MASK | uint | private static | Хранение маски длины регистра сдвига R2 |
| R3MASK | uint | private static | Хранение маски длины регистра сдвига R3 |
| R1MID | uint | private static | Хранение маски синхронизирующего бита регистра сдвига R1 |
| R2MID | uint | private static | Хранение маски синхронизирующего бита регистра сдвига R2 |
| R3MID | uint | private static | Хранение маски синхронизирующего бита регистра сдвига R3 |
| R1OUT | uint | private static | Хранение маски выходного бита регистра сдвига R1 |
| R2OUT | uint | private static | Хранение маски выходного бита регистра сдвига R2 |
| R3OUT | uint | private static | Хранение маски выходного бита регистра сдвига R3 |
| R1TAPS | uint | private static | Хранение маски полинома (битов для сложения по модулю два) регистра двига R1 |
| R2TAPS | uint | private static | Хранение маски полинома (битов для сложения по модулю два) регистра двига R2 |
| R3TAPS | uint | private static | Хранение маски полинома (битов для сложения по модулю два) регистра двига R3 |

Таблица 6. Описание и функциональное назначение методов класса A5\_1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Имя | Модификаторы | Тип возвращаемого значения | Аргументы | Назначение |
| clock | private | Void | – | Сдвигает один регистр (тактирование) |
| clockallthree | private | void | – | Тактирование всех трех регистров |
| clockone | private | uint | uint reg, uint mask, uint taps | Сдвигает один регистр сдвига |
| getbit | private | uint | – | Генерирует выходной бит в текущем состоянии |
| keysetup | public | void | uint[] key, uint frame | Вводит ключ и номер фрейма в алгоритм |
| majority | private | uint | – | Возвращает большинство из трех синхронизационных битов |
| NumToBin | public static | string | uint chislo | Перевод uint десятеричного числа в двоичную строку |
| parity | private | uint | uint x | Возвращает сумму байтов 32-битного слова (числа uint) по модулю два |
| Stream228 | public static | bool[] | uint[] AtoB, uint[] BtoA | Создание "длинной" выходной boolean последовательности из двух uint для шифрования |
| Stream228 | public | bool[] | – | Создание "длинной" выходной boolean последовательности из двух uint для шифрования |
| TwoStreams | public | void | out uint[] AtoBkeystream, out uint[] BtoAkeystream | Генерация двух выходных последовательностей для шифрования/дешифрования |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Лист регистрации изменений | | | | | | | | | |
| Изм. | Номера листов (страниц) | | | | Всего листов (страниц) в документе | № документа | Входящий № сопроводительного документа и дата | Подпись | Дата |
| измененных | замененных | новых | аннулированных |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |