МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
ФАКУЛЬТЕТ РАДИОТЕХНИКИ И КИБЕРНЕТИКИ

ЭССЕ ПО КУРСУ: ЗАЩИТА ИНФОРМАЦИИ

Обзор алгоритмов шифрования и возможных атак протокола GSM

Выполнил студент 312 группы
Прохоров Василий

Апрель 2007

1 СОДЕРЖАНИЕ

GSM – старое название Group Special Mobile, ну а современная расшифровка Global System for Mobile Communications – наиболее широко используемый стандарт мобильной связи, насчитывающий около 100 млн. абонентов.

2 РАЗВИТИЕ GSM

Стандарт является одним из первых цифровых систем цифровой мобильной связи, пришедший на смену аналоговым.
Развитие GSM началось в 1982 году, когда была создана Groupe Speciale Mobile, организация прогнозирования и исследования систем сотовой связи в Европе. В 1987 проведены испытания ряда систем, которые включили проверки спектральной эффективности, качества речи и радио-интерфейса, а в январе 1992 года с запуском первой сети GSM в Финляндии аббревиатура получила современную расшифровку. К концу года число сетей выросло до 14. На следующий год сеть была запущена неевропейской компанией. Такое бурное развитие послужило к закреплению за стандартом нового диапазона 1800МГц (изначально был тока 900МГц).
С 2002 году поддержку стандарта осуществляет 3GPP (3rd Generation Partnership Project).

3 АЛГОРИТМЫ GSM

Создание методов защиты и передачи информации в стандарте GSM велось в основном секретно, и выдавалось операторам связи только по мере необходимости. Разработчики полагались на Безопасность из-за Неизвестности, т. е. алгоритмы сложнее взломать, если они не доступны публично. Но согласно предположению Керкхоффа, наиболее безопасными являются системы, криптозащищенность которых зависит только от ключа, алгоритмы же, наоборот, должны быть открыты и подвергнуты исследованию для выявления уязвимостей.
Нет ничего тайного, что не стало бы явным, так произошло и с GSM. Раскрытие алгоритмов шифрования и аутентификации привело к снижению безопасности стандарта.
Но вначале разберем на сём основывается защищенность в протоколе.
В GSM определены следующие механизмы безопасности:
Аутентификация (авторизация идентификатора абонента)
Секретность передачи данных (Конфиденциальность идентификатора абонента)
Секретность абонента (Конфиденциальность сигнальных данных)
Секретность направлений соединения абонентов
Система построена на алгоритмах шифрования с открытым ключом, суть которых заключается в наличии у каждой стороны секретного и открытого ключа, при этом секретный не может быть выведен из открытого. Расшифровка сообщения, зашифрованного при помощи открытого ключа возможна, только если известен секретный ключ.
Также используются симметричные алгоритмы, суть которых заключается в наличии сеансового ключа, к-й используется как для шифрования, так и расшифрования сообщений.

3.1 Аутентификация

Позволяет избежать клонирования мобильного телефона абонента. Для этого абоненту выдается временный международный ид-й номер пользователя IMSI, который

действителен только в пределах зоны расположения а так же индивидуальный 128-битный ключ авторизации Ki. Схемы спроектированы так, что ни одно из этих значений напрямую через радио канал не передается.
Ключ Ki известен обоим сторонам.
В аутентификации используется SIM-карта и Центр Авторизации (Authentication Center AuC).
Auc генерирует 128 битовое значение RAND и посылает мобильной станции, в ответ получает 32-битное значение SRES=A3(RAND, Ki) которое сравнивает с вычисленным самостоятельно тем же алгоритмом A3. В мобильной станции A3 прошит в SIM-карте.

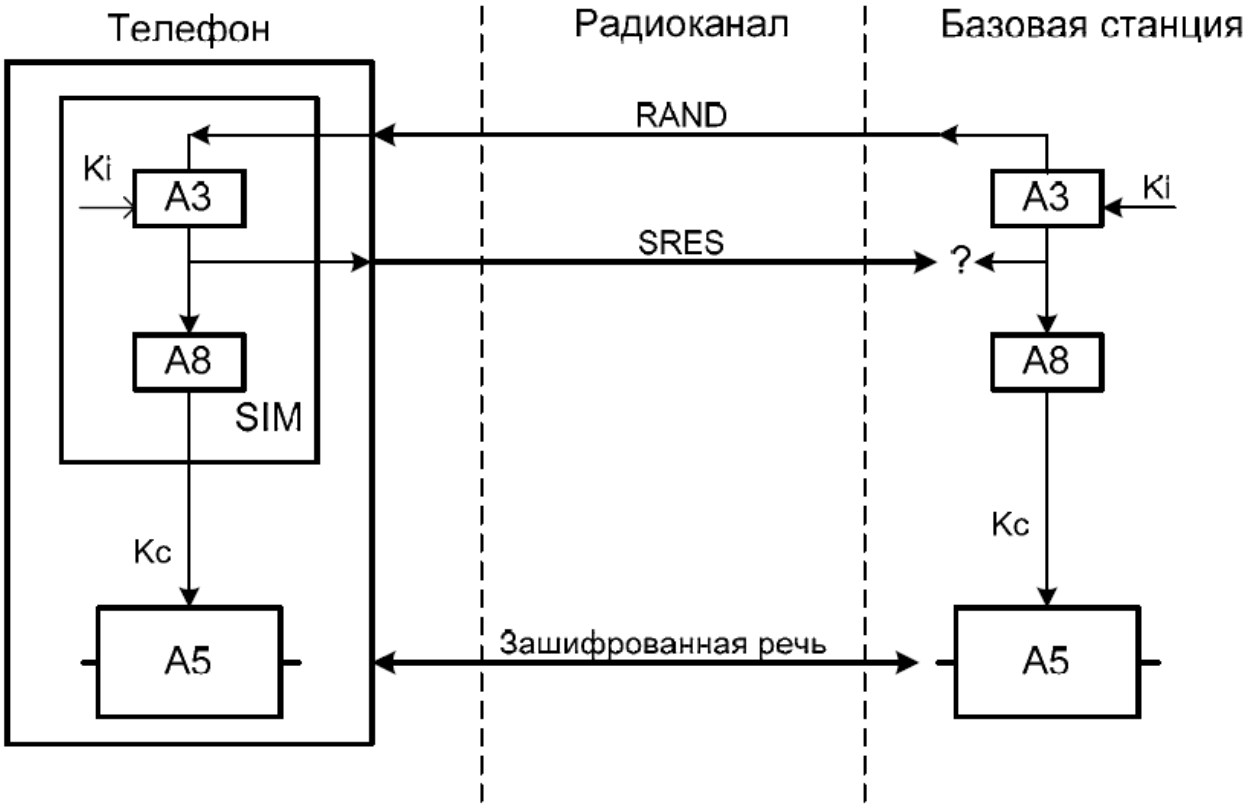
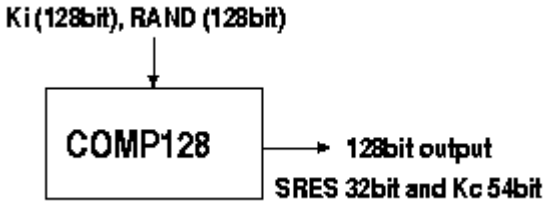


Рис 1. Идентификация в стандарте GSM

3.2 Генерация сеансового ключа

На мобильной станции производится алгоритмом A8, вновь используя полученный RAND и имеющийся Ki. Сеансовый ключ Kc вычисляется и в AuC.
С этого момента радиоканал считает шифрованным.
Сегодня реализация A3\A8 в основном использует алгоритм COMP128, который сразу вычисляет и SRES и Kc значение(см рис). Ключ Kc имеет длину 64 бит, образуется добавлением к 54 битам, полученным данным алгоритмом, десяти нулевых битов – это значение и является входом для алгоритма шифрования A5 разговора.
В мобильной станции A8 также как и A3 прошит в SIM-карте.



3.3 Передача информации

Осуществляется алгоритмом A5 по кадрам, который в качестве параметров шифрования получает сеансовый ключ Kc и 22-битный номер кадра Frame, а на выходе каждому кадру соответствует 114-битовая кодовая последовательность. Сеансовый ключ может использоваться несколько дней, т.к. аутентификация является необязательным действием при звонке по телефону.
Т.о. для дешифрации аналитик должен знать номер кадра и Kc.

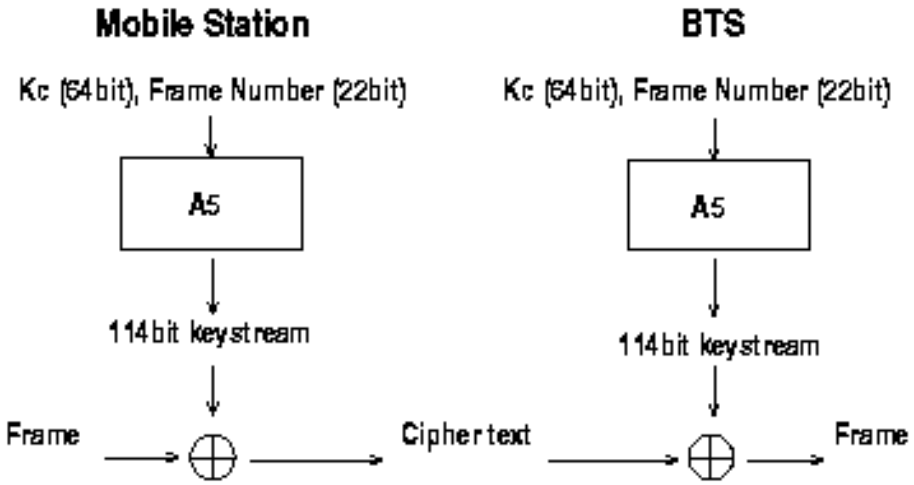
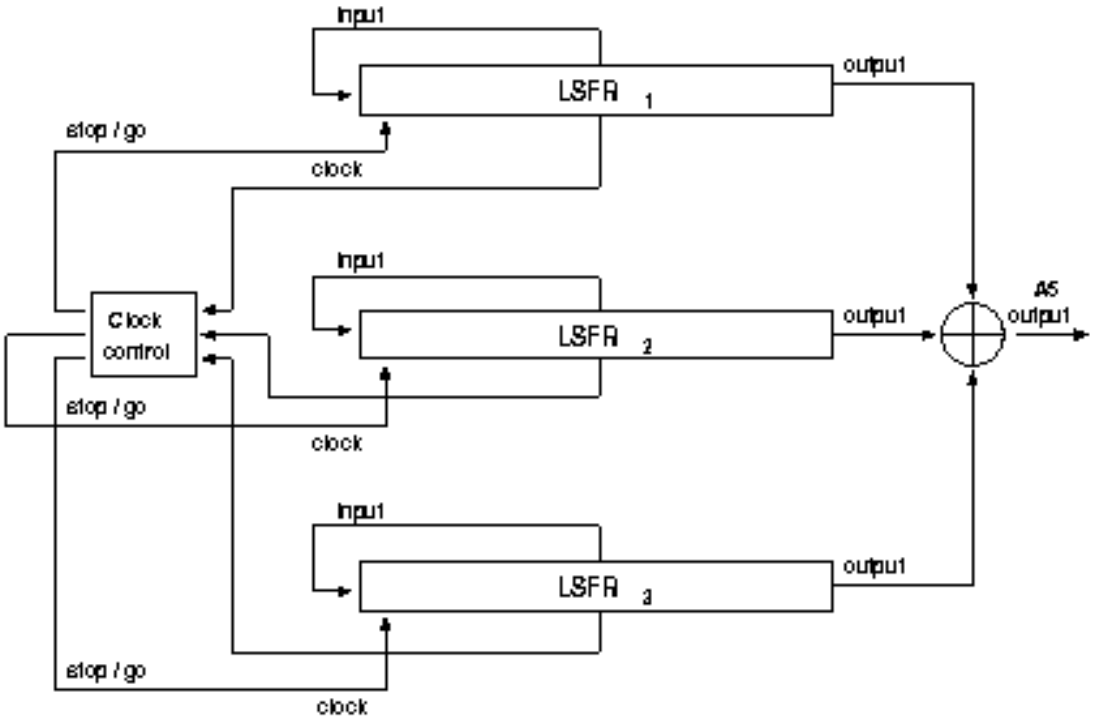


Схема алгоритма A5 используемого в европейских странах содержит 3 LSFR различной длины (19, 22, 23 бита), суммарной длиной в 64 бита. Для получения очередного бита ключевой последовательности, выходы всех регистров складываются по модулю 2. Все 3 регистра имеют управление сдвигом, т.е. можно запретить сдвиг по очередному сигналу тактового генератора.
Структура алгоритма A5 приведена на следующем рисунке:



Три LSFR-а инициализируются сеансовым ключом Kc и номером кадра. 64-битовый сеансовый ключ Kc сначала загружается в регистр бит за битом Потом все регистры синхронизируются (правило синхронизации большинства отключено). Все 64 бита ключа загружаются в регистр одинаково. 22-битный номер кадра также загружается в регистр таким же образом, но с этого момента применяется правило синхронизации большинства. После того, как регистры были таким образом инициализированы, производят 100 шагов и полученную последовательность отбрасывают. Следующие 228 бит составляют выходную ключевую последовательность первые 114 бит которой используют для шифрования кадра от MS к BTS, а остальные 114 обратно от BTS к MS. Для шифрования следующего кадра, схема инициализируется заново, и процесс повторяется.
В 2002-2003 было опубликовано много статей, в которых утверждалось, что стандарт GSM взломан, а прослушивать разговоры, и даже «клонировать» базовую станцию или терминал абонента.

4 ВОЗМОЖНЫЕ АТАКИ GSM

Во-первых следует отметить, по данным на конец 2006 года ученые во всем мире единогласно полагают, что одновременное прослушивание, перехват и расшифровка данных по радио каналу в РЕАЛЬНОМ времени невозможна. Однако видимо существуют иные способы взлома GSM. Рассмотрим несколько типов атак.

4.1 Лобовая атака A5

Сложность 2^54, в реальном времени невозможна. Единственный вариант записать перехваченные фреймы.
250 часов при одном чипе в 600Mhz, каждая реализация A5 выдает 1 бит за такт.

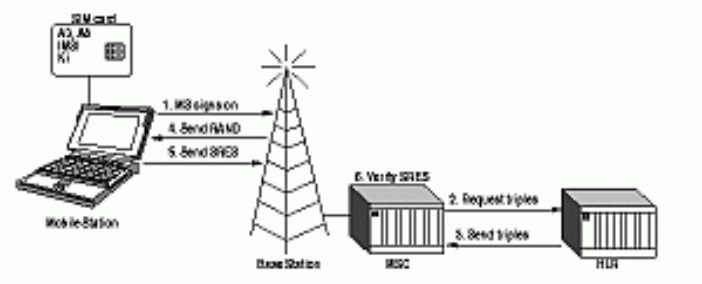
4.2 Атака A5 Разделяй и Властвуй

Позволяет уменьшить стойкость алгоритма с 2^54 до 2^45.

Основана на атаке открытого текста. Зная сегмент из 64битов открытого текста, аналитик пытается определить начальные состояния регистров LSFR, Кадры GSM содержат большое количество постоянной информации, например, заголовки кадров, что даёт шанс получить искомую последовательность.

4.3 Доступ к сигнальной сети

Основана на том, что от базовой станции до Центра Коммутации, Контроллеру Базовой Станции и другим компонентам оборудования оператора сигнал поступает открытым текстом по сигнальной сети SS7. Передача по сигнальной сети может осуществляться не тока по кабелю, но и через спутники или микроволновую линию, доступ к которым получить возможно, используя имеющееся в продаже оборудование.



4.4 Получение ключа из SIM

Знание секретного ключа Ki является ключевым в шифровании сообщений стандарта GSM, такоим образом получение этого ключа дает криптоаналитику возможность безпрепятственного получения открытого текста. Получить ключ с сервера является достаточно сложной задачей, однако есть и другая возможность – получение этого же ключа, но зашитого в Sim-карте.
Исследовательской группой ISAAC была обнаружена ошибка в алгоритме COMP128 которая позволяла при физическом контакте с картой проводить атаку. Также утверждалось что подобная атака возможна и в эфире.
С помощью PC и SmartCardReader было произведено около 150000 запросов к SIM на которые ушло около 8 часов. (6.25 запросов SIM в секунду). Карта генерировала SRES и сеансовый ключ, из этих данных путём дифференциального криптоанализа был вычислен секретный ключ.
Т.О. клонирование сим-карт производителем с целью передачи их 3-им лицам, практически оставляет законных абонентов безоружными.

4.5 Получение ключа из SIM карты в эфире

Провести эту атаку групее ISAAC не удалось, т.к. необходимое оборудование является незаконным в США. Заключается она в следующем: Когда сигнал BTS злоумышленника превышает сигнал базовой станции абонента, криптоаналитик может бомбардировать MS запросами нужного формата и получать соответствующий отклик. Возможно провести атаку в местах слабого сигнала базовой станции или местах его отстутствия, например в метро. Предположительное время атаки: 8-13 часов. Возможно разбить атаку на интервалы по неск. минут, что упрощает проблему физической реализации данного метода.

4.6 Получение ключа из AuC

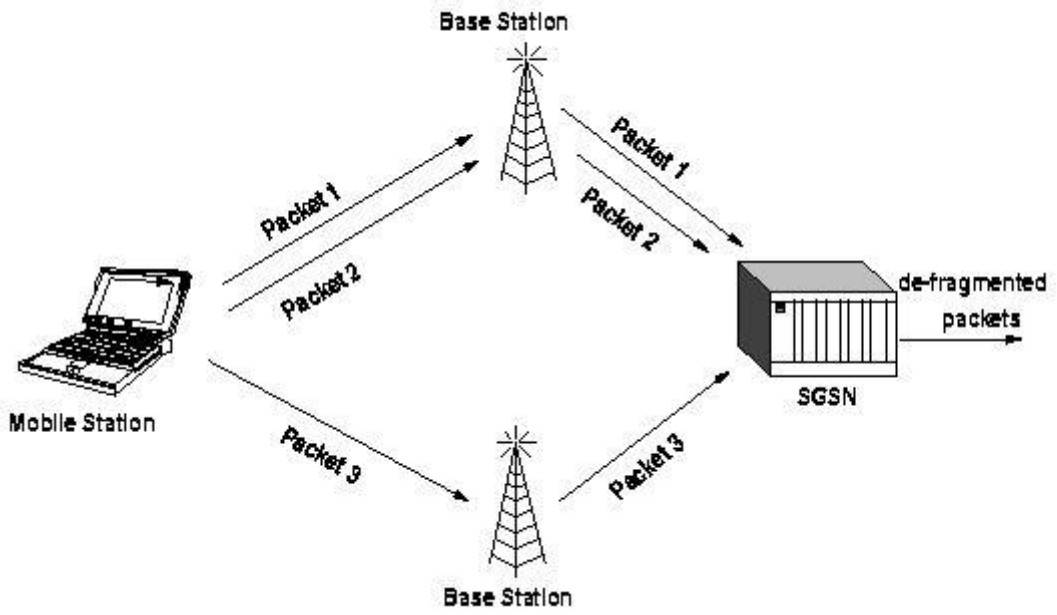
Основана на исследовании информации которая поступает от базового оператора к оператору осуществляющим роуминг в другой точке планеты в случае,конечно, если абонент использует роуминг в данный момент.

4.7 Взлом алгоритма A8

Заключается в поиске RAND, который производит заданный ключ Ki. Это представляется сделать возможным т.к. RAND и SRES передаются по эфиру открытым текстом.

4.8 GPRS и GSM

SGSN - Узел Обеспечения GPRS, который обрабатывает запросты от телефона, расшифровывая кадры и отсылая далее по назначению. Кадры шлются сразу параллельно на несколько базовых станции для увеличения скорости передачи данных, поэтому на одну конкретную BTS поступают последовательные кадры с непоследовательными номерами. До SGSN кадры поступают также в зашифрованным виде, что также затруднят ряд атак. Новый алгоритм A5 передачи данных по GPRS неизвестен на данный момент, поэтому данная область криптоанализа GSM станет доступной, когда станут известны новые алгориты шифрования GPRS, а это рано или поздно произойдет, так что работы криптоаналитакам на ближайщее будещее больше чем достаточно☺!



5 ПУТИ УСОВЕРЕШЕНСТВОВАНИЯ GSM

В первую очередь конечно необходимо заменить все sim-карты абонентов с целью избежания клонирования. Это не потребует оператору непосредственно взаимодействовать с производителями программного обеспечания и менять дорогостоящее оборудование серверов.

Замена алгоритма A5 на более стойкий, не позволит криптоаналитику записывать кадры и в offline режиме расшифровывать их, тем самым свести к минимуму возможность лобовой атаки.

Потребует достаточных финансовых вложений и повысит криптостойкость GSM так же и шифрование сигнальной сети. В данном случае оператору будет необходима поддержка производителей оборудования и программного обеспечения к нему.

6 ЗАКЛЮЧЕНИЕ

Вывод из всего этого простой: если кто-то захочет прослушать сеть GSM – он это сделает. Проблема возникает особенно остро, когда передаваемая информация представляет какую-то ценность, но, поскольку, современное использование этого стандарта предназначено в основном для массового «народного» использования, менять стандарт операторы не торопятся.

В качестве альтернатив использования протоколов мобильной связи можно назвать в первую очередь CDMA (относящийся к сетям третьего поколения, 3G-системы), в котором, в отличии от GSM, производится двухсторонняя аутентификация сторон, а также улучшены алгоритмы шифрования.

Конечно может порадовать, тот факт, что алгоритм на сегодняшний момент не удалось вскрыть в режиме online, но видимо и это лишь дело времени и развития человеческих способностей.

7 ПРИЛОЖЕНИЕ, ОСНОВНЫЕ ТЕРМИНЫ

A3
Алгоритм аутентификации, используемый в системе GSM. В настоящее время в большинстве сетей GSM используется алгоритм COMP128 как реализация A3/A8.

A5
Алгоритм шифрования, используемый в системе GSM. Существуют различные реализации, которые называются A5/1, A5/2, ... Алгоритм A5/1 известный как стойкий алгоритм шифрования секретной речи в эфире. A5/x (A5/2 ...) - это - более слабые реализации, рассчитанные для зарубежных рынков за пределами Европы. Также существует алгоритм A5/0, который вообще не содержит шифрование.

A8
Алгоритм для генерации ключа, используемый в системе GSM. В настоящее время в большинстве сетей GSM используется алгоритм COMP128 в качестве реализации A3/A8.

AuC
Центр Аутентификации. Регистр Центра Аутентификации используется в целях безопасности. Он обеспечивает параметры, необходимые для функции аутентификации и шифрования (RAND, SRES и Kc). RAND – это случайный вызов, генерируемый случайно. Другие два параметра генерируются из RAND и Ki абонента при помощи алгоритмов A3 и A8. Эти параметры помогают подтвердить идентификацию пользователя (SRES) и предоставить сеансовый ключ (Kc).

BSC
Контроллер Базовой Станции. BSC служит общим узловым пунктом между многочисленными BTS, которые все вместе формируют одну BSS и являются основой сети.

BSS
Подсистема Базовых Станций. BSS соединяет телефон с Подсистемой Сети и Коммутации (NSS). Она отвечает за прием и передачу. BSS может быть подразделена на две части:
Базовая Приемопередаточная Станция (BTS) или Базовая Станция.
Оператор Базовой Станции (BSC).

BTS
Приемопередатчик базовой станции, базовая станция, с которой связывается мобильный телефон.

COMP128
Односторонняя функция, которая в настоящее время используется в большинстве сетей GSM для A3 и A8. К сожалению, алгоритм COMP128 взломан, таким образом, он выдает информацию о своей аргументации при соответствующем запросе. Это нежелательный и неприемлемый побочный эффект односторонней функции.

GPRS
Сеть с Пакетной Передачей Данных. GPRS используется для высокоскоростной передачи между мобильным телефоном и какой-либо другой стороной. GPRS утилизирует многочисленные Базовые Станции в одной Подсистеме Базовых Станций. Мобильный телефон посылает различные пакеты в различные Базовые Станции, которые реконструируются в Узле Обеспечения GPRS. Это позволяет телефону использовать более высокую скорость передачи, чем скорость передачи, возможная в одном канале связи.

GSM
Глобальная Система Мобильной связи, мобильная система телефонной связи, в основе которой лежат многочисленные радио ячейки/соты (сотовая мобильная телефонная сеть).

HLR
Регистр Положения Домашних Абонентов. Регистр Положения Домашних Абонентов – это часть Центра Аутентификации. Регистр Положения Домашних Абонентов обеспечивает Центр Коммутации трехразрядной характеристикой случайной попытки. SRES и Секретным Сеансовым Ключом, основанном на секретном ключе абонента и случайной попытке, HRL отвечает за информацию о местоположении мобильного телефона в любое время.

ISAAC
Интернет Безопасность, Приложения, Аутентификация и Криптография. Небольшая группа исследователей в Университете Беркли, Калифорния, факультет вычислительной техники. A small research group in the Computer.
http://www.isaac.cs.berkeley.edu/

Kc
Секретный сеансовый ключ используется для шифрования трафика в эфире между BTS и мобильным телефоном. Секретный сеансовый ключ генерируется после каждой инициализации аутентификации Мобильного Центра Коммутации. Секретный сеансовый ключ вычисляется из Ki и случайной попытки, посланной Мобильным Центром Коммутации с алгоритмом A8. Мобильная станция и Регистр Положения Домашних Абонентов рассчитывают Секретный сеансовый ключ независимо друг от друга. Секретный сеансовый ключ никогда не передается по эфиру.

Ki
Секретный ключ, совместно используемый SIM и Регистром Положения Домашних Абонентов домашней сети абонента.

LSB
Самый младший двоичный разряд.

LSFR
Регистр сдвига с линейной обратной связью. Регистр, генерирующий выходной бит на основании его предыдущего состояния и полинома обратной связи.

MS
Мобильная станция, мобильный (сотовый)телефон.

MSC
Мобильный Центр Коммутации, центральный компонент Подсистемы Сети и Коммутации. Мобильный Центр Коммутации осуществляет функции переключения в сети. Он также обеспечивает связь с другими сетями.

NSS
Подсистема Сети и Коммутации, ее основная роль заключается в обеспечении связи между мобильными пользователями и другими пользователями, например, пользователями ISDN, пользователями неподвижных телефонов и т.д. Она также включает базы данных, необходимые для хранения информации об абонентах, и для обеспечения их мобильности.

SDA
Ассоциация Разработчиков Смарткарт – это бюджетная организация, пытающаяся обеспечить разработчиков непатентованной информацией о смарт картах.
http://www.scard.org/

SGSN
Узел Обеспечения GPRS. Узел Обеспечения GPRS отсылает пакеты Мобильным Станциям в пределах области своих услуг через многочисленные Приемопередатчики базовой станции. Узел Обеспечения GPRS также связывается с Регистром Положения Домашних Абонентов с целью аутентификации мобильной станции для включения шифрованной связи. Узел Обеспечения GPRS в GPRS удостоверяет мобильную станцию вместо Мобильного Центра Коммутации.

SIM
Модуль Идентификации Абонента. SIM идентифицирует абонента. Абонент может использовать одну SIM карту на многих GSM телефонах. Все звонки оплачиваются с одного счета и номер абонента остается неизменным. SIM карта содержит IMSI, Ki и алгоритмы A3 и A8. Предполагается, что SIM защищена от подделки, таким образом, из нее невозможно извлечь Ki.

SRES
Подтвержденный результат/Подписанные отклики. Это ответ, который MS возвращает в ответ на попытку, сделанную Мобильным Центром Коммутации во время аутентификации MS, соответственно аутентификация самого Мобильного Центра Коммутации. (или Узла Обеспечения GPRS в случае GPRS).

SS7
Сигнальная Система 7 используется в самых интеллектуальных сетях в качестве сигнального протокола. SS7 определяется ITU-T.
Симметричная Криптография
В симметричной криптографии для шифрования и расшифровки используется один и тот же ключ.

VLR
Гостевой Реестр Местоположения. Гостевой Реестр Местоположения сохраняет векторы аутентификации, сгенерированные Регистром Положения Домашних Абонентов, когда абонент не находится в своей домашней сети. Тогда по мере необходимости Гостевой Реестр Местоположения предоставляет Мобильным Центрам Коммутации эти векторы аутентификации.

8 ЛИТЕРАТУРА

1) Jovan Dj. Golic, Cryptanalysis of Alleged A5 Stream Cipher, http://gsmsecurity.com/papers/a5-hack.html
2) Slobodan Petrovic and Amparo Fuster-Sabater, Cryptanalysis of the A5/2 Algorithm, http://gsmsecurity.com/papers/a52.pdf
3) http://phreak.ru
4) Anon., GSM Cell phones Cloned, [referred 29.9.1999] http://jya.com/gsm-cloned.htm
5) Golic J. Dj., Cryptanalysis of Alleged A5 Stream Cipher, [referred 29.9.1999] http://jya.com/a5-hack.htm
6) Racal Research Ltd., GSM System Security Study, 10.6.1988, [referred 29.9.1999] http://jya.com/gsm061088.htm
7) GSM: вскрытие покажет Валерий Коржов http://www.osp.ru/nets/2004/03/150909/
8) http://www.contrterror.tsure.ru/site/magazine6/pdf/05-27-Shniperov.pdf
9) 15.01.2005 - Секреты GSM. http://www.interstar.ua/mobile/?main_menu=10&sub_menu=2&id=60
10) Кунегиным С. В. Алгоритмы открытых ключей http://www.aboutphone.info/kunegin/gsm2/08.html