Шифрование в стандарте GSM

Гарбачев Р.А. 215 гр.
24.03.2006

Система безопасности GSM.

Сотовая связь – одно из наиболее динамически развивающихся направлений рынка информационных технологий. За последние три года прирост абонентской базы сотовых операторов России составил в среднем 39 процентов в год от уже существующего количества пользователей. На конец февраля 2006 года число абонентов в России составило 128 миллионов человек. Таким образом, сотовый телефон есть почти у каждого жителя нашей страны.

С помощью мобильника люди общаются с друзьями и близкими, пишут смски, получают доступ в интернет, обмениваются информацией, которая может содержать комерческую, государственную тайну. Следовательно, что бы эта информация не попала в руки злоумышленников, то перед передачей по радиоканалу она должна быть зашифрована.

Система мобильной связи GSM вполне могла бы быть сильно защищенной. Она основывается на своде документов под названием MoU Groupe Special Mobile standard. Этот MoU Groupe Special Mobile standard был подготовлен в конце Холодной войны благодаря инициативе различных телекоммуникационных компаний Западной Европы. Техническую документацию GSM стандарта разрабатывал Европейский институт стандартов по телекоммуникациям (ETSI), а при создании схемы безопасности, которая должна была защитить новую систему от перехвата, прослушивания и мошенничества, большой вклад внесли спецслужбы стран НАТО.

Для максимальной отдачи от GSM разработчики ставили перед собой целью сделать его настолько же защищённым, насколько защищены проводные телефонные сети.

Система безопасности GSM состоит из трех основных частей: идентификация, аутентификация и шифрование данных.

Аутентификация – установление подлинности, то есть проверка и подтверждение номера с которого происходит звонок. При каждом подключении абонента к системе сотовой связи GSM происходит аутентификация по алгоритму A3. Так же существует алгоритм A8 при помощи которого генерируется сеансовый ключ. Оба алгоритма A3 и A8 прошиты в SIM карте, но у различных сотовых операторов они могут различаться.

Кратко рассмотрим алгоритм аутентификации телефона в сети. Для регистрации в сети телефон делает запрос у базовой станции. Базовая станция, получив запрос, передает телефону случайное число RAND. Терминал имея полученный RAND и собственный индивидуальный ключ SIM-карты Ki при помощи алгоритма A3 формирует SRES (Signed RESult) и передает его базовой станции. Аналогично SRES вычисляется и на базовой станции, причем Ki берется из базы данных сотового оператора. Затем происходит сравнение полученного и сгенерированного самой станцией ключей. Если значения SRES совпали, то идентификация телефона прошла успешно и начинается подготовка к обмену информацией. Алгоритм A8 используется для превращения части выхода A3 в Kc (сеансовый ключ используемый для шифрования при разговоре).

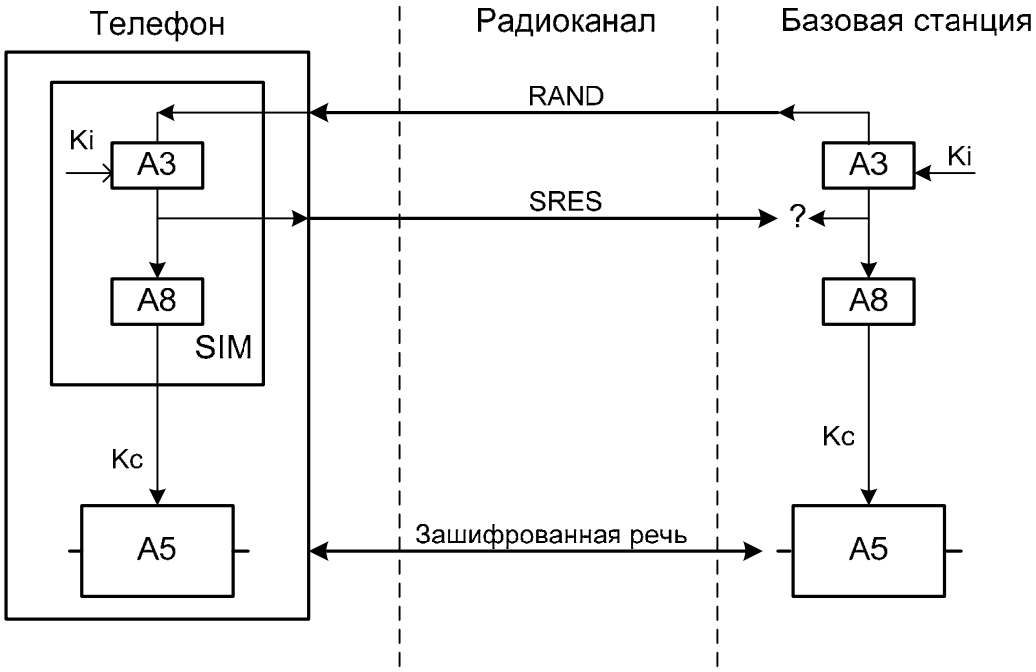


Рис 1. Идентификация в стандарте GSM

Итак, если пользователь подтвердил себя введя код, и телефон успешно зарегестрировался в сети, то можно начинать совершать звонки и передавать необходимую информацию. Из-за того, что передача сигнала происходит по радиоканалу для злоумышленника не составит особого труда перехватить его, причем пользователь даже и не заметит этого. Таким образом, для того что бы обеспечить секретность передаваемой информации необходимо применять шифрование данных. Отметим, что в стандарте GSM шифрование данных происходит только в «эфире»,то етсь на участке передачи телефон-базовая станция, далее передача по проводам происходит в незакодированном виде.

Шифрование в стандарте GSM осуществляется при помощи семейства протоколов A5. В A5/0 – данные при передачи по эфиру не шифруются. Версия A5/1 применяется в «избранных» странах, таких как США и страны Западной Европы. В остальных странах

используется ослабленная версия – A5/2. После того как шифры A5/2 и A5/1 были взломаны, была разработана модернизированная версия - A5/3 которая использует алгоритм Касуми.

Шифры семейства A5.

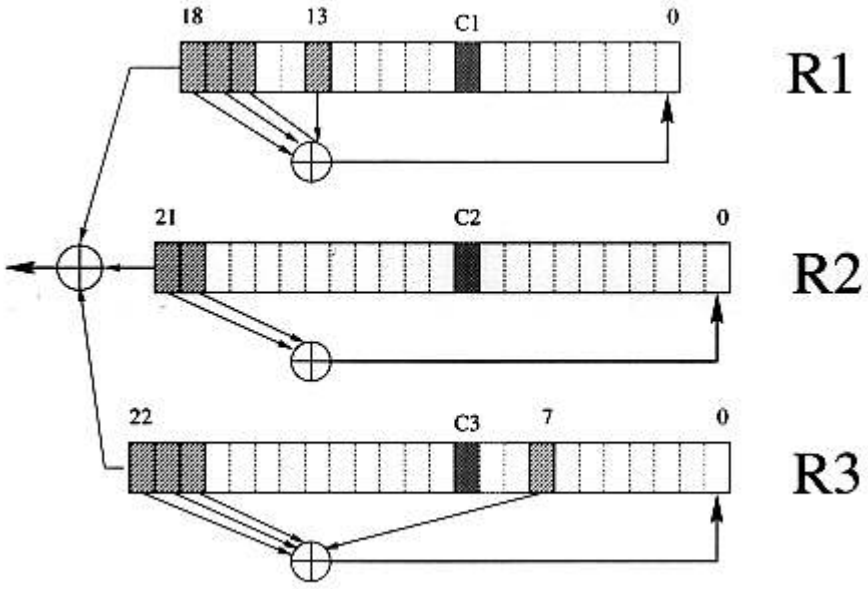
Шифр A5/0.

Разговор не шифруется и передается прямым текстом. Таким образом, криптоаналитик воспользовавшись простым сканером радиочастот может без особых проблем прослушать разговор.

Шифр A5/1

Рассмотрим более подробно эту модификацию. В стандарте GSM во время сеанса связи между Абонентом (далее А) и Базовой станцией (далее Б) посылается последовательность кадров каждые 4.6 мс. Каждый кадр заключает в себе 114 бит оцифрованной информации от А к Б и 114-ти бит от Б к А. Каждый разговор может быть зашифрован посредством нового сессионного ключа К. Для каждого кадра, К смешивают с общеизвестным номером кадра Fn, а результат служит в качестве начального состояния генератора, который производит 228 псевдослучайных бит. Эти биты складываются по модулю 2 с двумя частями по 114(114 + 114) бит не зашифрованного текста, что бы получить 114+114 бит шифротекста.

A5/1 состоит из трех регистров сдвига с линейной обратной связью с длиной в 19, 22 и 23 бит, которые обозначены как R1, R2 и R3 соответственно. Самай крайний справа бит в регистрах на схеме помечен как нулевой бит. Обратная связь регистра R1 осуществляется в битах расположенных в позициях – 13, 16, 17, 18; R2 – 20, 21; R3 – 7, 20, 21, 22 (см. Рис 2). Когда регистр работает, его сдвиги в ячейках обратной связи суммируются по модулю два и результат записывается в нулевой бит сдвинутого регистра. Три регистра максимальной длины с периодами 2^{19} -1, 2^{22} – 1 и 2^{23} -1 соответственно. Регистры сдвигаются по следующему мажоритарному правилу: в регистре имеется один бит для «синхронизации»(8 for R1, 10 for R2, 10 for R3). Есть мажоритарная функция f(x,y,z) = x&y +x&z +y&z (& - логическое И, + - логическое ИЛИ) которая калькулируется в каждом такте от трех битов синхронизации. И на данном такте сдвигу подвергаются только те регистры у которых биты синхронизации совпадают с f.



Процесс генерации псевдослучайных битов из сессионного ключа K и счетчика кадров Fn состоит из 4-х шагов:

-- Три регистра равны нулю, а затем проходят 64 цикла (причем управление сдвигом отсутствует). В течении данного периода каждый бит K(от младшего к старшему) складывается по модулю 2 с младшим битом каждого регистра.

--Затем, производится еще 22 цикла (причем опять отсутствует управление сдвигом) и младшие биты регистров складываются по модулю два с битами Fn (от младшего к старшему). Состояние регистров в конце этого шага называется начальным состоянием кадра.

--Над тремя регистрами производится еще 100 тактов с управлением сдвигом, но уже выходные псевдослучайные биты(последовательность) не генерируются.

--228 циклов с управлением сдвигом и генерируются 228 бит выходной последовательности. Причем, один выходной бит генерируется на каждом такте как XOR старших битов трех регистров.

Шифр A5/2.

В алгоритме A5/2 используется более слабая система шифрования, чем в A5/1, так как эта модификация создавалась на экспорт в страны не входящие в ЕС.

В A5/2 к трем основным регистрам добавлен еще 17 битовый, управляющий движением бит в остальных . Но криптоаналитиками было установлено, что для вскрытия системы достаточно прямым перебором (сложность 2^{16}) найти заполнение упровляющего регистра. Это осуществляется двумя кадрами по 114 бит сеанса связи(в первых двух кадрах шифруются одни нули).

Благодаря слабости в комбинирующей функции, позволяющей по выходной последовательности завладеть информацией об отдельных последовательностях узла усложнения. То есть имеется корреляция между одной из внутренних последовательностей и выходной последовательностью. Вследствии этого у одной внутренней последовательности можно восстановить начальное заполнение соответствующего регистра, а затем перейти на другую. Таким образом и может быть восстановлен весь генератор. Причем первым выбирается тот регистр, который проще для восстановления. Такой шифр вскрывается за 15 миллисекунд работы современных вычислительных машин.

Шифр A5/3

Основой алгоритма A5/3 служит алгоритм Касуми, утвержденный 3GPP, который в свою очередь был получен из алгоритма MISTY (Mitsubishi). Считается, что этот алгоритм обеспечивает требуемую криптостойкость.

Рассмотрим, различные атаки на алгоритмы шифрования стандарта GSM:

• Атака на длину ключа. Длина ключа равна 64 бит, из специально зануляют 10. Из-за этого система ослабляется на три порядка.

• Атака на алгоритм A5/1. Из-за присутствия конструктивных дефектов уменьшилась сложность перебора до 2^40. Помимо этого, ослабление происходит в том числе и из-за некореллированности трёх регистров: для любого регистра биты в других регистрах влияют только на управление смещением, но не на биты самого регистра.

• Атака на алгоритм шифрования A5/2.Первоначально создававшийся ослабленым, для его взлома нужно знать 2 кадра по 114 бит.

• Активная атака на протоколы семейства A5. В GSM была найдена слабость, из-за которой можно успешно провести активную атаку. Эта уязвимость выявели и описали израильские криптографы в составе: Элад Баркан, Эли Бихам и Натан Келлер.

В заключение можно сказать, что алгоритмы шифрования в стандарте GSM, а именно A5/1 и A5/2 оказались с незаметными недоработками. Атаки на оба алгоритма могут декодировать трафик в реальном времени, при этом достаточно использовать средней мощности персональный компьютер. И, таким образом, разработчикам не удалось создать достаточно криптостойкого стандарта. .

Литература.

1. Elad Barkan, Eli Biham, Nathan Keller, «Instant ciphertext-only cryptanalysis of GSM encrypted communication», http://cryptome.org/gsm-crack-bbk.pdf
2. Alex Biryukov, Adi Shamir, David Wagner «Real Time Cryptanalysis of A5/1 on a PC», http://cryptome.org/a51-bsw.htm , April 2000.
3. http://www.gsm-security.net/
4. И. Шахнович «Современные технологии беспроводной связи», Техносфера, 2004