інформації в Україні. НТУУ ”КПІ”. К. 2000. - с. 130-138.

УДК 621.396: 621.391

КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В СТАНДАРТЕ СОТОВОЙ СВЯЗИ GSM

Александр Корнейко, Денис Кравченко, Юрий Черевко
Киевский военный институт управления и связи

Анотація: **Розглянуті криптографічні властивості алгоритмів A3A8 і A5, що використовуються у стандарті системи стільникового зв'язку GSM. Показано, що при розробці алгоритмів криптоперетворень стандарту GSM був допущений ряд помилок, що знижують їх криптостійкість. Визначено, що для криптоаналізу алгоритму A3A8 можна застосувати так звану “атаку з обраним викликом” за умови забезпечення фізичного доступу до SIM-карти, а для A5 – атаку типу “балансування час-пам'ять”.**

Summary: **The cryptographic properties of the A3A8 and A5 algorithms, used in the cellular communications standard GSM, are considered. It was shown that there is a number of breaches in the design of the cryptographic transformations which reduce the crypt security. It was determined that one can use so called «attack with chosen call» for the crypt analysis of A3A8 provided the physical access to SIM-card, and «time-memory trade off attack» – for A5.**

Ключові слова: **Стандарт стільникового зв’язку GSM, криптоалгоритми A3, A5, A8, криптостійкість.**

Введение

В настоящее время системы сотовой связи (ССС) стандарта GSM находят все большее применение в обеспечении надежной и мобильной автоматической телефонной связи субъектов предпринимательской деятельности государственной и частной форм собственности, а также законодательных и исполнительных структур органов государственной власти. Однако в ССС передача информации между мобильной и базовой станциями происходит по радиоканалу, что накладывает достаточно жесткие требования на обеспечение их информационной безопасности, которая реализуется на основе соответствующих криптографических алгоритмов.

I Анализ встроенных механизмов криптографической защиты информации стандарта GSM

Стандарт GSM (Global System of Mobile Communications), который в настоящее время наиболее массово используется в ССС Европы в диапазонах частот 900 (GSM-900) и 1800 (DCS-1800) Мгц, а также в Америке в диапазоне 1900 (PCN-1900) МГц, уже при его разработке изначально предполагал достаточно мощные механизмы обеспечения информационной безопасности ССС. Так действующие нормативные документы организации разработчиков стандарта GSM определяют, что все ССС этого стандарта должны обеспечивать следующие механизмы защиты системных и информационных ресурсов:

- защита от несанкционированного доступа к мобильной станции (МС) с помощью парольного метода защиты;
- идентификация мобильного абонента ССС с помощью его уникального международного идентификационного номера (МИН);
- аутентификация (определение подлинности) абонента при каждом вхождении в связь с помощью алгоритма A3;
- конфиденциальность передаваемой по радиоканалу информации путём её шифрования с помощью алгоритма A5, где ключ шифрования вычисляется алгоритмом A8;
- секретность местонахождения абонента и направления его вызова.

Общее описание применения данных механизмов защиты информационных ресурсов ССС стандарта GSM приведено в Рекомендации ETSI\GSM 03.21. В данном документе указывается, что криптографическая защита информационных ресурсов ССС обеспечивается за счет использования алгоритмов A3, A5 и A8, носителем которых, за исключением A5, является SIM-карта абонента. Данная карта выполнена в виде съёмного блока МС и кроме алгоритмов A3 и A8 содержит также МИН и индивидуальный ключ аутентификации *i*-го пользователя (Ki).

Рассмотрим более детально перечисленные выше механизмы защиты стандарта GSM.

Исключение несанкционированного доступа к SIM-карте реализуется с помощью проверки пароля (PIN

ISBN 966-622-022-9

и PUK код), который вводится абонентом на мобильном телефоне перед его использованием. Данный пароль проверяется МС без передачи его в эфир.

Идентификация абонента осуществляется за счет использования ССС его МИН. Данный номер извлекается из SIM-карты МС и передаётся по радиоканалу на базовую станцию (БС). Следует отметить, что идентификация по МИН проводится только на начальном этапе взаимодействия абонента с ССС (при первом включении в сеть). После этого данному пользователю присваивается временный международный идентификационный номер (ВМИН), который передаётся с БС на МС в зашифрованном виде. Он действителен только в пределах локальной зоны расположения абонента.

Процедура аутентификации реализуется центром коммутации мобильной сети (ЦКМС) со стороны БС и SIM-картой абонента – со стороны МС. Последовательность действий при выполнении этой процедуры следующая (рисунок 1):

– МС посылает запрос на БС о предоставлении ей системных ресурсов;
– ЦКМС генерирует случайное 128-битное число RAND и, используя оборудование БС, посылает его на МС;
– МС, используя число RAND и индивидуальный ключ аутентификации Ki, по алгоритму A3 определяет отклик SRES (длиной 32 бита) и отправляет этот отклик через БС на ЦКМС;
– ЦКМС, имея все необходимые данные о каждом абоненте сети, производя аналогичные действия, также вычисляет SRES. При получении отклика с МС, ЦКМС сравнивает оба значения. Если они совпадают, то соединение устанавливается, в противном случае – связь с МС прерывается.

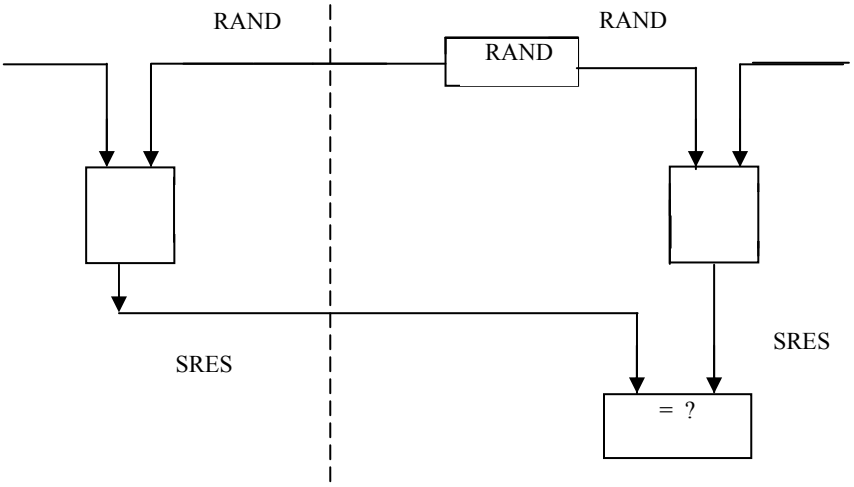


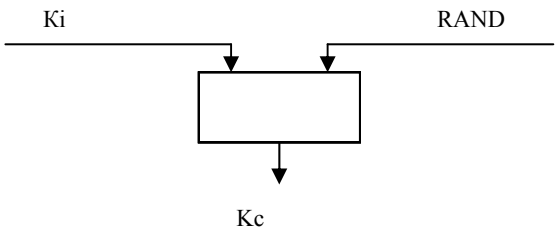
Рисунок 1 – Процедура аутентификации МС в стандарте GSM

Конфиденциальность передаваемой по радиоканалу ССС информации обеспечивается за счёт её шифрования с помощью алгоритма A5. Для этого используется ключ шифрования Кс, который вычисляется одновременно с откликом SRES, но по радиоканалу не передаётся (рис. 2).

Чтобы избежать неправильного формирования ключа Кс, БС совместно с числом RAND посылает МС числовую последовательность, которая связана с действительным значением Кс. Длина ключа Кс на выходе алгоритма A8 равна 64 битам.

После вычисления и проверки ключа Кс БС передаёт МС команду о переходе в режим шифрования. Мобильная станция, имея ключ шифрования Кс, приступает к зашифрованию и расшифрованию сообщений. Поток передаваемых данных шифруется побитно с помощью алгоритма A5 (рис. 3).

Алгоритм A5 выводит шифрующую последовательность длиной 114 бит для каждого кадра отдельно. На вход схемы поступает номер кадра (Nk) длиной 22 бита и ключ Кс длиной 64 бита. В обоих направлениях соединения используются две различные последовательности: одна для зашифрования выходящего пакета данных, вторая для расшифрования входного пакета данных. Номер кадра Nk меняется от пакета к пакету передаваемых сообщений, а ключ Кс – при каждом новом сеансе связи.



ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

Рисунок 2 – Процедура выработки ключа шифрования в стандарте GSM

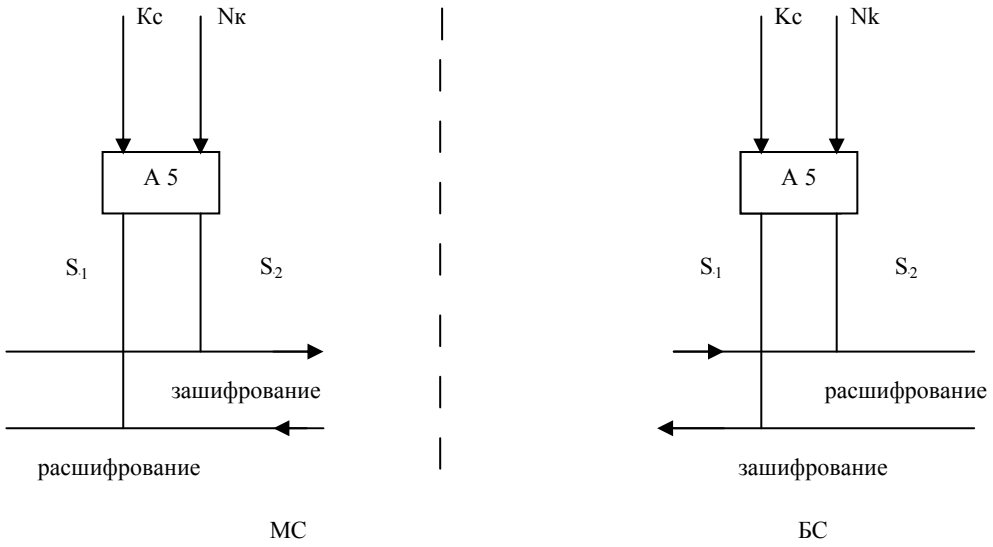


Рисунок 3 – Процедура шифрования сообщений в стандарте GSM

Стандарт GSM поддерживает два варианта алгоритма А5 (А5/1 – более криптостойкий алгоритм, А5/2 – менее криптостойкий алгоритм).

Секретность местонахождения абонента и направления его вызова обеспечивается за счёт использования ВМИН, который передаётся абоненту в зашифрованном виде, а также того факта, что при въезде в новую локальную зону абонент не передаёт по радиоканалу всю информацию о себе, а лишь зашифрованный ВМИН и номер локальной зоны, в которой он был получен. Тогда БС новой локальной зоны запрашивает у старой БС, номер которой передан МС, всю информацию об абоненте с данным ВМИН. В дальнейшем в этой зоне абоненту присвоится новый ВМИН. Таким образом, секретная информация не передаётся по радиоканалу, и абонент получается зарегистрированным в сети как бы под псевдонимом.

Указанный выше рекомендательный документ стандарта GSM описывает рассмотренные механизмы информационных ресурсов ССС лишь в самом общем виде. Более детальная техническая документация по механизмам защиты стандарта GSM доступна лишь ограниченному числу лиц из организаций-операторов ССС данного стандарта. Эта документация относится к одной из наиболее охраняемых коммерческих тайн GSM.

Однако, в последнее время на ряде форумов известных хакерских сайтов INTERNET появились сообщения, более детально описывающие механизмы безопасности GSM. Так нами были обнаружены опубликованные листинги программ алгоритмов А3, А5 и А8. Авторы данных программ, зачастую анонимные, не афишируют источников получения данной информации, но, как правило, практические проверки подтверждают их подлинность для ССС, эксплуатируемых, например, в Испании и Великобритании. Однако данные сайты не содержат каких-либо серьезных публикаций о криптографической стойкости стандарта GSM.

Поэтому, используя данные листинги программ алгоритмов А3, А5 и А8, проанализируем более детально механизмы их функционирования, оценим их криптографическую стойкость, а также рассмотрим возможные атаки на данные алгоритмы.

II Анализ стойкости алгоритмов криптозащиты стандарта GSM

Алгоритмы А3 и А8. На практике эти алгоритмы реализованы как единый алгоритм под названием А3А8. Принцип работы алгоритма А3А8 представлен на рис. 4.

Большинство известных публикаций о А3А8 указывают, что он поддаётся взлому только при условии физического доступа к SIM-карте. В терминах современного криптоанализа данная атака называется ***“атакой с выбранным вызовом”.*** Коротко рассмотрим ее суть.

Формируется ряд специальных вызовов RAND, которые посылаются в SIM-карту. Используя данный вызов и записанный ключ аутентификации Ki, SIM-карта вычисляет по алгоритму А3А8 значение отклика

SRES и возвращает его. Анализируя запросы и соответствующие им отклики на персональном компьютере возможно определить секретный ключ Ki. Для этого требуется сформировать порядка $1{,}5 \cdot 10^5$ запросов на SIM-карту. Техническая скорость обработки и вычисления отклика для SIM-карты составляет порядка 6,25 запросов в секунду, так что атака займёт около восьми часов.

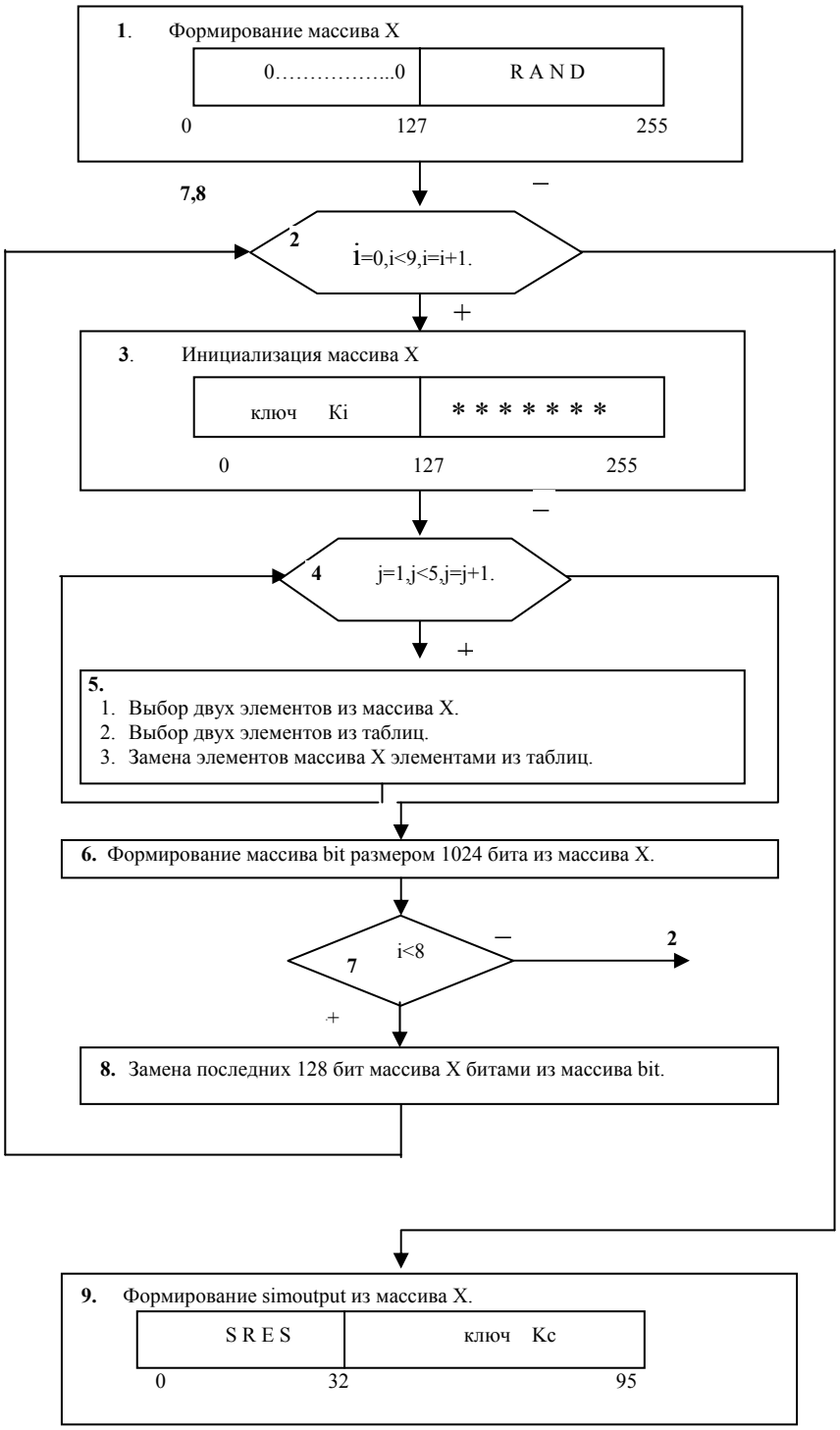


Рисунок 4 – Схема работы алгоритма A3A8

Атака использует слабость алгоритма A3A8, которая заключается в том, что имеется некий “узкий канал” в его структуре. В частности, выходные байты *i*, *i*+8, *i*+16, *i*+24 массива X (см. рисунок 4) в конце второго

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

общего цикла преобразования зависят только от байтов *i* и *i*+8 запроса (всего в алгоритме A3A8 производится 5×8 общих циклов). Следовательно, меняя байты *i* и *i*+8 запроса и оставляя постоянными всю оставшуюся часть запроса, анализируется изменение соответствующих откликов на эти запросы.

Так как отображения, получаемые в результате преобразования общих циклов, не биективны, то можно надеяться на совпадение байтов *i*, *i*+8, *i*+16, *i*+24 массива X после двух общих циклов преобразований. Согласно известному "парадоксу дней рождений" эти совпадения произойдут относительно быстро, так как ширина канала только 4 байта. Каждое такое совпадение используется, чтобы получить два байта *i* и *i*+8 ключа Ki (т.е. построить "2-R атаку" – в терминологии дифференциального анализа).

Таким образом, для получения двух ключевых байтов требуется сформировать $2^{(4*7/2 + 0,5)} = 2^{14,5}$ запросов к алгоритму A3A8. Но так как длина ключа составляет 16 байт, то для его полного восстановления потребуется $8 \cdot 2^{14,5}$ запросов.

Алгоритм A5. Данный алгоритм реализован на основе трех регистров сдвига с линейной обратной связью длиной 19, 22 и 23 бита (рис. 5). Регистры сдвигаются не регулярно. Закон движения схемы таков, что в каждом такте по крайней мере два регистра будут сдвигаться. Средние ячейки каждого из регистров с номерами 8, 10 и 10, соответственно, используются для определения сдвигающихся регистров в следующем такте (при этом сдвигаться будут только те регистры, у которых содержимое данных ячеек совпадает). Законом движения регистров управляет схема управления синхронизацией (СУС).

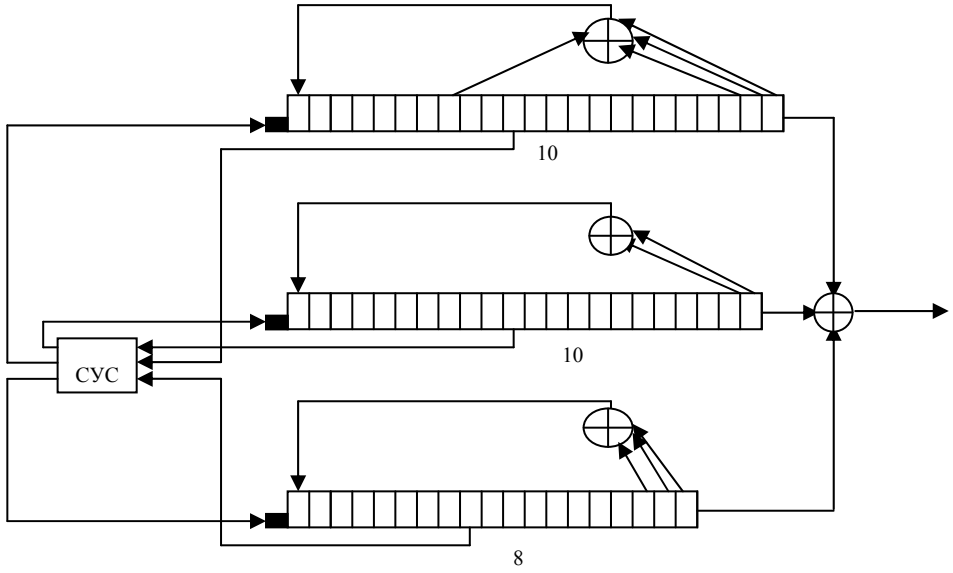


Рисунок 5 – Структурная схема алгоритма A5

Выходом алгоритма A5 является побитовая сумма выходных последовательностей трёх регистров. Далее, эта суммарная последовательность складывается по модулю два с открытым текстом. Нужно также отметить, что выходная последовательность используется частями. Первых 100 бит отбрасываются, а следующие 114 бит используются как шифрующая гамма, затем опять 100 бит отбрасываются, а следующие 114 бит опять используются как шифрующая гамма и т. д.

Анализируя алгоритм, можно заметить, что каждый из регистров будет простаивать 1/4 периода своей работы (под периодом следует понимать период данного регистра при его регулярной работе). Период самого длинного регистра составляет $T_{max} = (2^{23}-1)$. Если представить A5 как конечный автомат, то видно, что он имеет $2^{(19+22+23)}=2^{64}$ состояний и функция переходов является не обратимой.

Однако в [1, 2] найдено 2^{37} начальных заполнений, которые имеют периоды, близкие к малым множителям наибольшего периода T_{max}. Кроме того, более 40% из этих начальных заполнений имеют период, очень близкий к T_{max} непосредственно. В [1] говорится также, что эта слабость сохраняется при выборе других полиномов обратной связи и даже когда последовательности управления синхронизацией представляют собой псевдослучайные последовательности, не связанные с данными регистрами.

Таким образом, период выходной последовательности алгоритма A5 в 57% начальных заполнений не намного больше периода T_{max} самого длинного регистра.

Теперь рассмотрим возможные атаки на алгоритм A5. Данные атаки представим в виде стратегии с

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

известным открытым текстом. Будем также считать, что номер кадра Nk (называемый также открытым ключом A5) известен. Задачей криптоанализа является получение секретного ключа Кс, используемого в качестве начального заполнения регистров алгоритма.

Первая атака на алгоритм A5 заключается в переборе всех возможных начальных заполнений двух наименьших регистров длиной 19 и 22 бита, и восстановление начального заполнения наибольшего, используя выходную последовательность A5, – так называемая атака "грубой силой". Но трудоёмкость данной атаки будет составлять величину не $2^{(19+22)}=2^{41}$, а порядка 2^{45}, так как последовательность управления синхронизацией зависит также и от наибольшего регистра, что требует дополнительных вычислений.

Вторая атака на алгоритм A5 принадлежит к классу атак с общим названием "балансировка время-память". Применительно к A5 она впервые была предложена югославским математиком Голичем [3]. Атака основана на уже упомянутом раньше парадоксе "дней рождений". Она позволяет находить неизвестное начальное заполнение регистров за определённое время для известного отрезка гаммы на выходе A5.

Атака приводит к успеху, если $T \times M > 2^{64}$, где T и M – требуемое для вычислений время и память в 128-байтных словах, соответственно. Требуемое количество известных последовательностей гаммы при различных кадрах составляет T/102. Трудоёмкость данной атаки составляет порядка 2^{40}. Однако, на каждом шаге требуется решать системы линейных уравнений, так что реальная трудоемкость данной атаки будет выше и, следовательно, не сильно отличается от трудоемкости предыдущей атаки.

Следует также заметить, что эффективная длина ключа Кс, который служит начальным заполнением регистров A5, равна не 64 бита, а только 54, так как последние 10 бит заполняются нулями. Данное ослабление введено умышленно и реализуется в совместном алгоритме A3A8 (аутентификации и формирования ключа).

В заключение приведём несколько предложений, с помощью которых можно уменьшить трудоёмкость выполнения перечисленных выше атак.

Так как число состояний A5 относительно невелико (2^{64}), то атаку Голича можно усовершенствовать следующим образом. Пусть A – это подмножество множества всех возможных состояний алгоритма A5, для каждого из которых на этапе предвычислений найдены все дальнейшие состояния A5. Данную информацию будем сохранять на диске компьютера. Рассматривать же будем множество состояний B, с помощью которых вырабатываются биты реальной выходной последовательности A5. Будем искать совпадения в этих двух множествах, и любое найденное совпадение даст возможность определить фактическое начальное состояние алгоритма A5, используя информацию, записанную на диске.

Можно ускорить поиск совпадений в множествах A и B, используя для этого 64-битные выходные последовательности, вырабатываемые от каждого различного состояния A5, чтобы однозначно определить – порождена ли эта последовательность данным состоянием или нет. Для этого на диске необходимо сохранять только небольшие отрезки выходных последовательностей (от 115 до 179 знаков) и соответствующие им состояния. Такое число знаков выходной последовательности взято из-за того, что первые 100 бит не используются для зашифрования. Следовательно, будем искать совпадения состояний, сравнивая выходные последовательности, сгенерированные от этих состояний (т. е. сравнивая имеющуюся в нашем распоряжении реальную выходную последовательность A5, сгенерированную от искомого начального состояния, и 64-битные блоки, записанные на диске компьютера). Данная процедура поиска происходит быстрее, чем процедура, описанная в атаке Голича.

Укажем на ещё одну слабость алгоритма A5. Так как осуществление сдвига регистра в следующем такте зависит также и от содержимого одной из его ячеек, то алгоритм A5 является сингулярным устройством, т. е. граф его состояний состоит из циклов и хвостов. За счет этого длина периода выходной последовательности алгоритма A5 уменьшается. В общем случае имеется около четырёх различных состояний A5, которые в будущем дают одинаковые состояния. Также некоторые состояния A5 не имеют предшествующих состояний.

Выводы

Проведенный анализ криптостойкости алгоритмов A3A8 и A5, используемых для криптографической защиты информационных ресурсов ССС стандарта GSM, позволяет сделать следующие выводы:

1. Разработанные для использования в стандарте GSM алгоритмы криптопреобразований являются вычислительно стойкими и требуют значительных трудозатрат для их криптоанализа.
2. При разработке алгоритмов криптопреобразований стандарта GSM был допущен ряд ошибок, которые снижают их криптостойкость. Часть ошибок, по всей видимости, допущена случайно (низковесовые многочлены обратной связи, движение регистров зависит только от одного бита в каждом регистре), а часть – сознательно (64-битная длина ключа шифрования Кс, эффективная длина которого в дальнейшем

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

уменьшается до 54 бит).

3. Для криптоанализа алгоритма A3A8 можно применить так называемую атаку с “выбранным вызовом” при условии обеспечения физического доступа к SIM-карте. Данная атака требует формирования $1{,}5 \cdot 10^5$ запросов на SIM-карту и занимает около восьми часов.

4. На сегодняшний день лучшей атакой по восстановлению неизвестных ключевых алгоритма A5 является атака “балансировка время-память”. Трудоёмкость данной атаки является величиной порядка 2^{40}.

Литература: 1. M. Briceno, I. Goldberg, D. Wagner, A pedagogical implementation of A5/1, Springer-Verlag, May 1999. 2. A. Biryukov, A. Shamir, Real Time Cryptanalysis of the Alleged A5/1 on a PC, Computer Science department The Weizmann Institute Rehovot, December 1999. 3. J. Golic. Cryptanalysis of Alleged A5 Stream Cipher. - Proceedings of EUROCRYPT'97, LNCS 1233, pp. 239 - 255, Springer-Verlag 1997.

УДК 638.322

ОПТИМІЗАЦІЯ ПРОГРАМНИХ РЕАЛІЗАЦІЙ АЛГОРИТМУ ГОСТ 28147-89

Сергій Коваль, Олександр Тесленко
Національний технічний університет України "КПІ"

Анотація: **На базі визначення системного статусу програм криптографічних перетворень досліджуються методи досягнення максимальної швидкодії програм, які реалізують на сучасних ПЕОМ алгоритми ГОСТ 28147-89.**

Summary: **Based on examination of system status of cryptographic transformation programs, proposed different methods to achieve maximum productivity of GOST 28147-89 based algorithms.**

Ключові слова: **Криптографія, програмування, суперскалярна архітектура.**

I Вступ

В плануванні та проведенні політики інформаційної безпеки одним із найбільш доступних і поширених напрямків є використання криптографічних перетворень. Розвиток інформаційних технологій обумовлює тенденцію включення криптографічних програм у склад системного програмного забезпечення сучасних ЕОМ. На сьогоднішній день відома велика кількість криптографічних стандартів, які використовуються в криптографічних системах. Згідно з вимогами нормативно правових актів із криптографічного захисту інформації, в нашій державі використовується стандарт криптографічного перетворення ГОСТ 28147-89. Потенційний системний статус програм для криптографічних перетворень потребує ретельного й оптимального програмування алгоритмів стандарту із врахуванням особливостей архітектури конкретних ЕОМ. Зростання пропускної здатності фізичних каналів передачі даних у комп'ютерних мережах вимагає адекватного зростання швидкодії криптографічних програм. У зв'язку з цим велике практичне значення мають дослідження методів програмування, які б забезпечували оптимізацію програм за критерієм швидкодії (продуктивності) при реалізації алгоритмів ГОСТ 28147-89 на сучасних ПЕОМ.

II Основна частина

Оптимізація програм за швидкодією потребує від алгоритму виділення тих його частин, які найчастіше виконуються, а від процесора – виділення ефективної підмножини команд і умов їх виконання, які забезпечують мінімальну кількість тактів процесора.

Алгоритми за ГОСТ 28147-89 характеризуються вкладеною циклічністю, де зовнішній цикл забезпечує послідовну обробку 8-байтних блоків вхідних даних і містить один із трьох базових циклів. В тілі будь-якого із базових циклів багаторазово використовується основний крок криптографічного перетворення, який у свою чергу містить цикл