Чуркин Роман Владимирович
студент
Кротова Елена Львовна
канд. физ.-мат. наук, доцент
ФГБОУ ВПО «Пермский национальный
исследовательский политехнический университет»
г. Пермь, Пермский край

ОЦЕНКА КРИПТОСТОЙКОСТИ АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147-89

***Аннотация**: данная статья посвящена способам криптоанализа ГОСТ 28147–89. Авторами рассмотрены различные способы оценки криптостойкости этого алгоритма.*

***Ключевые слова**: ГОСТ 28147–89, метод «грубой силы», сдвиговая атака, метод «встреча посередине», дифференциальный метод, алгебраический метод.*

В связи с постоянным развитием криптоанализа и усилением мощностей вычислительных средств, все чаще стали успешно проводиться атаки на существующие алгоритмы, что приводит к появлению необходимости появления новых алгоритмов шифрования, либо совершенствования старых. Целью данной работы является проверка алгоритма ГОСТ 28147–89 на криптостойкость в современных реалиях.

ГОСТ 28147–89 относится к алгоритмам шифрования высокой стойкости. Алгоритм, положенный в основу этого стандарта, был разработан в Восьмом Главном управлении КГБ СССР в 1970-х годах. Сам же ГОСТ был введен в 1990 году и используется по сей момент.

Оценка криптостойкости

Метод «грубой силы»

В этом методе проводится перебор всех возможных вариантов ключа, пока не будет найден искомый. ГОСТ 28147–89 имеет 256-битный ключ, который разбивается на 8 блоков по 32 бита. В данном случае необходимо найти 2^{256} вариантов ключа. Необходимый ключ будет найден в результате перебора примерно за 2^{255} тестовых операций шифрования. Если допустить вероятность, что в руках криптоаналитика будет использоваться самый мощный суперкомпьютер современности Тяньхэ-2, занимающий первую строчку в списке TOP500 и имеющий производительность 33.86 петафлопс, с количеством вычислительных ядер 3.12 млн. Проведя подсчеты, было установлено, что, при вычислении ключа, пройдет $3.5*10^{66}$ секунд или $1.1*10^{59}$ лет. Полученный результат свидетельствует о невозможности взлома подбором за разумное время при текущем уровне развития вычислительных систем. Также стоит заметить, что подобный результат был достигнут благодаря большой длине ключа.

Сдвиговая атака

Так как раунды при шифровании ГОСТом имеют лишь незначительные отличия, к нему применим метод «сдвиговой атаки». Этот тип атаки основывается на том, что криптоаналитику известен открытый текст. Отечественные ученые А.Г. Ростовцев и Е.Б. Маховенко нашли большой класс слабых ключей, которые приводят к постепенному уравнению шифрования с периодом 1, 4 или 8 циклов, при использовании которых алгоритм вскрывался с помощью всего 4-х открытых текстов и шифротекстов к ним с достаточно низкой сложностью. Но вероятность использования подобного ключа крайне мала.

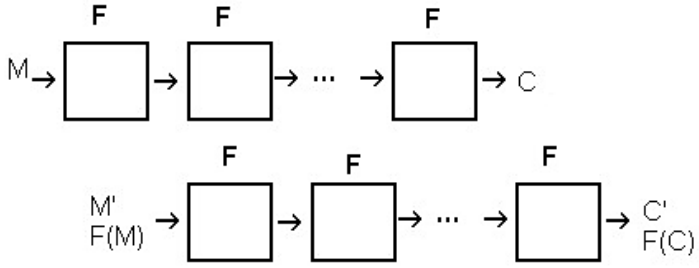

Рис. 1. Сдвиговая атака

Как видно на рис. 1 сдвиговая атака использует принцип что ML = M'R1. Но подобное работает только в том случае, если на каждом раунде используется один и тот же ключ. В ГОСТе же в каждом раунде используется одна восьмая ключа, а в последних 8 раундах, ключ берется в обратном порядке, что делает реализацию подобной атаки не менее трудоемкой, чем методом грубой силы.

Методом сдвиговой атаки был полностью взломан алгоритм упрощенной 20-раундовой версии ГОСТ 28147–89.

Метод «встреча посередине»

Данный метод применяется для атак на блочные шифры и обладает меньшей трудоемкостью, чем метод грубой силы.

В методе Динура-Данкельмана-Шамира используется метод встречи для 8 итераций алгоритма. Пусть при зашифровании алгоритмом ГОСТ открытый текст P после первых 8 итераций переходит сам в себя (P неподвижная точка для первых восьми итераций), тогда выходом после 24 итераций будет по-прежнему P, а выходом после 32 итераций – некоторый шифртекст C. Тогда, учитывая ключевую развертку алгоритма ГОСТ, получаем две пары входа-выхода на 8 итераций алгоритма (P,P) и (∈,P) (∈ и P получены из C и P перестановкой 32-битных полублоков). При случайном равновероятном выборе ключа вероятность того, что P – неподвижная точка для 8 итераций алгоритма ГОСТ равна 2^{-64}.

Следовательно, вероятность того, что на всем доступном материале встретится неподвижная точка для 8 итераций $1-\left(1-\frac{1}{2^{64}}\right)^{2^{64}} \approx 1-e^{-1} \approx 0{,}63$. Общая трудоемкость метода составляет $1.5*2^{192}$ операций зашифрования при необходимом материале известных пар открытого шифрованного текста с вероятность успеха равна 0,63.

Для полного ГОСТа, в 32 итерации, подобный метод трудно применим, в связи с тем, что вероятность встречи неподвижной точки стремится к нулю.

Взлом ГОСТа Николя Куртуа алгебраическими и дифференциальными методами

Алгебраический метод, которым воспользовался Куртуа: на первом этапе используются такие свойства ГОСТ 28147–89, как существование неподвижной точки для части шифрующего преобразования, а также так называемой точки отражения. Благодаря этим свойствам из достаточно большого количества пар открытых-шифрованных текстов выбирается несколько пар, которые позволяют рассматривать преобразования не на 32, а лишь на 8 раундах. Второй этап состоит в том, что по полученным на первом этапе результатам 8-ми раундовых преобразований строится система нелинейных уравнений, неизвестными в которой являются биты ключа. Далее эта система решается. Но в связи с тем, что система из нелинейных уравнений, то ее решение является самым сложным этапом. Трудоемкость именно этого этапа определяет трудоемкость всего метода в целом. Получившиеся результаты оценки трудоемкость показали, что подобный метод ничем не лучше метода грубой силы.

Дифференциальный метод криптоанализа базируется на эксплуатации свойств, используемых в криптографических примитивах нелинейных отображений, связанных с влиянием значения ключа на зависимости между разностями пар входных и пар выходных значений данных отображений. Он использует множество пар текстов анализ которых позволяет выделить некий ключ, либо его фрагмент, который с некоторой вероятностью является искомым, либо близким к искомому. Куртуа использует модифицированный вариант дифференциального метода. Анализ проводится для S-блоков, отличных от действующих и от предложенных в ISO. В работе приводятся дифференциальные характеристики для небольшого числа раундов. Реализация этого метода для большего числа раундов им не проводилась, также, ничем не обосновано заявление Куртуа, что изменение S-блоков не повлияет на стойкость ГОСТа. Кроме того, не проводился анализ S-блоков, которые были в дополнении к стандарту ISO/IEC. При попытке использования других блоков В. Рудским и А. Дмухом, было выяснено, что подобный метод ничем не лучше полного перебора.

Как мы видим, несмотря на то, что развиваются вычислительные мощности, совершенствуются методы криптоанализа, ГОСТ 28147–89, созданный в прошлом веке, все еще остается недосягаем для полного взлома.

Список литературы

1. ГОСТ 28147–89 // Википедия [2016–2016] [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/?oldid=77571017 (дата обращения: 02.05.2016).

2. ГОСТ 28147–89: «Не спеши его хоронить». Часть 1. Стойкость алгоритма // КриптоПро [2000–2016] [Электронный ресурс]. – Режим доступа: https://www.cryptopro.ru/blog/2013/08/27/gost-28147–89-ne-speshi-ego-khoronit-chast-1-stoikost-algoritma (дата обращения 3.05.2016).

3. Криптоанализ ГОСТа 28147–89 // Википедия [2016–2016] [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/?oldid=78069746 (дата обращения: 03.05.2016).

4. Панасенко С.П. Алгоритмы шифрования. Специальный справочник [Текст] / С.П. Панасенко. – СПб.: БХВ-Петербург, 2009 – 81 с.

5. Сдвиговая атака // Википедия [2016–2016] [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/?oldid=78069895 (дата обращения: 02.05.2016).