УДК 681.3.06:519.248.681

ОЦЕНКА ПАРАМЕТРОВ КЛЮЧА КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ

С.В. Дуденко
(представил д.т.н., проф. Ю.В. Стасев)

В статье рассматриваются параметры криптографической системы и проводится оценка её стойкости к атаке методом полного перебора на основе распределенных вычислений с расчетом минимальной длины ключа.

Криптографические системы разрабатываются с учетом требования стойкости к различным видам криптоанализа [1, 2]. Метод полного перебора всех возможных ключей требует от криптоаналитика знания лишь используемой криптографической системы, что обуславливает его широкое использование.

Однако для решения задачи нахождения ключа методом полного перебора необходимы значительные вычислительные ресурсы. Благодаря тому, что данная задача поддаётся распараллеливанию, возникает вопрос о возможности использования сетевых технологий для её решения. Internet, объединяющий многие тысячи рабочих станций, позволяет эффективно решать трудоемкие задачи путем координированной и одновременной работы большого числа компьютеров. Такой подход, реализующий возможности компьютерных сетей, называется методом распределённых вычислений [1]. Быстрое развитие и широкое распространение сетевых технологий и вычислительной техники делает этот метод наиболее перспективным.

В связи с тем, что удельная вычислительная сложность алгоритма шифрования пропорциональна длине ключа и чрезмерное увеличение её ведёт к увеличению временных затрат, задача сводится к определению оптимальной длины. Вычислительно стойкая криптографическая система должна удовлетворять условию $\mathbf{t_\sigma \geq t_{ц.и.}}$, где $\mathbf{t_\sigma}$ – время проведения успешного криптоанализа; $\mathbf{t_{ц.и.}}$ – время ценности информации.

Время ценности информации определяется разработчиком в соответствии с требованиями нормативных документов. Так закон Украины «Про державну таємницю» от 21.01.1994 года определяет сроки в 5, 10, 30 лет. Исходя из этого, будем проводить дальнейшие расчеты.

Длина ключа определяется по формуле

$$l_m = log_m N, \qquad (1)$$

где $\mathbf{m}$ – основание системы исчисления символов ключа; $\mathbf{N}$ – множество ключей, достаточное для противостояния криптоанализу.

Множество ключей можно определить как

$$\mathbf{N} = \left(\mathbf{t_б} \cdot \mathbf{I} \cdot \mathbf{k}\right) / \mathbf{P_д}, \qquad (2)$$

где **I** – сила атаки; **k** – константа, равная количеству секунд в году (31587840); $\mathbf{P_д}$ – допустимая вероятность проведения успешного криптоанализа.

Силу атаки можно определить как **I = f(γ, b)**,где **γ** – количество проверок ключей на одной ЭВМ в секунду; **b** – количество ЭВМ, участвующих в атаке. Сила атаки **I** есть функция от числа ЭВМ, участвующих в криптоанализе, и соответствующей им производительности, которая измеряется количеством производимых проверок ключей в секунду. В конце января 1997 г. компания RSA Data Security, Inc анонсировала криптографический конкурс. Цель конкурса – оценка криптостойкости федерального стандарта США DES [2] и симметричных систем с переменной длиной ключа на основе криптоалгоритма RC5. Так, во время одной из самых сильных атак, проводимой на RC5-32/12/6, пиковая производительность достигала 440 млн. ключей в секунду с привлечением 4500 единиц вычислительной техники [1]. В соответствии с законом Мура, каждые 18 месяцев происходит увеличение производительности вычислительной техники в два раза. Принимая во внимание динамику развития Internet, можно прогнозировать силу атаки на будущее.

Таблица 1

Показатели прогнозируемых атак

Год	2002	2010	2015	2030
Сила атаки (млн.кл./сек)	3520	112640	901120	922746880

Полагая допустимую вероятность проведения успешного криптоанализа, равную единице, и подставив формулу (2) в (1), получим формулу нахождения оптимальной длины ключа

$$\boldsymbol{l}_{\mathbf{m}} = \boldsymbol{log}_{\mathbf{m}}\left(\mathbf{t_{ц.и.}} \cdot \mathbf{I} \cdot \mathbf{k}\right) \qquad (3)$$

Используя данные табл. 1 и соответствующие требования по времени ценности информации, получим таблицу параметров минимальной длины ключа. Строки табл. 2 соответствуют основанию системы исчисления символов ключа, а столбцы времени – силе прогнозируемой атаки (млн.кл./сек).

Таблица 2

Параметры оптимальной длины ключа

$\mathbf{t_{ц.и.}}$ / **I** / **m**	1 год	5 лет		10 лет		30 лет	
	3520	3520	112640	3520	901120	3520	922746880
2	57	60	65	61	69	63	81
4	29	30	33	31	35	32	41
5	25	26	28	26	30	27	35
9	19	19	21	20	22	20	26
10	18	19	20	19	21	20	25

Как видно из табл. 2, ключ длинной 64 бит, поддерживаемый большинством современных криптографических систем (SAFER, FEAL, LOKI и др.), уже не обеспечивает необходимую стойкость. Данные табл. 2 составлены без учета возможности создания специализированной ЭВМ для атаки на определенную криптографическую систему. Так, используя компьютер, созданный для определения ключа DES стоимостью 100 тысяч американских долларов, существует возможность нахождения используемого 56-битного ключа в течение 6 часов [3]. Анализ стоимости проектных работ и разработка архитектуры такой ЭВМ были выполнены Винером [4]. Использование для нахождения ключа суперкомпьютеров подробно рассмотрено в [5]. Например, суперкомпьютер Intel ASCI Red Intel (США), имеющий 7264 процессора, позволяет найти используемый 64-битный ключ в среднем за 3,2 месяца, а 70-битный за 17 лет. Также необходимо учитывать, что в среднем перебор уже 50 % +1 ключей приводит к успеху.

Однако помимо проблемы времени, затрачиваемого на перебор всего пространства ключей, задача поиска используемого ключа имеет другой аспект. Криптоаналитик должен иметь возможность распознать дешифрованное сообщение как открытый текст. Если дешифрованное сообщение представляет собой обычный текст (русский, английский и т.д.) то задача решается довольно просто. Если же текстовое сообщение перед шифрованием было каким-то образом сжато, то проблема распознавания открытого текста усложняется, а если был зашифрован файл, содержащий числовые данные, то задача автоматизации процесса распознавания становится практически невыполнимой. Поэтому для применения метода полного перебора ключей криптоаналитик должен обладать априорной информацией о структуре и содержании открытого текста.

Основываясь на проведенных расчётах и в соответствии с международными требованиями, на сегодняшний день криптографическая система должна поддерживать минимальную длину ключа, равную 128 бит, с возможностью генерирования ключей длинной в 192 и 256 бит.

ЛИТЕРАТУРА

1. *Чмора А.Л. Современная прикладная криптография – М.: Гелиос АРВ, 2001. – 256 с.*
2. *Алфёров А.П. Основы криптографии – М.: Гелиос АРВ, 2001. – 480 с.*
3. *Столлингс В. Криптография и защита сетей: принципы и практика. – М.: Изд. дом "Вильямс", 2001. – 672 с.*
4. *Wiener M. Efficient DES Key Search // Proc. of Crypto'93 published by Springer-Verlag, 1993.*
5. *Пудовченко Ю.Е. Когда наступит время подбирать ключи // Защита информации. Конфидент. – 1998. – № 3 (21). – С. 65 - 72.*

Поступила 29.04.2002

***ДУДЕНКО Сергей Васильевич**, адъюнкт ХВУ. В 1995 году окончил ХВУ. Область*

научных интересов – способы и средства безопасной передачи данных в информационно-вычислительных сетях.