УДК 681.3.06

ИССЛЕДОВАНИЕ СТОЙКОСТИ АЛГОРИТМОВ ШИФРОВАНИЯ ПРИ ИСПОЛЬЗОВАНИИ СОВРЕМЕННЫХ ЭВМ

А.А. Смирнов[1], В.Ю. Ковтун[2]
([1]Кировоградский национальный технический университет,
[2]Харьковский университет Воздушных Сил им. И. Кожедуба)

В статье проводится исследование стойкости симметричных алгоритмов шифрования со случайным ключом к криптоанализу с использованием высокопроизводительных вычислительных систем.

стойкость симметричных алгоритмов шифрования, криптоанализ

Формулировка проблемы. В современных автоматизированных системах управления, защита от несанкционированного доступа, обеспечение целостности и достоверности информации, осуществляется посредством применения системы защиты информации, особое место в которой принадлежит программно-техническому комплексу защиты информации. В его основу положены криптографические преобразования информации. Как известно, все криптографические преобразования характеризуются их стойкостью к вскрытию и производительностью. В дальнейшем, наше внимание будет обращено к вопросам обеспечения стойкости и криптоанализу, а именно объемам перебора ключей. **Анализ литературы** [1, 2] показал, что, в связи с развитием информационных технологий и математических методов криптоанализа, существующие оценки времени взлома современных, как симметричных, так и асимметричных криптоалгоритмов, с использованием высокопроизводительных вычислительных систем требуют уточнения. **Целью статьи** является получение временных оценок взлома критопреобразований со случайным ключом с использованием современных вычислительных систем.

Основной материал. Как известно, существующие на сегодняшний момент подходы к криптоанализу основываются на переборе некоторого объема ключей, отличие их состоит лишь в некоторых начальных предположениях, направленных на уменьшения объема перебора. Для осуществления перебора большого объема ключей потребуются значительные вычислительные ресурсы. До недавнего времени, вычислительные ресурсы являлись стратегическим ресурсом государств и транснациональных компаний, но со временем, большинство серьезных университетов и компаний среднего уровня обзавелись своими суперкомпьютерами. В открытой печати начали публиковаться перечни (TOP 500) пятисот самых мощных в мире эксплуатируемых суперкомпьютеров и крупнейших суперкомпьютерных центров (СКЦ) мира

[3]. Для составления списка используется достигнутая максимальная производительность по тесту Linpack parallel. Также большое внимание следует уделить существующим инициативным программам по привлечению незадействованных вычислительных мощностей пользователей сети Internet [4].

Введем классификацию суперкомпьютеров по следующим признакам: страна-обладатель, технологическая реализация, операционная система, область применения. Все результаты исследований отображены в приведенных ниже табл. 1 – 6.

Таблица 1

Страны – обладатели суперкомпьютеров

	кол.	%	$R_{max\ Sum}$ (GF)	$R_{peak\ Sum}$ (GF)	Processor Sum
США	305	61,00%	1569959	2317312	522894
Великобритания	41	8,20 %	124409	235390	42328
Германия	24	4,80 %	71303	96227	15820
Япония	21	4,20 %	139417	191946	33243
Китай	17	3,40 %	59542	101137	16934
Австралия	11	2,20 %	34460	54919	8394
Израиль	9	1,80 %	23514	43270	6452
Франция	8	1,60 %	23512	36572	7930
Южная Корея	7	1,40 %	31599	44044	5152
Канада/Италия	по 6	по 1,20 %	22048/14537	41424/23252	6708/4740
Бразилия/Индия/ Голландия/Новая Зеландия/ Саудовская Аравия/Швейцария	по 4	по 0,80 %	12409/11379/ 33320/9883/ 11966/34368	23669/21691/ 43177/23520/ 24518/48526	3844/3354/ 13760/3768/ 3936/14888
Мексика/Тайвань	по 3	по 0,60 %	6078/7562	11861/12205	2118/2152
Бельгия/Ирландия/ Норвегия/Испания	по 2	по 0,40 %	4651/5515/ 4025/29771	8320/8052/ 7200/44386	1300/1680/ 1000/4924
Россия/Беларусь/ Болгария/Финляндия/ Индонезия/ЮАР/Швеция	по 1	по 0,20 %	5355/2032/ 1860/1710/ 1789/1716/4999	8131/2534/ 3328/1824/ 3200/2304/6025	924/576/ 640/304/ 500/384/886
Всего	500	100%	2304687,73	3489965,54	731533

Из табл. 1 видно, что лидирующие позиции занимает США. Из стран бывшего СССР представлены только Россия и Белоруссия, занимающие 24 и 25 места. Прослеживается четкая зависимость между местом, занимаемым теми или иными странами в рассматриваемом списке, и уровнем инвестиций в информационные технологии в этих странах (США – 305 суперЭВМ (61%)). Классифицируем суперкомпьютеры по архитектуре и технологической реализации (табл. 2 – 4). Подавляющее большинство реализовано на скалярной архитектуре процессоров – 486 (97%), и лишь 14 реализовано на векторной. По типам архитектуры: Cluster – 360 (72%), MPP – 104(20,8%), Constellations – 36 (7,2%). Как видно из табл. 3, подавляющее число вычислительных систем построены на базе процессоров, производимых США. При этом, лидером является корпорация Intel, производящая 57% процессоров. Однако суперЭВМ строятся не на одном процессоре, а на нескольких десятках, а то и сотнях тысячах.

Таблица 2

Коммуникационные интерфейсы (interconnect technology family)

	кол.	%	$R_{max\ Sum}$ (GF)	$R_{peak\ Sum}$ (GF)	Processor Sum
Gigabit Ethernet	249	49,80%	611419	1177332	191564
Myrinet	101	20,20%	334534	507047	91244
SP Switch	42	8,40%	261965	389900	67226
Infiniband	27	5,40%	127772	189024	28592
Proprietary	20	4,00%	529656	679042	253344
Crossbar	17	3,40%	113869	146822	15866
NUMAlink	15	3,00%	65645	72120	11632
Quadrics	14	2,80%	89107	116831	30052
Cray Interconnect	7	1,40%	91443	111550	24620
Mixed	4	0,80%	69794	88086	14640
RapidArray	3	0,60%	7430	9159	2081
Fireplane	1	0,20%	2054	3053	672

Таблица 3

Семейства процессоров

	кол.	%	$R_{max\ Sum}$ (GF)	$R_{peak\ Sum}$ (GF)	Processor Sum
Intel IA-32	205	41,00%	561624	1052342	184712
Intel EM64T	82	16,40%	248458	414068	58864
Power	73	14,60%	877775	1205294	327622
AMD x86-64	55	11,00%	231067	312109	68789
Intel IA-64	46	9,20%	215683	266919	45064
PA-RISC	17	3,40%	29671	54944	14784
Cray	8	1,60%	44734	53267	3034
Alpha	4	0,80%	24487	34416	15160
NEC	4	0,80%	48955	54456	6072
Sparc	4	0,80%	18872	38062	6112
Hitachi SR8000	2	0,40%	3362	4090	1320

В табл. 4 отображено соотношение количества суперкомпьютеров к числу процессоров, используемых в них.

Таблица 4

Число процессоров

	кол.	%	$R_{max\ Sum}$ (GF)	$R_{peak\ Sum}$ (GF)	Processor Sum
33-64	2	0,40%	6615	11533	106
65-128	6	1,20%	18267	21510	704
129-256	4	0,80%	10524	12030	920
257-512	126	25,20%	248872	367718	58016
513-1024	252	50,40%	713390	1201633	200521
1025-2048	67	13,40%	318488	520525	99490
2049-4096	26	5,20%	236229	375824	75808
4k-8k	10	2,00%	199135	277587	70736
8k-16k	5	1,00%	181279	219917	53200
32k-64k	1	0,20%	91290	114688	40960
64k-128k	1	0,20%	280600	367000	131072

В табл. 5 приведена классификация областей применения вычислительных комплексов, далее приведены операционные системы, под которыми работают приведенные в TOP 500 вычислительные системы (табл. 6).

Таблица 5

Область применения

	кол.	%	$R_{max\ Sum}$ (GF)	$R_{peak\ Sum}$ (GF)	Processor Sum
Не указана	257	51,40%	1558099	2225933	498421
Геофизика	47	9,40%	116100	237754	39374
Финансы	43	8,60%	107148	192693	31956
Полупроводники	38	7,60%	80141	155202	25986
Исследование погоды и климата	17	3,40%	79964	127411	17790
Телекоммуникации	16	3,20%	36460	63430	10966
Эталонное тестирование	13	2,60%	26980	35905	6536
Базы данных	11	2,20%	23047	42427	7338
Игры	7	1,40%	20918	37421	6068
Обработка информации	6	1,20%	116741	147227	47656
Создание цифрового содержания	6	1,20%	13161	20332	3564
Автомобили	5	1,00%	10587	16736	3152
Оборона	5	1,00%	9430	15155	2624
Создание изображений	4	0,80%	7992	18577	3338
Исследования	4	0,80%	20625	28755	7768
Цифровая носители	4	0,80%	12350	22219	3884
Энергия	3	0,60%	10017	13766	2696
Науки для жизни	3	0,60%	5527	9382	1328
Космические исследования	2	0,40%	7118	14156	2624
Информационные услуги	2	0,40%	3594	6656	1664
Прогноз погоды	2	0,40%	6228	11494	1856
CFD	1	0,20%	16180	24576	3072
Экономика	1	0,20%	1980	2112	352
Медиа	1	0,20%	3755	7200	1000
Программное обеспечение	1	0,20%	8893	10752	80
Развлечения	1	0,20%	1652	2693	440
По направлениям применения					
Промышленность	265	53,00%	660673	1220885	206417
Исследования	121	24,20%	1170835	1586233	394322
Академическое	71	14,20%	355746	519099	98730
Секретное	22	4,40%	50902	72541	12760
На продажу	17	3,40%	52544	68545	15640
Правительственное	4	0,80%	13988	22662	3664

Таблица 6

Операционные системы

	кол.	%	$R_{max\ Sum}$ (GF)	$R_{peak\ Sum}$ (GF)	Processor Sum
Linux	371	74,20%	1194684	1977196	333177
Unix	100	20,00%	469944	689596	137968
Mixed	19	3,80%	551787	702971	246400
Mac OS	5	1,00%	37228	60995	72
BSD Based	4	0,80%	48955	54456	6072
Windows	1	0,20%	2090	4752	660

Мы рассмотрели список самых мощных в мире компьютеров столь подробно и разносторонне не случайно. Он послужит нам отправной точкой для исследования стойкости алгоритмов шифрования со случайным ключом в случае использования для их взлома современных ЭВМ. Допустим, что рассматриваемые нами криптопреобразования идеальны, то есть оптимальным методом их взлома будет прямой перебор всех возможных ключей данного алгоритма. Очевидно, что в этом случае стойкость криптосистем будет определяться длиной ключа. При проведении данного исследования предполагалось, что криптоаналитик обладает всей информацией относительно используемого алгоритма, за исключением данных о секретном ключе, и ему доступно для анализа закрытое сообщения. Предполагается, что идеальный алгоритм лишен каких-либо недостатков, снижающих его стойкость. Предположим также, что генерация ключа компьютером происходит за один такт его работы, а операция дешифрования мгновенна. Определив отношение количества ключей к быстродействию самого мощного компьютера, мы получим нижнюю оценку сложности дешифрования сообщения для идеального алгоритма. По некоторым оценкам производительность компьютера, деленная на его стоимость, увеличивается в 10 раз за каждые 5 лет [2].

Определим, что $x(t)$ – непрерывная функция, показывающая быстродействие компьютеров в момент времени t. Исходя из принятой гипотезы и начальной точки отсчета ($t_0 = 0$ в 1946 г.), функция выглядит следующим образом: $x(t) = C_0 \cdot 10^{t/5}$, где начальная точка отсчета $C_0 = 100$ мощность первого компьютера ЭНИАК.

Введем следующие обозначения: S – мощность алфавита, из которого извлекаются символы для ключа; l – длина ключа; $\|\{K\}\| = s^l$ мощность множества ключей; $T_M(\{K\}, x(t))$ – максимальное время перебора ключей; $D(\{K\}, x(t))$ – математическое ожидание времени дешифрования; t_{opt} – оптимальный момент времени начала дешифрования; $T_b(\{K\}, x(t))$ – время безопасности системы (зависит от двух параметров времени начала дешифрования t и его длительности D).

При сделанных предположениях время перебора всех ключей в заданном ключевом пространстве в момент t (максимальное время дешифрования сообщения) составит $T_м = ||\{K\}||/x(t)$, а среднее время дешифрования сообщения половину максимального времени: $D = 1/2\ T_м = 1/2\ (||\{K\}||/x(t))$. Исходя из прогноза об увеличении мощности компьютерных средств, можно было бы просто принять за основу, что длительность перебора через 100 лет должна составить некоторое заранее за-

данное время, например один год, и составить следующее уравнение типа $||\{K\}||/C_1 \cdot x(t + 100) > 1$, из которого следует, что необходимая длина ключа должна быть 136 – 137 бит. Однако, можно дать более точные и полезные оценки для того, чтобы не расходовать впустую силы на те задачи, время которых еще не пришло.

Рабочая модель для расчета времени безопасности системы шифрования (1) состоит из суммы двух действующих факторов момент начала дешифрования плюс сложность дешифрования. Минимум этой функции назовем максимальным временем безопасности $T_б$ идеальной системы шифрования. Прилагательное "максимальный" введено только для того, чтобы подчеркнуть идеальность исследуемых алгоритмов – в реальной жизни криптосистемы обладают определенными недостатками, снижающими их криптостойкость. Коэффициент $C_1 = 31\ 536\ 000$ возникает при переходе от операций в секунду к операциям в год, и используется в основном для удобства.

$$T_б = \left[t + \frac{\|\{K\}\|}{2 \cdot x(t) \cdot C_1} \right] \to \min. \qquad (1)$$

Для определения минимума этой функции найдем ее производную и решим уравнение $T_б = 0$.

В результате решения и упрощения получаем следующее значение момента времени t_{opt}, в котором достигается минимум функции $T_б$, то есть оптимальное время начала криптоанализа:

$$t_{opt} = 5 \lg \left[\frac{\|\{K\}\| \cdot \ln(10)}{10 \cdot C_1} \right]. \qquad (2)$$

Подставив $||\{K\}||$ в эту формулу, можно получить значение момента времени t_{opt}. Время безопасности идеальной системы шифрования определяется значением функции $T_б$ в этой точке. Подставив в (1) мощность множества ключей $||\{K\}||$ в исследуемой системе и значение t_{opt} можно найти ее время безопасности $T_б$.

Среднее время дешифрования определяется по следующей формуле:

$$D = \left[\frac{\|\{K\}\|}{2 \cdot C_1 \cdot x(t_{opt})} \right]. \qquad (3)$$

Самый неожиданный и интересный факт, на наш взгляд, заключается в том, что, если подставить значение t_{opt} в формулу (3) и произвести необходимые упрощения, то длительность начатого в оптимальный момент дешифрования, независимо от длины ключа, всегда одна и та же:

$5 / \ln 10 = 2{,}171472409516$ года (739,13 дней или 19 035,12 часов).

Стойкость (в годах) алгоритмов с различной длиной ключа, исходя из наших оценок, приведена в табл. 7.

Таблица 7

Стойкость алгоритмов с различной длиной ключа

Длина ключа (бит)	Кол-во ключей	Оптим. время начала дешифрования	Длительность дешифрования	Окончание дешифрования
70	1,18 * E 21	64,7 (2010,7 г.)	2,17	66,87 (2012,87 г.)
75	3,78 * E 22	72,2 (2018,2 г.)	2,17	74,37 (2020,37 г.)
90	1,24 * E 27	94,8 (2040,8 г.)	2,17	36,96 (2042,87 г.)
128	3,4 * E 38	152 (2098 г.)	2,17	94,15 (2100,17 г.)
137	1,74 * E 41	165,5 (2111,5 г.)	2,17	167,69 (2113,69 г.)
256	1,15 * E 77	344,6 (2290,6 г.)	2,17	286,79 (2292,77 г.)

Выводы. Таким образом, проведенные исследования современного состояния вычислительных мощностей суперЭВМ, а также введение рабочей модели, позволяет оценить надежность проектируемых и эксплуатируемых систем защиты информации в автоматизированных системах управления, что является одним из основных факторов при их разработке.

ЛИТЕРАТУРА

1. *Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996. – [Электр. ресурс]. – Режим доступа: http://cacr.math.uwaterloo.ca/hac.*
2. *Головашич С.А. Безопасность режимов блочного шифрования // Радиотехника. – 2001. – Вып. 119. – С. 135-145.*
3. *Top 500 supercomputers site. – [Электр. ресурс]. – Режим доступа: http://www.top500.org.*
4. *Differential-linear cryptanalysis, Langford, S. K. and Hellman, M. E. Advances in Cryptology Crypto '94, 1994.*

Поступила 4.04.2006

Рецензент: доктор технических наук, профессор В.В. Сидоренко, Кировоградский национальный технический университет.