УДК 003.26

С. М. Калиновский

Институт бизнеса БГУ, *Минск*, *Беларусь*, *kalina19901958@gmail.com*

КЛАССИФИКАЦИЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ ПО СТОЙКОСТИ

В работе дается классификация криптографических систем по стойкости. Дается понятие криптографической стойкости. Определены условия для существования криптографических безусловно стойких (*абсолютных*, *теоретически недешифруемых*) *систем и требования к условно стойким криптографическим системам. Приведены достоинства и недостатки стойких криптографических систем.*

Ключевые слова: *криптографическая стойкость*, *криптографическая система*, *криптографический алгоритм*, *энтропия*, *криптографический ключ*, *криптограмма*

S. Kalinouski

School of Business of BSU, *Minsk*, *Belarus*, *kalina19901958@gmail.com*

CLASSIFICATION OF CRYPTOGRAPHIC SYSTEMS BY STRENGTH

The paper gives a classification of cryptographic systems by strength. The concept of cryptographic strength is given. Conditions for the existence of cryptographic unconditionally secure (*absolute*, *theoretically indecipherable*) *systems and requirements for conditionally secure cryptographic systems are determined. The advantages and disadvantages of strong cryptographic systems are given.*

Keywords: *cryptographic strength*, *cryptographic system*, *cryptographic algorithm*, *entropy*, *cryptographic key*, *cryptogram*

В сфере информационных технологий используются криптографические методы. В настоящее время они применяются не только для зашифрования сообщений, но и в других областях жизнедеятельности человека. Криптографические методы работают в банковской сфере при использовании платежных карт, для проведения различных транзакций, аутентификации, цифровой электронной подписи, в обеспечении информационной безопасности, при проведении жеребьевки и других отраслях.

Во многом практическое использование этих методов зависит от их стойкости. Стойкость – это способность криптографической системы противостоять попыткам ее математического анализа. От стойкости криптографических систем зависит сам факт получения информации из криптограммы. Если стойкость слабая, то имеется вероятность получения из перехваченных сообщений достоверных сведений. Классическим примером вскрытия криптографических систем является чтение переписки, зашифрованной немецкой шифровальной машиной «Энигма».

Оценка стойкости криптографической системы является задачей очень трудной, так как отсутствуют критерии такой оценки. Никто с полной уверенностью не может определить надежность криптографических систем, поэтому установлены меры по определению условий дешифруемости криптосистемы.

Эти условия выработал в своих работах американский инженер, криптоаналитик и математик К. Шеннон, используя энтропийный подход. Были определены условия для существования криптографических безусловно стойких (абсолютных, теоретически недешифруемых) систем. Такие системы не могут быть вскрыты без знания ключа даже с учетом перехвата крипто-

грамм и использованием бесконечных вычислительных возможностей по их математическому анализу.

Рассмотрим энтропию дискретного сигнала.

Энтропия системы, имеющей N возможных состояний

$$H(x) = -\sum_{i=1}^{N} p(i) \log p, \tag{1}$$

где $p(1), p(2), \ldots p(i), \ldots p(N)$ – вероятность появления элементов алфавита $x_1, x_2, \ldots x_i \ldots x_N$.

Для случая, когда вероятность появления для всех элементов алфавита одинакова

$$p(1) = p(2) \ldots = p(N) = \frac{1}{N} \tag{2}$$

отсюда

$$H(x) = -\sum_{i=1}^{n} \left(\frac{1}{N}\right) \log\left(\frac{1}{N}\right) = \log N. \tag{3}$$

Необходимые условия существования безусловно стойкой (абсолютной, теоретически недешифруемой) системы:

1. Система является безусловно стойкой, если любая криптограмма не добавляет сведений, зашифрованных в этой криптограмме.

$$I(E, M) = 0, \tag{4}$$

где I – количество информации; E – криптограмма; M – сообщение.

Количество информации при перехвате криптограммы равно нулю без знания ключа.

$$I(E, M) = H(M) - H(M / E), \tag{5}$$

где $H(M)$ – энтропия источника сообщения; $H(M / E)$ – условная энтропия сообщения, если перехвачена криптограмма.

Также можем сказать, что $P(M) = P(M / E)$, т. е. знание криптограммы не изменяет вероятность сообщения.

2. Количество ключей должно быть не меньше количества сообщений

$$L^N \geq m^n, \tag{6}$$

где L – объем алфавита ключевых данных; N – длина ключа; m – объем алфавита сообщения; n – длина сообщения.

3. Длина ключа должна быть не меньше длины сообщения.

Прологарифмируем неравенство

$$\log L^N \geq \log m^n \tag{7}$$

отсюда длина ключа равна

$$N \geq \frac{n \log m}{\log L}. \tag{8}$$

Достоинства безусловно стойких криптографических систем:

1. Абсолютная (теоретическая) стойкость применяемых систем, позволяющих с гарантией недешифруемости передавать и хранить любые данные.

2. Достаточно просты в изготовлении и применении.

Недостатки безусловно стойких криптографических систем:

1. Большой объем ключевой информации,

2. Сложность организационной структуры доставки ключевой информации.

Исходя из этого, такие системы применяются для шифрования наиболее важных конфиденциальных сведений. Наиболее широкое использование получили условно стойкие криптографические системы, которые практически могут быть вскрыты, но в течение необозримо большого времени и при условии проведения математического анализа на множестве вычислительных средств. Необозримо большое время – это время в течение которого полученные сведения уже никому не будут нужны, например, 200 лет.

При их применении должны соблюдаться следующие требования:

1. Количество ключей должно быть непереборно велико.

Требование выполняется достаточно просто. Если взять ключ длиной 256 бит, то общее число ключей будет равно 2 256 = 1,16 · 1 077, при работе на ЭВМ производительностью 106 бит в секунду полное время перебора составит 3,67 · 1 063 лет. Если скорость работы ЭВМ повысить на 3 порядка, т. е. к производительности 109 бит в секунду, то длину ключа необходимо увеличить на 10 бит. При использовании для математического анализа 1 012 компьютеров существенного влияния на вывод о непереборности не окажет.

Таблица 1

Зависимость количества попыток перебора ключа от его длины

Длина ключа	Количество попыток
58	288 230 376 151 711 744
59	576 460 752 303 423 488
60	1 152 921 504 606 846 976
61	2 305 843 009 213 693 952
62	4 611 686 018 427 387 904
63	9 223 372 036 854 775 808
64	18 446 744 073 709 551 616
65	36 893 488 147 419 103 232

Из табл. 1 [7] видно, что при увеличении длины ключа на 1 бит количество попыток перебора ключа увеличивается примерно в 2 раза.

2. Статистика сообщений должна быть исключена из статистики криптограммы.

Пусть применяется шифр простой замены, который имеет в русском алфавите 32! = = 2,63´1035 возможных комбинаций. Полный перебор занял бы много времени.

Однако по частоте появления букв в русском алфавите можно легко вычислить переданное сообщение. Частота появления русских букв показана в табл. 2 [6]. Для этого необходимо посчитать частоту повторения букв в криптограмме. Букву с самой большой частотой принять за пробел или знак препинания, с чуть меньшей за «о», с самой меньшей за «э» или «щ» и так далее по тексту криптограммы. Чем больше объем криптограммы, тем больше статистики и тем легче эта криптограмма дешифруется. Кроме того, необходимо учитывать избыточность русского языка, ведь многие слова можно, например, представить без гласных букв, и они будут понятны.

Таблица 2

Частота появления русских букв

Буква	Частота	Буква	Частота	Буква	Частота	Буква	Частота
о	0,09	в	0,038	з	0,016	ж	0,007
е	0,072	л	0,035	ы	0,016	ш	0,006
а	0,062	к	0,028	б	0,014	ю	0,006
и	0,062	м	0,026	ь, ъ	0,014	ц	0,004
н	0,053	л	0,025	г	0,013	щ	0,003
т	0,053	п	0,023	ч	0,012	э	0,003
с	0,045	у	0,021	й	0,01	ф	0,003
р	0,04	я	0,018	х	0,009		

Вероятность появления пробела и знаков препинания – 0,174.

3. Криптографические системы должны не подлежать дешифрованию и в том случае, когда известны некоторые части открытой информации, переданные в перехваченной криптограмме.

Знание части сведений, зашифрованных в криптограмме не должно влиять на возможность вскрытия некоторых ключевых данных для дешифрования следующей части криптограммы. При невыполнении этого требования криптографическая стойкость криптосистемы значительно уменьшится.

4. Исключение так называемого «чтения назад».

Требование предполагает, что знание (захват) криптографических средств, алгоритмов и протоколов без знания ключа не дает возможности вскрыть уже переданные сообщения.

Существуют также криптографические системы временной стойкости, которые не относятся к безусловно и условно стойким.

Криптографические системы по стойкости можно разделить на три класса:

1) безусловно стойкие (абсолютные, теоретически недешифруемые) криптографические системы;

2) условно стойкие криптографические системы;

3) криптографические системы временной стойкости.

У безусловно и условно стойких криптографических систем существуют свои достоинства и недостатки, однако, они нашли свое применение в информационных системах для гарантированного закрытия информации различного характера. Использование криптографических систем временной стойкости ограничено, время их работы определяется необходимостью закрытия информации хотя бы на небольшой срок.

Предложенная классификация может быть применена для выбора класса криптографической системы при проектировании информационной системы.

Список использованных источников

1. *Харин*, *Ю. С.* Математические основы криптологии / Ю. С. Харин, В. И. Берник, Г. В. Матвеев. – Минск : БГУ, 1999. – 319 с.

2. *Гатченко*, *Н. А.* Криптографическая защита информации / Н. А. Гатченко, А. С. Исаев, А. Д. Яковлев. – СПб. : НИУ ИТМО, 2012. – 142 с.

3. *Шеннон*, *К.* Теория связи в секретных системах [Электронный ресурс]. – Режим доступа: https://www.enlight.ru/crypto/articles/shannon/shann__i.htm. – Дата доступа: 03.04.2023.

4. *Салий*, *В. Н.* Криптографические методы и средства защиты информации [Электронный ресурс] / В. Н. Салий. – Режим доступа: https://www.sgu.ru/sites/default/files/textdocsfiles/2017/10/18/saliy_v.n._kriptograficheskie_ metody_i_sredstva_zashchity_informacii.pdf. – Дата доступа: 03.04.2023.

5. *Шурховецкий*, *Г. Н.* Криптостойкость алгоритмов шифрования [Электронный ресурс] / Г. Н. Шурховецкий. – Режим доступа: https://mnv.irgups.ru/sites/default/files/articles_pdf_files/shurhoveckiygnkriptostoykost_algoritmov_shifrovaniya.pdf. – Дата доступа: 03.04.2023.

6. Основные понятия криптографии [Электронный ресурс]. – Режим доступа: https://studfile.net/preview/5388759/#:~:text=Относительная%20частота%20появления%20пробела%20или,сообщение%20или%20набор%20случайных%20символов. – Дата доступа: 03.04.2023.

7. Влияние длины ключа [Электронный ресурс]. – Режим доступа: http://deepedit.ru/vliyanie-dliny-klyucha.html. – Дата доступа: 03.04.2023.