ВЗАИМОСВЯЗЬ ХАОТИЧЕСКИХ СИСТЕМ И КРИПТОГРАФИИ

Г. Д. Когай, Т. Л. Тен, А. М. Буркитбаев

Карагандинский экономический университет Казпотребсоюза

В данной статье выявляется взаимосвязь между объектами изучения в теории хаоса и криптографии. Сделаны выводы о возможности использования траектории динамических систем с хаосом для представления и передачи информации. Цель исследования рассмотреть общие понятия хаотической системы, изучить различия между криптографией классической и криптографией на осноке теории хаоса. Актуальность исследования в том, что известные свойства хаотических систем, таких как экспоненциальное расхождение траекторий, эргодичность, смешивание, можно использовать в криптографии при разработке новых схем шифрования.

Ключевые слова: *криптография, теория хаоса, безопасность, генератор, псевдослучайность, энтропия.*

INTERRELATION CHAOTIC SYSTEMS AND CRYPTOGRAPHY

G. D. Kogay, T. L. Ten, A. M. Burkitbayev

Karaganda Economic University of Kazpotrebsouz

This article reveals the relationship between the objects of study in chaos theory and cryptography. Conclusions on the possibility of using the trajectories of dynamic systems with chaos for representing and transmitting information. The purpose of the study to consider the general concept of a chaotic system, examine the differences between the classical cryptography and cryptography based on chaos theory. Urgency studies that known properties of chaotic systems, such as the exponential divergence of the trajectories, ergodicity, mixing, can be used in the development of new cryptography encryption schemes.

Keywords: *cryptography, chaos theory, security, generator, pseudorandomness, entropy.*

Криптография занимается проблемой защиты информации путем ее преобразования. Криптография решает задачи конфиденциальности, аутентификации, целостности и ряд других с ними связанных. Практическая криптография изучает методы шифрования данных, управления ключами и сертификатами, создания цифровой подписи. Криптоанализ решает условно противоположенные задачи, в частности, преодоление защиты и несанкционированное дешифрование данных (без знания ключа) [1].

Все имеющиеся традиционные системы криптозащиты (методы шифрования, генераторы псевдослучайных чисел) можно рассматривать как динамические системы, в которых осуществляется преображение открытого текста в шифротекст (таблица 1).

Таблица 1.

Взаимозависимость объектов изучения в теории хаоса и криптографии

Теория хаоса	*Криптография*
Хаотическая система	Псевдохаотическая система
– нелинейное преобразование	– нелинейное преобразование
– бесконечноечислосостояний	– конечноечислосостояний
– бесконечноечислоитераций	– конечноечислоитераций
Начальное состояние	Открытый текст
Заключительное состояние	Шифротекст
Начальные условия и параметры	Ключ
Асимптотическая независимость начального и конечного состояний	Запутывание
Чувствительность к начальным условиям и параметрам, смешивание	Распыление

Можно предположить, что известные характеристики систем хаоса, таких как экспоненциальное расхождение траекторий, эргодичность, смешивание, окажутся нужными в криптографии, например, при разработке свежих методов шифрования) [2].

С точки зрения акцентов и объектов исследования, между криптографией и теорией хаоса имеются фундаментальные различия:

1) криптографияисследуетэффектконечногочислаитерационныхпреобразований (п <∞), тогда как теория хаоса исследует асимптотическое поведение системы (п →·∞);

2) классические системы хаоса представляются неким множеством (объектом) фазового пространства, который чаще всего может иметь дробную размерность, другими словами являться фракталом. В криптографии же используются всевозможные комбинации переменных, не зависящих друг от друга, что позволяет сделать систему максимально непредсказуемой (рис. 1);

3) в компьютерной криптографии рассматриваются системы с конечным числом состояний, а пространство состояний систем хаоса задаются бесконечным множеством непрерывных или дискретных значений. Из этого следует, что все модели хаоса, реализованные при помощи компьютера, являются приближенными.

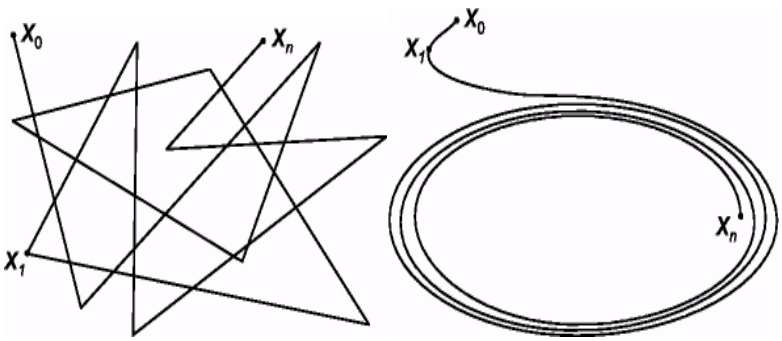

Рис. 1. Фазовые портреты криптографической и хаотической систем

Идеальная безопасность объекта возможно только в том случае, если он абсолютно непредсказуем для внешнего наблюдателя, то есть криптоаналитика. Это предполагает, что все вероятные состояния в равной степени возможны и не зависят от предыдущих состояний. Иначе говоря, последовательность состояний характеризуется равномерным законом распределения вероятности и не имеет корреляций (паттернов). Понятие абсолютной непредсказуемости равносильноистинной случайности. Кроме того, истинно случайную последовательность часто называют белым шумом. Источником может быть хаотическая система, имеющая большое количество степеней свободы. К примеру, замкнутая система с идеальным газом [3].

В реальном мире, криптографические системы обеспечивают некоторую практическую безопасность, которая гораздо слабее и меньше, чем идеальная. Это обусловлено эксплуатационной и экономической целесообразностью. Понятия случайности и непредсказуемости соответственно сменяются на псевдослучайность и вычислительную непредсказуемость. Выходит, что псевдослучайный объект не отличим от истинно случайного объекта при помощи доступных вычислительных средств криптоаналитика. Аналогично, поведение вычислительно непредсказуемого объекта не может быть спрогнозированно вычислительными средствами криптоаналитика.

Естественно, истинно случайный объект является алгоритмически случайным и псевдослучайным (рис. 2). Но понятия псевдослучайности и алгоритмической случайности различны: псевдослучайная строка создается компактным генератором, но аналитикоказывается не в состоянии построить этот генератор и спрогнозировать эту последовательность.

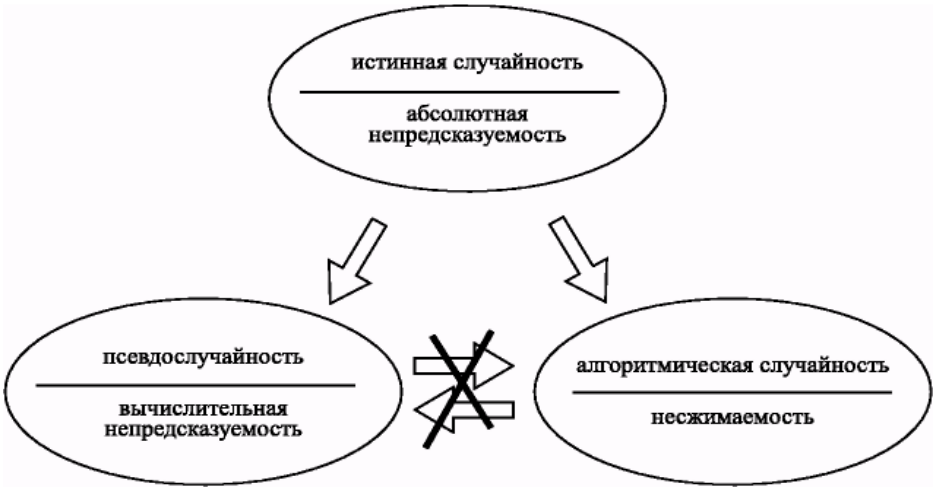

Рис. 2. Эквиваленты классов понятий

Естественный хаос (вещество, природа, вселенная) обладает колоссально громадной размерностью, бесконечным количеством

состояний и невообразимой сложностью «системы итерационных функций» [4]. Однако, благодаря самоорганизации, энтропия таких систем гораздо меньше, чем у «совсем случайной» системы того же масштаба. Многомерные хаотические системы нельзя использовать в шифровании, так как они не репродуцируемы. С другой стороны, генерация ключей с помощью «естественного» хаоса уже сейчас широко применяется.К примеру, акустический шум в системном блоке компьютера.

Детерминированный хаос, который мы собираемся применить в шифровании, имеет малую размерность и бесконечное множество состояний. Очевидно, что такие системы являются «более предсказуемыми», чем естественных хаос, однако они могут быть смоделированы человеком. Для оценки случайности таких систем мы рассмотрим энтропию Колмогорова – Синая и заметим, что детерминированный хаос способен порождать алгоритмически случайные последовательности. Кроме того, в смешивающей системе, выборка x_n, x_{n+k}, x_{n+2k}, x_{n+3k} …· является асимптотически случайной ($k \to \infty$), другими словами, с увеличением k члены выборки будут становиться все менее зависимыми [5, 6].

В криптографических приложениях выбор значения управляющего параметра определяет непредсказуемость системы, если параметр хаотического отображения использовать в качестве ключа, то все пространство допустимых ключей должно соответствовать хаотическому режиму.

Список литературы

1. Тен Т. Л., Бейсенби М. А., Когай Г. Д. Криптографические системы по управлению детерминированным хаосом : монография. Гамбург : LAP LAMBERT Academic Publishing, 2014. 228 с.

2. Бейсенби М. А., Тен Т. Л., Когай Г. Д., Томилова Н. И., Тайлак Б. Е. Разработка криптографических систем и управление детерминированным хаосом : монография. Караганда : КарГТУ, 2012. 200 с.

3. Бейсенби М. А., Тайлак Б. Е., Тен Т. Л., Томилова Н. И., Когай Г. Д. Формализация взаимосвязи детерминированного хаоса и криптографии // Фундаментальные и прикладные исследования, разработка и применение высоких технологий в промышленности : материалы XIII Международной научно-практической конференции. СПб., 2012.

4. Колесов В. В., Залогин Н. Н., Воронцов Г. М. Шифрование цифровой информации при использовании генераторов с хаотической динамикой // РЭ. 2008. Т. 53. № 4. С. 459–467.

5. Loskutov A. Y., Shishmarev A. I. Control of dynamical systems behavior by parametric perturbations an analytic approach // Chaos. 1994. V. 4, No2. P. 351–355.

6. Marino I. P., Lopez L., Sanjuan M. A. F. Channel coding in communications using chaos // Physics Letters A. 2002. 295. P. 185–191.