
Good
Morning
Make positive thoughts and enjoy
every moment of this day!

CHAOS BASED SECURITY

Dealing With Huge & In Secure

THE DEFINITION

It is from Two Opposite Integral Parts

1. Chaotic Cryptography
2. Chaotic Cryptanalysis

Chaotic Cryptography

Chaotic cryptography is the application of the mathematical chaos theory to the practice of the cryptography, the study or techniques used to privately and securely transmit information with the presence of a third-party or adversary.

Chaos Theory

Chaos theory is a branch of mathematics focused on the behavior of dynamical systems that are highly sensitive to initial conditions. 'Chaos' is an interdisciplinary theory stating that within the apparent randomness of chaotic complex systems, there are underlying patterns, constant feedback loops, repetition, self-similarity, fractals, self-organization, and reliance on programming at the initial point known as *sensitive dependence on initial conditions*. The butterfly effect describes how a small change in one state of a deterministic nonlinear system can result in large differences in a later state, e.g. a butterfly flapping its wings in Brazil can cause a hurricane in Texas.[1]

THE USES of Chaos Theory

The use of chaos or randomness in cryptography has long been sought after by entities wanting a new way to encrypt messages. However, because of the lack of thorough, provable security properties and low acceptable performance, chaotic cryptography has encountered setbacks.

THE MECHANISM

1. In order to use chaos theory efficiently in cryptography, the chaotic maps should be implemented such that the entropy generated by the map can produce required Confusion and diffusion

[*Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.*

Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.[2] *Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state.*

THE MECHANISM

1. Properties in chaotic systems and cryptographic primitives [Algorithms and Protocols] share unique characteristics that allow for the chaotic systems to be applied to cryptography.
2. If chaotic parameters, as well as cryptographic keys, can be mapped symmetrically or mapped to produce acceptable and functional outputs, it will make it next to impossible for an adversary to find the outputs without any knowledge of the initial values. Since chaotic maps in a real life scenario require a set of numbers that are limited, they may, in fact, have no real purpose in a cryptosystem if the chaotic behavior can be predicted.

TYPES OF CHAOS BASED SECURITY

1. The concept of chaos cryptography or in the other words chaos-based cryptography can be divided into two major groups:
2. The asymmetric and symmetric chaos-based cryptography.
3. The majority of the symmetric chaos-based algorithms are based on the application of discrete chaotic maps in their process.

CHAOS BASED IMAGE ENCRYPTION

1. The Bourbakis and Alexopoulos in 1991 proposed supposedly the earliest fully intended digital image encryption scheme which was based on SCAN language.
2. Later on, with the emergence of chaos-based cryptography hundreds of new image encryption algorithms, all with the aim of improving the security of digital images were proposed.
3. However, there were three main aspects of the design of an image encryption that was usually modified in different algorithms (chaotic map, application of the map and structure of algorithm). The initial and perhaps most crucial point was the chaotic map applied in the design of the algorithms

CHAOS BASED IMAGE ENCRYPTION

1. The speed of the cryptosystem is always an important parameter in the evaluation of the efficiency of a Cryptographic algorithm, therefore, the designers were initially interested in using simple chaotic maps such as tent map, and the logistic map.
2. However, in 2006 and 2007, the new image encryption algorithms based on more sophisticated chaotic maps proved that application of chaotic map with higher dimension could improve the quality and security of the cryptosystems.

CHAOS BASED HASH FUNCTION

1. Chaos-based hash functions, take advantage of entropy generated by chaotic maps to digest the message.
2. A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula.
3. Message digests are designed to protect the integrity of a piece of data or media to detect changes and alterations to any part of a message. They are a type of cryptography utilizing hash values that can warn the copyright owner of any modifications applied to their work.
4. Message digest hash numbers represent specific files containing the protected works. One message digest is assigned to particular data content. It can reference a change made deliberately or accidentally, but it prompts the owner to identify the modification as well as the individual(s) making the change. Message digests are algorithmic numbers.

CHAOTIC MAPS

1. In mathematics, a chaotic map is a map (= evolution function) that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time parameter.
2. Discrete maps usually take the form of iterated functions. Chaotic maps often occur in the study of dynamical systems.

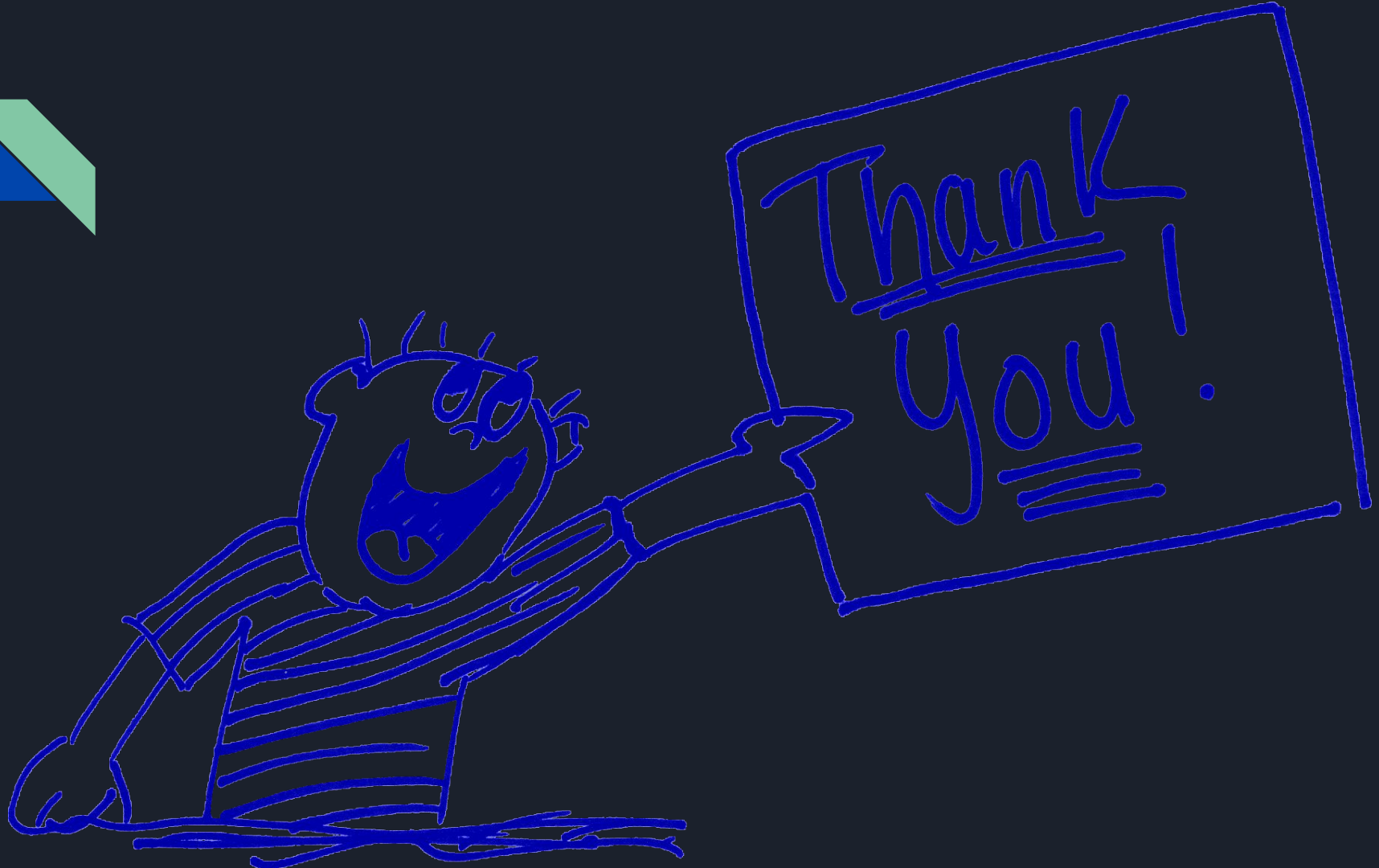
CHAOTIC MAPS

1. Chaotic maps often generate fractals. Although a fractal may be constructed by an iterative procedure, some fractals are studied in and of themselves, as sets rather than in terms of the map that generates them.
2. This is often because there are several different iterative procedures to generate the same fractal.

CHAOS BASED RANDOM NUMBER GENERATION

1. The unpredictable behavior of the chaotic maps can be used in the generation of random numbers.

2. Some of the earliest chaos-based random number generators tried to directly generate random numbers from the logistic map.


Thank
You!