How chaos can lead to security

Introduction:

Although the title may seem like a juxtaposition, chaos can really lead to security. This essay will explore an example of using chaos for security. This example honestly surprised me and I want to share with you this example because it shows how seemingly irrelevant objects can become unique solutions to a crucial issue especially in the modern world. The example that this essay will explore is the use of lava lamps in cryptography.

Chaos Theory:

Before we continue, we must understand the Chaos Theory. Now the Chaos Theory does not really have a universal mathematical definition, but the most used definition gives it three properties. The three properties are: it must be sensitive to initial conditions, it must be topologically transitive and it must have dense periodic orbits. Now I know that I threw a bunch of properties at you which I don't blame you if you don't understand them (trust me I don't either). However I will only focus on the first property (the sensitive dependence on initial conditions). Lucky for you (and for me) this is the easiest property of the Chaos Theory to understand. In the simplest terms, it is like the widely known “Butterfly effect” where small changes can lead to larger and different outcomes.

Lava Lamps:

Before we continue even further, we must also understand how lava lamps work. Lava lamps have two liquids inside and these two liquids have nearly the same densities and cannot mix together so they are two different fluids. These two liquids are: water-based solution and a wax mixture (which is slightly denser than the water at room temperature). At the bottom of the lava lamps there is a light bulb which apart from lighting the lamp up, it also heats up the substances. At a certain temperature the wax will begin to expand due to the heat and become less dense causing the wax to ascend to the top. Lava lamps have a temperature gradient (the bottom is the hottest and the top is the coolest) and at the top/as it cools, the wax will begin to become denser than water and so it sinks downwards. Now lava lamps can be linked to the Chaos Theory since the wax will never form the same shape again. This is because it is very sensitive to initial conditions meaning that any small environmental changes, such as temperature, will change the shape of the "lava blobs". Therefore, we can describe lava lamps as chaotic and unpredictable systems.

Cryptography and Lavarand:

The internet is a global network which connects devices to allow for communication and the exchange of information. Everyday there is a high amount of information being sent over the internet and, while not all, a lot of this information is sensitive and private. So the security of these types of data have become so essential in today's world. Cryptography is the study of securing information using protocols to prevent unauthorised access to any private information. The most common or known protocol is encryption which essentially scrambles data into an unreadable format (ciphertext) and requires a key to reverse this into the format it was in (plaintext). Now encryption must be totally random because if there are any

patterns, hackers can pick up on these patterns using mathematical analysis thus hackers will have an easier time guessing the key used for encryption which will lead to them decrypting the information for their use. For encryption to be random, computers alone cannot be used since they are designed to give a logical output due to an input. As a result, if they were given the instruction to encrypt data, they will produce something predictable and if they were given the instructions to encrypt the same data at a different time, they will encrypt the data in the same way. A computer can theoretically encrypt data using an algorithm called the “Pseudorandom number generator” (PRNG). Yet this algorithm has problems with it such as producing the same encryption result if given the same input. Consequently, a new algorithm must be used to ensure random results, this new algorithm is called the "Cryptographically secure Pseudorandom number generator" (CSPRNG). Why is it used? This algorithm passes statistical randomness tests meaning that this algorithm is capable of producing unpredictable results. In addition, an attacker will not be able to predict the outputs of this algorithm even if it has partial access to it. The CSPRNG needs random data to be able to create a random and unpredictable output. This leads me onto how lava lamps are used to feed this algorithm the random data that it needs. We have explored how lava lamps are chaotic thus they are used by certain cloud-based and security companies such as Cloudflare. In the lobby of Cloudflare's headquarters (located in San Francisco), there is a wall of around 100 lava lamps with a camera constantly taking pictures of it, with each image being able to create a new seed (the input for encryption process). Furthermore, the fact that people are allowed to walk by and be captured in these images adds to the randomness and helps to create more random data.

Image conversion:

These images are converted into matrices. A matrix is an array of numbers and values that are arranged in rows and columns which represent the x axis and the y axis. The x and y coordinates within an image matrix correspond to the location of a pixel (the smallest area of an image) in an image. These pixels will contain a colour and so a numerical value must be assigned to it so that it conforms to its colour and brightness. A grayscale image is represented as a 2D matrix and each pixel has an intensity value ranging between 0 (black) and 255 (white).Coloured images are made of 3 2D matrices which represent red, green, blue and each pixel will have an intensity value ranging between 0 (dark) and 255 (full intensity of red, green or blue). These matrices are turned into seeds for the CSPRNG through the use of hash functions. The hash functions takes the values of the matrices and switches it around so that it can be random.

Conclusion:

Although this isn't the only method that is used in cryptography, it is a strong method and would be considered unexpected by many. I hope that I was able to show how mathematics was implied in this method in a simple way. I hope you enjoyed my essay and I thank you for reading it.

Darius

Sources:

https://en.wikipedia.org/wiki/Chaos_theory

https://www.cloudflare.com/learning/ssl/lava-lamp-encryption/

https://medium.com/ai-ml-interview-playbook/mathematics-behind-images-understanding-matrices-and-filters-cd581846f060

https://lavalamplights.wordpress.com/2011/07/25/how-does-the-lava-lamp-work/