DISCRETE MATHS

S.E.E.D

(Security Enhancement through Encrypted Designing)

GHORI ZEEL JIVRAJBHAI

7984313073

ghorizeeljkvrz@gmail.com

INTRODUCTION

In the current world, cybercrime has become a common sighting. It is very common for sites and accounts to be hacked, for information to be stolen, or in general the involuntary transfer of the power of the account, whether it be business-based, or person-based.

Our solution, whilst implementing discrete mathematics, is an attempt in order to make such sites and accounts more secure from these hacking attempts.

THE MAIN PROBLEM

As aforementioned, the increase in cybercrime has been tremendous in recent years. With nearly every daily life need now being eased with the help of technology, the whole world is going digital.

But with this, comes the risk of losing your personal or confidential information to an unwanted party. This is very common, because of due negligence of the user or because of some cases of fishing or hacking.

This can only be solved in two ways. One is increasing awareness among the people about such problems, and the second is to increase the security of the user. The awareness part being mostly the role of the government, we can mostly focus on making such websites more secure from any external, unwanted guest.

THE SOLUTION

Nowadays, each and every website has a captcha system for user verification. A captcha, whether it be numeric code, a bunch of images, or a simple tick mark of human verification, is another step towards security. But this is very easy for any person or an intelligent bot to answer correctly nowadays.

We have tried to introduce a concept in which a set of pictures are given to the user, and they have to select the correct ones in order to access their classified information. We call this concept as :

S.E.E.D $\rightarrow$ Security Enhancing through Encrypted Designing

This concept can be seen as industry-based, with further scope for improvement. For instance, a company can give its employs the three/four correct images that they have to select in order to go forward. Clearly, this information is another criterion apart from the username-password that is only between the company and the employ. These three/four images would be part of a larger bunch of pictures that we would provide the company with.

Hence, the main role of S.E.E.D would be to design such paintings according to the company's need, supply them with a bunch of possible designs, and give them a matrix to be used as a replacement for the traditional captcha.

The designs to be made can easily be made with the help of discrete mathematics and the simple application of the modulus operator. The basic idea is to divide a document into a large number of rectangles. These rectangles can now be filled with the modulus operator, by using a key and the colours given to us by the company. This can also be seen as similar to linear hashing in an art form.

In such a way, we can form a vast amount of designs with only a certain number of colours, simply by changing small constants in the key used to fill this, hash table-like, design canvas. Of those, we can provide the company with enough designs in a matrix form, for them to use for security purposes.

The Working of S.E.E.D

The design can be implemented with the use of a modulus operator. Imagine every single element of this, image matrix, as a separate design. This can be formulated by making simple tables of 3x3 or 4x4 or 5x5, or so on, sizes based on the complexity level we want to create. Let us take the example of the given matrix, which essentially consists of 9 3x3 cells.

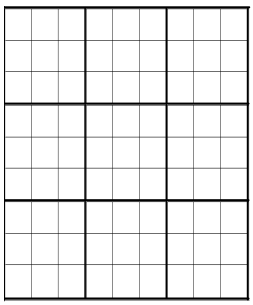

Figure 1: The S.E.E.D Design

Each cell of this design can now be filled automatically with the colours we get from the user, by using the key designated for the same. In such a way, we can, in a similar form of linear hashing, fill all the cells with the colours in a random pattern to generate one image of the matrix. For this, we have to take one single 3x3 cell at a time.

Let us take, for example, the colours yellow, green and blue. Let the sample key for hashing be $n^2 + 3n + 2 \pmod 9$. As we get the values of the square, by inserting n from 0 to 8, we can consequently fill the colours. For example,

For n = 0, key = 2, hence, 2 has colour yellow
For n = 1, key = 6, hence, 6 has colour green
For n = 2, key = 3, hence, 3 has colour blue
For n = 3, key = 4, hence, 4 has colour yellow
For n = 4, key = 5, hence, 5 has colour green
For n = 5, key = 7, hence, 7 has colour blue
For n = 6, key = 8, hence, 8 has colour yellow
For n = 7, key = 0, hence, 0 has colour green
For n = 8, key = 1, hence, 1 has colour blue

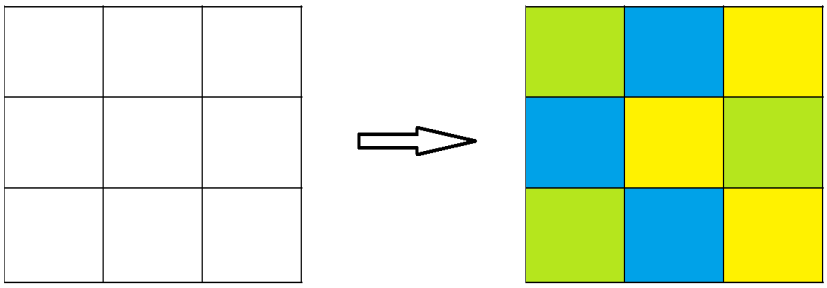

Figure 2: A single element

Many such images can thus be formed by varying the key by a definite amount, in order to randomize the colour-filling pattern and to get different images. This would thus provide us with the final matrix of the desired size.

The only requirement would be to change the constant term or any other coefficient of the provided key, which could vary according to the user's need. Hence, in a similar fashion, we can get the final complete S.E.E.D matrix.
The key used in filling the respective boxes are:

1. $n^2 + 3n + 1 \pmod 9$
2. $n^2 + 2n \pmod 9$
3. $n^2 + 4n + 5 \pmod 9$
4. $n^2 + 3n + 2 \pmod 9$
5. $n^2 + 2 \pmod 9$
6. $2n^2 + 4n + 1 \pmod 9$
7. $n^2 + 6n + 4 \pmod 9$
8. $n^2 \pmod 9$
9. $3n^2 + 2n + 1 \pmod 9$

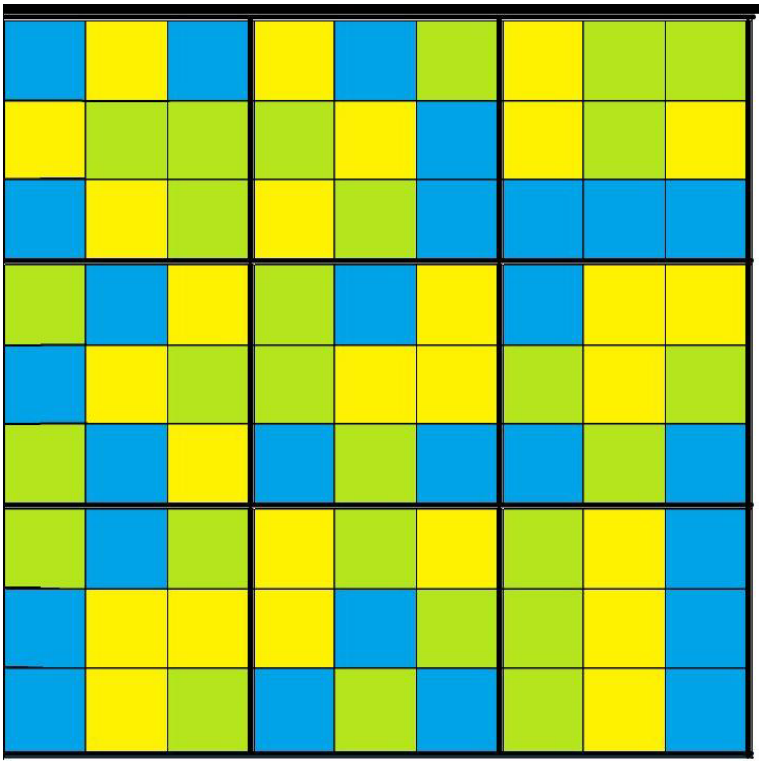

Figure 3: The Complete S.E.E.D Design

This way, we can obtain the final design, which could now be used. Each 3x3 cell is a possible option to be selected. Out of the 9 available, the company can select the 3 correct ones, which would be required to get further access. This would therefore solve our problem, of attempting to further increase the security of a website or any application per se.

In this example of a simple accumulation of 9 3x3 matrices with only 3 correct images, the probability that an unwanted guest might enter would be:

$$\text{Probability(P)} = \frac{\text{Number of correct choices}}{\text{Total choices}}$$

$$\text{P} = \frac{1}{C_3^9} = \frac{1}{84}$$

Clearly, with just a small sample size of 9 cells, the probability that an unwanted guest can enter whilst knowing the username and password is negligible. This would help increase the security and verify the user, even if the username and password are leaked or hacked. This goes without saying that the number of options can also be increased, a grid of 16 4x4 cells, 25 5x5 cells, according to the level of security. All we need from the user are the colours and the n for

making n^2 nxn cells.

An additional level of security can also be added. Given that even human error is possible while selecting the correct design, the user can be given 3 chances to select the design which he deems correct. If wrong thrice, then the account can be locked for fishy activity. This can now only be opened from the higher authority of the company.

Scope of Improvement

Even if we tried our absolute best to perfect this concept in our eyes, we do realize that this project can be improved in certain ways. These improvements can be:

- **User-Product Interaction**

  Another concept of Discrete Mathematics that can be used in this project is the concept of encryption and decryption. An important part of a product is the user and product interaction. In order to improve this communication, the key for hashing can be provided to the user in an encrypted form. Thus, the key is safe with us, but the user can change the constants of the key. This way, the functioning of the product will not change and the user can get the designs of their choice.

  This would give the user a choice, as to which design they do or do not want to keep in their matrix, making it more user-friendly and more interactive.

- **Image S.E.E.D**

  The biggest drawback right now might just be the fact that only colours are being filled to make designs. Another way can be the use of images that can also be taken from the user. This would give the S.E.E.D matrix an extra visual appeal to the user whilst performing the same function.

- **Public Based Concept**

  Though this concept can broadly be seen as applicable in an industrial set-up, this can also be used for individual purposes. This can easily be done by making the S.E.E.D matrix as a link from when the person enters their username-password to the opening of the information they want to access. In simpler terms, it would act like a two-way authentication code. One being the username and password, second being the matrix itself.

  This concept, though provides a good level of security and can be very helpful from a business or industrial point of view, it can also be expanded to cater for the needs of the individual person.

- **Pixel Art Form**

  Due to our limited knowledge, we were only able to implement our concept using colours and hashing logic. But this can be made very advanced by using the knowledge of pixels. If we are able to figure out a key, such that we can traverse through the different pixels on the screen, then this concept can have a variety of applications.

  Not only can it be used for increasing security, but the final matrix can also be more eye-catching, more attractive. And even apart from it, this concept can then also be used to form various pixel art projects, designs, modern art, etc. The application would not only be limited to security but it can also be extended to art, design, and marketing

  Even other improvement concepts can be used in this case to make the application more widespread and make the working more smooth.

COMMERCIALIZATION

It's simple to observe that the target audience of this product is going to be various companies, industries, start-ups etc. The demand for this product, if executed successfully, can be huge. As the whole world is going digital, cyber security is something that everyone in the world can take benefit of.

In order to commercialize our product, we need to approach various companies, introduce them with our idea of S.E.E.D and pitch them what can be the new system of security. Everything is bounded by two steps of authentication, all under the control of the overlooking company.

Future Scope

Though right now the commercialization would only be from an industrial point of view, this can further be extended to the common public for use. Various activities for an individual person also do require a high level of security, which can be given to them via S.E.E.D