Securing Student Data Privacy using Modified Snake and Ladder Cryptographic Algorithm

Dr. Kamaladevi Kunkolienker[1]
Dept. of Philosophy, P.E.S' R.S.N. College of Arts and Science, Farmagudi – Ponda – Goa - India

Vaishnavi Kamat[2]
Computer Engineer
India

***Abstract*—Transformed by the advent of the Digital Revolution, the world deals with a gold mine of data every day. Along with improvement in processing methods for the data, data security is of utmost importance. Recently, there was a noticeable surge in online learning during the pandemic. Modifying their workflow strategies, the educational institutions provided courses for students designed to suit the need of the hour. This opened up the avenue for a greater number of students to take part in the online learning. With the increase in number of students registered, there exist a substantial repository of data to deal with. Hackers have been targeting student data and using it for illegal purposes. In this research paper, an attempt has been made by modifying the classic Snake and Ladder game to perform encryption on short text student data to ensure data privacy. The Novel algorithm maintains simplicity yet produces a strong cipher text. The algorithm stands strong against the brute-force attack, cipher-only attack, etc. Decryption also uses same key as used for encryption, the key being symmetric in nature. New variable keys are generated every time the algorithm is used.**

***Keywords*—Student data; privacy; encryption; decryption; snake and ladder; variable keys**

I. Introduction

The 'Digital Revolution' is providing us abundant data which has to be dealt with caution. It was evidently noted that since there is lack of awareness of cybersecurity among the students, they tend to ignore the threat and turnout to be the most vulnerable target for the cyber-attacks. Though most of the students in the survey knew about the online risks and threats, but they lacked to understand basic knowledge about privacy [1]. In an empirical study among the students, it was explored that the students expressed concerns about their online data privacy and believed that the teachers or concerned authorities should put in efforts to safeguard it [2]. Hence, Cryptography will play a vital role in securing the data. This paper puts forth a novel algorithm for encryption and decryption for the short text. Board games as we know stimulate brain areas responsible for developing cognitive skills and memory. Here, the board games serve a different purpose altogether. The modified version of the board game will perform encryption and decryption activities for the desired short text placed on the board. The classic snake and ladder game is used with a twist to generate the cipher text.

A. Role of Technology in Education

Educational institutions with the help of technology have made great strides in improving the understanding and interaction of the students. Students are provided with different online opportunities in terms of courses, tutorials, workshops, seminars to enhance their academic growth. With rise in these opportunities provided, there is enormous rise in the collection of student related data through registrations, personalization preferences and feedbacks.

B. Student Data

The student data usually consist of their personal details, demographic details, student preferences, evaluation reports, faculty observations etc. This data is essential for parents, faculty and policymakers to enable them to streamline their plan of action according to the student requirements.

Most of the organization store the student data and provide it to firms which help them analyze this data using technology like data mining, where several unseen underlying patterns can be highlighted in text.

II. Student Data Privacy

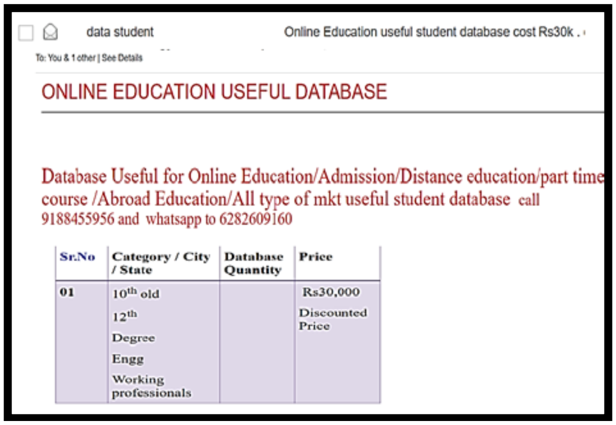
A crucial aspect that needs to be taken care of is to prevent the exploitation of these data-driven systems by the hackers. Hackers can get hold of this data through performing remote attacks on the system, by eavesdropping and can misuse the data, leading to identity theft, creation of fake accounts, modification of student details, etc. [3].

Though the student data has a very good potential and scope for bringing in improvements on various fronts, it is also a matter of concern. Digital learning captures real time information of students and along with their personal information the data captured may be used by hackers for non-educational purposes. It also discusses several legal provisions to safeguard the student data privacy [4].

In order to safeguard the sensitive student data while transferring online or stored on the administrative systems, it should be efficiently encrypted to withstand the possible attack [5].

A. Impact of Student Data Breach

Student data once hacked can open up not only their personal details to the hackers but also the details about their parents and their bank accounts which they use to pay the student fees. The exhaustive student information is sold by hackers through spam mails; a sample snapshot of the email is depicted in Fig. 1 (The snapshot was taken from authors' personal email).



□ data student Online Education useful student database cost Rs30k .

To: You & 1 other | See Details

ONLINE EDUCATION USEFUL DATABASE

Database Useful for Online Education/Admission/Distance education/part time course /Abroad Education/All type of mkt useful student database call 9188455956 and whatsapp to 6282609160

Sr.No	Category / City / State	Database Quantity	Price
01	10th old 12th Degree Engg Working professionals		Rs30,000 Discounted Price

Fig. 1. Snapshot of Email Selling Student Data.

Students in their teens are vulnerable to the data breach activities as they are either unaware of the reality or fall prey to the attackers' malicious intents. Data like unique identification number, name, date of birth can be misused leading to identity theft. Identity theft can falsely implicate an innocent student and ruin their life in a big way. Students with weak financial background can be targeted by 'pretext calling' using this stolen data and in the need of the job or suddenly winning a lottery, the students give away more and more private and confidential information with respect to them and their family. 'Phishing' being the most common attack where the attacker posing as authorized person sends out emails to the student email address available from the hacked institution database and requests them for further information and talks about next course of action to take place from the student's side. Students, believing the sender provide the necessary information and are duped, documents are misused, photographs are inappropriately utilized for gaining profits. An instance where a student's photograph gets misused, can draw the student towards the dark world. Harassment, Stalking and human trafficking can take place at a bigger scale if the student data is not handled with utmost care [6] [7].

III. Literature Review

The Snake and Ladder game is directly applied to perform Steganography, which hides the data in a media like images. The algorithm uses concepts on Image Processing like Pixel Value differencing are used along with the development of the snake and ladder game on the data [8].

This research paper consists of a survey of different scenarios from different research papers, for example, storing protected data for platform like Facebook, concerns when mobile systems are used for payments and their key generation. It also surveys a concept called as Software Defined Networking – a new approach in designing, building and managing networks [9].

This paper illustrates how a game of scrabble can be utilized to generate cipher text for big length data. Several permutations and combinations of words are possible making it difficult for the attacker to guess the actual words directly hence providing good security to the plain text [10].

Security to E-Learning System is provided by Elliptic curve. cryptography algorithm and content is filtered using Decision tree algorithm. Cryptography along with Data Mining techniques proves to be a good combination. Several Data Mining Classification Techniques are compared to figure out which yields good results [11].

Another technique to ensure data privacy is the use of Digital signature. They use a different sort of balance cryptography. It is generally used for monetary exchanges, configuring dispersion, and in various circumstances where it is necessary to identify bogus or changing. Other techniques like DES and RSA Algorithm are frequently used cryptographic techniques [12].

IV. Cryptology

Heraclitus, one of the most influential thinkers in ancient Greek Philosophy expressed hid deep philosophical insights in aphoristic and cryptic form. His writings are full of riddles which are cryptic in nature. He liked this pungent oracular style as it required a penetration of thoughts which provoked human thinking and it helped him in maintain the confidentiality of his writings [13].

Cryptology as a tool of technology is a culmination of techniques for ensuring the secrecy and/or authenticity of information. Cryptology has two main branches in the form of 'cryptography' and 'cryptanalysis' [14].

A. *Components of a Cryptosystem*

- Plain Text - It is the message or information that sender intends to send. Example in our case will be the student's name, date of birth, etc.
- Cipher Text – It is the result of transformation on the plain text after encryption algorithm has been applied.
- Key – It is a piece of information that will scramble the plain text as required by the algorithm.
- Encryption algorithm – It consists of sequence of steps of how and when to apply the key to the plain text to produce the cipher text.
- Decryption algorithm – It consists of sequence of steps of how and when to apply the key to the cipher text to get back the plain text [15].

Fig. 2 illustrates the various components in order of their reference.

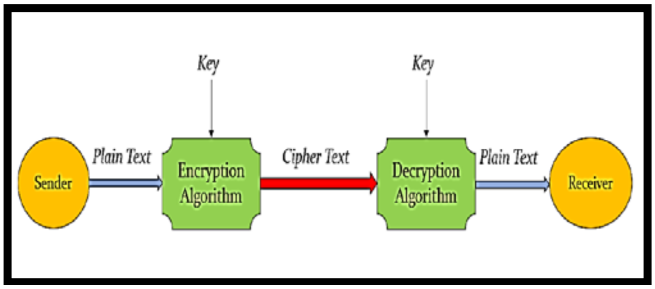


Fig. 2. Components of Cryptosystem.

B. *Cryptography*

The science and art of secret writing has its inscription since the beginning of human civilization. Ancient civilizations of India, Egypt, China, Japan testify the evidences of use of cryptography. The goal of cryptography is to provide secure communication over insecure channel [16].

C. *Cryptanalysis*

Working upon the weakness, improves the strength. This is the principal upon which cryptanalysis is based. Analyzing and understanding the cipher text, trying to decipher it without the knowledge of plain text to identify the weakness and work upon it.

D. *Goals of Cryptography*

- Confidentiality – A cryptosystem ensures that no one other than the sender and the receiver is able to read the input data.
- Integrity – During transmission of data, the cryptosystem should not allow any unauthorized person to modify, alter, change or delete the data.
- Authenticity – The sender and the receiver should be able to identify and validate each other [16].

V. Snake and Ladder Encryption Algorithm

A. *Concept of the Proposed Algorithm*

The proposed algorithm titled 'Snake and Ladder Encryption Algorithm (SLEA)' gets its name from the classic game of Snake and Ladder. 'SLEA' is a 'block cipher' with variable length, symmetric keys. In the block cipher category, the input plain text is divided into fixed size of blocks and then encrypted. Block ciphers are mainly characterized by the block size and its key. Here, though a fixed size block is used for encryption, still the cells only which contain the data are encrypted, the vacant cells on the board are not considered for the encryption. This speed up the process and key variable key length shorter [17]. Symmetric keys mean same keys are used for encryption and decryption. The algorithm provides three layers of encryption. One through character set mapping and the second layer through placement of the snakes and ladders on the board and third through the snake and ladder game moves. The sender and the receiver should have the same interface setup so that pre-decided objects can be shared before the encryption and decryption process begins through the secured channel.

Sample plain text considered for the purpose of illustration is "SMILE IS JOY". Length of the plain text including the blank space is 12 characters.

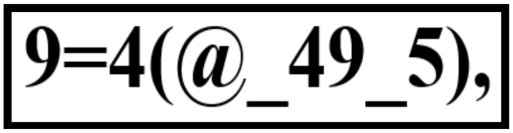
Character Set - The plain text will be first mapped to the characters set and an intermediate cipher text will be generated. There are 'n' number of character sets pre-decided between the sender and the receiver available to both when the algorithm interface is installed from the setup file.

Here for the illustration following character set is considered given in Table I. As for the alphabets, numbers can also be mapped to the character set.

Level 1 encryption- the given plain text 'SMILE IS JOY' will be mapped to intermediate cipher text as illustrated in Fig. 3.

B. *Snake and Ladder Board*

The game board is of the size 4x4, consisting of 16 cells. Fig. 4 shows the pattern for inserting the plain text data is always from left to right direction, whereas the traversal of data alternates in direction every time. A minimum of two snakes and two ladders adds sufficient complexity to the data. As the size of input data increases the board size also can be increased and so are the number of snakes and ladders on the board.



9=4(@_49_5),

Fig. 3. Level 1 Intermediate Encrypted Text Output.

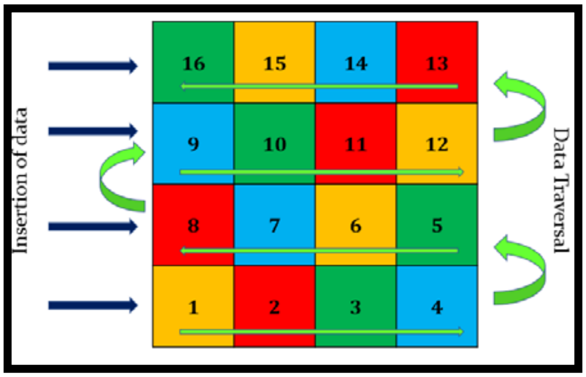


Fig. 4. Modified Board.

TABLE I. Character Set Mapping

A	**#**	I	4	Q	{	Y	,	5	q	“	%	]	n	$	’	+	b
B	**1**	J	5	R	7	Z	&	6	z	”	<	{	]	^	‘	-	c
C	**2**	K	}	S	9		__	7	j	:	>	}	[	~	$	/	e
D	**?**	L	(	T	+	0	a	8	k	‘	^	@	o	`	n	*	d
E	**@**	M	=	U	/	1	s	9	m	’	f	&	p	=	.		
F	**;**	N	!	V	*	2	y	.	~	(	i	%	r	|	y		
G	**3**	O	)	W	:	3	h	,	“	)	g	#	u	<	x		
H	**8**	P	6	X	-	4	t	;	”	[	l	?	v	>	w		

C. Snake and Ladder Encryption Algorithm

Step 1: Create a 4x4 board and select any one arrangement of the snakes and ladders from the predetermined set.

Step 2: Place the level 1 encrypted text onto the 4X4 board.

Step 3: Note the last data entry cell on the board. (This step ensures that the vacant cells are not traversed, hence less time taken for encryption process.).

Step 4: Point the 'marker' to the first cell on the board and roll the dice till all of the entries on the board are visited at least once. Simultaneously, frame the data from the visited cells into a sequence, which is our cipher text to be transmitted or stored.

Step 4.1: Travel the cells on the boards depending on the count on the dice.

Step 4.2: At the end of the traversal for that particular move, if a ladder is encountered- climb up and record the data in the cell in to the cipher text sequence. Similarly, if a snake is encountered- drop down and again record the data in the cell in to the cipher text sequence.

Step 4.3: At any point of time if looping takes place, i.e. dice and cell on the board remain same, do not record the data and roll the dice till the number on the face of dice is different. This resolves looping.

Step 5: If the current cell visited on the board is the last cell, check if there exist any unvisited cells on the board. (Unvisited entries may be due to sudden climbing using ladder or dropping down through the snake). Repeat the process till all cells on the board have been visited at least once.

D. Encryption Algorithm Illustrated

Fig. 5 shows the mapped text on the game board with snakes and ladders already placed on the game board. Table II provides stepwise execution of the encryption algorithm.

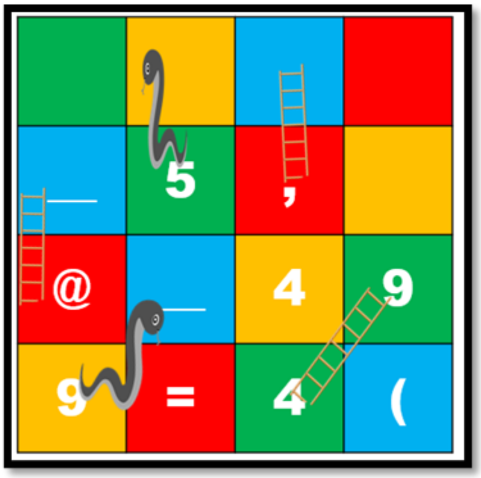


Fig. 5. Mapped Text on the Board.

TABLE II. STEPWISE ILLUSTRATION

Dice Roll Count	***Number on the Dice Face***	***Ladder / Snake at the end of traversal***	***Cipher Text Generated***
1	**3**	**YES**	**9=4**
		Ladder	**9=49**
2	**1**	**NO**	**9=494**
3	**1**	**YES**	**9=494__**
		Snake	**9=494__9**
4	**6**	**YES**	**9=494__9** **No change in the cipher text**
		SNAKE - LOOPING	
5	**5**	**NO**	**9=494__9=4(94**
6	**4**	**NO**	**9=494__9=4(94__@__5**
7	**3**	**NO**	**9=494__9=4(94__@__5,**
		End of Characters on the Board	**Extra places not counted**
End of Characters on the Board - Check if all entries are visited.			
All entries are visited on the board			

Final Cipher Text Generated is shown in Fig. 6, which consists of 17 characters.

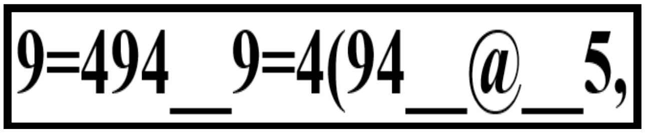

9=494__9=4(94__@__5,

Fig. 6. Final Cipher Text.

Original Plain Text: "SMILE IS JOY"

Length of original plain text: 12

Generated Cipher Text: 9=494__9=4(94__@__5,

Length of Generated cipher text: 17

E. Snake and Ladder Key Generation during Encryption

For the decryption of the cipher text at the receiver side, we need a Key that will help us get back the plain text. As the cipher text is generated, simultaneously the key is also generated. The key is the numbers on the face of dice plus the pattern number for the board arrangement for snake and ladder plus the character set pattern used.

F. Snake and Ladder Decryption Algorithm

The receiver side will use the key transferred through the secured channel and decode the cipher text. Table III provides stepwise decryption.

TABLE III. DECRYPTION USING KEY

Key	*Cipher Text*	*Board Arrangement*
3	**9=494__9=4(94__@__5,**	*Figure 7*
3 1	**9=494__9=4(94__@__5,**	*Figure 8*
3 1 1	**9=494__9=4(94__@__5,**	*Figure 9*
3 1 1 5	**9=494__9=4(94__@__5,**	*Figure 10*
3 1 1 5 4	**9=494__9=4(94__@__5,**	*Figure 11*
3 1 1 5 4 3	**9=494__9=4(94__@__5,**	*Figure 12*

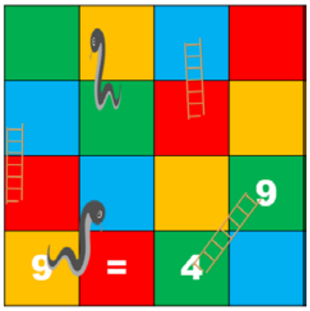


Fig. 7. Key 3.

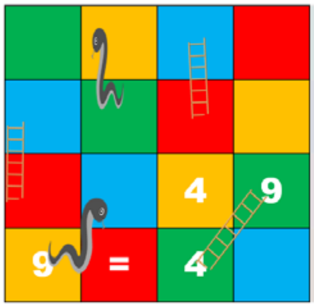


Fig. 8. Key 1.

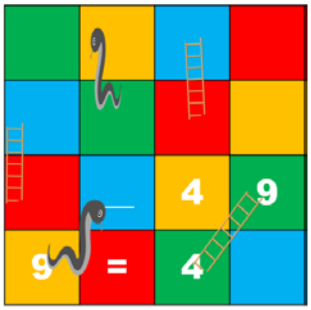


Fig. 9. Key 1.

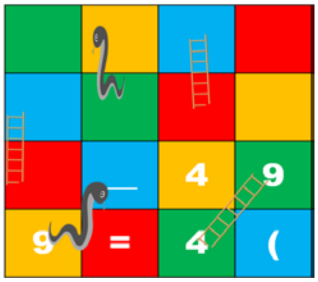


Fig. 10. Key 5.

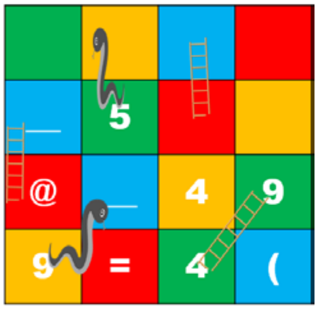


Fig. 11. Key 4.

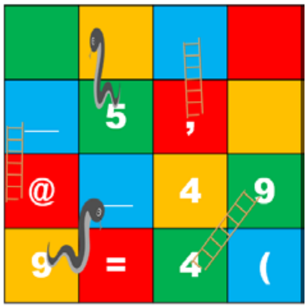


Fig. 12. Key 3.

VI. SECURITY ASPECT

In this section, we will analyze the strength of the snake and ladder algorithm against several types of attacks. Snake and Ladder Cryptographic algorithm provides three levels of security.

Level 1: First, in the form of character mapping set. The set consist of 68 characters mapped uniquely to each other. For every encryption, the character mapping will be changed. If any intruder tries to guess the mapping it will be difficult to select from 248003554243683059960099041856917158104739920135536767237171073801822144571218329600000000000000000 options, that is 68! (68 factorial). This step considerably increases the security in a simple manner.

Level 2: Second, in terms of the placement of the snakes and ladders on the board. The board is selected of 4x4 as it can hold average length of information like student name, roll number, subject name, etc. Depending upon the data length per student, the size of the board can be increased to 5x5 or 6x6 accordingly. For every encryption, the number of snakes and ladders can be decided and a different arrangement of snakes and ladders can be selected from the predefined pattern.

For the current illustration, a board of 4x4 consists of 2 snakes and 2 ladders, sufficient for adding complexity to the encryption process. When the interface will be setup between the sender and the receiver, these predefined patterns and arrangements will be known to both. So, during encryption, along with the key the unique pattern identification number is to be attached before transfer of the cipher text.

Understanding the complexity provided by the placement of snakes and ladders – consider, the 4x4 board with two snakes and two ladders. Initially, total available cells on the board for the placement were 16. Placing the 1st snake -16 options available, placing 2nd snake – 15 options available, placing 1st ladder 14 options available, placing 2nd ladder – 13 options available. It is difficult to gauge the positions by simple guessing.

Level 3: Third, the algorithm itself. The manner in which the cipher text will be generated by rolling the dice will be different every time. And occurrences of the snakes and ladders in the route will change the course of cipher text generated.

Now, we will slide through several types of attacks possible during encryption and how the algorithm provides resistance to them.

Ciphertext Only Attacks – In this kind of attack, the encrypted message is intercepted by the attacker. This attack will be successful only if the corresponding plain text is retrieved from the encrypted message.

The Snake and Ladder algorithm has a huge initial character base to transform the plain text into unmeaningful message. The cipher text characters are further jumbled by the movements in the game. So, it is impossible for the attacker to know the plain text within a finite time without the authentic keys.

Known Plaintext Attack − The attacker knows the partial plaintext for the generated ciphertext. So, the attacker’s task is to study the remaining cipher text, derive the key if possible and get the plain text.

The Snake and Ladder algorithm holds an advantage with respect this attack. Since, the plain text is neither used as direct part of cipher text nor as part of key formation, and even if the attacker knows that it is the student data that the algorithm is dealing with, it cannot conclude anything directly only from the cipher text.

Man in Middle Attack – Mostly, this attack can target the public key cryptosystems. Here, key exchange has to take place before communication begins.

In the Snake and Ladder algorithm, since key is simultaneously generated with the cipher text and also transmitted with it, this attack does not affect the encryption algorithm.

Chosen Plaintext Attack – The attacker has the ability to encrypt plain text of his choice and generate corresponding cipher text in the given system. By performing this act, the attacker tries to study the relation between plain text to cipher text generation.

In the Snake and Ladder algorithm, at level one itself the attacker will have to go through and execute 68! possibilities.

Brute Force Attack – Try several combinations of keys, to decrypt the cipher text.

In the Snake and Ladder algorithm, though the dice has only 6 faces, we don’t know how many times it will be rolled, because the dice rolling depends on the length of the text to be encrypted when it is placed on the board. This is the advantage of the variable nature of the key, which makes it difficult to guess what it is. And if one tries to do so, it might require exponential time [18] [19].

Running Time Analysis – the problem statement is - with how many minimum dice rolling can the text on board be traversed at least once. There are three important factors affecting this, one is the number of filled places on the board, second variable number of snakes and ladders do affect the traversal and the number appearing on the dice face.

For illustration, a 4X4 board was considered, means total number of blocks to be traversed 16. So, running time would be close to O (16 * C), where C is a constant and dice is assumed to have 6 faces. 16 because the block has to be visited at least once. C includes the time including waiting for the dice to roll again and repetitive traversal of the blocks, and climbing up and down the ladders and snakes, respectively. General running time is O (N * D * C) where N is the number of blocks on the board, D is the number of faces on the dice, if dice of a greater number of faces used and C remains the constant.

VII. Advantages and Disadvantages of the Snake and Ladder Algorithm

A. Advantages

- The nature of the game makes the moves during the encryption unpredictable, which strengthens the cipher text.
- Time required for execution is comparatively less as the encryption is not done on entire block but only the part of data present in it.
- Key generation is simultaneous to encryption process.
- Rolling the dice makes the key Variable in length and the Variable key makes it difficult for the attackers to predict the nature of the key.
- Though, there are large number of students, each student’s data in a school / college repository is limited to certain details. Hence, encrypting this short length data with this flexible size algorithm avoids unnecessary space and time complexities.
- Considering the best or average time cases (number on the dice face from 6 to 4, every time it rolled) the algorithm can be considerably fast or average during encryption.

B. Disadvantages

- As the board size increases, the complexity for the algorithm’s implementation increases.
- Considering the worst case (number on the dice face from 3 to 1, every time it rolled) the algorithm can be a bit slow during encryption.

VIII. Conclusion

The ‘randomness’ of the ‘dice’, ‘movements’ on the ‘board’ add the twist to the generation of the cipher text just as required. Since, student data can be categorized into distinct fields like their first name, last name, date of birth etc. this algorithm on the board of 4x4 is most suitable to encrypt the data part by part and store it in the same manner. Though there exist several cryptographic algorithms that provide cipher text, the Snake and Ladder algorithm consumes minimum time and generates the cipher text in length close to the length of plain text and key length is maintained less than cipher text length, hence reducing overall processing time.

Future research could examine improving the key transmission from sender to the receiver. Also, improvements in hardware can considerably increase the efficiency of the algorithm.

As mentioned before, the student data breach can have devastating psychological effects on the students. The pillars of the nation have to be necessarily protected against these hidden cyber-attacks. Ensuring the confidentially of the student data while collecting, proper cryptographic techniques to be used while storing or transmitting, and enforcing strict laws modified according to the emerging cyber-attacks are some of the basic steps that need to be enforced by the concerned authorities.

References

[1] Gabra A. A., Sirat M. B., Hajar S., Dauda I. B. , Cyber Security Awareness Among University Students: A Case Study, International Journal of Advance Science and Technology, Vol. 29 No. 10S, pp. 767-776, 2020.

[2] Lorenz Birgy, Sousa Sonia, Tomberg Vladimir , Privacy Awareness of Students and Its Impact on On-line Learning Participation –A Case Study. 1st Open and Social Technologies for Networked Learning (OST), Tallinn, Estonia. pp.189-192, 2012.

[3] Townsend A. (2021), 3 Reasons Higher Education is a Cyberattack Favorite https://www.onelogin.com/blog/3-reasons-higher-ed-hacked.

[4] Stahl W., Karger J., Student Data Privacy, Digital Learning, and Special Education: Challenges at the Intersection of Policy and Practice, Journal of Special Education Leadership, Vol- 29 No. (2), 2016, pp. 79-88.

[5] Carr R. (2018), The Rise of Education Data Breaches https://www.zettaset.com/blog/education-data-breaches/.

[6] Bandler J., Merzon A., Cybercrime Investigations- A Comprehensive Resource for Everyone, Published by CRC Press, 2020, pp. Chapter 2.

[7] Clough J., Principles of Cyber Crime, Published by Cambridge University Press, 2015, pp. 417- 419 and 209-212.

[8] Seth J. R., Snake and Ladder based Algorithm for Steganographic Application of Specific Streamline Bits on Prime Gap Method, International Journal of Computer Applications, Volume 94 – No 3, 2014.

[9] Lokesh V., Jayaraman S., Guruprasad H. S., A Survey on Network Security and Cryptography, International Journal of Advance Research In Science And Engineering, Vol. No.3, Issue No.10, 2014, pp. 56-54.

[10] Kamat V.K., Scrabble-O-Graphy: An Encryption Technique for Security Enhancement. In: Sa P., Bakshi S., Hatzilygeroudis I., Sahoo M. (eds), Recent Findings in Intelligent Computing Techniques. Advances in Intelligent Systems and Computing, Vol 707. Springer, Singapore, pp. 2019, pp. 115-124.

[11] Patil Vijaya, Vedpathak Aditi, Shinde Pratiksha, Vatandar Vishakha, Janrao Surekha, E-learning system using cryptography and data mining techniques, International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 01, e-ISSN: 2395-0056, Jan-2018.

[12] Mangore Anirudh K. , M. Roberts Masillamani, Efficient Cryptographic Encryption Techniques for Data Privacy Preservation, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8, Issue-7S, May 2019.

[13] Kunkolienker K., Sri Aurobindo's Views on Heraclitus' Philosophy: A Synthesis, Proceedings published by WASET, EISSN: 2010-3778, 2017.

[14] Stallings, W., Cryptography and Network Security (4th Edition), Published by Pearson Education, 2006, pp. 28 – 35.

[15] Buchmann, J., Introduction to Cryptography, Published by Springer New York, 2013, 69– 71.

[16] Padhye, S., Sahu, R., Saraswat, V., Introduction to Cryptography, Published by CRC Press, 2018, pp. Chapter 1.

[17] Aumasson Jean – Philippe, Serious Cryptography- A Practical Introduction to Modern Encryption, Published by No Starch Press, 2017, pp. 53-55.

[18] Henk, C.A., van Tilborg, Encyclopaedia of Cryptography and Security, Published by Springer, 2011, pp. 153-156.

[19] Swenson, C., Modern Cryptanalysis – Techniques for Advanced Code Breaking, Published by Wiley, 2012, pp. Chapter 5.