Journal of Management and Service Science, 2021,
Vol. 01, Iss. 02, S. No. 004, pp. 1-9

Cryptography: Security and Integrity of Data Management

Faisal Abbasi[1], Pawan Singh[2]

Amity School of Engineering and Technology, Amity University, Lucknow, India[1,2]
faisalabbas2599@hotmail.com[1], pawansingh51279@gmail.com[2]

How to cite this paper: F. Abbasi and P. Singh (2021) Cryptography: Security and Integrity of Data Management. *Journal of Management and Service Science,1(2), 4, pp. 1-9.*

https://doi.org/10.54060/JMSS/001.02.004

Received: 17/05/2021
Accepted: 27/05/2021
Published: 30/05/2021

Abstract

Internet always deals with data. Basically, data is any type of digital information that has been stored in the servers. With the advancement of technology, billion tons of data have been accumulated over the internet. Protection of these data is very crucial as; theft of these data will lead to damages beyond imagination. Data Security is protection of these data and privacy, which prevent hacker from unauthorized access to computers, applications, and data servers. Data security is achieved by implementing Cryptography. Cryptography is a technique in which data is encrypted and stored in the databases, so that if by chance anyone gets access to these data, it will of no use to them. There are many cryptography algorithms that are widely used to encrypt and decrypt data, some of them are AES algorithm, stream ciphers, DES algorithms, etc. The concept of cryptography is not only limited to text encryption but also it has a wide application in visual cryptography, watermarking, steganography, etc. Now a day's security of communication has become very important, especially after people have started using internet banking. Everything on world wide web is all about confidentiality, integrity, and authentication.

Keywords

Data Encryption and Decryption, Compression, Cryptography Concepts, Security, and Integrity.

1. Introduction

When we heard the word "cryptography", the first thought that comes to our mind is that it is something related to computers. But you will be surprised to know that history of cryptography is dated back to 4000 years ago (Egyptian Civilization). It was the Egyptians, who first developed the art of hiding data in the form of texts. Cryptography has played a very important role in the world war. You must hear of the German cryptography machine enigma and how Americans hired their best brain to decode the message. Coming to present it has very vital role in 21st century. Cryptographic systems are mainly used in military,

banks, the diplomatic, government and commercial services. With the invention of computers and communication system the private sector organization started using the computers and storing information in digital forms. This led to the security issues of these data and that is why cryptography came into picture. The main purpose of cryptography is to provide security. Initially cryptography was used to protect national secrets and files. It was very uncommon among the public and people also did not know much about it. But when banks, financial organization started online transactions they needed a way to protect that data, so they also started using cryptographic systems. Now cryptography is used everywhere, where data security is priority (Ekert, 1991).

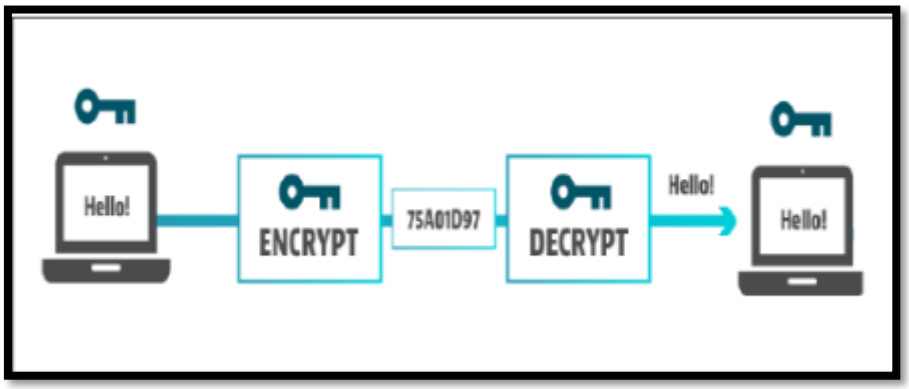

Figure 1. Cryptography Techniques.

2. Historical Techniques

2.1. Caesar Cipher

This methodology of encryption and decryption is one of the oldest and was invented by Julius Caesar, who was the emperor of Rome, during the war of Gallic. In this method what he did was he replaced sequential order of alphabetical system by the letter that comes three places ahead of that letter in the alphabet. For example, A was replaced by X, B was replaced by Y and C was replaced by Z. In technical term you can say that he performed the shift operation by 3. This algorithm is one of the oldest one and thus it very easy to break. Despite being the easiest to break, at historical time it was considered one of most difficult one to break. But it has its own importance as it led to development of more advanced form of cryptographic techniques. (Jirwan, 2013).

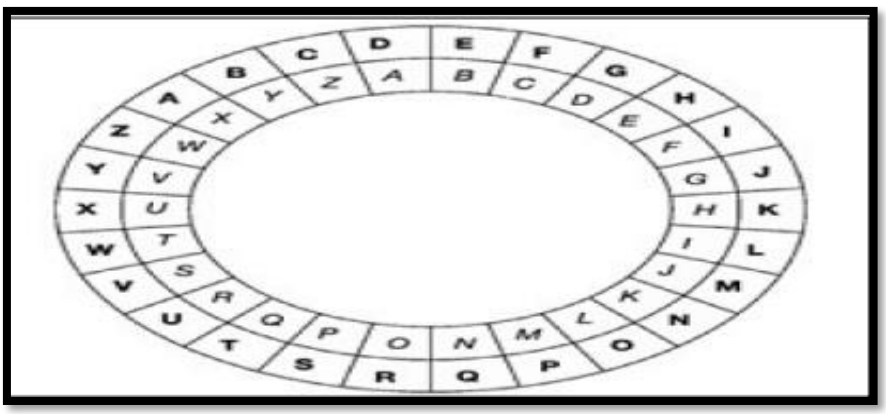

Figure 2. Caesar cipher encryption wheel.

2.2. Simple Substitution Cipher

It is also known as monoalphabetic cipher. This was the first cipher in which key model was used. In this model alphabets were written in proper sequential order and above it was represented random permutation of alphabets. Thus, this serves as a key for encrypting and decrypting the code. The person who was having this key can only decrypt the message. Though it was a good method for encrypting the message, but this can be easily broken by probability of occurrence of letters. For example, CAN is QDN.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	**I**	**Q**	**M**	**T**	**B**	**Z**	**S**	**Y**	**K**	**V**	**O**	**F**
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	**R**	**J**	**A**	**U**	**W**	**P**	**X**	**H**	**L**	**C**	**N**	**G**

Figure 3. Substitution Cipher.

2.3 Transposition Cipher

In this method there defined certain rules along with key to encrypt and decrypt key. Transposition is the method of modification of letters in the text using keys and certain rules. This is not the single techniques instead it is a whole family of cryptographic techniques. One of the simplest transposition ciphers is columnar cipher. It is of two types first complete columnar transposition cipher and incomplete columnar transposition cipher. In this method we write the text that has to be encrypted in horizontal and width of the text should be exact equal to the width of the key. For example, “second division advancing tonight” is the message that we want to encrypt. So, the first step is that we will write the message horizontally. (Callas, 2007)

S E C O N D
D I V I S I O
N A D V A N
C I N G T O
N I G H T X

If we are using complete transposition cipher, then we will use it null character in place of position where no letters are written. As you can see it is marked with cross. Now, if we encrypt the message using the key “321654” the text is going to be “Cvdng eiaii sdncn donox nsasdt ouvigh”. Now if you are using incomplete cipher then you need not to write null character at empty space. So, this makes it more difficult to decipher the text without key.

3. Modern Algorithm

3.1. Stream ciphers

With the advancement of modern computers, the encryption techniques took a completely new direction. Where earlier people used to do it manually, now people started using computer to encrypt and decrypt messages. They developed a method of generating the key with the help of pseudorandom generators. A pseudorandom generator is program that generates the

completely unique key that unpredictable to guess. A stream ciphers is relatively simple and very fast type of encryption algorithm. Pseudorandom generators are used to generate the key which is then XOR with the message to produce the encrypted cipher text. In stream cipher we use same key to encrypt and decrypt data. For example, there is message "0100110100010" which has to encrypted. First a key will be generated with the help of pseudorandom generator after that it is XOR with the message. Suppose the key is "00000101111111". Then the message we will get after XORing it will be "10011111000101".

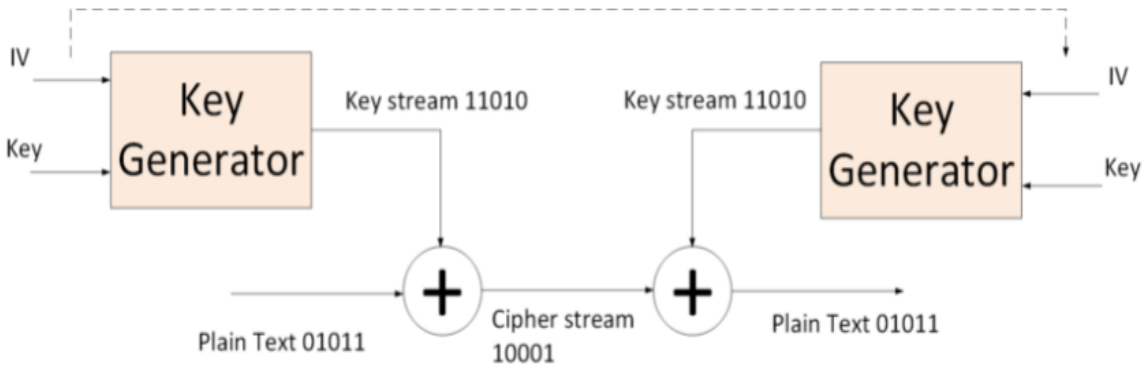

Figure 4. Stream Ciphers.

One time pad is example of stream ciphers. The one-time pad is very fast in encryption and decryption. But the disadvantage here is it is very difficult to practice as the length of key should be equal to the length of the message. One time One time pad has perfect secrecy it is secure from only cyber text attacks, but the attacks are possible. Shannon proved that number of keys should be more than the number of messages that cipher can handle. Thus, it is hard to practice. Stream ciphers are used in https and web. (Massey, 1986).

3.2. Block Ciphers

Block ciphers contains of both algorithms i.e., encrypting algorithm and decrypting algorithm. There is a key K that is given to the encryption algorithm E to produce the ciphertext C. Expression for that C=E (K, P). The same is key passed to decryption algorithm D to produce the plaintext. P=D (K, P). To make block cipher more secure we use pseudorandom permutation. The key is kept is secret therefore an attacker will not be able to decrypt the block cipher and will get any output from the input. In block cipher we ensure randomness of key thus making it attack proof from the attackers. In other words, you can say that attackers will not get any pattern from the input or output. Block cipher work on the two values:

1) Length of the block.
2) Length of the key.

In order to be secure these two values are very important. Block ciphers works on 64-bit block or 128-bit block. It is important to keep the block size in estimated length, they should not be too large. The ciphertext should be small size. Suppose we want to encrypt 24-bit message and the block with 128-bit blocks, firstly we have to convert the message into 128-bit otherwise the block cipher will not process.

When it comes to memory footprint, we need at least 128-bit memory to work with and process a 128-bit block. Most CPUs have a register. Isn't too large to match. Dedicated hardware circuits are needed otherwise. Can be used to put this into action. A 68-bit, a 128-bit, and a 256-bit in most cases, even blocks with a size of 512 bits are sufficient. (S. Tayal, 2003)

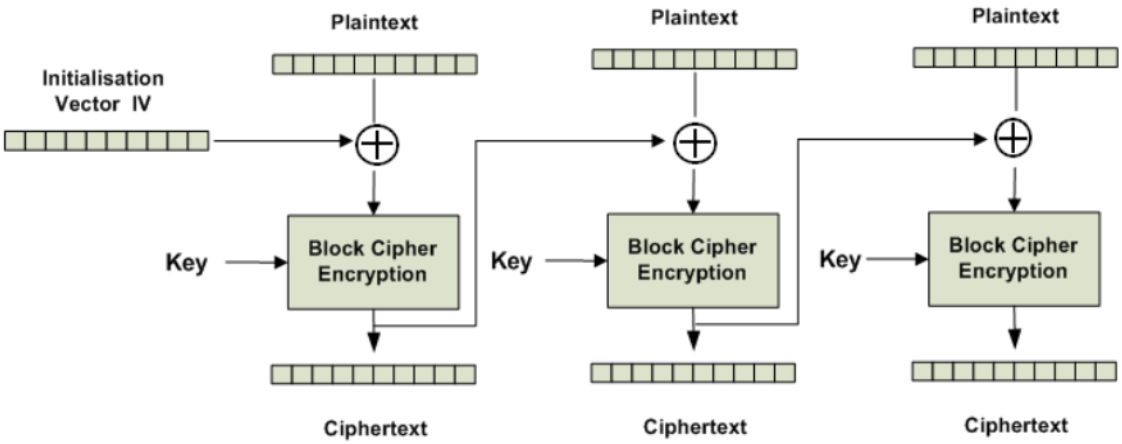

Figure 5. Block ciphers.

3.3. Public key Systems

The definition of cryptography got completely changed after the invention of public key encryption. In early 70s the application of cryptography was only limited to military and secret agency. After the invention of public key encryption, cryptography got spread into other fields and private organization. Public key encryption has an advantage over other cryptography techniques as one has not to depend on private channels for communication. Following are the features of public key encryption.

1.The use of public key encryption allows for key distribution over public networks, potentially simplifying the system's initial implementation and making maintenance simpler as parties enter or exit.

2.The need to store a large number of secret keys is reduced by using public key encryption. Even if both parties want to be able to communicate safely, each should store their own private key in a secure manner. Other parties' public keys can be stored insecurely or accessed when needed.

3.In open environments, public key cryptography is more appropriate, particularly when parties who have never met before want to communicate and interact securely. For example, a merchant might be able to disclose their public key online, and anybody who wants to make a transaction will use the merchant's public key if they need their credit card information encrypted.

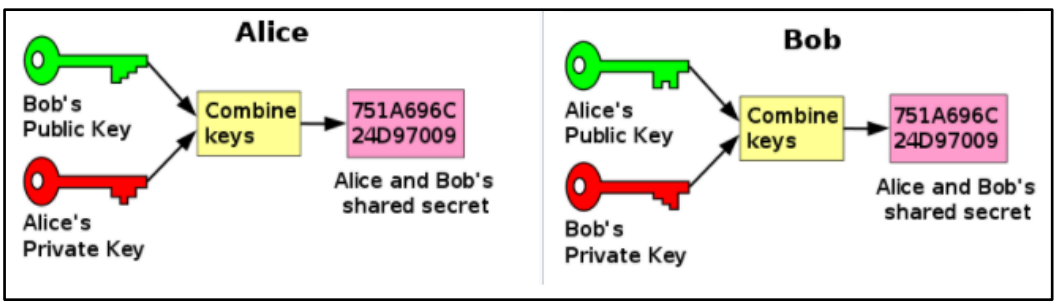

Figure 7. Public Key Ciphers.

4.DES Symmetric Encryption

Data encryption standard is the block cipher and uses 64-bit blocks to encrypt and decrypt data. It takes 64-bit of input plaintext at one end and produces 64-bit of output cipher text at another end. National Bureau of Standard wanted to protect the computer and communication data that is why developed the data encryption standard. The input we give to this algorithm is of 64-bit but we use key only of 56-bit because we want to keep 8-bits for parity checking of data. In this algorithm we use two different techniques of data encryption which is diffusion and confusion. These two techniques are applied on the text as substitution and then we applied permutation to the text. This whole process is called round. In DES we have 16 rounds which means we apply above process 16 times. After every process the block is divided in two halves namely the right half and left half. Each half is of 32-bit long. We applied all the 16 rounds on the block and after the 16 rounds we joined the right half and left half. In every round, we shift the key bits and select 48 bits out of 56 bits. Then we expand the bits of right bits which is of 32 bits into 48 bits by applying extended permutation and then we XOR it with the 48 bit of the key and permute it again. The result thus obtained is XOR it with the left half. The same process is repeated 16 times and thus the cipher text is obtained. (Schneier, 2004)

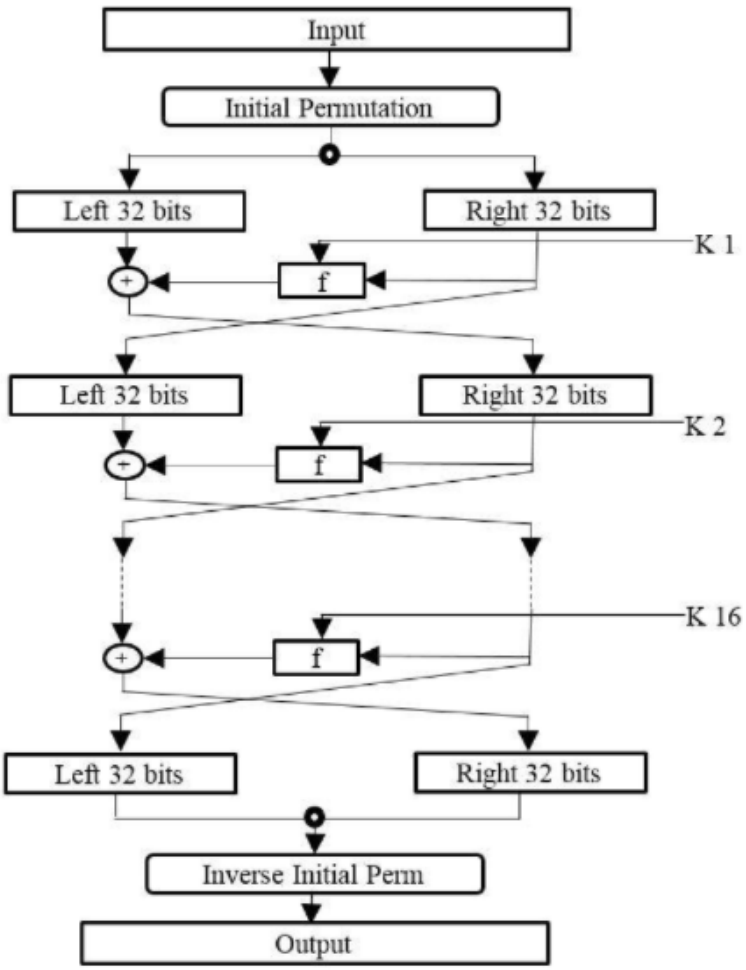

Figure 7. DES Encryption

5.AES Encryption Algorithm

Advance encryption system is one of most used type of encryption algorithm used and was developed as an alternative to DES algorithm. It also works on the process of permutation and substitution. In this method, the plaintext is turned in to block and then algorithm is applied to it. One of the major benefits of using the AES algorithm is that it uses the different key length which makes it faster safe and flexible. AES is the most widely cryptography techniques used. It is used in many applications.

1.Wireless security.

2.Processor security.

3.File encryption. (Pawan Singh, 2020)

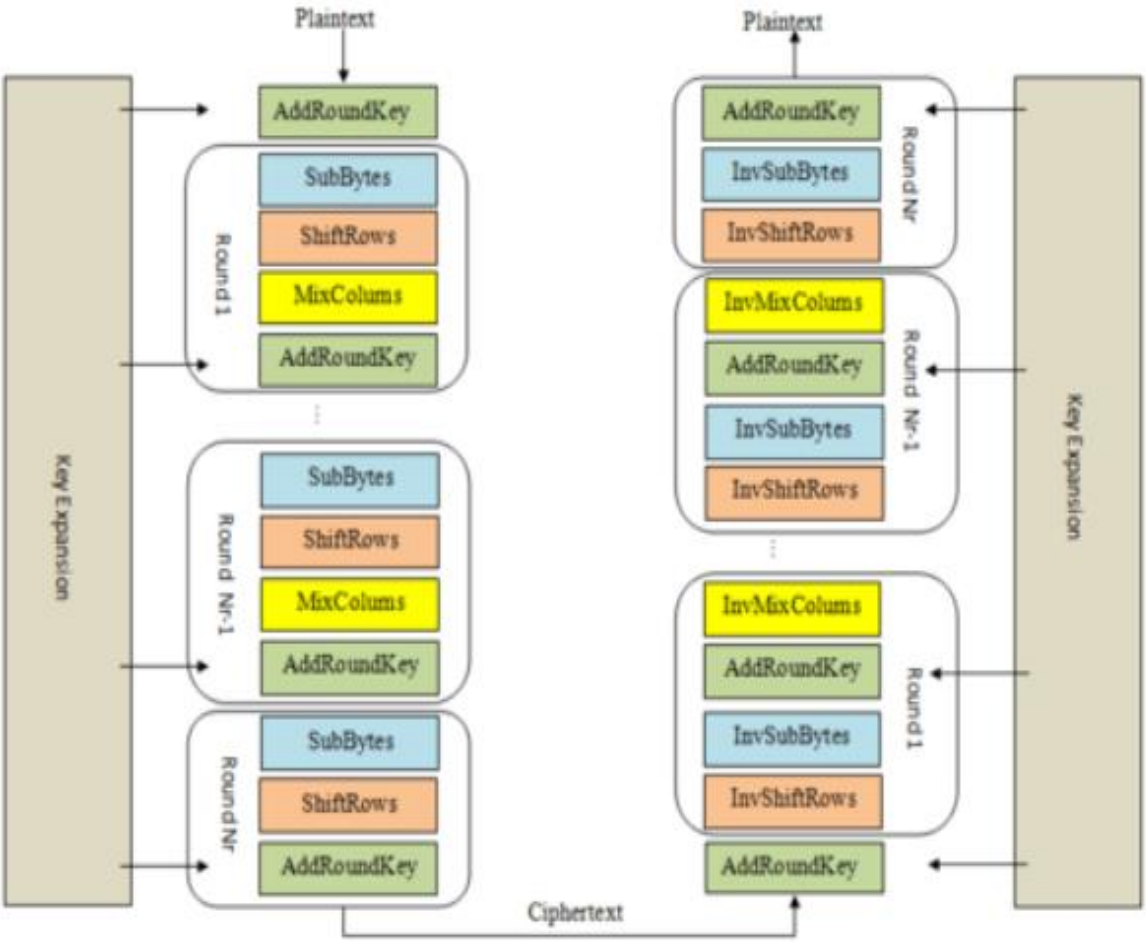

Figure 8. AES Encryption.

Table 1. Stream cipher vs Block ciphers

Block Cipher	Stream Cipher
It works on block of plain text. For example, 8 block, 24 blocks, etc.	It works on plain text 1 byte at a time.
It uses 64 bits or more.	Uses only 8 bits.
Easier to implement and is less complex.	it is more complex.
Works on two principles confusion and diffusion.	Works only on confusion.
It is nearly impossible to reverse encrypted text.	quite simple to reverse encrypted text.

Comparison between stream and block cipher and why block ciphers are way secure than stream ciphers.

Table 2. AES vs DES Comparison between two types of algorithms and why advance encryption is better than data encryption.

Advance Encryption Standard	Data Encryption Standard
The length of the key can be 128 bits,256 bits.	The length of the key is fixed that is 56 bits.
Each process has number of rounds that are depended only on key length. Example 10 rounds for 128 bits length key.	It has fixed number of rounds that is 16 rounds.
Based on substitution permutation network.	Based on festal network
The selection process is secret but accepted open public comment.	Only selection process is secret.
More secure than DES cipher.	Only triple DES is secure than usual DES.

6. Conclusion

Cryptography has become one of very important in our life and plays crucial role in attaining the aims of security and privacy goals which include the authentication, integrity, confidentiality and no-repudiation. It was developed in other to accomplish these goals. Cryptography plays a crucial role in providing reliable, strong and robust network and data security. In this paper, it has been depicted and presented the evolution of cryptography techniques over the years. Cryptography will continue to emerge with IT and business plans in regard to protecting personal, financial, medical and ecommerce data and providing a respectable level of privacy.

References

[1] F. Abbasi and P. Singh (2021) Quantum Cryptography: The Future of Internet and Security Analysis. Journal of Management and Service Science,1(1), 4, pp. 1-12.

[2] A. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” Phys. Rev. Lett. 67, 661 (5 August 1991).

[3] Ekert, Artur. "What is Quantum Cryptography?" Centre for Quantum Computation –Oxford University. Conger., S., and Loch, K.D. (eds.). Ethics and computer use. Commun. ACM 38, 12 (entire issue).

[4] Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov. 2002.

[5] Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003.

[6] Jirwan, A. Singh and S. Vijay, "Review and Analysis of Cryptography Techniques," International Journal of Scientific & Engineering Research, vol. 3, no. 4, pp. 1-6, 2013.

[7] S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology.

[8] J. Callas, "The Future of Cryptography," Information Systems Security, vol. 16, no. 1, pp. 15-22, 2007.

[9] J. L. Massey, "Cryptography—A selective survey," Digital Communications, vol. 85, pp. 3-25, 1986.

[10] B. Schneier, "The Non-Security of Secrecy," Communications of the ACM, vol. 47, no. 10, pp. 120-120, 2004.

[11] N. Varol, F. Aydoğan and A. Varol, "Cyber Attacks Targetting N. Varol, F. Aydoğan and A. Varol, "Cyber Attacks Targetting Android Cellphones," in the 5th International Symposium Tirgu Mures, 2017

[12] S. Yadav, P. Singh (2020) Web Application and Penetration Testing. Journal of Informatics Electrical and Electronics Engineering, 1(2), 3, 1-11.

[13] S. K. Tomar and P. Singh (2021) Cyber Security Methodologies and Attacks. Journal of Management and Service Science, 1(1), 2, pp. 1-8.