RESEARCH REVIEW JOURNALS
Volume-04
Issue-03
March -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Analysis on Encryption Algorithm in Cryptography

[1]Hemlata and [2]Dr Yashpal Singh

[1]Research Scholar, Kalinga University, Naya Raipur, Chhattisgarh
[2]Research Supervisor, Kalinga University, Naya Raipur, Chhattisgarh

ARTICLE DETAILS

Article History
Published Online: 15 March 2019

Keywords
Decryption, Encryption, Algorithm

ABSTRACT

The modern cryptography and cryptanalysis, which compose the technology of encryption and decryption cryptology. In cryptography we encrypt the message to secure our message from the attacker, so that he can't read our message for any sort of misuse. Suppose we apply encryption algorithm in coded form on plain text called cipher text. We use key in encryption because plain is simple and cipher is coded. The main emphasis of cryptography study to show to design good (secure and fast) encryption algorithms. In crypto analysts, we take a reverse process suppose we have cipher text and we don't have key because in encryption we use key. Suppose attackers want to attack on our data. When he attacks he only have cipher text to attack. He only have cipher text to attack to know the plain text the process of decoding the cipher text into plain is called cryptoanalysis. In cryptoanalysis the intruder tries to find out the loophole in the encryption technique that is applied on the data to make it secure. After lot of studies and finding the intruders starts working on the loopholes to find out the plain text of that cipher texty.

1. Introduction

All the phases have different activity out of which first two phases will encrypt image on the bases of prime and Fibonacci numbers third phase will use for transformation image to text data and last two phases will work for encryption at text level. At text level fourth phases is work on Group-Code Technique which is responsible for encrypt data at text level as well as compress data and in fifth phase data is finally convert in ciphertext which is found in bits form. And also for decryption there are 5 phases introduced which are just apposite of these phases.

Cryptography technique is a type of technique for secure communication in the presence of he adversaries. Cryptography is the study to construct and analyse the methods that prevents from the intruders to read the personal data. Why do we need cryptography the question arises. Suppose we have a person and he is sending a message to another person called receiver named as sita there we need a medium or a channel through which the first person sends the data called sender through internet the question comes in mind that is it safe or not. If the first person named ram is sending message to sita and if the third person who is hacker changes the message in between the way to sita. Cryptography is basically used for gaining security. Suppose the sender is sending a message HELLO by the help of cryptography it changes the plain text into cipher text like symbols of same bits of some extra bits to confused the intruder and not able to reach to that information that the sender is sending to the receiver. When a plain text or message is converted in the form of codes is cipher text and also called encryption. When message travels and at the end reached to the receiver and is decrypted means opposite of encryption again cipher text converted into the plain text while the process of decryption is forms. It is used to secure security by the various encryption technique are used by this message cannot be understood by the third party intruders after applying cryptography. When we are receiving that the message is end to end encrypted means in between and no one hacks that message. Cryptography is used to provide security to protect the important information by converting data into the unrecogniseable form. While transferring only the person whom we are sending can only read this. Both the keys may be same or different for encryption and decryption.

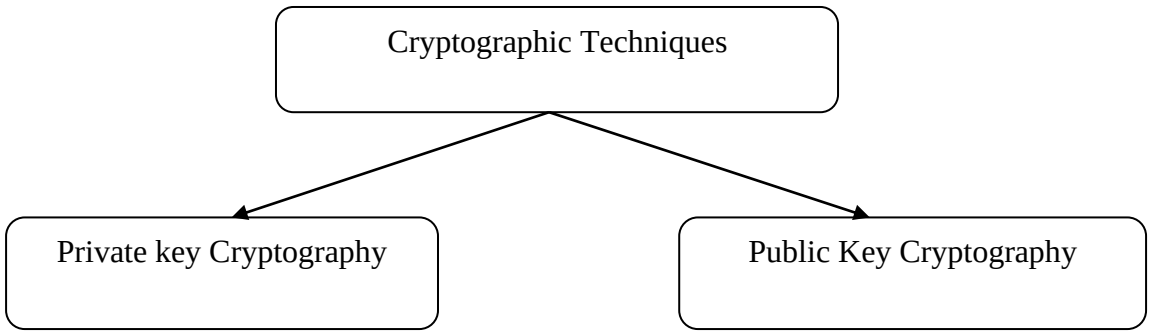

Figure 1: Types of Ccryptography

2. Review of Literature

Hai Yu and Zhiliang Zhu proposed a technique based on image reconstruction using some adjacent pixel characteristics. According to the different characteristics of different bit level binary images, the proposed encryption scheme reconstructs the image at the bit level. Two parts of information, the significant one and the unimportant one, are treated differently and processed separately. Simulations and cryptanalysis both show that the proposed image encryption scheme is more efficient and yields better level of security.

K.C. Ravishankarand M.G.Venkateshmurthy proposed technique segments the image into regions of fixed size. These regions act as units for processing the image. Selective Encryption makes it possible to encrypt only a part of the image leaving the rest of the image unaltered. Here, the regions covering the part of the image are considered for encryption. Selective Reconstruction deals with decrypting only a part of the encrypted image. Both the methods give a fair amount of reduction in the encryption time. Once the segmentation and permutation of regions is completed, the regions are encrypted independently.

3. About Encryption

An encryption/decryption system is also called a cipher, or a cryptosystem. Accordingly, the encryption machine is called anencipher, and the decryption machine is called a decipher. The message for encryption is called the plaintext, and the encrypted message is called the cipher text. When Key if encryption = Key of decryption , the cipher is called a private-key cipher or a symmetric cipher. For private-key ciphers, the encryption-decryption key must be transmitted from the sender to the receiver via a separate secret channel. When Ke 6= Kd, the cipher is called a public-key cipher or an asymmetric cipher. For public-key ciphers, the encryption key Ke is published, and the decryption key Kd is kept private, for which no additional secret channel is needed for key transfer.

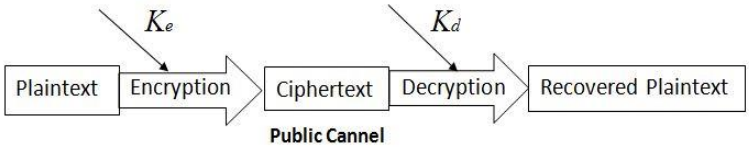

Figure 2: The Encryption and Decryption Procedures of A Cipher

Following the widely-acknowledged Kerckhoff s' principle in the cryptology community, it is assumed that all details of the encryption/decryption algorithms are known to attackers. This means that the security of a cipher relies on the decryption key Kd only. Thus, the main task of cryptanalysis is to reconstruct2Master Thesis of Zhejiang University the key, or its equivalent form that can successfully decrypt all or partial contents of any plaintext encrypted by the cipher.

4. Encryption Algorithm

1. Symmetric vs. Asymmetric Encryption Algorithm

When both the keys are similar for encrypted and decryption is called symmetric key cryptographic when both the keys are different for encrypted and decrypted that it is called asymmetric key cryptography. Encryption it is a technique through which we transmit our information by converting the readable form by applying keys on it. Encryption algorithm are used to convert normal data into the coded form. Opposite of this technique is decryption as it is we inverted the process called decryption sometime same codes are needed to decryption the data different codes are to be used for the decryption of data. Decryption is used to convert the coded data into the normal form or we can convert cipher text to plain text key. Key means combination of bits and string that is used for plain text into cipher text and cipher text into plain text. Basically, the use of this is for secure transaction or communication anything that can be done in between sender and receiver like 123ABC. So many of our sites and emails are to be saled our data so it is a very alarming situation for us all. To protect our data it is necessary to enhance the security using digital image processing. For this there are techniques to use are steganography, cryptography, encryption to keep our data highly confidential for future use also. By digital image the secret message and the secret image is to be sent across. Firstly, the encryption step is used for converting the cipher image using AES technique by this it firstly resizes the original size of the particular image.

2. Symmetric Key Cryptography (Secret Key Cryptography)

So, care should be taken while exchanging keys between the sender and the receiver. Symmetric key cryptography is also called secret key cryptography and private key cryptography. This is very easiest type of encryption method involves only one key means same key for both side encryption and decryption in other words coded to uncoded, cipher to decipher or in applying code are removing codes. just like same key is used for locking and unlocking decryption technique. Encryption technique system is the most popular example of symmetric key cryptography. It is not that much complex and the power that is used in computation is lesser and transmit the data in bulk. Symmetric key cryptography technique takes less time in execution.

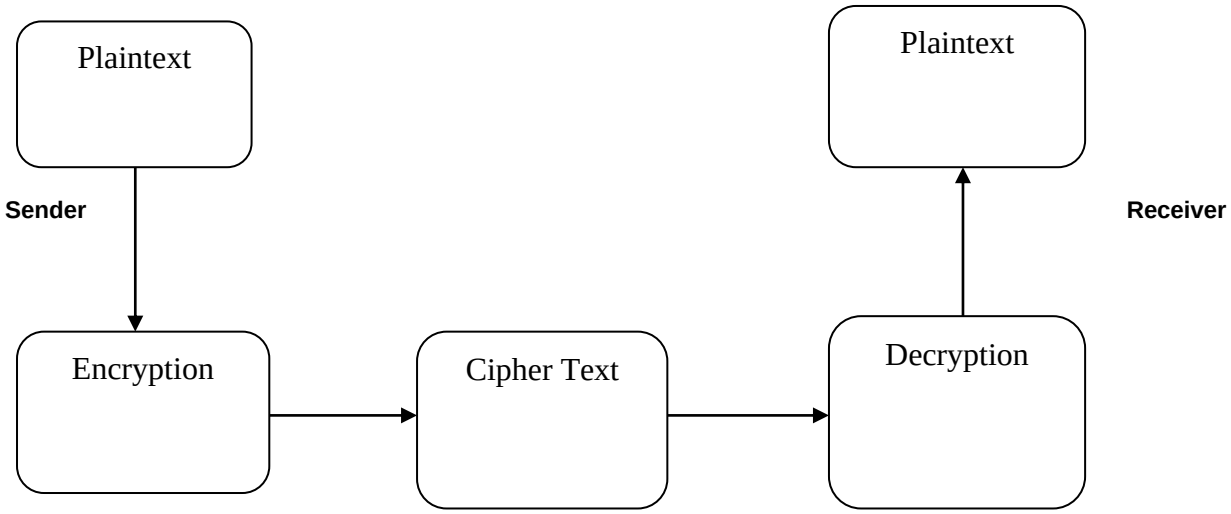

Figure 3: Symmetric Key Cryptography

3. **Asymmetric Key Cryptography (Public Key Cryptography)**

Asymmetric key cryptography is the technique where two keys are used. One key is used to lock or encrypt the plaintext, and another to unlock or decrypt the cipher text. Neither key can do both the functions. One of these keys is published or made public and the other is kept private. This technique has comparatively slower data rate throughputs than the symmetric key technique. Asymmetric key cryptography is also known as public key cryptography. In this type of cryptographic technique two keys are used for encryption and decryption purpose like one key is used for applying lock on the plain data in the forms of code to increase security to save from the third party like hackers and intruders and the different key is used for unlocking the codes means to convert cipher text into plain text. One key is public key that is known to every one that's why it is named as public key. Another key is private key only the private person means important and authenticate person that can access have private key. These two keys are private key and public key. suppose we are making any project so if any projects are required in the project then only private person can do all that editing.is example of private key and public key is that is known to everyone .In asymmetric cryptography in this the sender is using the public key for the purpose of encryption then the message can be decrypted with the help of private key only and only. And if the sender is using the private key to encrypt the plain text into cipher text then for the purpose of decryption only and only. Public key is used because the technique we are using is asymmetric it is necessary to use two different keys on both the sides. Asymmetric key cryptography takes more time in execution. In comparision with symmetric key cryptography it is more complex and more power in computation is required. Ellipse curve technique, DSA Technique, RSA Technique is the example of Asymmetric key cryptography. The purpose of this asymmetric key cryptography is exchanging two secret keys.No any problem by using different two keys diffie hellmen technique.

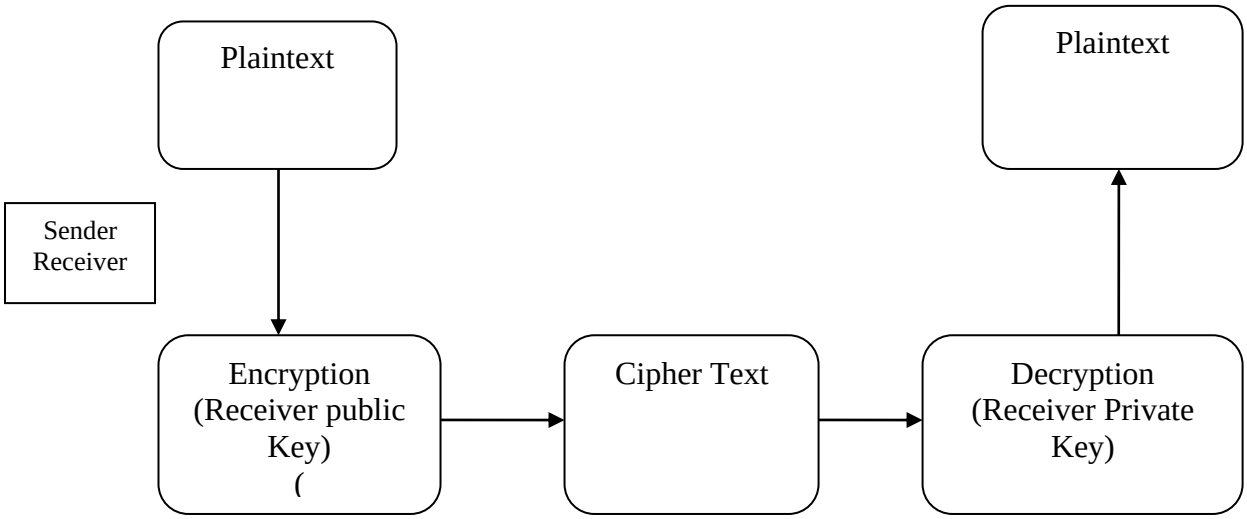

Figure 4: Asymmetric Key Cryptography

5. Conclusion

Hash functions are irreversible functions. Once the hash value is generated, the original text cannot be generated back from it. A one-way hash function takes variable-length input that may be a message of any length, even thousands or millions of bits and produces a fixed-length output; say, 160-bits. The hash function ensures that, if the information is changed in any way, even by just one bit then, an entirely different output value is produced.

1.Stream and Block Encryption

A stream cipher is an encryption system which works over a given sequence of input bits. Most stream ciphers work by generating from the key a long sequence of random-looking bits, which are then combined (by bitwise XOR) with the data to encrypt. This is a (crude) emulation of one-time pad .A *block cipher* is a generic cryptographic element which works over "blocks" which are sequences of bits with a fixed length (e.g. 128 bits for AES). The block cipher is a permutation of the blocks; the key selects which permutation we are talking about. A block cipher alone cannot process an arbitrary long message; the block cipher and the data must be used within an elaborate construction called a mode of operation (also often called a "chaining mode").There is a chaining mode for block ciphers called "CTR" as "counter mode": in this mode, the block cipher is used to encrypt successive values of a counter (the counter having the size of a block). The resulting encrypted blocks are then concatenated, resulting in an arbitrarily long sequence of bits which depend only on the key. It suffices then to XOR that sequence with the data to encrypt. In other words, CTR mode turns a block cipher into a stream cipher. Another popular chaining mode is CBC, which does*n't* fit the model of a stream cipher. With stream ciphers, what must be avoided at all costs is reusing the same key-dependent sequence of bits for two distinct messages; this would yield the infamous "two-times pad" which can be broken quite easily (by exploiting redundancies in the two encrypted messages). With a block cipher in CTR mode, this translates to reusing the same counter values.

This is why CTR mode requires a random *Initial Value* (IV) which is the counter value you begin encryption with. By choosing a new random IV, with sufficiently large blocks, you avoid with very high probability any overlap in the sequences of counter values that you use. The concept of IV is not specific to block ciphers; some stream ciphers also use an IV (e.g. the one in thee STREAM). When a stream cipher has an IV, reusing the key is no problem -- provided that you use proper IV (i.e. IV generated with a cryptographically strong RNG in the complete space of possible IV, with uniform probability). However, some other stream ciphers do not have an IV, in particular the widely used RC4. Reusing the same key would mean reusing the exact same sequence of generated bits, and that's bad. Note that some chaining modes other than CTR also need an IV, which should be unique for each message encrypted with a given key. Block ciphers do not alleviate the need for that.

2.Attack Scenarios

In addition to the more pragmatic approach of matching the security of an encryption scheme against the computational capabilities of the adversary, there exists a tradition in symmetric cryptography to link the security requirements of a cipher to its external dimensions. The ambition is to design ciphers which are optimal in the sense that they cannot be attacked in a significantly more efficient way than any other conceivable cipher with the same external dimensions. Or with other words, that their security can only be increased by increasing at least one external dimension. If a cipher fails to satisfy this requirement, then this is considered to be a *certification weakness*, regardless of the practical implications .The discussion above raises two questions: (1) what exactly do we consider being the external dimensions of a cipher? And (2) what is the maximal In the case of encryption, the task of the adversary Eve consists in recovering unknown parts of the plain text, or better yet, recovering the secret key.

Different attack scenarios can be distinguished depending on what information Eve can obtain, and to what extent it can interfere in the communication between Alice and Bob. From the crypto graphical point of view, a cryptographically strong cipher should be secure enough against all kinds of attacks. For most ciphers, the following attacks corresponding to different scenarios should be checked (from the hardest to the easiest):

3.The cipher text-only attack - attackers can only observe part of the cipher texts

This type of attack only assumes that Eve is capable of capturing encrypted text. As this is likely to be the case (otherwise there would be little reason to encrypt the messages in the first place), encryption schemes succumbing to cipher-text only attacks are considered to be particularly insecure.

4.The known-plain text attack - attackers can get some plain texts and the corresponding cipher texts

A known-plain text attack requires Eve to have access to (parts of) the plain text corresponding to the captured cipher text. This additional requirement is typically rather easy to fulfill. A good example is an online payment on the Internet: while the browser and the server will exchange several kilobytes of encrypted data, it is likely that the only unknown part is a 16-digit credit card number.

5.The chosen-plain text attack - attackers can choose some plain texts and get the corresponding cipher texts

Some attacks only succeed when the plain texts have a specific form. In order to mount such attacks, Eve must find a way to influence the encrypted plain texts. A practical example is a secure connection between Alice and her mail server. By sending carefully crafted mails to Alice, Eve can get the server to encrypt the plain texts she needs.

6.The chosen-cipher text attack - attackers can choose some cipher texts and get the corresponding plain texts

This attack requires Eve to have control over the cipher texts sent to Bob, and to be capable of monitoring how they are decrypted. For example, Eve could try to attack a pay TV decoder by feeding it with special cipher texts and analyzing its output. Notice that such attacks will not work if the receiver has a means to check the integrity of the cipher texts.

7.Chosen-IV attacks

If the encryption scheme takes as input an IV, Eve might have means to control this value as well. At the receiver side, the IV typically needs to be derived from a header which is prefixed to the cipher text. Hence, if Eve can corrupt cipher texts, she can most likely modify the IV used during decryption as well.

8.Adaptively chosen-plain text/cipher text/IV attack

In order to mount one of the attacks described above, Eve will typically need to obtain the encryptions or decryptions of a whole series of chosen data blocks. When the choice of a

certain block depends on the results obtained from previous blocks, the attack is called adaptive. One could still imagine other attack scenarios. Related key attacks, for instance, where an attacker manages to obtain pairs of plain texts and cipher texts encrypted with different but related secret keys such attacks are worth studying when block ciphers are used to construct hash algorithms, for example. However, in the context of encryption schemes, these attacks are of limited relevance, since they can easily be prevented by choosing an appropriate key generation procedure, without affecting the efficiency of the scheme in any significant way.

In these kinds of attacks, cipher text-only attack is the easiest and the most common attack, due to the fact that the communication channel is generally accessible for attackers. Known/chosen-plain text attacks are possible when an attacker can temporarily access the encryption machine, or he can successfully guess the plain texts or some segments. Chosen-cipher text attack is possible when an attacker can have a temporary access to the decryption machine. The last three kinds of attacks, which seem to seldom occur in practice, are feasible in some real applications and have become more and more common in the digital world today.

References

1. Sinha and K. Singh, “A technique for image encryption using digital signature”, Optics Communications, 2003, 1-6, www.elsevier.com/locate/optcom.
2. Mok Shin, D. HoanSeo, K. Bo Chol, H. Wmn Lee, and S. Kim, “Multilevel Image Encryption by Binary Phase XOR Operations”, IEEE Proceeding in the year 2003.
3. F. Belkhouche and U. Qidwai, “Binary image encoding using 1D chaotic maps”, IEEE Proceeding in the year 2003.
4. W. Ying, Z. DeLing, J. Lei, et al., “The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System”, Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December, 2004.
5. Anish Gupta, K.B.Singh, R. K. Singh. Study of Web Crawling Policies, International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2013.
6. Anish Gupta, Priya Anand. Focused Web crawling and Its approaches, International Conference on Futuristic Trend on Computational Analysis and Knowledge Management, 2015, IEEE Digital Library.
7. Dushyant Kumar, Dr. P.K. Dwivedi. *A Study on In-Time-Frequency Algorithm.* Cosmos: An International Journal of Management, 7(2): 1-3, 2018.
8. Agarwal, Nidhi and Jaiswal, S., (2018). “A Study On Job Satisfaction Among Female Teachers”. Globus: An International Journal of Management & IT, 2018, *9*(2).
9. Agarwal, Nidhi and Shiju,P.S., (2018). “A study on CMS with web usage solutions”. International Journal of Advance Research and Development, 2018, 3(2), 1683-1685.
10. Kumar, Puneet, “A Global Change in Education through Information Technology & Communication”. Gyanodaya : The Journal of Progressive Education’, pp 22-26, 2008.
11. Khasim, Sayed, “The Discussion on Breaching Information Security”, Cosmos Journal of Engineering & Technology, 4 (2): 29-33, 2014.
12. Kumar, Puneet and Gupta, Ruchika, Information System's Security by using Matrices and Graphs, Conference proceedings on Information Security and Mobile Computing, pp. 62-66, 2008.
13. Agarwal, Nidhi and Pundir, Neelam, “Information and Communication and Its Importance”. Ambikeya Journal of Education, 8(1): 40-42, 2017.
14. Dr. Sangeet Vashishtha, Pooja Sharma, Big Data- New Trend of Change in Complex Corporate World. Globus An International Journal of Management & IT, 10(1): 4-6, 2018.
15. Agarwal, Nidhi and Gupta, Ruchika, “Role of Technology for the Efficiency of HR Management”, Information and Communication Technology: Challenges & Business Opportunities, Excel India Publishers, Delhi, pp. 174-176, ISBN: 93-80697-95-3, 2011.
16. Anuradha. “Study in Technological Challenges in Digital Libraries”, Cosmos An International Journal of Art & Higher Education, 4(2): 9-11, 2015.
17. Mishra, Shivani and Soni, Dr. Anita. “A Study on Technology, Thinking Styles, and Content of Education”, Cosmos An International Journal of Art & Higher Education, 5 (2): 1-4, 2016.
18. Adarsh Tiwari, Dr. Sudesh Kumar. *A Study on Business Drivers to Receive Cloud Computing.* Cosmos Journal of Engineering & Technology, 8(1), 1-3, 2018.
19. Gupta, Ruchika and Kumar, Puneet. “Information Technology Business Value Assessment: A Case of State Bank of India”. Globus: An International Journal of Management & IT, 42: 30-34, ISSN:0975- 721X, 2013.
20. Sharma, Dr. Seema. “Technology, E-Learning and Social Media with Reference to Academic Achievement”, Cosmos An International Journal of Art & Higher Education, 6 (1) : 7-8, 2017.
21. Misra, Lisha and Saxena, Dr Aakash. *A Study on Security Goals for Wireless Network.* Cosmos Journal of Engineering & Technology, 8(1), 2018.
22. Umesh A. Patel, Nita Brahmbhatt. “Implication of Six Sigma to Improve Library Services in Academic Libraries”, Globus Journal of Progressive Education,4(2): 1-3, 2014.
23. Kiruthiga Devi M, Dr. Sudesh Kumar. Artificial Intelligence, Machine Learning And Cognitive Computing with Profound Learning Technique. Globus An International Journal of Management & IT, 10 (1): 23 – 26, 2018.
24. *Dr Gandhi Singh Chauhan. Criteria To Select Library Automation Software.* Cosmos: An International Journal of Management, 5(2): 1-5, 2016.
25. Surishma Singh, Adnan Nasir. Digitalization of Education through Understanding of ICT. Globus Journal of Progressive Education, 8(1), ISSN: 2231-1335, 2018.

