Cryptography with High Throughput:A survey

Bhoomika Modi, Vinit Gupta
Department of Computer Engineering,
Hasmukh Goswami College of Engineering, Vehlal
Gujarat Technological University

***Abstract*- Cryptography is primary requirement in any type of area. Cryptography is used for secure the data and communication between two parties. Some organization may have large set of data and some may have small set of data. Sometimes large data needs low security and small data needs high security. For that purpose various symmetric and asymmetric algorithms are used like DES, 3DES, AES, BLOWFISH, IDEA, RSA. In this research algorithms are used for encryption and decryption and measure the performance and throughput according to speed, time, memory. In these all algorithms some arithmetic and logical operations are performed.**

***Index Terms*- Cryptography, Encryption, Decryption, Security, DES, Blowfish, 3DES, AES.**

I. INTRODUCTION

With the increase of security, hacking and cracking of information has also increased. If user want to secure the information then cryptography is necessary. For that block cipher encryption and decryption technique is used. In block cipher, symmetric technique like DES, AES, 3DES, Blowfish are used. In symmetric cryptography, same key is used for encryption and decryption process. In the cryptography plain text is converted in the cipher text by using key. To convert plain text to cipher text, encryption algorithm is applied on text using key. And to convert cipher text to plain text decryption algorithm is applied on cipher text using key. Some algorithm requires key generation before encryption and decryption steps. For that three main processes are required:
Key generation,
Encryption,
Decryption.

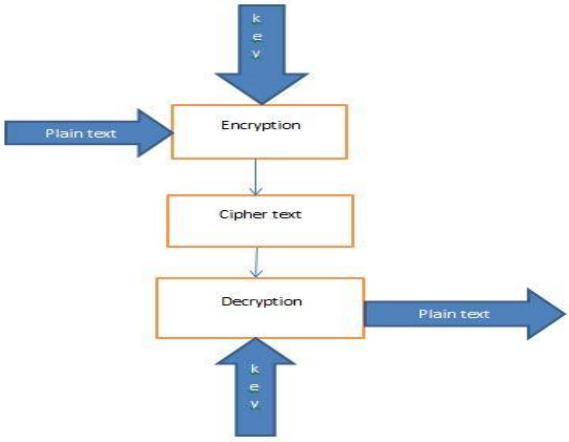

Fig:1. Encryption and Decryption process

II.THE ORETICAL BACKGROUND & LITERATURE REVIEW

2.1 THEORETICALBACKGROUND

2.1.1Cryptography

There are lots of algorithm like DES, AES, 3DES And Blowfish that are too much popular in cryptography world. These all algorithms are used in various application like in database, communication, shopping, blogging, web feeds, internet banking and many more. In all these algorithms, different types of operations are performed like bitwise XOR, Substitution, Shifting and many more.

2.1.2 ALGORITHMS USED IN CRYPTOGRAPHY:

AES (Advanced encryption standard):

It is founded by Rijndael. It has 128 bit block size with 128 bit (10 cycles of repeating), 192(12 cycles of repeating) or 256(14 cycles of repeating) bits of key size. In this algorithm XOR, mix columns, shift rows, add

round key operations are performed. This algorithm suffers from brute force attack because if attacker have dictionary of words in English then can easily find the word which is used as a key.

DES (Data Encryption standard):

This algorithm uses 64 bit of plain text and key with 56 bit. It also works on various shifting and XOR operation. DES has a main problem of key. It's key size is too much small so attacker can easily get the plain text.

3DES (Triple Data Encryption Standard):

It is updated version of the 3DES. It performs same operation as a DES but the difference is that it is encrypted by 3 times so it is more secure than DES. The main problem is that it use 3 times level of encryption. It becomes very much slower than other method.

Blowfish:

Blowfish is the fastest and secure than above three algorithms. It has a variable key length of 32 to 448 bits and has a 64 bits of block size. Its main advantage is that it is freely available for all users and unpatented. These all have some weak points. Like long range of key provides high security than short. Complex structure of the algorithm increases execution time.

New Enhanced algorithm:

Mr. Nilesh has proposed new algorithm to overcome above algorithm's disadvantage. In this algorithm he has used 128 bit block size and also key size is 128 bit. He has used simple shifting and logical XOR operation. At first the 16 character is converted in the 128 binary form and also key is converted in the binary form.

Then the operations are performed on it. Here first and last steps execute one time only but in between some steps are repeated N times so it provides high security and attacker cannot know that how many times he has to repeat that steps.

This algorithm also shows the throughput on the processor core 2 duo of 1GB RAM. It shows the 100KB, 1MB, and 10MB throughput compared to other algorithms. And it is clear that this algorithm gives high throughput than others.

It also prevent from brute force attack. It gives the output very fast than other algorithm and also provides security.

2.2 LITERATUREREVIEW

Literature review is the whole survey of the research. It shows different analysis of the algorithms and also shows comparison based on performance. Here authors have explained about their algorithm according to their research. This survey is based on asymmetric and symmetric block cipher cryptography.

2.2.1 Performance Comparison of Data Encryption Algorithms (IEEE, 2005)[1]

According to title, here performance comparison of different data encryption algorithm have explained. For that various block cipher algorithm like DES, AES, 3DES, and Blowfish are used. Encryption algorithm are used in field like banking, e-commerce and online transaction. These algorithms are applied on different input of different size and key. For implementation java language is used. After all this algorithms is verified on the two hardware platforms P-2 266 MHZ and P-4 2.4 GHZ. They also measure the performance, execution time, and result on block cipher mode.

Advantage:

- Blowfish is fastest algorithm for implementation.

Disadvantage:

- Java is used for implementation and it has very slow speed. So it will work very slowly for various algo's performance measure.

2.2.2 Cryptanalysis of Modern Cryptographic Algorithms (December 2010,IJCST)[2]

Cryptography is used to secure the message and data and prevent the attacks. Here two types of algorithms are used (1) symmetric algorithm and (2) asymmetric algorithm. Other modern or latest algorithms are also used for symmetric and asymmetric cryptography. In symmetric algorithm AES, DES, and IDEA are used and in asymmetric RSA is used. For implementation Cryptool is used.

According to author the main security requirements are:-
1. Authentication
2. Data integrity
3. Confidentiality
4. Non repudiation

Here above algorithms suffer from some kinds of attack like in DES, it also suffers from brute force attack. In AES, it suffers from xsl attack. Now in RSA, suppose "e" is too small then also attackers can attack.

In symmetric algorithm for encryption and decryption the same keys are used so it will be easy for sender and receiver. In asymmetric algorithm for both encryption and decryption keys will be different.

Advantage:

- Modern cryptography gives better performance for ex: in IDEA it use 64 bit P.T so it will be easy for decrypt and also AES and RSA are used for large message so can provide security.

Disadvantage:

- For long message it requires too much time for CPU according to key increase.

2.2.3 A Novel Approach for Enciphering Data of Smaller Bytes (August 2010, IRCSIT) [3]

Cryptography model can be changed according to the size of data. Sometimes, small size of data needs high security and long data needs lower security. R.Satheeshkumar explained about the small size of data. He has used improved symmetric algorithm. Here he has used 4-bit key as secret key for the small P.T.

This 4-bit secret key can be any binary form and can be change in every character of the P.T. This key is used for encryption and decryption of the small data. It provides simple and secure encryption and decryption.

Then after author have used 4-bit shared key for secure transmission b/w sender and receiver. This key is used for encrypt the 4-bit secret key and it also can be any binary form and this key is shared b/w two communication parties. Each time key is incrementing by 1 bit so now key is encrypted to 9-bits.

For key management issue he has used the two level encryption method. At first stage, data is encrypted by secret key and then at second stage, this key is encrypted using shared key. For that ASCII converter, bitconverter, division, multiplier operations are used.

Advantage:

- Encrypting small size of data is easy and provides high level of security. It takes short time for completion of process. Key distribution will also be easy.

Disadvantage:

- It is easy for process and provides high security but large key usage will be more secure than small data.

2.2.4 DES, AES and Blowfish: Symmetric key cryptography algorithm simulation based performance analysis (2 December 2011, IEEE) [4]

Here author explained about symmetric algorithm and their performance according to speed, block size and key size parameters. Algorithms are DES, AES, and Blowfish. They are applied on different encryption modes of block ciphers like ECB, CBC, CFB, and OFB. He shows the result on these modes.

For ECB mode, DES is used as an encryption technique. Time consumption is also shown by graph. In ECB mode blowfish require less processing time than other two. The experiments are done using AMD processor with 2 GB of RAM. CFB requires less processing time than ECB and CBC. Here for implementation, java is used.

Advantage:

- AES is better than DES but Blowfish is too much better than other two. And OFB is also better than ECB and CBC.

Disadvantage:

- AES suffers from brute force attack and Blowfish from weak keys problem.

2.2.5 A Comparative Study of Six Most Common Symmetric Encryption Algorithms across Different Platforms (2012, IJCA) [5]

Mr. Ramesh told about six symmetric algorithms on different platforms. For that RC6, UMARAM, UR5, DES, 3DES, and RC2 are used. RC2 is block cipher of 64-bit block size and key size is b/w 8 to 128. RC6 has a block size of 128 bit and key size also support to 128,192,256. UMARAM and UR5 are new algorithms. They both uses transformation, XOR gate and AND gate.

In UMARAM, key generation process generates 16 keys during 16 rounds. These algorithms are applied on the different OS like windows XP, windows 7, and vista.
These algorithms are applied for the both text and image data. For image data, speed of UMARAM is good in all the above OS. For text data UR5 is the best in speed on different OS.

Advantage:

- UR5 and UMARAM are the better algorithm than 3DES in speed and time consumption.

Disadvantage:

- In comparison with AES and Blowfish, UR5 and UMARAM don't give better performance.

2.2.6 Performance Evaluation of Cryptographic Algorithms: DES and AES (2012, IEEE) [6]

Author shows the performance evaluation of DES and AES. These algorithms calculate CPU time, memory and computation time. After the programing, it compares to the avalanche effect.
This implementation has been done in the MATLAB 7.0 software. For our PC, it requires Intel Pentium(R) Dual Core CPU T4300 at 2.1GHz, 1.19 GHz with 2GB of RAM and 500 GB of hard disc capacity. In DES avalanche effect is too much less, but in AES, this effect is very high. Memory required for DES is 43.3 KB and simulation time for that is 0.32 per second. In AES, memory required is 10.2 KB and time is 0.0304 sec.
Advantage and disadvantage are according to parameter speed, memory and time which are shown above.

2.2.7 UR5: A Novel Symmetrical Encryption Algorithm With Fast Flexible and High Security Based On Key Updation (April 2012, IJARCSSE) [7]

Here author explained about the UR5 symmetrical algorithm. It avoids the key exchange between the two parties and also reduces the time for processing. According to author, UR5 gives higher rate than other algorithm. It encrypt 64 bit plain text by using key size of 64 bit. It is the simple and very helpful against hackers. Its **S BOX** generation is the backbone of the algorithm and uses 8 columns and 256 rows. Each consist 8 bits. It replaces input by other code to the output. It also uses the XOR operation, round key. It is applied on a text by using software MS Visual C++ and for hardware Intel(R) Pentium(R) 4 CPU 2.8GHz 1GB of RAM required.

Advantage:

- Attacker can't know the key even he have the P.T and C.T.
- It reduces the delay taken for the encryption and decryption process.

Disadvantage:

- Key is updating at each packet so many keys are required and key distribution becomes problem.

2.2.8 Modern Encryption Standard (MES): Version-II (2013, IEEE) [8]

Here author explained about new encryption technique called modern encryption standard (MES-II). In this method, modified vernam cipher method with different block size is used. Here block size is taken from left to right and then combined them by taking 2^{nd} half and 1^{st} block. Again this vernam method is applied from left to right. Author has applied on various P.T and gets different result. This method is free from different attacks like brute force attack, known plain text attack and differential attack. Basically it is used for short message like SMS, or any password. It gives random set of character for input stream. Cipher text file contain a sequence of 65 single ASCII character. It may be byte wise or bit wise encryption.

Advantage:

- It is best for short message like SMS and password. And generate random characters.

Disadvantage:

- It is not working for long message.

2.2.9 Fault Attacks on AES with Faulty Cipher texts only (2013, IEEE) [9]

Here author explained about the fault attacks on the AES with only faulty cipher text. Old fault Attacks sometimes require the ability to encrypt twice the same plaintext, to get one or several pairs of correct and faulty cipher texts corresponding to the same message. Author says that attackers don't know the input message and has only access to the faulty C.T. He explained this attack on the AES-128 on the last four rounds. He has used non-uniform fault model to recover the correct keys with time complexity using only faulty C.T. On 9^{th} and 8^{th} round of

AES, he assumed that attacker is able to encrypt the unknown group of plain text and to inject on a byte. According to him fault model covers a large set of faults like injected fault is only assumed to disturb byte in such way that the distribution of faulty value is biased.

For the attack on the 7^{th} and 6^{th} round he assumed that attacker is able to inject a fault on a diagonal of the state during encryption. Diagonal means set of four bytes. By using fault model, this four bytes are processed in four tuples, and in mix columns operation, they are manipulated together.

Advantage:

- Attacker doesn't know the encrypted message so he cannot obtain a pair of correct or faulty C.T from plain text.

Disadvantage:

- Require faulty cipher text for applying the faulty model and in best case it may not be present.

2.2.10 The New Cryptography Algorithm with High Throughput (Jan 2014, IEEE) [10]

Mr. Nilesh has explained about the new algorithm for increase high throughput. He has used some arithmetic and logical operation for encryption and decryption. Here, pain text and keys are of 16 character and they are converted in the binary 128 bit. And then by using XOR, arithmetic and logic operations, these character are encrypted. Here some steps are repeated N times for more security.

It gives high throughput on processor P4 processor with only 1 GB of RAM. It gives throughput of 100KB, 1MB and 10MB.

Advantage:

- It gives higher throughput and prevent the brute force attack.
- Some steps are repeated N times so security will more.

Disadvantage:

- Steps are repeated N times so receiver cannot know at which point he has to stop and he will continue his process.

Table: 1:Result table

	Paper	**Technique Used**	**Algorithm**	**Merits**	**Demerits**
3.1	A performance comparison of data encryption algorithm[1]	Symmetric algorithm	flexible and simple to implement	Blowfish is fastest algorithm for implementation	Java is used as tool its too much slow.
3.2	Cryptanalysis of Modern Cryptographic Algorithms[2]	Symmetric And Asymmetric algorithm	DES,AES,IDEA,RSA	Modern cryptography gives better performance.RSA is much better.	For long message requires too much time for CPU according to key
3.3	ANovelApproach for Enciphering Data of Smaller Bytes [3]	Symmetric Algorithm	4 bit secret and sgared key for encryption and decryption	Small size data encryption is easy and secure	Don't provide large size data encryption

3.4	DES,AES and Blowfish: Symmetric key cryptography algorithm simulation based performance analysis[4]	Symmetric Algorithm	DES,AES,and Blowfish,ECB,CBC,OFB,	Blowfish is good than other two.	AES suffers from brute force attack and blowfish from weak keys problem
3.5	A Comparative Study of SixmostCommonSymmetricEncryption Algorithms across Different Platforms[5]	Symmetric Encryption	RC6,UMARAM,UR5,DES,3DES, RC2	In speed and time UMARAM and UR5 is good performer	Not comparative with AES and Blowfish
3.6	Performance Evaluation of Cryptographic Algorithms: DES and AES[6]	Symmetric Algorithm	DES,AES	Described in description	Described in description
3.7	UR5: A Novel Symmetrical Encryption Algorithm With Fast Flexible and High Security Based On Key Updation (april 2012,IJARCSSE)[7]	Symmetric Algorithm	UR5	Attacker cant know the key even have P.T and C.T.reduce delay	So many keys required bcz updating each time
3.8	Modern Ecryption Standard (MES)Version-II[8]	Symmetric Algorithm	Modern Encryption Standard(MES-II	Best for short message like SMS and password	Not working for long messages
3.9	Fault Attacks on AES with FaultyCiphertexts Only[9]	Symmetric algorithm	AES	Attacker cant know pair of correct/faulty message	Require faulty C.T for applying model
3.10	The New Cryptography Algorithm with High Throughput[10]	Symmetrci Algorithm	Advances of AES,DES,3DES,Blowfish	Provide high security and throughput.few steps repeated N times	Receiver can't know at which point he should stop process

III. CONCLUSION

This all study is literature survey of the cryptography algorithm. And also we show that which is the better and which is not. All paper hasits own advantage and disadvantage. Here any one can see that how we can get the more efficient output and can increase the throughput of the algorithm and it also shows that which algorithm is more and less time consuming.so we have concluded that how to choose the better algorithm in block cipher for high throughput.

REFERENCES

[1]. Nadeem, A. ;Javed, M.Y. "A Performance Comparison of Data EncryptionAlgorithms" Information and Communication Technologies, 2005. ICICT 2005.First International Conference Publication Year: 2005 , Page(s): 84 – 89.

[2]. NeetuSettia.“Cryptanalysis of modern Cryptography Algorithms”.International Journal of Computer Science and Technology. December 2010.

[3] S.R.Kumar, E. Pradeep, K. Naveen and R. Gunasekaran, "A Novel Approach for Enciphering Data of Smaller Bytes", International Journal of Computer Theory and Engineering, 2(4), 1793-8201, pp. 654-659,2010.

.

[4]. J.Thakur,Nkumar.”DES,AES,and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”. International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250- 2459, Volume 1, Issue 2, December 2011).

[5]. Ramesh G and Umarani R, "A Comparative Study of Six most Common Symmetrie Encryption Aigorithms across Different Platforms", International Journal Of Computer Applications, Vo1.46, No.13, May 2012.

[6]. Akash Kumar Mandal, and ,Mrs.ArchanaTiwari, "Performance Evaluation of Cryptographic Algorithms:DES and AES", 2012 IEEE Students'conference on Electrical, Electronics Computer Science, 2012.

[7]. Ramesh G, Umarani. R, ” UR5:A Novel Symmetrical Encryption Algorithm With Fast Flexible and High Security Based On Key Updation”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012 Page 16-22. 2010.

[8]. R.Sircar,G.Sekhon, N.Nath.” Modern Ecryption Standard (MES) : Version-II”, (978-0- 7695-4958- 3/13, DOI 10.1109/CSNT.2013.111,2013,IEEE).

[9]. Thomas Fuhr, ElianeJaulmes, “Fault Attacks on AES with Faulty Ciphertexts Only”,(978-0-7695-5059-6/13, DOI 10.1109/FDTC.2013.18,2013,IEEE).

[10]. D.Nilesh,Malti N,” The New Cryptography Algorithm with High Throughput”,ICICI- 2014,jan 3-5(978-1-4799-2352-6/14,IEEE).