Indian J.Sci.Res. 17(2): 327-335, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

A COMPARATIVE STUDY ON PERFORMANCE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS IN ONLINE BANKING TRANSACTIONS

[1]C.Sruthi, [2]T.Abirami [3]G. PremaArokia Mary [1]Student, Department of Information Technology, Kumaraguru College of Technology, sCoimbatore, Tamilnadu, India, 641 049
, [2]Student, Department of Information Technology, Kumaraguru College of Technology, Coimbatore, Tamilnadu, India, 641 049
[3] Asst. Professor, Department of Information Technology, Kumaraguru College of Technology, Coimbatore, Tamilnadu, India, 641 049
[4]S.Kanagaraj Asst. Professor(II), Department of Information Technology, Kumaraguru College of Technology, Coimbatore, Tamilnadu, India, 641 049
E-mail: [1]sruthi.15it@kct.ac.in, [2]abirami.15it@kct.ac.in, [3] premaarokiamary.g.it@kct.ac.in
[4] kanagaraj.s.it@kct.ac.in

***Abstract*—** In today's internet world, with online transactions almost every second, terabytes of data being generated every day on the internet, thus in such a case securing information or sensitive data is a challenge too. Security is the degree of resistance or confrontation to, or protection from, harm and threats. Thus, safety plays an important and vital role in online banking transactions where disclosure of any data results in huge loss. Network security involves the permission or license of access to data in a network. Resources can include files, database, emails etc. Safety is the protection of these resources from unauthorized users that brought the development of network security. Network security consists of the policies and practices that can be adopted to prevent unauthorized access, misuse, modification during their transmission and also to ensure the transmitted is protected and authentic. Cryptography is an integral part of modern world information security making the virtual world a safer place. Cryptography is a process of making information unintelligible to an unauthorized person and hence it provides confidentiality to authentic users. There are various cryptographic algorithms that can be used. Preferably, a user needs a cryptographic algorithm which is of low cost and high performance. There are several algorithms with a cost performance trade off. Thus, amongst the cryptographic algorithms existing, we choose an algorithm which best fits the user requirements and objectives. In, this process of choosing cryptographic algorithms, a study of strengths, weakness, cost and performance of each algorithm will provide valuable insights and difference. In our paper, we have analyzed in detail the performance and cost for universally used cryptographic algorithms like DES, RSA, AES and so on, by applying these algorithms in online banking transactions.

Keywords —RSA, AES, DES, mRSA, modified AES.

I. Introduction

The demand for the existing personal communications is navigating the development of new networking techniques. In the wireless communication such as online banking transactions, the security of the data plays the vital role. The objectives of introducing and practising the online-banking services and transactions are to benefit the users with profits, fast service, improved productivity, customer satisfaction, 24×7 operations & cost savings with ease. To improve the security of the data being transmitted various techniques are employed. The internet is an essential and fundamental part of our daily routines of life, and the proportion of population who await to manage their banking accounts anywhere, anytime is continuously increasing. So due to this enormous growth of online transactions, internet banking has become a very crucial and important component of any financial institution's strategy and various organizations too. Information about financial institutions, their users, and their fund transactions is, inevitably, extremely sensitive and should be secure. As many online banking transactions being processed by the central computer system, security of that central system is the major affair for the banks. Serious devastations can occur due to the lacking security. Hence securing the customer accounts as well as their sensitive details have become the primary problem for the banks. So, the internet banking system should have provision to guarantee to solve the issues and problems regarding authentication and non-repudiation, so that only authorized and authentic people alone can access an internet banking account of specified user, and the information viewed and provided must remain and maintained private and it should not be modified by other unauthorized users or the bank. The important method used to provide the confidentiality to the sensible information is the data encryption and decryption techniques of cryptography. Network security is encountered to be more important when the volume of the data becomes larger and complex.

Cryptography:

Cryptography is the art of transforming the information into scrambled or in unintelligible format that is impossible to understand by unauthentic users. It relates to the study of mathematical techniques and principles related to the aspects of information security such as the confidentiality, data integrity, authorization and authentication of the data. The technology used for this is

[1]Corresponding Author

called as the cryptology. When the user defined input data may in any of the format such as the text, or an image which is plain, is converted into an unintelligible form called as the cipher text or cipher image which is the encrypted form. This process is referred to us as encryption. To convert the data into encrypted form, the user should provide the specific cryptographic algorithm for encryption. The reversible process in which the original data or message is recovered is called as the decryption process. [4] There are four main objectives of cryptography: -

1. **Confidentiality:** It guarantees that the sensitive information can only be accessed by authorized users/entities and ensures that data is not made available or disclosed to any unauthorized user or entity causing disclosure of information.

2. **Data integrity:** It is a service which deals with the unauthorized alteration or manipulation of data (provides protection from manipulation). This property refers to data or information that has not been manipulated, destroyed, or lost in a hostile or accidental manner.

3. **Authentication:** It is a service related to identification. This function applies to both entities and information itself. Two parties entering a communication should identify each other.

4. **Non-repudiation:** Non-repudiation is a service that guarantees to prevent the denial of an electronic message by the sender or the receiver [4] [6].

II. Related Work

Digital Signature

Digital signature is an electronic signature for demonstrating the authenticity of digital messages or documents and is used to indicate the identity of sender's message or signer of document, and ensure that the original content of the message or document sent by the sender has not been altered by unauthorized third parties. Digital signatures are easily transmitted, unique and can be automatically time-stamped. A valid digital signature gives a receiver of the message, a reason to accept that the message was created by a known or genuine sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not manipulatedby any unauthorized entities in transit (integrity) [4].

Types of Cryptography

Symmetric-key cryptography refers to one of the encryption techniques in which both the sender and receiver share the same key [8]. Thus, the secrecy of the key is maintained and the key is kept private. It works with high speed. Symmetric key ciphers are performed as either block ciphers or stream ciphers. A block cipher enciphers or encrypts input in blocks of plaintext, in case the input form used by a stream cipher is individual characters as opposed to block cipher. Block ciphers encipher the information by breaking it down into blocks and encrypting data in each block. A block cipher enciphers data in fixed sized blocks. A stream cipher operates on a single bit at any time [6].

Public-key cryptography or asymmetric-key cryptography or asymmetrical cryptography which refers to any cryptographic system which requires two separate keys, one of the two keys is a secret key and the other key is public key. One key (public key) locks or enciphers the plaintext, and the other (private key) unlocks or deciphers the cipher text. Neither key can implement both encryption and decryption operations by itself [8]. The public key of the user may be published without compromising security cases, while the private key must not be revealed to any unauthentic users as it may rise security issues and situations. The major drawbacks of asymmetric ciphers include their speed and strength of security. They are much slower than the symmetric key algorithms [6].

Online Banking

Internet banking, also known as e-banking or virtual banking, is an electronic payment system that enables customers to conduct transactions on a website operated by the financial institution with their bank names and allows a user or the customer to execute financial transactions via the internet. By online banking, one can do multiple things from home, office or elsewhere which includes request for cheque book, debit card, account details etc.The electronic banking system addresses several arising trends: customers' demand for anytime,anywhere service, product time-to-market imperatives and increasingly complex back-office integrationchallenges. The challenges that oppose electronic banking are the considerations of security and privacy ofinformation[12]. Without the secure communication and transmission, online banking could not operate. Each person who is the user or the customer can enter the banking website with their PIN number. The two different security methods or techniques for the online banking are: PIN/TAN system and the signature based online banking. In PIN/TAN (Transaction Authentication Number) systems PIN represents password for the user login and TANs represents one-time passwords required to authenticate financial transactions such that no transactions can be performed without a valid TAN. Attackers are misleading the users by stealing the login data and valid TANs. A method to attack signature based online banking methods is to manipulate such that the correct transactions are shown on the screen and forged transactions are signed

in the background.The different live systems that provide security to the internet banking or online banking systems are: RSA, DES, SHA, Blowfish, Diffie Hellman, MD5, AES. These are the most efficient open source software algorithms [5].

RSA

RSA is an algorithm used to encrypt and decrypt the information and messages. It is asymmetric cryptographic algorithm that is it works on two different keys (public and private key). RSA refers to RonRivest, Adishamir and Leonard Adleman. Rivest-Shamir-Adleman is the most commonly used public key encryption algorithm used to encrypt and decrypt the data. It provides integrity, authenticity, confidentiality and non-reputability of electronic communications and storage. RSA can be used both for encryption process as well as for digital signatures. The security of RSA is generally concerned to be on the basis on how it is equivalent to factoring [3] [7].

DES

The Data Encryption Standard (DES) is a symmetrickey algorithm used for the encryption of electronic data and information. DES works by using the same key for both encryption and decryption of a message. DES is a block cipher since the key and algorithm is applied on the block of data rather than applying to bits. By using, permutation and substitution the 64-bit plain text is converted into cipher text by encryption. The confusion and diffusion are the encryption techniques on which the DES relies on. Confusion refers to substitution and here specially chosen data are substituted for the input data. The choice of the data depends on the plain text and the cipher key. Diffusion refers to permutation and here data or the bits are permuted or transposed. Both the confusion and diffusion depend on the plain text and the key [3].

AES:

The National Institute of Standards and Technology (NIST) have created AES (Advanced Encryption Standard), that describes an encryption method, which is a new Federal Information Processing Standard (FIPS) publication. AES is a privacy transfigure for IPSec and Internet Key Exchange (IKE) and has been developed and recommended by NIST to replace the Data Encryption Standard (DES) in 2001, which was starting to become vulnerable to brute-force attacks. AES is designed to be more secure than DES: AES provides a larger key size, while ensuring that for an invader or intruder, the only known approach left to decrypt a message is to try every possible key to invade the original content of the message or information. AES algorithm can reinforce any combination of data (of about 128 bits). AES has a variable key length, the algorithm can specify a 128-bit key (which is the default), a 192-bit key, or a 256-bit key [1] [3].

Performance Criteria

The following factors are analyzed as the performance criteria, such as the tunability, computational speed, the key length management, the encryption ratio and the security of data against attacks. [11] [4]

1. **Tunability** - It could be very advisable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Static definition of encrypted part and encrypted parameters bounds the usability of the scheme to a restricted set of applications.

2**. Computational Speed** - In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements within a short span.

3. **Key Length Value** - In the encryption methodologies, the key management is the important feature that shows how the data is encrypted and how keys are organized. The symmetric algorithm uses a variable key length which is of the longer lengths. Hence, the key management is a considerable feature in encryption processing.

4. **Encryption Ratio** - The encryption ratio is the measure of the amount of data that is to be encrypted. Encryption ratio should be minimized to reduce the complexity on computation.

5. **Security Issues** - Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-cipher text attack and various other attacks.

FACTORS ANALYSED	SYMMETRIC KEY ENCRYPTION					ASYMMETRIC KEY ENCRYPTION	
	AES	DES	TRIPLE DES	BLOWFISH	RC4	RSA	DIFFIE-HELLMAN
Encryption Ratio	High	High	Moderate	High	Low	High	High
Speed	Fast	Fast	Fast	Fast	Slow	Fast	Slow
Key Length	128-, 192-, or 256-bit	56-bit key	112-168 bits	32 bits to 448 bits.	256 bytes	> 1024 bits	Key Exchange Management
Tunability	No	No	No	Yes	No	Yes	Yes
Security Against Attacks	Chose n-Plain, Known-Plain text.	Brute force	Brute Force, Chosen –plain text, Known plain text	Dictionary Attacks	Bit Flipping attacks	Timing Attacks	Eavesdropping.

Fig-1. Cryptographic algorithms performance comparison

Thus, various cryptographic algorithms have been analyzed based on the performance criteria parameters.

PROBLEM DESCRIPTION

While making online payments and transactions (transferring money from one account to another), the online bankers are always concerned about the hackers and anti-social elements. Hacking permits the unethical hackers to invade the accounts of online bankers, and spend their money. Availability of confidential and sensitive information which is just secured by a user name and password, makes it vulnerable to such threats and security issues. Although,most of the banks try to make their sites secured by implementing latest network security software, the security threats continue to be alive.Online banking is becoming increasingly popular as it brings comfort, simplicity and rapidity to consumers. Common techniques established by fraudsters today, to obtain login credentials for users' online banking accounts include phishing, pharming, keylogging, man-in-the-middle and man-in-the-browser attacks etc.Regardless of the method employed, fraud is a global circumstance that is continuouslydeveloping in order to exploit security gaps.However,securing an online banking channel has many concerns and characteristics to it and specially each needs to be addressed individually. A crucialchallenge met by banks when upgrading their security infrastructure is deciding and concluding which technologies to adopt and which parts of their infrastructure to change or upgrade.

III. Methodology

The proposed changes to AES algorithm can be implemented in any programming language. The implementation environment was as follows:

1) The Permutation box is of 128-bit instead of two 64-bit permutations. This reduced the computation time further and the inter bit delay differences achieved are very less.

2) The implementation was on a dedicated hardware designed for the algorithm on 180nm CMOS technology. Therefore, the over heads of the processor and OS performance were taken into consideration. The original AES implementation was done by authors on the same FPGA platform. The highest throughput achieved was 1Gbps using rolled architecture of 128-bit data bus. Our implementation of modified AES using the rolled architecture of 128-bit data bus achieved a throughput of 2.087Gbps on Xilinx Vertex4 FPGA. The only drawback of our method is larger memory used for storing the 128-bit permutation box.

The implementation results for our design are:

1) The design was successfully clocked at 163MHz.

2)Total gates required for encryption and decryption were:

107K gates (including memory in equivalent gate terms).

3) The throughput is 163MHz*128/10 = 2.087Gbps.

4) Power consumption is 23.84mw at 163Mz.

5) The scrambling of data bits with our permutation box has resulted into less inter-path delay differences.

The proposed method achieved a throughput of 2.087 Gbps which means 16.305M, 128-bit blocks per sec or 61.332ns for each block of 128-bit data. We have tested on Vertex 4 FPGA platform. The most important contribution of our implementation is that the inter bit delay differences are very less. The maximum delay between the most critical path and shortest data path from input to output is found to be 1.0118ns. This result has helped us in reducing the clock period, as the data arrival uncertainty was reduced. The modified AES algorithm is firmer and more powerful and strong than the AES algorithm. The difference between the encoding calculated time for the captured e-banking transaction records and packets using Modified- AES and AES is expected to be acceptable, which forms, using Modified-AES a better solution in banking systems.

E-Banking security tier using confidence building metric and modified AES

Every account holder (client) registered and identified by the Bank will be able to use online banking and transaction services. For every transaction that is done by the client of the bank with the bank system is encrypted using 128-bit modified AES algorithm. The primary concern in this part of the design is the key distribution. The key has to be renewed every time whenever the bank asks to change the access and transaction password of the client. This is normal practice with the banks to request or make it mandatory to the client to change the access and transaction passwords regularly. The passwords become invalid after every certain period is rolled. Then, additionally another level of security using Confidence Building Metric (CBM) is suggested. Such that, in order to increase the protection by still getting faster computation, we may use the concept of Confidence Building Metrics (CBMs) based on the certain parameters of access to the bank portal by the account holder. The CBM is mapped on a scale of 0 to 10. The value of CBM increases with the following list of events as mentioned below:

- MAC id of the computer regularly used.

- Time slot in day or night whichever is used often or regularly.
- IP address of the machine regularly used for transaction.
- Use of virtual keyboard used each and every time the transactions made.
- Amount of transaction within a certain limit proclaimed before by the client.

Each of these parameters or events mentioned above increments the CBM by a certain value. The distribution of these values can be based on a design consideration of the bank. Similarly, the CBM also reduces whenever certain events do occur as mentioned below:

- New MAC id used other than the regularly used one.
- Transactions being done at odd hours others than the regular ones.
- Different IP address of the machine or device other than the regularly used one.
- Virtual keyboard not used.
- Amount of transaction exceeds the pre-declared or announced limit.
- New access and transaction password set.

The banks will maintain a set of security questions already configured or registered by the client. The banks may make the registration of security questions and their answers mandatory. Whenever the CBM decrements or reduces than the previous value a security question is asked to the client from the set on randomly. And whenever the CBM increments or increases, no security issues or questions are asked and the transaction can be done based on the access required and transaction passwords while the encryption is compulsorily done for every data transfer. This makes a three-tier system of verification and validation of the authentic client requesting the banking transaction.

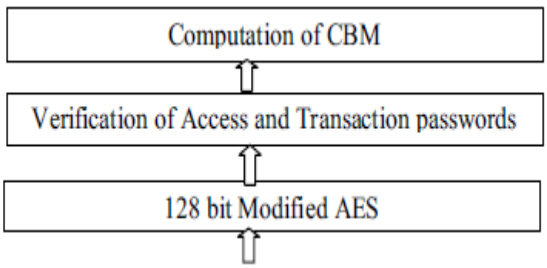

Fig-2. Tier structure of security system

The advantage of the above system is that it can be implemented on any platform at the client side including even the mobile phones with any OS. [2]

Secure Transaction in online banking system using IB-mRSA (Identity Based Mediated RSA):

Mediated RSA (mRSA) involves a special entity, called a SEM an on-line partially trusted server. To sign or decrypt a message, Alice must first obtain a message-specific token from the SEM. Without this token Alice cannot use her private key. To retract Alice's ability to sign or decrypt, the administrator commands the SEM to stop providing tokens for Alice's public key. At that instant, Alice's signature and/or decryption capabilities are invalidated. For scalability reasons, a single SEM serves for many users. One of the mRSA's advantages is its transparency: The main idea behind mRSA is the splitting of an RSA private key into two parts as in the threshold RSA. One part is given to a user while the other is given to a SEM. If the user and the SEM collaborate, they employ their respective half-keys in such a way that is functionally equivalent to classical and standard RSA. The fact that the private key is not held in its totality by any one party is explicit to the outside, i.e., to the those who use the corresponding public key. Also, knowledge of a half-key cannot be used to derive the entire private key. Therefore, neither the user nor the SEM can decrypt or sign a message without mutual consent.

Identity based Encryption:

Identity-based encryption and digital signatures are important tools in modern secure communication. In general, identity-based crypto- graphic methods promote easy introduction of public key cryptography by allowing an entity's public key to be derived from some arbitrary identification value such as an email address or a phone number.Identity-based cryptography greatly reduces the need for, and have dependence on, public key certificates. Mediated RSA (mRSA) is a simple, practical and effective method of splitting RSA private keys between the user and the Security Mediator (SEM) [9] [10]. Neither the user nor the SEM can evade one another since each signature or decryption must involve both parties. mRSA allows fast and fine-grained control (revocation) over users' security privileges. However, mRSA still relies on public key certificates to derive public keys.Mediated cryptography (such as mRSA) still depends on public key certificates to derive public keys. IB-mRSA conferred here is a variant of mRSA that combines or includes identity-based cryptography and mediated cryptography. IB-mRSA is simple, secure and very efficient and effective.

Objective in proposed System:

A unidirectional stand-in re-encryption schemes with chosen cipher text security in the standard model.

- Including non-interactive temporary delegations.
- A secure chosen-cipher text from attacks while keeping them efficient and robust.
- Introducing of arbitrary delegates of public keys in the system.

In order to provide effective and secure banking transactions, there are two technology issues needed to be resolved:

- **Security**: It is the primary concern of the Internet-based industries or organizations. The lack of security may result in serious destructions or lead to many unwanted issues.
- **Authentication:** Encryption may help make the online transactions (such as banking transactions) more secure and stable, but there is also a necessity for the provision to guarantee that no alteration of data is made at either end of the transaction.

Steps involved in Proposed System:

Step 1: The client first sends a message to the CA containing the client's identity (ID). We use e-mail addresses as a unique identifier of clients to the system that will be used to compute the public exponent for each one

Step 2: The CA server checks the client's identity. Only if this identity is valid according to the sorted data, the CA looks after all key setup. The first four parameters are generated in the same approach as depicted in standard IB-mRSA in which a public key EKi is computed.

Step 3: CA produces a corresponding private key Instead di is effectively split into two parts, d^{bank} and d^{sem} in which the banksecretly holds and a SEM secretly holds.

Step 4: At the first session, the CA generates the list of client's identities or specifications and stores it in encrypted database for security reasons and privileges. This shared secret key is needed between the CA and SEM for state maintenance. The hash function is a one-way function that maps a variable-length message into a fixed-length value which is called a hash code.

Step 5: Following the computation of the above values, CA provides the client the public key certificate, EKi, and the token (OIDi, j, K_{client}) iscreated for each session.

Step 6: After receiving the token from CA, the client sends a request to the bank by launching a message m that includes the client one-time ID encrypted with the received public key along with K_{client} that is used to verify the client.

Step 7: The bank receives the above response, confirms that the content of a response is not stale by verifyingK_{client}, and then forwards the received message to the SEM for authentication purpose.

Step 8: SEM checks that the client is not retracted by comparing both of $k^{bank}{}_{client}$getting from bank and $k_{CA}{}^{client}$ getting fromCA. If so, it signs the requested message with its private key for the purpose of producing a partial signature.

Step 9: If the bank's half signature fails verification (i.e. it signs a different message or includes an incorrect signature counter), the bank terminates the protocol and ceases that a malicious attack has occurred. If there is no error, the banking system allows the genuine client to perform the online transactions as required by the client. In this case, no signature storing is required for the signer to prove the server's evading.

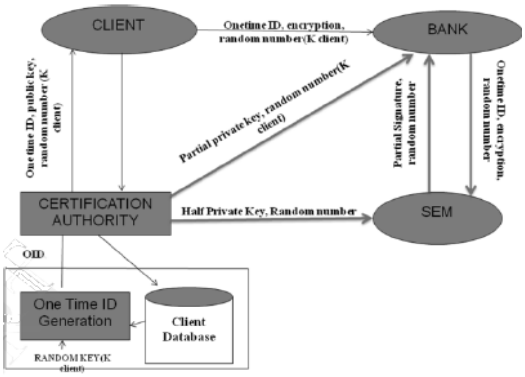

Fig-3. Secure Transaction in online banking system using IB-mRSA

Modules:

There are four modules in the proposed systems

- Certificate Authority Module
- Key Generation (One Time ID)
- Key Splitting Module
- Security Mediator Module (SEM)

Certification Authority:

Certification Authority (CA) module is the central of the whole architecture corresponding to a trusted third party that issues certificates.

The CA architecture is explicit to the sender of a message and to the verifier of a signature because the encryption and verification approaches remain the same as in classical and standard RSA. The purpose of CA server is to generate client bunch and Security Mediator (SEM) bundle that

enclose the required security component for electronic banking transactions by splitting private keys into two parts, one for the client and the other for the SEM.

Key Generation (one Time ID):

One-time ID Module is a user's substantialspecification, which has two properties:

(i) an attacker cannot specify who is communicating or participating even when he intrudes on one-time ID.

(ii)one-time ID can be used only once.

Key Splitting:

Getting private keys split into two halves send through the one half of the Bank another sends through the mediator (SEM). Using this key for decryption action.

Security Mediator:

Security Mediator (SEM) module is an online partially trusted server. The SEM can remove the need for certificate revocation list since the private key operations cannot take place after revocation. A SEM can be arranged to operate in a state or stateless model. The former involves storing per user state (half-key and certificate) while, in the latter, not kept as per user state; however, some extra processing is sustained for each user request. The trade-off is clear: the former and it is fast request handling against the latter and somewhat slower request handling. SEM can evade one another since each signature or decryption must involve both parties. mRSA allows fast and fine-grained control (revocation) over users' security advantages. However, mRSA still depends on public key certificates to derive public keys.

Experimental Results:

To validate the goals and to validate the experiment with the proposed model's implementation and design, a number of tests with different key sizes are made. First experiment, communication latency is measured by varying the key size, which directly affects message sizes is measured. Latency is calculated as round-trip delay between clients and the CA.

Key Size(bit)	Message Size(byte)	Average Latency(ms)
512	125	5.13
1024	205	6.72
2048	298	10.9

Fig-4. Average latency in key and message size

The second experiment, the IB-mRSA results are obtained by measuring the time starting with sending of client's identity message to the CA and ending with the client encryption and bank decryption process time will be measured as seen below.

Processor	Key length(Bit)		
	512	1024	2048
PI-233 MHZ	25.32	40.1	255.7
pIII-500 MHZ	10.5	14.8	82.5
pIII-700 MHZ	9.5	10.3	55.7
pIII-933MHZ	8.9	7.3	43.9
PIV-1.2 GHz	7.53	9.3	58.7

Fig-5. Processor speed and key lengths

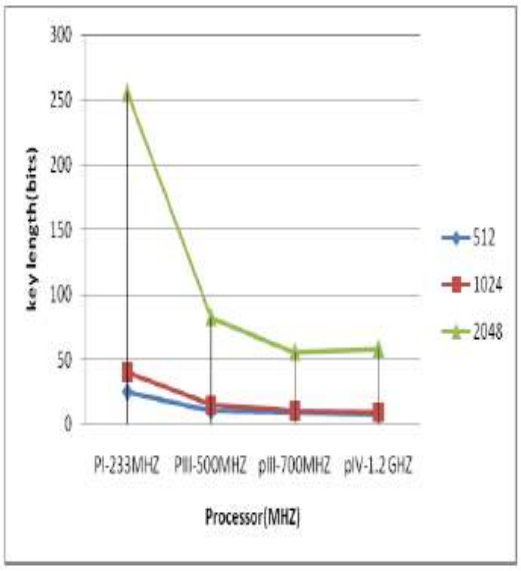

Fig-6. Processor speed and key length

This model is provided to evaluate the performance metric average latency based on parameters, key size and message size. Using IB-mRSA algorithm low average latency is achieved compared to other algorithms.

IV. Conclusion

Online-banking or E-banking is a form of banking where money is transferred through an exchange of electronic signals between financial institutions or organizations. The security of data record transaction has brought many concerns from different perspectives: government, businesses, banks, individuals and technology. Financial

institutions are achieving the security of online-banking data record transaction by methods of cryptography, which deals with encryption of data. The strength of encryption is not based on the secrecy of the applied algorithm since this would generally be made known to a number of parties. The strength of the encryption lies in the fact that the secret or the private keys are known only to the holder of the key. It is thus important that the procedures are in the place to generate keys in a secured environment, these keys are stored safely, and encryption and decryption keys of sufficient size are used. This is the special importance to a bank which would not be able to afford significant breaches of security in banking transactions or to their systems from both financial and reputational perspectives. Safe system is the complete spectrum of security measures that will determine the security of a given system. Thus, the internet banking system designers must ensure that measures are in place to prevent eavesdropping, that secret and that tampering will be detected. Further there should be procedures in place to ensure that encryption algorithms can be changed.The proposed AES model is a new encryption algorithm that is based on AES using open source symmetric key encryption algorithm. This modified AES algorithm provides better security for the online banking services such as transactions and overcomes the problem of computational overhead by reducing the calculation time of the given algorithm. A new innovated E-Banking Security Tier using Confidence Building Metric (CBM) and Modified AES was offered to make another level of protection.Another solution tosecure transaction using a new modelcryptography technique is IB-RSA and mainadvantage of the proposed IB-RSA model is using one time-ID foreach transaction. In that transaction ID usingonly once. This model to evaluate theperformance metric average latency based onparameters, key size and message size. Using IB-mRSAalgorithm low averagelatency is achieved compared to other algorithms.

References

[1]Abhilesh S. Jadhao, Shital B. Kumbhalkar, “Technical Review On Secure Banking Using RSA And AES Encryptor Methodologies”,IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), Volume 11, Issue 1, Ver. IV (Jan. - Feb .2016), PP 01-04.

[2] Adel Khelifi, et ol, “Enhancing Protection Techniques of E-Banking Security Services Using Open Source Cryptographic Algorithms”, 2013 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/DistributedComputing.

[3] Gurpreet Singh, Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, International Journal of Computer Applications (0975 – 8887), Volume 67– No.19, April 2013.

[4]AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram, “Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms”, International Journal of Engineering Research andApplications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037.

[5] Kishore Kumar, K.Imran Shareef, M.Nomitha, S.Kamala, “ Improved Protection Technique For E-Banking Security Services Using Cryptographic Algorithm”, AIJREAS Volume 1, Issue 7 (2016, July).

[6] Neha Garg,Partibha Yadav,” Comparison of Asymmetric Algorithms in Cryptography”, IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1190 – 1196.

[7] Nentawe Y. Goshwe, “Data Encryption and Decryption Using RSA Algorithm in a Network Environment”, IJCSNS International Journal of Computer Science and Network Security, Vol.13 No.7, July 2013.

[8] M.Preetha, M.Nithya, “A Study And PerformanceAnalysis of RSA Algorithm”, IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139.

[9] S.Rajalakshmi, S.V.Srivasta, “Identity based Encryption Using mRSA in Electronic Transactions”, Information Technology Journal 6(3):435-440, 2007.

[10] S. Renuga Devi, S. Chidambaram, V. Manimaran, “Secure Transaction in Online Banking System UsingIB-mRSA”, International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 1, January- 2013.

[11] Sumit Sharma, Mrs. Shobha bhatt, “Comparative Analysis - Performance, Efficiency and Security Measures of Block Cipher Algorithms”, International Journal of Engineering Development and Research, Volume 3, Issue 3, 2015.

[12] Yi-Jen Yang, “The Security of Electronic Banking”, 2403 Metzerott Rd.Adelphi, MD. 20783.