IMPROVED PROTECTION TECHNIQUE FOR E-BANKING SECURITY SERVICES USING CRYPTOGRAPHIC ALGORITHM

KISHORE KUMAR N[1], K.IMRAN SHAREEF[2], M.NOMITHA[3] and S.KAMALA[4]
[1]Assistant professor in ECE, ADITYA COLLEGE OF ENGINEERING, Madanapalle, A.P., INDIA
[2, 3, 4] Students, Dept. of ECE, ADITYA COLLEGE OF ENGINEERING Madanapalle, A.P., INDIA
E-Mail: kishorenanabala@gmail.com[1]
imranshareefk@gmail.com[2]

ABSTRACT:
In today's world most of the banking transactions are done using the e-banking. The security and the privacy features are the major concern for the e-banking users and it needs to be improved rapidly. Due to the cryptanalysis techniques, it is difficult to provide the security for the customers by using the conventional algorithms. This project deals with the important issues regarding how to enhance the transition to more secure cryptographic and encryption algorithms in the financial sector. This project recommends that adopting and implementing open source application is considered as a better replacement to the conventional algorithms. We proposed a modified algorithm for AES, in which substitute bye, shift row will remain same as in the original AES while the mix column is replaced by the 128 permutation operation followed by add round key operation. Comparative study with the previous algorithms represents the advantages of the modified AES algorithm and its high ability to overcome the problem of computational overhead by using the permutation box.

INTRODUCTION:

Now-a-days banks are offering wide range of services to the customers and customers can directly interact with their accounts at anytime from anywhere. E-banking refers to the banking where money is transferred by exchanging the electronic signals. The security is the major problem for the users. They are facing a risk of someone breaking into their accounts. Therefore, it is very important to build a system that secures the details of the customer. Regarding the security, many vendors have developed various algorithms in software-based systems. To continue the growing in the e-banking and its services, the security features need to improve.

E-Banking came into existence in greater numbers because of low operating costs. First it is in the form of ATM's and phone transactions. Recently it transformed to internet a new channel between customers and banks which benefits both. The main aim of e- banking services is to provide the customers a much faster services with low cost. From the last twenty years, banking sector has chosen a new method of banking based on the progress of information technology. In addition to these customers, transaction and communication abilities are fastened based on information technology.

Electronic banking has been used in different sectors like government, individuals, business, banks and technology. Financial institutions are pressuring the banks that they should provide more services to the customers. As many of the transactions being processed by the central computer system, security of that system is the major concern for the banks. Serious damages can occur due to the lack of security. Hence securing the customer accounts as well as their details have become the primary problem for the banks.

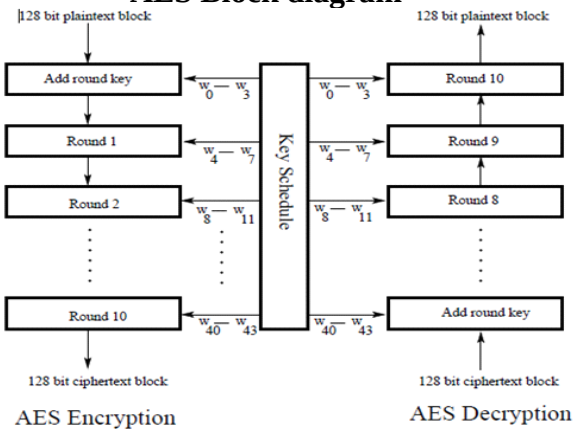
OVERVIEW:

In this project a cryptographic algorithm named Modified AES algorithm is designed and its performance of the algorithm is compared with already existing different AES designs. To assure the confidentiality triple DES and RC4 algorithms are used for symmetric ciphers while using the internet banking systems.

For asymmetric ciphers RSA is most widely used as it possess 1024-bit key. In RC4 algorithm one key in every 256 keys is a weak key and compared to DES it is faster. Internet banking is an electronic payment system that enables customers to conduct transactions on a website operated by the financial institution with their bank names.

By e-banking one can do multiple things from home or office which includes request for cheque book, debit card, account details. Without the security, online banking could not operate. Each person can enter the banking website with their PIN number. The two different security methods for the online banking are: PIN/TAN system and the signature based online banking. In PIN/TAN systems PIN represents password for login and TANs represents one time passwords to authenticate transactions. Attackers are deceiving the user s to steal login data and valid TANs. Phishing and phirming are the two well examples for those attacks. A method to attack signature based online banking methods is to manipulate such that the correct transactions are shown on the screen and faked transactions are signed in the background.

AES Block diagram



EXISTING SYSTEMS:

The different existing systems that provide security to the internet banking are: RSA, DES, SHA, Blowfish, Diffie_Hellman, MD5, ElGamal , AES. These are the most efficient open source software algorithms.

RSA:

RSA is an algorithm used to encrypt and decrypt messages. It is asymmetric cryptographic algorithm. RSA refers to RonRivest, Adishamir and Leonard Adleman. It includes both the public key and private key. It provides integrity, authenticity, confidentiality and non-reputability of electronic communications and storage. It was introduced at the time of electronic mail arise. The encryption and authentication takes place in RSA without sharing of private keys. Each person is having of public key and his own private key. Encryption can be done by anyone having the private keys, they can also verify the key. But decryption can be done only by the person having the private key. RSA can be combined with a cryptosystem which is having a secret key to form a RSA digital envelope.

DES:

DES works by using the same key to encrypt and decrypt a message. DES is a block cipher as the key and algorithm is applied on the block of data rather than bits. By means of permutation and substitution the 64 bit plain text is converted into cipher text by encryption. The confusion and diffusion are the encryption techniques that DES depends on. Confusion refers to substitution; 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; here data or the bits are permuted or transposed. Similar to the confusion, diffusion also depends on the plain text and the key.

Triple DES:

Triple DES refers to triple Data Encryption Standard. It is a symmetric-key block cipher which is similar to the DES algorithm but is applied three times for

each data block and hence named triple DES. When the DES algorithm became less secure due to the key size, the enhancement has been made to the same algorithm instead of building up a new algorithm. The electronic payment industry uses Triple DES for their security and they are continuously developing standards for their use. Many Microsoft soft wares use this algorithm to protect the password and content of their systems.

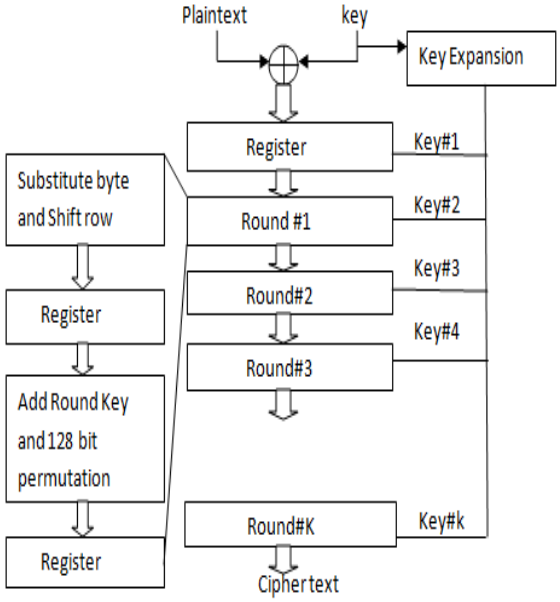
SHA:

SHA is a secure Hash algorithm. There are many series of cryptographic hash functions, designed by the national security agency. It is very hard for an attacker to break your password when using this Hash algorithm as he requires more computing power to calculate the hash. SHA algorithm is employed in many applications and protocols. It has used not for security but for ensuring that data has not changed due to corruption.

MD5:

MD5 is an algorithm that is used to verify the integrity of the data by creating the 128-bit message digest from data input that is unique to that particular data which is same as a fingerprint to the particular individual. This MD5 algorithm is not as fast as that of MD4 algorithm. The third message digest algorithm of Rivest is MD5. It is having a small hash value that contemplates a birthday attack. Many flaws were found when it was designed.

MODIFIED AES ALGORITHM:



APPLICATIONS:

The AES algorithm is used in the applications such as the authentication need to be provided for the data and it should modify only by the authorized person.

- Public sector companies
- Financial institutions
- Airports and shipping
- Retail market
- Technology services
- Trade and commerce
- Money transfer, etc.

Secure communication:

RFID
Image encryption
Internet banking
ATM networks

Secure Storage:

Any confidential documents
Personal information
Government documents
FBI files
Personal storage devices

FUTURE ENHANCEMENT:

It has been demonstrated that the proposed modified AES algorithm shows better performances over existing AES algorithm. Replacing the mix column operation with the permutation box is the better solution to increase the throughput and reduce the computations. CBMs can be used to secure the e-banking transactions.
Future work will focus on reducing the memory for the permutation box. Some improvement in the permutation AES and applying this algorithm to each transaction record will be the enhancement.

CONCLUSION:

E-banking is a form of banking where money is transferred through an exchange of electronic signals between financial institutions. 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 e- Banking data record transaction by methods of cryptography, which deals with encryption of data. In this paper, we have proposed 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 e-banking services and overcomes the problem of computational overhead by reducing the calculation time of the algorithm. In modified AES algorithm instead of using Mixcolumn, we use the permutation step, taking from Data Encryption Standard (DES) algorithm. Comparative study with traditional encryption algorithms is shown the superiority of the modified algorithm. A new innovated E-Banking Security Tier using Confidence Building Metric (*CBM*) and Modified AES was presented to be another level of protection. The CBMs are computed based on certain parameters and can be implemented on any platform at the client side. Some improvements on the deployment of our modified AES will be considered as a future work taking into consideration on the importance level of each e-banking transaction record.

REFERENCES:

[1] Schneier, Bruce, "Open Source and Security". Crypto−Gram, 1999, Counterpane Internet Security,Inc. http://www.counterpane.com/crypto−gram−9909.
[2] Y.-K. Lai, L.-C.Chang, L.-F.Chen, C.-C.Chou, and C.-W. Chiu, "A novel memoryless AES cipher architecture for networking applications", in Proc. IEEE Circuit and Systems Symp, May 2004.
[3] I. Verbauwhede, P. Schaumont, and H. Kuo, "Design and performance testing of a 2.29 Gb/s Rijndael Processor", IEEE Jour. Of Solid-State Circuits, pp. 569–572, 2003.
[4]C.-L. Horng, "An AES cipher chip design using on-the-fly key scheduler", Master Thesis, Dept. Electrical Engineering, National Tsing Hua University, Hsinchu, Taiwan, June 2004.
[5]C.-P. Su, T.-F.Lin, C.-T. Huang, and C.-W.Wu, "A high-throughput lowcost AES processor", IEEE Communications Magazine, vol. 41, no. 12, pp. 86–91, Dec. 2003.