IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN: 2278-487X, p-ISSN: 2319-7668
PP 33-37
www.iosrjournals.org

Cryptography – Security in E-Banking

Uma Dixit
Department of Mathematics, University Post Graduate College, Osmania University, Hyderabad, India

Abstract: *Electronic Banking which is also called E – Banking is a source of obtaining information about bank and its various services via Internet. E - Banking is now the basic essence of Banking services. Information technology has bought major changes in the operating environment of the Banking sector. The innovative techniques implemented by banks are in the form of Automated Teller Machines – ATM's, Online Banking, Telephone Banking, Mobile Banking etc,. The security and privacy of the information is the major concern in all Internet Banking techniques. Also the online Banking system is vulnerable to attacks related to user authentication.*
The objective of this paper is to discuss various data encryption techniques based on cryptographic technologies and review various methods of E-Banking security.
Keywords: *E-banking, Security, Encryption, Decryption, Cryptography*

I. Introduction

Electronic banking- which provides various banking services through internet- changed the ways of business conducted in banks drastically. Also called as online banking, it tremendously helped in reduction of banking transaction costs and increasing the benefits to customers by various integrated services. Security and privacy are the main expected features in the field of online banking. On-line transactions need utmost security to avoid possible fraudulent transaction of any kind. All kinds of information and various services for transactions are available for the users through internet. The encryption of information is the source of security and privacy in this online banking. The security is provided in the form of password, pin code, biometric, digital signature, steganography etc.

The banks have to ponder more and invest on data and information security due to the continuous surge in usage of online and mobile channels [4] and due to the various associated threats. Managing the security in online banking and phone banking is the highest challenge than compared to other transaction services.

Cryptography has a major role in the banks and other financial service firms to ensure them that all their important various data transactions are processed securely. It makes a message unintelligible or unreadable to everyone except to legitimate users and it is also a technique to develop a way to authenticate the source of messages and ensure that the message had not been counterfeited while in transit.

Cryptosystem- which is an encryption and a decryption process, involving the methods of hiding information through the use of keys. The role of keys is to determine the functional output of the cryptographic algorithm. It specifies the transformation of an original message to an encrypted message and vice versa. Consequently, security of cryptographic algorithms relies on secrecy of the key.

The whole idea of cryptography is Encryption and Decryption where in Encryption is a process in which plain text data is converted into an unintelligible or unreadable text called cipher text and decryption is the process of transforming data that has been rendered unreadable back to its normal form [1].

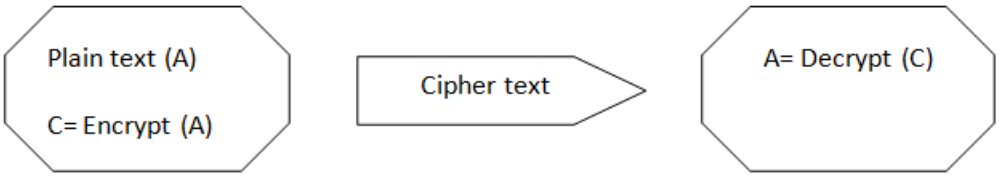


Fig 1. Cryptosystem

The encryption algorithms were used for all the security processes and the algorithms required the use of software-based techniques which provided counter methods to avoid security attacks. The banks now are incorporating data encryption, based on strong cryptographic methodologies [3] into their communication channels in order to cross check the data transaction and avoid manipulations and have secured network communication and transactions.

II. Literature review

The review is focused on providing the information associated with technology based services of banks and the security techniques adapted globally. Online banking now a days plays a crucial role at each level on day to day transactions.

Goldreich [1] in 1998 discusses the importance of cryptography, which is primarily used to keep the information secret. [3] has discussions on the cryptographic methodologies used in banking industry to have secured transactions. [4] gives information on various electronic transactions which come in various forms of debit / credit cards etc., and techniques used to stop an unauthorized person from accessing the personal data or information of the user.

In 2000, a network working group N. Haller [6] designed a One Time Password system to counter the attacks on networking systems used by legitimate users. The authentication process includes generation of single use one time passwords, which are nothing but pass phrases run by multiple iterations.

SMS based mobile banking [7] to enhance the security was discussed and also the use of symmetric AES, advanced encryption standard, cryptographic algorithms to secure SMS.

In 2009, Embedded crypto-biometric authentication scheme is combination of the cryptography and biometric technique to improve the level of security for person authentication was proposed by [11]. By combination of the cryptography that encrypted the images then transmitted to the secure channel and by using biometric that the images of fingerprint acquired from the user encrypted for the authentication.

In 2014, Avhad, Prashant R., and R. Satyanarayana [10] discussed how a middle man attacker can tap the internet channel between user and server during the process of transaction and can extract the information and get user details like passwords etc., they proposed a three factor secure authentication method using smart cards, passwords and biometric.

Cryptographic methodology used in banking equipments

In the 1970s, A crypto algorithm called Lucifer algorithm, devised by Horst Feistel, was evaluated and after some changes to the internal functions and reducing the key size from 112 bits to 56 bits, the complete algorithm that became the Data Encryption Standard (DES) was published in the *Federal Register* in 1975.

Financial institutions started using DES and began to create security infrastructures to protect their binary coded data stored in computer systems and also to protect transmission during electronic transactions. But the hackers set up a program whereby anyone with an Internet-connected computer could penetrate a portion of their computer's resources - usually when the screen saver was running and the user was not actually working on the computer - to search part of the DES key space.

Then the new algorithm came into picture. There were two major algorithms for replacing DES. Triple DES (sometimes called TDES or 3DES), or Advanced Encryption Standard. 3DES uses the original DES algorithm three times to encrypt the data. Using either two or three 56 bit DES keys,

In 2002, the AES came into picture, the advanced encryption standard (AES). In cryptography, the Advanced Encryption Standard (AES) is also known as Rijndael algorithm. Rijndael is an iterated block cipher which supports variable block length and key length, specified as 128, 192 or 256 bits.

Murphy and Robshaw introduced an alternate of AES by embedding AES in cipher called BES which uses algebraic operations.. Nicolas courtois and Joseph pieprzyk worked on new methodology, finding that AES can be written as an quadratic equations also.

III. Electronic banking – security using cryptography

3.1 ATM

The introduction of the ATM also known as Automatic Teller Machine proved to be an important technological development that enabled financial institutions to provide services to their customers in a 24X7 environment. The ATM has enhanced the convenience of customers by enabling them to access their cash wherever required from the nearest ATM. The basic concept is that a person with a valid card can conduct any banking transaction without visiting a branch. They are well known for its convenience to the customers, cost-effectiveness to the bank and most importantly it is an extremely secure banking method. The functions of ATMs depend on authorization of a transaction by the bank via a secure communications network.

Moving from operating systems to Microsoft Windows® technology has led to greater connectivity and interconnectivity of ATMs. Vast networks—including ATMs, branch systems, phone systems and other infrastructure connected via the Internet—are targets of logical security threats. Logical attackers include hackers who create viruses intended to compromise an ATM‘s operating system and hackers who install malware to violate the confidentiality, integrity or authenticity of transaction-related data.

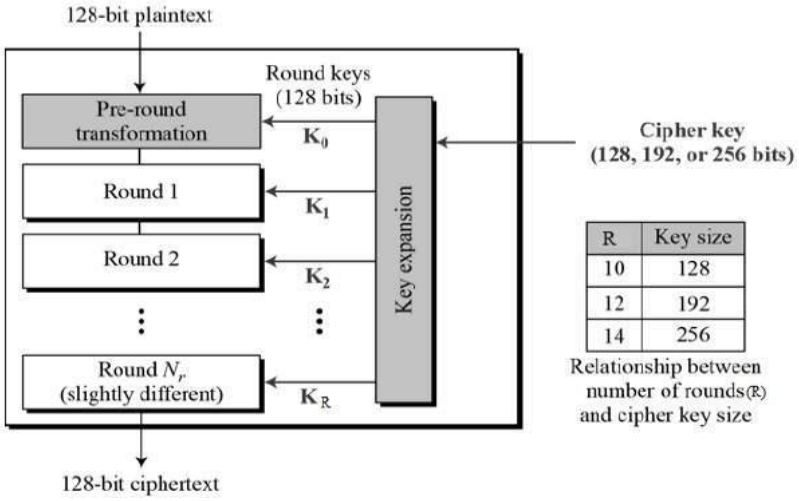
Various Encryption algorithms are built into the communication network to prevent unauthorized transactions . presently the pin which is entered on ATM should be converted to encrypted pattern before send-

ing it over the network. Every ATM has encrypted pad which encrypt pin on ATM. Manually the keys are added on ATM earlier, now these keys can come from switch (systems to which ATM's are connected).

An embedded Crypto-Biometric authentication scheme for ATM banking systems has been proposed. The customers fingerprint is required during a transaction. The fingerprint image is encrypted via 3D chaotic map as soon as it is captured, and then transmitted to the central server using symmetric key algorithm. The encryption keys are extracted from the random pixel distribution in a raw image of fingerprint, some stable global features of fingerprint and from pseudo random number generator. Different rounds of iterations use different keys. The decryption takes place at the banking terminal using the same key. Earlier the transactions in ATMs were encrypted with DES, but the transaction processors required the use of the more secure Triple DES .

There were still a many fraudulent withdrawals from ATMs, which banks often claim are the result of fraud by smart intruders. The Advanced Encryption Standard (AES) algorithm adds support for the new encryption standard AES, with Cipher Block Chaining (CBC) mode, to IPSecurity (IPSec).

The development in AES triggered a transform for IPSec and Internet Key Exchange (IKE) and took over the Data Encryption Standard (DES). AES functions in such a way that it is more secure than DES: AES offers a larger key size, while ensuring that the only known approach to decrypt a message is for a fraudster is to try all possible key options. AES has a variable key length--the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key [2]. some of the most Advanced encryption technologies are used to protect the Automated Teller Machines.



R	Key size
10	128
12	192
14	256

Fig 2. Advanced encryption standard

3.2 CARDS – (Debit, Credit or Smart)

Electronic card allows a cardholder to make a payment or a purchase by electronic fund transfer. The common types of cards are credit cards and debit cards. Electronic cards are usually embossed plastic cards, which comply with the ISO/IEC 7810 ID-1 standard. The Electronic cards usually have an embossed card number which complies with the ISO/IEC 7812 numbering standard.

Magnetic stripes were introduced on debit cards in the 1970s when the ATMs came in. The magnetic stripe could store card data which could be read by physical contact and by swiping on the machine. But it was easy to intrude into data encoded on magnetic-stripe. Magnetic-stripe credit cards are also much easier to counterfeit than chip and PIN varieties. As magnetic-stripe cards don't require any PIN , they offer no protection against any kind of frauds. The cause that the chip and PIN cards are more secure than magnetic stripe cards is that they require a four-digit PIN for authorization. It is the easiest way to know that the cardholder is the real owner of the card.

All the data and communications are protected by cryptography, making chip and PIN cards more difficult to hack. The EMV smart chip where EMV stands for Europay, MasterCard and Visa, the three companies that created this microchip authentication system for credit, debit and ATM cards is the small chip embossed on cards.

A smart card is a card with embedded integrated circuits which can process data by receiving input using ICC application and delivering the output. There are two broad categories of ICCs. A smart card which is called Memory card, contains only non-volatile memory storage components, and perhaps some specific security logic. The other Microprocessor cards contains volatile memory and microprocessor components. The card generally is embedded with a hologram to avoid counterfeiting.

Using smart cards is a form of strong security authentication. There are issues related to the security in authenticity and integrity. The weaknesses of existing authentication scheme such as password and PIN number helped fraudsters to steal the information stored in ATM smartcards which lead to the loss of money in bank account and private information misuses. The mitigation of the authentication issues on the ATM smart card encouraged towards the embedded biometric and cryptography approaches . The most innovative and trusted in smart card security came in form of Fingerprint biometric. Later on the idea of authentication system using biometrics combined with other technologies such as fuzzy extractor [8], Global System for Communication (GSM) and Radio Frequency Identification in ATM smart card [10] were developed.

3.3 Mobile Banking

Authenticating users over the phone or on website is the most important factor for any business, where transactions are carried out using insecure Internet channel. The modern communication medium is very much exposed to various threats. One time password (OTP) is used to prove one's identity over the wireless channel. A One Time Password (OTP) is a password which is valid for only one Login Session or transaction.

The OTP sent to user's registered mobile number as SMS is most commonly used technique for user authentication. The user can receive the OTP via text message. OTP SMS which is one of the Smart way of sending a Pin, is a system to send to anyone's mobile phone a "one time password" for their money transfer and payment operations and Internet Banking login. Neither the person nor anyone else can use for a second time these five digit one time passwords generated by OTP SMS

But the OTP SMS sent normally as plain text is vulnerable to various attacks along the communication channel. The user needs to know the PIN to read the OTP. The user can proceed with the business transaction, only after this authentication. This process provides end-to-end-encryption of the OTP SMS.

The OTP which is encrypted can be decrypted only if the 4 digit PIN entered by the user at his mobile is correct. Since the PIN is known only to the user, it provides two levels of authentication. Only if PIN and OTP are correct the user is allowed to proceed with the m-banking transaction that he initiated.

The OTP generated is encrypted using the powerful AES algorithm. The generated OTP value is encrypted using powerful AES algorithm and sends it to users.AES is an iterative and asymmetric key block cipher that uses three keys strengths of 128, 192 and 256 bits. The AES uses 128 bits as a block for encryption and decryption. It is one of the perfect cryptography algorithms to protect personal data. [7]. The encrypted AES tool converts the input plain text to cipher text in a number of required repetitions based on the encryption key. The AES decrypt method uses the same process to transform the cipher text back to the original plain text using the same encryption key. It is very difficult to break even using brute force attack. The encrypted OPT password is send to mobile through Bluetooth technology or modem [6]. The drawback of this method is that it has large system load for encryption and decryption.

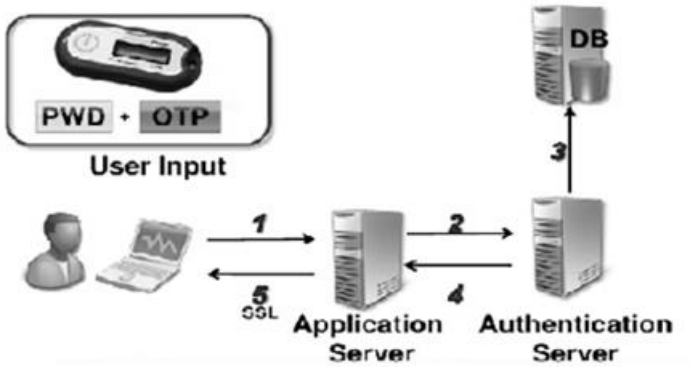


Fig 3. OTP workflow

Although OTPs are in some ways more secure than a static memorized password, users of OTP systems are still vulnerable to fraudulent attacks. OTPs should therefore not be disclosed to any third parties, and using an OTP as layered security is safer than using OTP alone; one way to implement layered security is to use an OTP together with a password that is exclusively with the the user (and never transmitted to the user, as OTPs often are).

IV. Conclusion

In the future, the need for data security and integrity will continue to require our careful thought and consideration. For carrying out critical transactions like fund transfers, the banks, at the least, need to implement robust and dynamic two-factor authentication through user id/password combination and second factor like a

digital signature or OTP/dynamic access code through various modes (like SMS over mobile phones or hardware token).

An embedded Crypto-Biometric authentication scheme for ATM banking systems has been proposed. The claimed user's fingerprint is required during a transaction. The fingerprint image is encrypted via 3D chaotic map as soon as it is captured, and then transmitted to the central server using symmetric key algorithm. The encryption keys are extracted from the random pixel distribution in a raw image of fingerprint, some stable global features of fingerprint and/or from pseudo random number generator. Different rounds of iterations use different keys. The decryption takes place at the banking terminal using the same key.

We have already described the major challenges of online transaction which is mainly security. The design of an algorithm with combination of conventional and advanced security can ensures e-security using three layer security systems . These three layers are:

1: Conventional E-security using Username and PIN number.
2: Biometric security using Fingerprint or Iris recognition.
3: Mobile security using GPS or mobile SMS.

References

[1]. Goldreich, Oded. Foundations of cryptography. (1998): 3.
[2]. Advanced Encryption Standard (AES), Cisco Systems, Inc. 2004
[3]. "Cryptography":http://en.wikipedia.org/wiki/Cryptography "How crypto is being used in bank ing": www.mbanking.blogspot.com/.../how-**c**rypto-is-being-used-in-banking.ht
[4]. "SecureElectronicTransaction(SET)":http**://**en.wikipedia.org/wiki/Secure_Electronic_ Transaction
[5]. V. S. Miller, Use of elliptic curves in cryptography, in: H. Williams (Ed.), Advances in Cryptology CRYPTO 85 Proc., Vol. 218 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 1986, pp. 417-426. doi:10.1007/3-540-39799- X_31.
[6]. N. Haller, The s/key one-time password system, Network Working Group.
[7]. Kewin Chikomo, Ming Ki Chong, Alpan Arnab, Andrew Hutchison, "Security of Mobile Banking".
[8]. Yang, Dexin, and Bo Yang. A new password authentication scheme using fuzzy extractor with smart card. Computational Intelligence and Security, 2009. CIS'09. International Conference on. Vol. 2. IEEE, 2009.
[9]. Avhad, Prashant R., and R. Satyanarayana. A Three-Factor Authentication Scheme in ATM. 2014
[10]. Shi, Peipei, Bo Zhu, and Amr Youssef. A rotary pin entry scheme resilient to shoulder-surfing. Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for. IEEE, 2009.