E-BANKING: CRYPTOGRAPHY WITH UNIQUE IDENTITY

Anuradha Khatri*

Isha Budhiraja*

ABSTRACT

In the field of Banking and Insurance, security and privacy have become the essence. On-line transactions always need security. Every type of information and transaction is available for the customers through internet. But this online banking requires a lot of security and privacy as the encryption of information is not sufficient. These days security is provided in the form of password, pin code, digital signature etc. In this paper we will discuss UTII(Unique Thumb Impression Identity) which will not allow the online transactions and account information possible for the unauthorized user even when he has the authorized user's ATM card,debit or credit card. UTII will allow a user to give his/her unique identity proof which can not be matched with any other in the world. In this paper we will discuss how the UTII will work with cryptosystem.

Keywords: *Banking; security; cryptography; UTII; encryption; decryption*

*Sr. Assistant Professor, FIMT, Guru Govind Singh Indraprastha University, New Delhi

INTRODUCTION

External threats and the increasing usages of online and mobile channels [4] along with regulatory requirements are driving banks to invest information security .Managing security is more challenging in online banking and phone banking as compared to other service delivery channels. Loaded with money, the ATMs have become a target of opportunity for thieves.The ATM has become American's banking stations –with many banks accepting deposits, counting money, dispensing each and providing balance information at these units. Apart

from the data security and risk mitigation issues, the banking, financial services and insurance (13FST) verticals are seeking scalability and reliability from its IT infrastructure to drive business growth. Cryptography is very important for data security.

CRYPTOGRAPHY IN BANKING

Cryptography is one of the way for banks and insurance firms to ensure them that all commercial and private transaction are processed securely. When we speak of modern cryptograph, we are generally referring to cryptosystems because the cryptography of today involves the study and practice of hiding information through the use of keys, which are associated with web-based applications, ATMs Ecommerce, Computer passwords and the like. Many companies are incorporating data encryption and data loss prevention plans, based on strong cryptographic techniques into their network security strategic planning programs.

Cryptography [3] refers almost exclusively to *encryption*, which is the process of converting ordinary information called plaintext into unintelligible gibberish (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A *cipher* (or *cypher*) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". This is a secret parameter (ideally known only to the communicants) for a specific message exchange context. A "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

TYPES OF CRYPTOGRAPHIC ALGORITHMS

The three types [2] of algorithms that will be discussed are (Figure I):

Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.

Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.

Hash Functions: Uses a mathematical transformation to irreversibly “encrypt" information.

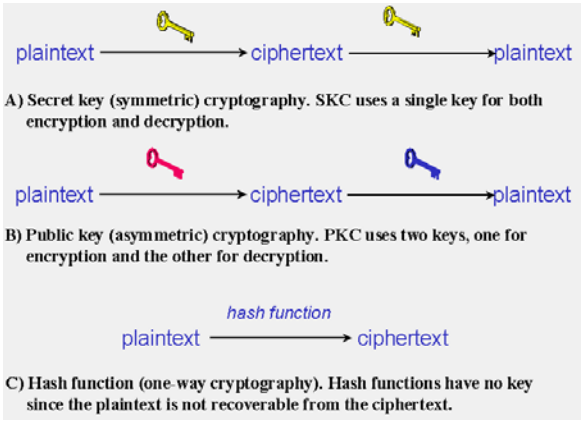

FIGURE: I

DUTIES OF A CRYPTOGRAPHER

A cryptographer [9] is one who practices or studies cryptography, a field primarily involved with keeping secret information secret. The banking industry requires the services of cryptographers to hide and protect credit card information, account numbers, transaction data and the personal data of individual customers. Financial cryptographers secure the information stored in the bank’s database as well as when data is transferred between two systems, such as during a funds transfer. Cryptographers [11] are sometimes referred to as cryptographic technicians. They are often employed by banks and insurance firms for preventing and detecting frauds. They are responsible in a firm for securely storing and transmitting sensitive data and information. For this, they use the concept of data compression and encryption. Cryptographer control the employee password encryption to ensure unauthorized personnel cannot access company records. In banks cryptographer hide and protect credit card information Account number, transaction and the personal data of individual customer.

USE OF CRYPTOGRAPHY TO SOLVE SECURITY ISSUES IN BANKING AND INSURANCE FIRMS

A 128-bit encryption browser or a browser that support Server Gated Cryptography(SGC) can be used in banks. SGC [7] allows a browser using 40-bit encryption to function as of it has 128-bit encryption for the duration of the session. Browsers using 128 –bit encryption provide the highest level of commercially available security for your financial transactions. Encryption transforms the banking transactions you send over the internet into code that can then be translated by us.

Technologies such as the Internet which has greatly facilitated the transaction and exchange of all kinds of information, require a high level of protection to keep these exchanges secure and private. The need of data encryption is undeniable. Information related to bank and insurance companies are exchanged over networks. Without effective encryption ,transactions would be vulnerable to criminal interference.

Cryptographic techniques for implementing secure Electronic transaction [5] that came in many forms including digital checks , debit cards, credit cards and stored value cards. Privacy, authenticity and no repudiation(prevention of later denying having performed a transaction) are the usual security features for Electronic transaction system.These security goals can be achieved via digital signatures [6], based on public key cryptography. Such a cryptosystem uses a secret key and public key. The secret key is used to create a digital signature and the public key is needed to verify the digital signature. Electronic transaction basically include three types of transactions withdrawal, payment and deposit.

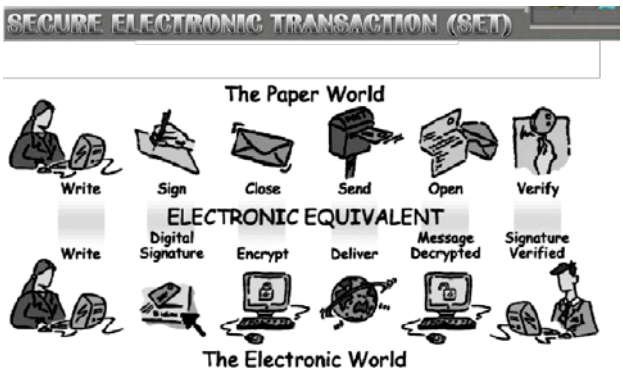

FIGURE :II

Cryptography is also used these days for (SMS based secure mobile) M-banking (Mobile banking). Symmetric Cryptographic techniques where common secret key is shared among bank customer and bank server are used for secure M-banking.

A hardware security module (HSM) [8] is a type of secure cryptoprocessor targeted at managing digital keys, accelerating cryptoprocesses in terms of digital signings/second and for providing strong authentication to access critical keys for server applications. The cryptographic material handled by most HSMs are asymmetric key pairs (and certificates) used in public-key cryptography. Some HSMs can also handle symmetric keys and other arbitrary data

Some ATM networks now use smart cards which enable the use of public key cryptography. A user's card then contains their private key and a certificate, signed by the card issuer, to confirm their public key value . the ATM authenticates the cards by issuing a challenge for the card to sign.

EFFECT OF LEGAL RULES ON CRYPTOGRAPHY

The TABLE: I [2] shows that legal rules act differently in cryptographic and non-cryptographic settings. The cryptographers' syllogism is based on the assumption that users will employ strong cryptography. If users indeed employ strong cryptography, then by definition privacy is at the maximum. That is Box I in Table 1. Legal rules in such circumstances can only have the effect of reducing privacy. Clipper and other mandatory key escrow schemes belong in Box II, and result in the wider availability of previously-private information.

Table I.

	Crypto Transactions	**"Ordinary" (Non-Crypto) Transactions**
No Regulation	**SECRECY** Strong crypto allows anonymity.	**DISCLOSURE** Market result is wide availability of information.
Regulation	**DISCLOSURE** Regulation leads to wider availability of information, as in Clipper.	**"DISTRIBUTED PRIVACY"** Legal rules protect information -- information available only to selected 3rd parties

However, its users very often will *not* employ strong cryptography. In such circumstances, the role of legal rules shifts 180 degrees. In an *unregulated* setting we will expect widespread disclosure of private information, as shown in Box III. In today's marketplace, the operators of databases often seek to profit from their information about customer transactions. They "data mine," in current parlance. Against this backdrop of widespread disclosure, legal rules can actually promote privacy. It is of course true that legal rules cannot offer the same guarantee of anonymity as does strong cryptography. Legal rules, at best, can promote what might be called "distributed privacy." In a world where a great many transactions will not be anonymous, we face a choice between Box III -- disclosure through the marketplace -- or Box IV -- reduced disclosure on the basis of legal rules. In Box IV, transactional information is distributed from the consumer to other parties such as the bank. The bank, however, is under legal obligations not to reveal that information except where legally permitted.

UTII WITH CRYPTOGRAPHY

Mainly the most of transactions security and privacy during e-banking depends on the password or PIN code. which are easily vulnerable to criminal interference. Passwords or pin codes can be forgotten or lost, yet identification through a physiological trait is a foolproof security and verification method. That is why we must use the user's personal unique identity. In this paper we are using UTII(unique thumb Impression identity) because every person has his own thumb impression nobody can copy it like signature.

For Electronic transaction system these security goals can be achieved via UTII based on public key cryptography. When request is made for transaction the user will have to give his thumb impression for identity proof just like password and information will be encrypted.Such a cryptosystem uses a secret key and public key. The secret key is used to create a thumb impression and the public key is needed to verify that thumb impression. Then thumb impression will be matched within the bank record just like digital signature for the decryption of the encrypted transaction or account information, if no match found no electronic transaction will take place.

Once a file is encrypted, you do not have to worry about a person reading your sensitive information related to your account, as an encrypted file is completely useless without the UTII needed to decrypt the information. It simply cannot be read.

CONCLUSION

The use of electronic payments will spread widely in coming years. We expect to be able to buy products easily from home over the Internet. Face-to-face transactions will increasingly be done by debit card, credit card, and emerging forms of smart cards.

Within the cryptography community, an ongoing research project has been to devise ways of assuring privacy while performing electronic financial transactions. For instance, cryptography is already used in many bank-to-bank transactions. UTII will add more security features with cryptography. As Internet commerce grows, most people assume that more cryptography will be deployed between users and their banks -- the risks of plaintext transmission for huge numbers of financial transactions can be readily reduced with cryptographic systems. Over time, cryptography with UTII can be increasingly used within organizations for security purposes, such as by requiring strong authentication before granting access to sensitive databases. New generations of users may be more comfortable with cryptography using UTII than current users, there are important economic, psychological, and other reasons why consumers may choose not to act anonymously. Consumers will need to reveal their names and credit ratings to borrow money, key management problems will persist, and banks may retain strong incentives to offer better terms to customers who agree to let the banks know their unique identity.

REFERENCES

[1]. Narendra Kumar Tyagi, “Nullifying the Impacts of Security Threats on e-Business using Cryptography with e-BSP” National conference INDIACOM-2011 at Bharati Vidyapeeth Institute of Computer Applications and Management, Paschim vihar, New Delhi , 10-11th March 2011.

[2]. Peter P. Swire "The Uses and Limits of Financial Cryptography:A Law Professor's Perspective" In Proceedings of Financial Cryptography. 1997, 239-258.

[3].“Cryptography”:http://en.wikipedia.org/wiki/Cryptography [4].“How crypto is being used in banking”:www.mbanking.blogspot.com/.../how-**c**rypto-is-being-used-in-banking.ht.

[5].“SecureElectronicTransaction(SET)”:http**://**en.wikipedia.org/wiki/Secure_Electronic_Transaction

[6]. www.ijcsit.com/docs/Volume%203/.../ijcsit20120303105.pdf

[7]. www.us.hsbc.com/.../ ...

[8]. en.wikipedia.org/wiki/Hardware_security_module

[9]. www.wisegeek.com/what-does-a-cryptographer-do.htm

[10].www.garykessler.net/library/crypto.html

[11].www.ehow.com› Job Search & Employment