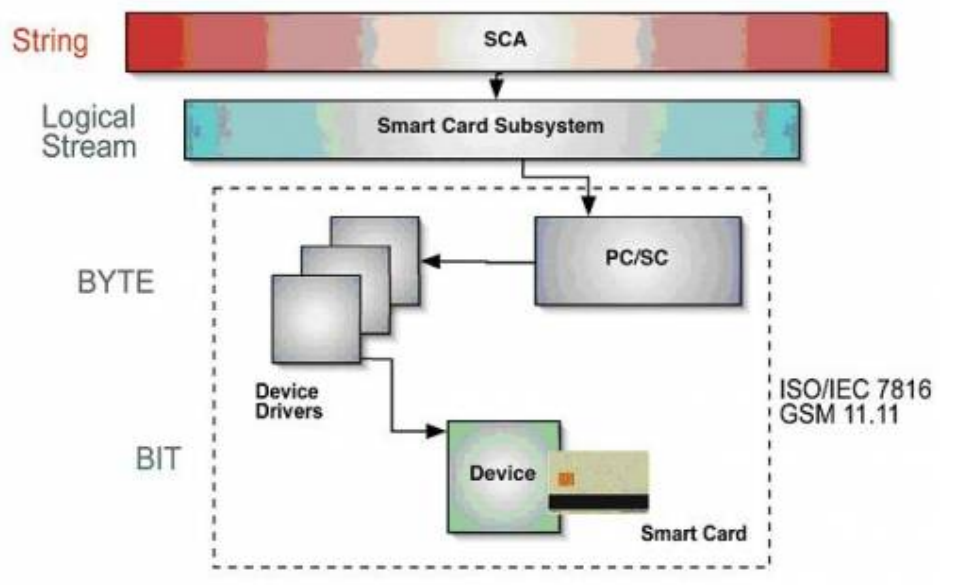
CRYPTOGRAPHY IN SMART CARDS



By

K.Kranthi Kumar
III B.Tech-CSE
Kranthi_kornipati@yahoo.co.in

A.Anand Sai
III B.Tech-EEE
Anandsai_b4u@yahoo.co.in

V.R.S & Y.R.N College of Engineering & Technology

Chirala

CRYPTOGRAPHY IN SMART CARDS

ABSTRACT

In the age of universal electronic connectivity, of viruses and hackers of electronic eaves dropping and electronic fraud there is indeed no time at which security does not matter. The issue of security and privacy is not a new one however, and the age-old science of cryptography has been in use, since people had information that they wish to hide. Cryptography has naturally been extended into realm of computers, and provides a solution electronic security and privacy issue.

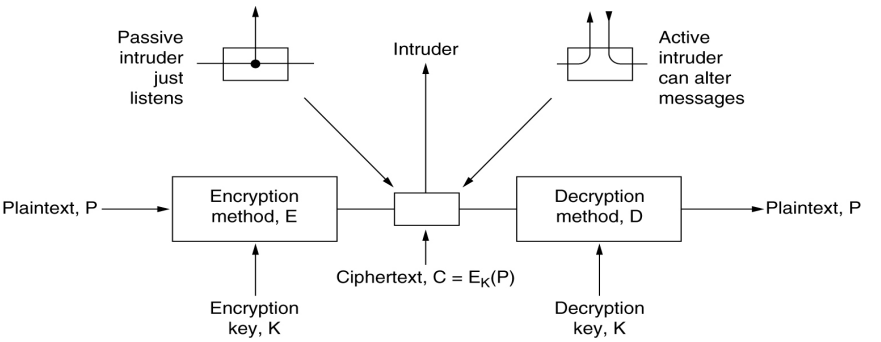
As the technology increases, Smart Cards (e.g.: SIM cards, Bank cards, Health cards) play very important role in processing many transactions with high level of security.

This security level achieved by means of Cryptography. In this paper we are presenting an introduction to cryptography, basics of Smart Cards, the role of cryptography in Smart Cards, and the processing of an example transaction involving security (Bank Card).

1. INTRODUCTION

Cryptography comes from the Greek words for – "**secret writing**". Cryptography is the science of enabling secure communications between a sender and one or more recipients. It deals with a process associated with scrambling plain text (ordinary text, or clear text) into cipher text (a process called encryption) then back again (known as decryption).

Fig: The Encryption model



An intruder is hacker or cracker who hears and accurately copies down the complete cipher text. Passive intruder only listens to the communication channel. But, active intruder can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver.

Cryptography concerns itself with four objectives:

1. Confidentiality (the information cannot be understood by any one for whom it was unintended).
2. Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected).
3. Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information).
4. Authentication (the sender and receiver can confirm each others identity and the origin/destination of the information).

2. TYPES OF ENCRYPTION

We have two variations

- Symmetric encryption
- Asymmetric encryption

In symmetric encryption, same key is used for both encryption and decryption. Consider a situation where Alice, a user from company A, is electronically communicating with Bob, a user of company B.

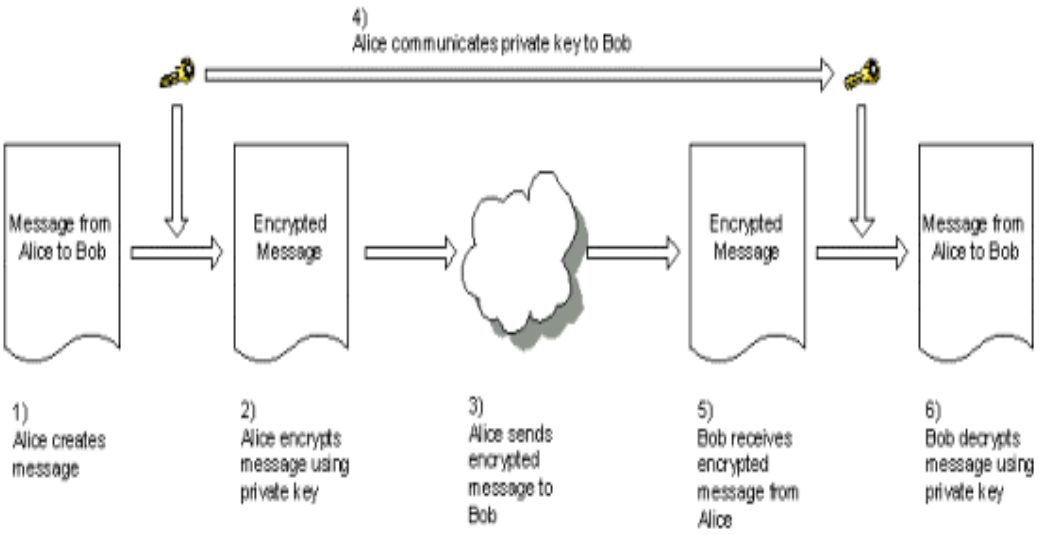


Fig: Symmetric communication between Alice and bob

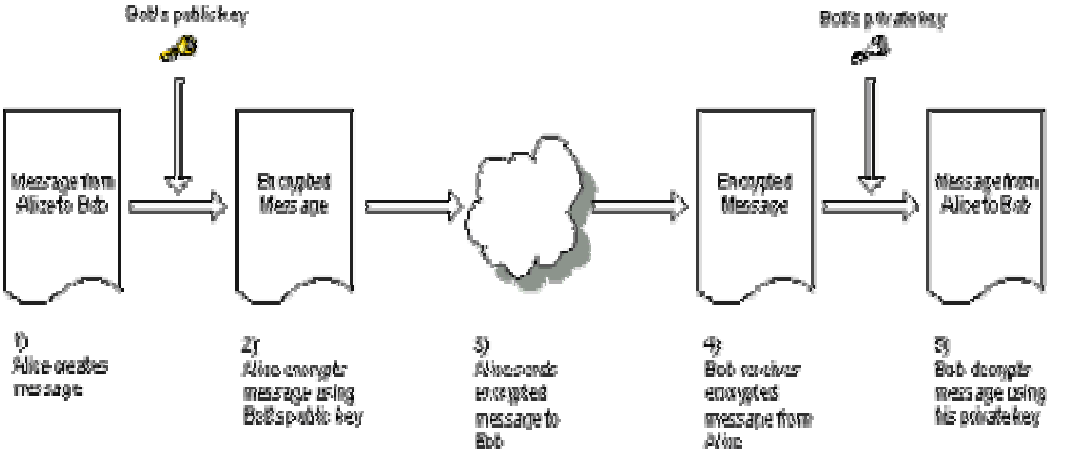
In this example, Alice would encrypt her message using a key, and then send a message to Bob. Alice would separately communicate the key to Bob to allow him to decrypt the message. To maintain security and privacy, Alice and Bob need to ensure that the key remains private to them.

Symmetric encryption can be implemented by

- **DES –** The Data Encryption Standard
- **AES –** The Advanced Encryption Standard
- Cipher modes

.In Asymmetric encryption, separate keys are used for encryption and decryption

Fig: Asymmetric communication between Bob and Alice



Here, Alice is sending a message to Bob. Alice creates her message then encrypts it using Bob's public key. When Bob receives the encrypted message, he uses his secret, private key to decrypt it. As long as Bob's private key has not been compromised then both Alice and Bob know that the message is secure.

Asymmetric Encryption can be implemented by

- Ø **RSA** (Rivest, Shamir, Adleman)
- Ø Other public key Algorithms

3. APPLICATIONS OF CRYPTOGRAPHY

The following are some of the applications of cryptography.

- Digital Signatures
- Digital Certificates.
- Message Digest.
- Secure Socket Layer.
- Secure E-Business
- Secure IP.
- Challenge/Response systems (**Smart cards**).

In this paper we are concentrating on Smart Cards.

4. SMART CARDS

Smart cards are an ideal means to provide the required level of security. In recent years, smart card technology has quickly advanced and by now reached a state where smart cards easily integrate into public key infrastructures. Today's smart cards provide memory, and they have cryptographic coprocessors that allow them to generate digital signatures using the RSA.

a) Architecture:

A smart card is a credit card sized plastic card with an integrated circuit (IC) contained inside. The IC contains a microprocessor and memory, which gives smart cards the ability to process, as well as store more information.

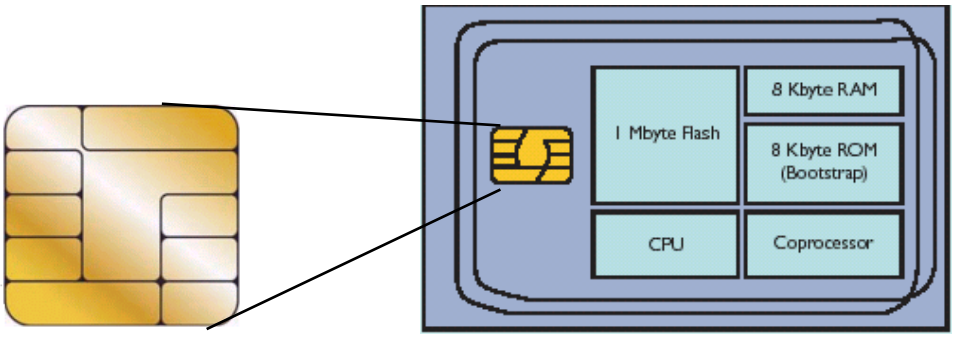


Fig: Contact chip and Smart card architecture

The above figure shows the architecture of smart card, which contains RAM, ROM, FLASH memory, and a Coprocessor. Smart cards uses RAM for temporary storage and ROM as a bootstrap for loading the operating system. Flash memory allows much higher data storage capacity on the card. It has an on-chip dedicate Coprocessor called **Crypto Processor** with key generation and asymmetric algorithm acceleration.

Contact chip is a standard transistor that was created from a lithographic process as a series of etched and plated regions on a tiny sheet of silicon.

A smart card can be used for payment transactions, such as purchases, and non-payment transaction, such as information storage and exchange.

b) Role of Cryptography:

The smart card provides two types of security services user authentication and digital signature generation. Smart cards are specifically designed to perform these services with a high level of security. Authentication of users means proving that users

are **who they say they are**. There are various ways to implement authentication using a smart card, but in this paper we are presenting smart cards with crypto processors.

Smart cards data storage capability structure is comparable with directory structure of disk media.

The main structure is based on three component types:

- Master File (MF), the root directory
- Dedicated file (DF), application directories or sub-directories
- Elementary file (EF), data files.

On the smart card there is only one Master File that contains some data files with global information about the smart card and its holder.

Dedicated files are directories that can be set under the root directory. Each application has a directory of its own. An application directory can have one or more sub directories.

Each directory has some specific elementary files, which contains secret cryptographic keys. All Dedicated and Elementary files have access conditions to execute a command on a file.

c) Cryptographic computations by Smart Cards:

The maximal length of data that can be encrypted by the smart card and that is not stored on the smart card is 8 bytes. The command that provides the encryption is called INTERNAL AUTHENTICATION and is developed to authenticate the smart card to the outside world. The command requires a random number from the outside world and a secret key that is stored on the smart card. The random number is encrypted with a secret key by the smart card to access the information.

The smart card is also able to compute a Message Authentication Code (MAC) over data that is stored on the smart card. A MAC that is computed by the smart card is also called a stamp.

All data is stored unencrypted on a smart card. A smart card can encrypt data that is stored in specific files on the smart card. The encryption is possible for a file that has access condition ENC (ENCrypted) for the read command.

d) Storage of Secret keys on Smart Card:

The architecture of smart cards allows storing secret cryptographic keys in safe manner. The stored keys can only be used to perform cryptographic computations but not for reading. The keys are stored in specific data files called EF_KEY. The initial secret keys are written on the smart card during the initialization process performed by the card issuer. To write a new secret key Knew on the smart card, secret keys are needed that are (already) stored in the smart card.

Smart card makes use of two kinds of secret keys.

- Management key
- Operational key

A management key is used to encrypt another management key or an operational key is also called a Key Encrypting Key (KEK).

An operational key is used by the smart card to perform data cryptographic operations

5. APPLICATIONS OF SMART CARD

Smart cards are used for huge range of applications today. A few common examples of applications are briefly described below.

i) SIM cards:

A common application for Smart Cards is for mobile phones. The central security processor of a mobile phone is provided by a global system for mobile communication SIM (Subscriber Identity Module). The use of SIM cards has radically improved security of digital phones compared to the older analogue devices.

ii) Bank Cards:

Increasingly credit and debit cards are being used, using the contact chip rather than being swiped. The security feature offered by Smart Cards protect consumers from the cards being cloned as it is much more difficult to copy a chip protected cryptographically than a magnetic strip.

iii) Health Cards:

Increasingly, Smart Cards are being used to store a citizen's medical data. The cards are carried by the citizen and can contain information such as list of allergies,

current and past medications, past treatment history, disease history and doctors notes. This enables medical information to be easily accessed in an emergency.

Consider the scenario how a smart card works for banking.

Stage 1: This is the initial process where the enrollment of customer can takes place; the image and details of customer are saved on card.

Stage 2: After the enrollment process money loaded and wallet value is updated.

Stage 3: When customer inserts the card for money, the system read the data from the card, to verify the validity of customer.

Stage 4: After verification the machine facilitates to credit or debit on the customer's account. Finally the wallet value is updated.

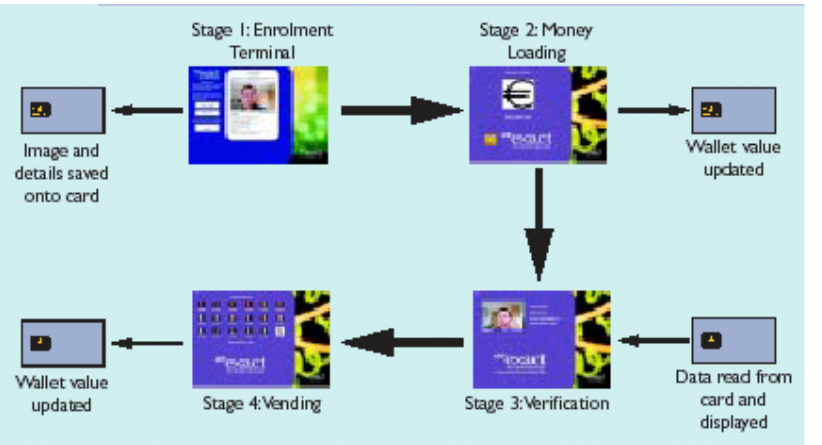


Fig: Evaluation Scenario of Smart cards

6. MERITS/DEMERITS

High-level security can be achieved using cryptography in smart cards. Data present in the smart card is more secured and can be viewed only by the authorized persons only.

Although this system is very effective as protection, due to the large amount processing power needed to run this system it is impossible for use on older, slower computers without the necessary processing power to use such an extensive encryption system.

Weak-authentication may break the security provided by the smart card.

7. CONCLUSION

Cryptography provides a solution to the problem of security and privacy issues. The usage of cryptography in Smart Cards became very popular. Smart card technology can be implemented for multi-applications such as Bankcards, SIM cards, and Health cards.

As card technologies continue to develop we can expect to see advanced cards interacting directly with users through displays, biometric sensors and buttons. This will open up many exciting novel applications, and further increase the usability of Smart Cards.

8. REFERENCES:

U.R.L's:

1. http://www.cryptography.com
2. http://www.smartcardbasics.com
3. http://www.faqs.org/faqs/cryptography-faq

Text Books:

1. "Computer Networks" By Andrew S. Tanenbaum.
2. "Cryptography" By William Stallings.

Magazines:

1. PC Quest.
2. Electronics for You.