



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

MULTIPURPOSE SMART CARD USING ADVANCED ENCRYPTION STANDARD ALGORITHM

Nusrath A

Embedded System Technologies, Department of Electrical and Electronics Engineering,
Nehru Institute of Engineering and Technology, Anna University,
Coimbatore - 641105, Tamil Nadu, INDIA

Abstract: Smart card is one of the greatest achievements in the world of information technology. Smart cards have many applications such as health, ID verification and access control, electronic purse card, banking card, payphone card, passport card and license card. Since, there are many kinds of smart cards, it is difficult to carry and protect them. Losing one card means losing a lot of important information. As everyone knows, carrying and protecting one smart card is easier and more comfortable than carrying two or more smart cards. Multipurpose smart card is a smart card with many different applications in one smart card. Multipurpose smart card would be giving all services and making data processing and data transfer more efficient and secure. We choose three most important cards such as health card, aadhaar cards and passport cards to be combined in one smart card and find an encryption method to make it enough secure. It should also be efficient in transferring information. The advanced encryption standard algorithm should be effective encryption system for these three applications in a multipurpose smart card.

Keywords: AES, multipurpose smart card

I. Introduction

Smart card is also called a cheap card or integrated circuit card. It is the youngest and cleverest member of the family of identification cards. The smart card is defined as a device, which includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or memory chip alone. The card interacts with a reader through direct physical contact or with a remote contactless radio frequency interface. The smart cards play a vital role in today's life. There are different smart cards for different purposes. For example- credit cards, debit cards, voting cards, Aadhar cards (in INDIA), etc. These different cards are to be carried by the people wherever they go, for different purposes. Smart cards are used for data storage, transaction and processing with strong security authentication. Smart cards do not have component such as power resource, display area or keyboard. As mentioned above, smart cards are very useful these days, but there are problems with them. Since, there are many kinds of smart cards, it is difficult to carry many cards and protect them. You may lose, leave or forget one of them and it means that you lose important personal information. Another problem with smart cards is limitation of storage in smart cards. Smart cards need to transfer data in a short time and encrypt them very fast. So, having an efficient encryption system is very important. Therefore, we have decided to design a cryptosystem for multipurpose smart cards. Multipurpose smart card is a smart card with many different applications in one smart card. The main aim of the project is to develop a multipurpose smart card for various applications such as: health, passport and aadhaar card and find an encryption method to make it enough secure.

II. Multipurpose smart card

In the multipurpose smart card three applications are implemented. The applications are health, passport and aadhaar card.

a) Health system: Healthcare organizations worldwide are implementing smart health cards supporting a wide variety of features and applications. Smart health cards can improve the security and privacy of patient information, provide the secure carrier for portable medical records, reduce healthcare fraud, support new processes for portable medical records, provide secure access to emergency medical information, enable compliance with government initiatives and mandates, and provide the platform to implement other applications as needed by the healthcare organization.

b) Passport system: The ePassport or a digital passport is a combined paper and electronic passport that contains biometric information that can be used to authenticate the identity of travelers. It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or center page, of the passport. Document and chip characteristics are documented in the International Civil Aviation Organization's (ICAO) Doc 9303. The passport's critical information is both printed on the data page of the passport and stored in the chip. Public Key

Infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented.

The currently standardized biometrics used for this type of identification system are facial recognition, fingerprint recognition, and iris recognition. These were adopted after assessment of several different kinds of biometrics including retinal scan. The ICAO defines the biometric file formats and communication protocols to be used in passports. Only the digital image (usually in JPEG or JPEG2000 format) of each biometric feature is actually stored in the chip. The comparison of biometric features is performed outside the passport chip by electronic border control systems (e-borders). To store biometric data on the contactless chip, it includes a minimum of 32 kilobytes of EEPROM storage memory, and runs on an interface in accordance with the ISO/IEC 14443 international standard, amongst others. These standards intend interoperability between different countries and different manufacturers of passport books.

c) Aadhaar card: We all know in this web based world our security, our performance and most importantly our identification holds high priority. Keeping in mind all these factors aadhaar card has been launched by the government which is also called as UID i.e. unique identification card or number as it was issued by unique identification authority of India (uidai) to all citizens above five. In this the unique number of an individual is linked with his biometric data so as to check his identity. Since one uid is allotted to only one person, it enables to verify ones identity universally. It is based on the biometric and demographic information of an individual which helps to alienate the risk of all the fictitious activities which are very much prevalent in today's world.

These smart cards allow the devoid and needy persons in approaching various services. It helps them to prove their identity at multiple places. A person's aadhaar number can be used at various places like for booking tickets online, for opening bank accounts, for permitting admissions in universities, applying for passport and at many other places where one need to give their identity proof. This number could be used to enjoy any of the beneficiary schemes allotted by the government. Due to the increasing terrorism in our country it has become very important to record each and every movement of an individual in companies and industries and other expected places.

III. Block diagram

Smart Cards are secure portable storage devices. Reader provides a path for an application to send and receive commands from the card. Middleware are smart card software, they are communication link between application on the computer and code located on smart card. The card used for health, passport and aadhaar card.

Figure 1: Block diagram of card end
CARD END

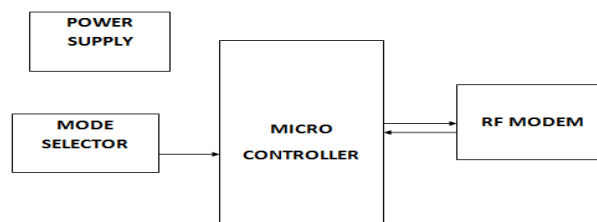
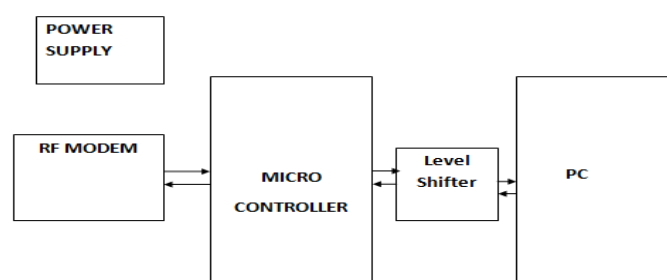


Figure 2: Block diagram of smart card receiver end
RECIEVR END



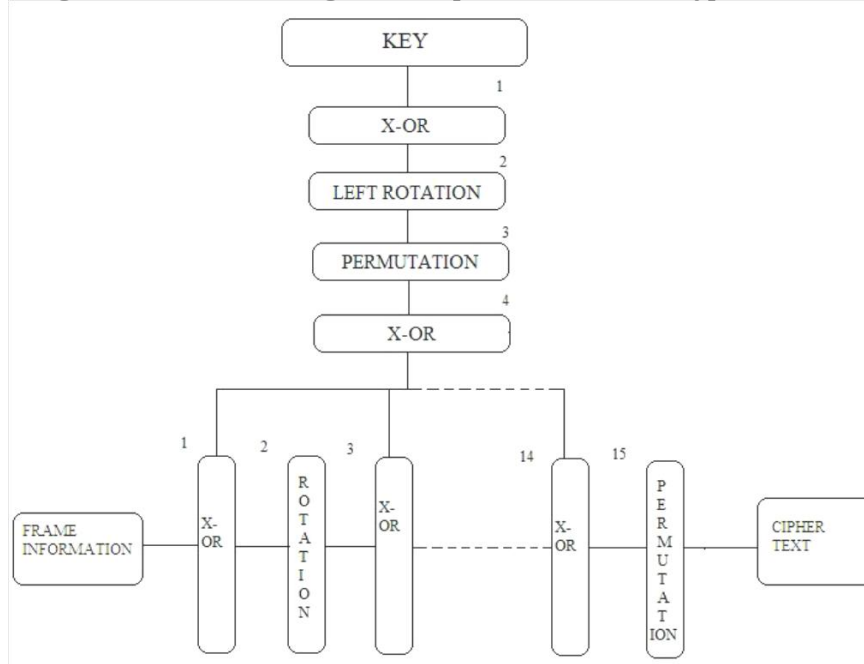
III Algorithm

AES (Advanced Encryption Standard) is used in the multipurpose smart card. The AES is now the industry standard for encryption. The NSA employs it for protecting secret information and industry uses the algorithm for creating commercially available encryption products. File encryption and email encryption are two common applications for AES. File encryption protects the information on your hard disk or thumb drive. With encryption, your data will be secure even if your computer is hacked or your USB drive stolen. Email

encryption protects your messages as they journey through the cloud and keeps them from being read by unintended recipients. The design of AES algorithm consist of following steps

- ☐ Cipher Text Creation
- ☐ Bit Rotation
- ☐ EX-ORing Operation
- ☐ Permutation

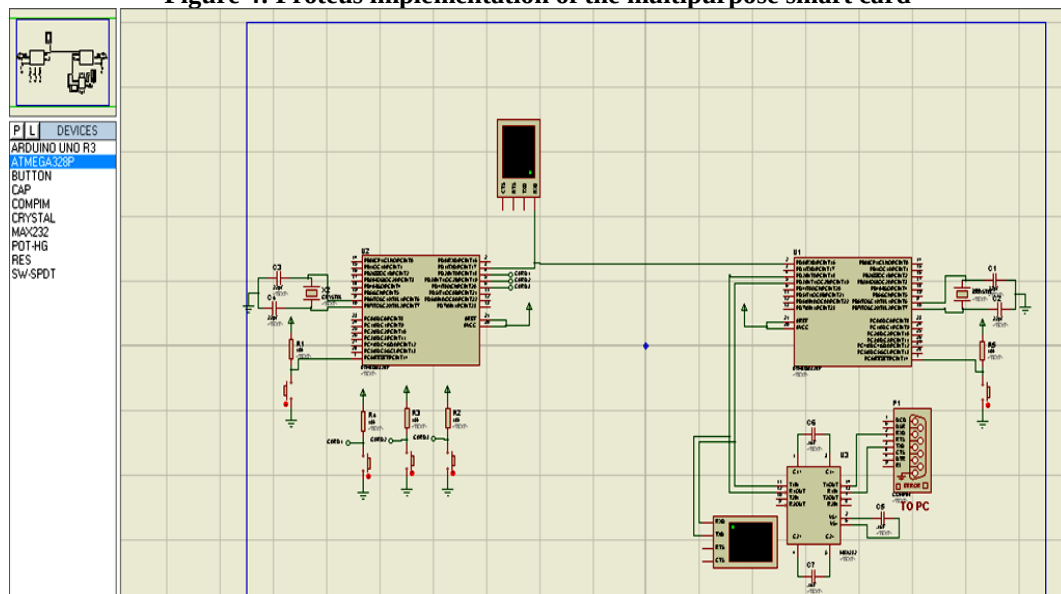
Figure 3: Basic Block Diagram of Implementation of Encryption in AES



IV. Simulation Analysis

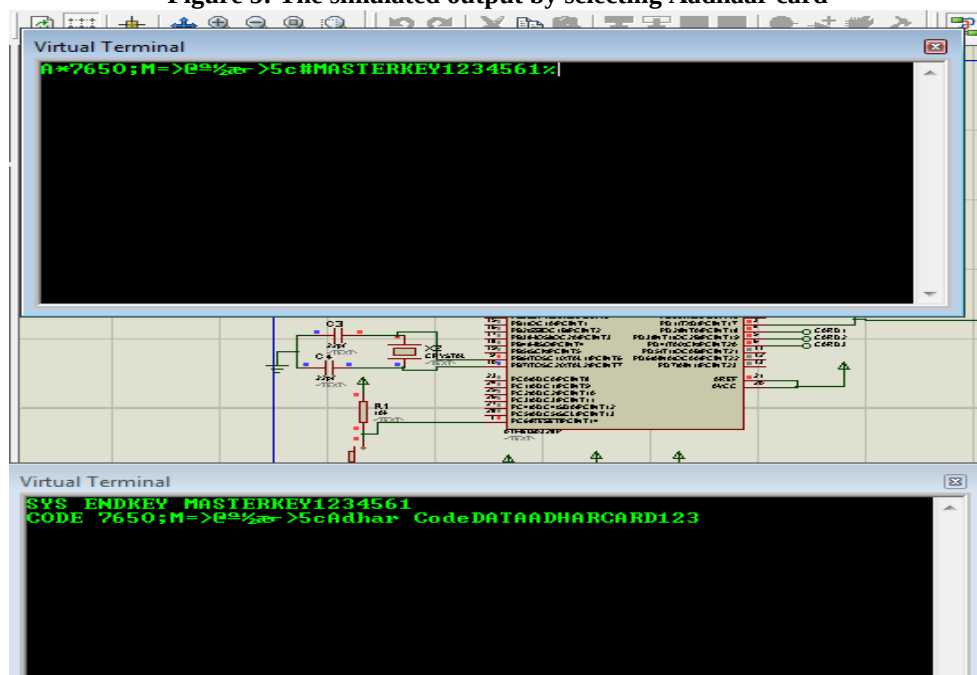
Multipurpose smart card is a smart card with many different applications in one smartcard. Multipurpose smart card would be giving all services and making data process and data transfer more efficient and secure. The multipurpose smart card in implemented by using the proteus and arduino software. The input part consists of three buttons that indicate the three applications. User cannot run two applications at the same time. Access to each application is possible only after exiting other applications. It means it is not possible to run more than one application at the same time. The AES algorithm is used for this card. The AES algorithm is done by using embedded c language.

Figure 4: Proteus implementation of the multipurpose smart card



Here we can see the ATMEGA328 microcontroller in encryption and decryption side. The three buttons in the encryption side indicate the three applications such as: health, passport and aadhaar card. The MAX232 is act as the level shifter.

Figure 5: The simulated output by selecting Aadhaar card



V. Conclusion

AES (advance encryption standard) algorithm is one of the useful and efficient algorithms for high level data transfer. Multipurpose smart card is much better than carrying different card. In this part we design and implemented the multipurpose smart card by using software. This card can be used for three applications such as passport system, aadhaar card and health card. The multipurpose smart card done by re-programming the microcontroller embedded in the single application smart card. The ATMEGA328 microcontroller used in encryption and decryption part of the card. This microcontroller provides the high data storage. In future the one smart card can be used for all the application.

VI. References

- [1]. D. R. Hankerson, S. A. Vanstone, A. J. Menezes.(2003), "Guide to Elliptic Curve Cryptography,".
- [2]. W. Rankl, W. Effing, "Smart card handbook," (2004)3rd ed., John Wiley and Sons Ltd., Baffins Lane, England: Spring Verlag.
- [3]. J. A. Menezes, C. Paul, V. Oorschot, S. A. Vanstone (2001)"Handbook of Applied Cryptography," 5th ed.
- [4]. T. Abdurahmonov, M. H. Helmi, Y. E. Thiam, (2010) "The Implementation of Elliptic Curve Binary Finite Field for the Global Smart Card," Proceedings of 2010 IEEE Student Conference on Research and Development (SCORED 2010).
- [5]. T. Abdurahmonov, Y. E. Thiam, M. H. Helmi,(2010) "Improving Smart Card Security Using Elliptic Curve Cryptography over Prime Field".
- [6]. S.Arora, (2007)"Information Security-Siddhartha Arora Final," Available:http://www.porvoo12.net/MSc_Information_Security.pdf.
- [7]. C. Sanchez-Avilaf, R. Sanchez-Reillo, (2001)"The Rijndael Block Cipher (AES Proposal): A Comparison with DES," 0-7803-6636-0/01/ 02001 IEEE, pp. 229-234.
- [8]. S. Omar, H. Djuhari, (2004)"Multi-purpose student card system using smart card technology. Information technology based higher education and training," ITHET 2004. Proceedings of the Fifth Internationalconference on, pp. 527-532.
- [9]. A. B. Mohamed, A. A. Hamid, K. Y. Mohamed (2009) "Implementation of an Improved Secure System Detection for E-passport by using EPCRFIDTags,"
- [10]. A. Kleijhorst, van der Velde.E T, Baljon.M H, Gerritsen.M J G M,Oon.H,(1997) "Secure and Cost-Effective Exchange of Cardiac Images over the Electronic Highway in the Netherlands," 0276-6547/97 1997 IEEE,pp. 191-194.