Encryption Algorithms Used for Secured Communication

Kulkarni Laxmi G.[1], N. A. Dawande[2]

[1]University of Pune, Dr. D. Y. Patil College of Engineering, Ambi-Talegaon, Pune, India

[2]University of Pune, Department of Electronics and Telecommunication Engineering,
Dr. D. Y. Patil College of Engineering, Ambi-Talegaon, Pune, India

Abstract: ***With the development of the digital devices, computers and networks, our world relies more and more on the digital data. In many cases, storing data safely is a very big concern. These data have to be protected so as to prevent the possible unauthorized access. Many technologies have been used to improve the security of the data storage. Encryption is a process of coding information which could either be a file or mail message in into cipher text a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data. Decryption is the exactly opposite process of converting encoded data to its original un-encoded form which is nothing but plaintext. Here we are introducing some encryption algorithms.***

Keywords: RC4, AES, Chaos based algorithm

1. Introduction

Encryption is now commonly used in protecting information within many kinds of civilian systems. Encryption is the process of coding messages (or information) in such a way that third parties cannot read it, which only authorized parties can. It doesn't prevent hacking but it prevents the hacker from reading the data that is encrypted. In an encryption scheme, the message or information or referred to as plaintext is encrypted using an encryption algorithm, which turns it into an unreadable text referred to as cipher text. And this is usually done with the use of an encryption key. This encryption key specifies how the message is to be encoded. An authorized party is able to decode the cipher text using a decryption algorithm, which requires a secret decryption key that adversaries do not have access to.

There are two basic types of encryption schemes: public-key encryption and symmetric-key. In public-key schemes, the encryption key is published for anyone to use and encrypt messages. But, the receiving party has access to the decryption key and is capable of reading the encrypted messages. This encryption is a relatively recent invention. In symmetric-key schemes, the encryption and decryption keys are the same. Communicating parties must agree on a secret key before they wish to communicate. Symmetric-key encryption is also known as private-key schemes.

2. RC4 Encryption Algorithm

Ronald Rivest of RSA developed the RC4 algorithm. This is a shared key stream cipher algorithm requiring a secure exchange of a shared key. The algorithm is serial as it requires successive exchanges of state entries based on the key sequence. This algorithm has been released to the public and is implemented by many programmers. The algorithm is used identically for encryption and decryption as the data stream is simply XORed with the generated key sequence. This encryption algorithm is used by standards such as IEEE 802.11 within Wireless Encryption Protocol using a 40 and 128-bit keys.

The VOCAL implementation of the RC4 algorithm is available in different forms. The forms include original optimized software and varying levels of hardware complexity utilizing UDI instructions. When special assistance hardware is not available, the byte manipulation/exchange operations are implemented via software. In the algorithm the key stream is completely independent of the plaintext used. The permutation is a function of the variable length key. An 8 * 8 S-Box (S0 S255), where each of the entries is a permutation of the numbers 0 to 255. There are two counters i, and j, both initialized to 0 used in the algorithm.

3. AES Algorithm

[1] Here they design and realize an encryption system based on the algorithm on ARM(S3C6410), which can encrypt and decrypt the information in many kinds of memorizers, such as U Disk, SD card and mobile HDD. In this paper, they designed and implemented an encryption system to encrypt the stored data based on ARM (S3C6410).The system that uses Human-Computer Interaction and Visualization technology provides several encryption algorithms and key generators. In this paper, they designed and implemented an encryption system to encrypt the stored data based on ARM (S3C6410). The PN sequences with good properties are generated from chaotic map and the system provides two kinds of encryption algorithm, one is stream cipher with X OR operation, the other is a hybrid algorithm of AES and chaos. The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data which is established by the U.S. National Institute of Standards and Technology (NIST). In order to improve the security of the private information in memorizer, this inherits the advantages of in this paper.

"Design of a secure chat application based on AES cryptographic algorithm and key management" this paper presents the design and implementation of a software application for the provision of secure real time

communication services between workstations, based on the AES prototype cryptographic algorithm and an advanced secret key management system[3]. The application has been designed based on the requirements of a military unit, so as to allow groups of authenticated users to communicate and read the transmitted messages. This application can be used as the basis for the design of an integrated communication system for a military organization. The present design confines its operation within the limits of a local area network.

"FPGA implementations of advanced Encryption standard: a survey" presents the AES based on the Rijndael Algorithm which is an efficient cryptographic technique that includes generation of ciphers for encryption and inverse ciphers for decryption[4]. Advanced Encryption Standard (AES) is the most secure symmetric encryption technique that has gained worldwide acceptance. Higher security and speed of encryption/decryption is ensured by operations like Sub Bytes (S-box)/Inv. Sub Bytes (Inv. S-box), Mix Columns/Inv. Mix Columns and Key Scheduling. Extensive research has been conducted into development of S-box /Inv. S-Box and Mix Columns/Inv. Mix Columns on dedicated ASIC and FPGA to speed up the AES algorithm and to reduce circuit area. Fault attacks are powerful and efficient cryptanalysis techniques to find the secret key of the Advanced Encryption Standard (AES) algorithm.[5] "A Robust Fault Detection Scheme for the Advanced Encryption Standard," this paper shows that these attacks are based on injecting faults into the structure of the AES to obtain the confidential information. A number of countermeasures have been proposed to protect the AES implementation against these attacks. In this paper, they have proposed a fault detection scheme for the Advanced Encryption Standard. They present its details implementation in each transformation of the AES. The simulation results show that the fault coverage achieves 99.999% for the proposed scheme. The proposed fault detection scheme has been implemented on Xilinx Virtex-5 FPGA. Its area overhead and frequency degradation have been compared and it is shown that the proposed scheme achieves a good performance in terms of area and frequency.

[7]When neural network with fast parallel computing and complex behavior of chaotic dynamics, it is one of the best choice for designing encryption algorithm. With chaotic neural network by analyzing the complex dynamic behavior and the characteristics of parallel processing, neural network-based chaotic encryption algorithm AES is presented, which can help AES algorithm to overcome the traditional key only because of security caused by the characteristics of lower and raise the AES security algorithm.

To improve the efficiency of Advanced Encryption Standard (AES) algorithm on ARM processor, an optimization of AES was introduced and realized on ARM920T processor. [8] One-time key expansion was adopted. In the algorithm, Sub Bytes () and Mix Columns () were defined as T-table to store, which could increase the speed. The proposed algorithm programmed by C language was simulated and debugged on the ARM Develop v1.2 platform. Different implementations were compared in storage space and processing speed and a variety of different key length algorithm performances were given. The experimental results show that the execution speed of the presented algorithm improves significantly.

4. Chaos Based Encryption Algorithm

The paper which presents Encryption used for video is "Chaos-Based Encryption Algorithm for Compressed Video" shows chaos-based encryption algorithm called the chaotic selective encryption of compressed video (CS ECV) which exploits the characteristics of the compressed video [2]. Encryption is needed to protect the multimedia data Compared with text encryption; multimedia encryption has some unique characteristics, such as the large size, high throughput, and real-time processing. An efficient, secure, and lightweight encrypt ion algorithm is desirable to protect the compressed video. A video clip is generally compressed in a transform Domain with some type of entropy coding To protect a compressed video, encryption techniques can be applied to the original data, such as block swapping, or the data can be transformed using DCT or wavelet coefficients, entropy-coded bit streams, or format headers. The encryption has three separate layers that can be selected according to the security needs of the application and the processing capability of the client computer. The chaotic pseudo-random sequence generator used to gene rate the key-sequence to randomize the important fields in the compressed video stream has its parameters encrypted by an asymmetric cipher and placed into the stream. The resulting stream is still a valid video stream. CSECV has significant advantages over existing algorithms for security, decryption speed, implementation flexibility, and error preservation.

Chaotic system has fine cryptology characteristic property.[6] The chaotic array has exceeding sensibility initial condition and system parameter, as well as the chaotic array long range evolves bearing fruit be not allowed to forecast the characteristic property. Meanwhile, the chaotic system has nice characteristic of secure communication such as randomness, the extreme sensitivity to the parameter and the initial value. Chaotic cryptology becomes an important research of modern cryptology forward position, and it has vastly developing a prospect. Nowadays, for the public cryptography algorithm (DES, AES, RSA, ECC etc.), the security of cryptography mostly depends on the security and randomness of the cipher key. In the information theory which was founded by Claude Shannon, he used strict mathematic methods to prove that: any cryptography, except dynamic key changing system, can be cracked in theory. New AES chaotic encryption algorithm can changing the key, because of the traditional AES algorithm have disadvantage on the security. First this article introduces a few basic theories about AES algorithm, summarizes chaotic cryptology research current situation, chaotic mapping in common use and the theory and principle of chaos. Especially importantly it introduced some main factors that regarded with the security of the sequence cryptograph. They focus on the chaotic theory and AES algorithm, and develop an AES dynamic key changing system based on chaotic theory. A novel AES algorithm based on two dimensional Logistic mapping and Chebyshev mapping he is presented. The one chaotic mapping is the primary mapping; the other

one is the secondary mapping which has the interferential function. We bring forward one kind of new chaotic encryption algorithm which combines the two dimensional logistic mapping and Chebyshev mapping.

The Rijndael Algorithm was chosen for the Advanced Encryption Standard (AES) in 2001 and formally published in FIPS Publication 197. Since Rijndael was released as a candidate a number of cores were created to test and benchmark the algorithm in both hardware and software [9]. Rijndael was chosen partly based on its ability to be efficiently implemented in Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs). In ASIC design, heavy use of combinational logic is advantageous. In FPGA designs each logic cell has local memory available and all free logic cells are equally valuable for design use. A survey of published AES architectures found they did not fully take advantage of ROM blocks to simplify and shorten critical paths in the algorithm's rounds. This paper will present a T-box design that will utilize FPGA memory in a core with a standard 32-bit bus width that will sustain a throughput of 20 Mbyte/sec. Advanced Encryption Standard (AES) specification is documented in the National Institute of Standards and Technology's (NIST) FIPS 197 publication.[5] J. Daemen and V. Rijmen submitted Rijndael as part of NIST's AES contest. Candidates for the contest were tested based on strength of the algorithm against attacks, maximum throughput, and resources required for both software and hardware implementations. Rijndael was originally designed with a variety of key lengths and variable block lengths in mind. When the variable block length requirement was dropped, Rijndael was amended to a fixed 128-bit block length. Since the chosen core would be a US Federal Standard all teams participating had to openly publish their standard and must be free of Intellectual Property. The finalists were evaluated equally, but each submission differed in implementation costs, throughput, and versatility in implementation. Flexible algorithms that could run efficiently across Application Specific Integrated Circuits (ASICs) for smart cards, 32-bit microprocessors, and even 8 bit microcontrollers proved a challenge during final selection. On October 2nd, 2000 NIST announced that Rijndael was the winner and new AES standard, based on the evaluation criteria, peer review, and excellent performance across a number of target platforms. AES supports multiple key sizes (128,192, and 256 bits) and is used as a block cipher with a message size of 128 bits. The block cipher structure can be used in a variety of modes to create a secure stream cipher based on AES encryption and/or decryption. Using the basic Electronic Code Book (ECB) mode, a 128-bit message is encrypted with a key of 128, 192, or 256 bits to produce a 128-bit cipher text. A key expansion is first performed on the initial key values, based on a key schedule, to generate unique keys for all rounds of encryption. The key schedule was developed to use small amounts of memory, have no symmetries, have efficient diffusion of keys, and be non-linear. Diffusion allows small changes in a previous key to cause significant changes in the next expanded key. Elimination of symmetries and linear functions allows generation of expanded keys that resist attacks and analysis on the cipher text. A perfect key expansion would generate seemingly random keys that are unique and easily computed from the initial and subsequent expanded keys. With no pattern to attack, the attacker would have to pick from all possible keys for every round of the algorithm. AES uses rotations, XOR operations for permutations, and table lookups from an S box table specified in FIPS 197 for direct substitutions on each byte of the key.

5. Conclusion

There are various types of encryption algorithms, which can are useful in many applications. Out of this RC algorithm is the easiest algorithm to implement but also is easy algorithm to crack comparatively. Advanced Encryption Standard (AES) and Chaos based encryption system are quite developed encryption algorithms. The Advanced Encryption Standard is a specification for the encryption of electronic data. It is the modified algorithm of DES (Data Encryption Standard). The Data Encryption Standard is a previously predominant symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world.

References

[1] Chunlei Wang, Guangyi Wang, Yue Sun and Wei Chen"ARM Realization of Storage Device Encryption Based on Chaos and AES Algorithm" 2011 Fourth International Workshop on Chaos-Fractals Theories and Applications
[2] Chun Yuan, Yuzhou Zhong, and Yuwen He, "Chaos Based Encryption Algorithm For Compressed Video," Chinese Journal of Computers, Vol.27 No.2, Feb 2004, pp.257- 263.
[3] Nikolaos G. Bardis, Konstantinos Ntaikos, "Design of a secure chat application Based on AES cryptographic algorithm and key management"
[4] Shylashree.N; Nagarjun Bhat; V. Shridhar, "FPGA Implementations of advanced Encryption standard: a survey" Directory of Open Access Journals (Sweden), Jan 2012
[5] Hassen Mestiri; Noura Benhadjyoussef; Mohsen Machhout; Rached Tourki, "A Robust Fault Detection scheme For Advanced Encryption tandarad," Directory of Open Access Journals(Sweden), Jan 2013
[6] Rui Zhao, Qingsheng Wang, and Huiping Wen, "Design of AES algorithm Based On Two Dimensional Logistic and Chebyshev Chaotic Mapping," Microcomputer
[7] Yi Li, and Xingjiang Pan, "AES Based on Neural Network of Chaotic Encryption algorithm," Science Technology and Engineering, Vol.10 No.29, Oct 010, pp.7310- 7313.
[8] Ruxue Bai, Hongyan Liu, and Xinhe Zhang, "AES and its software implementation based on ARM920T," Journal of Computer Applications, Vol.31 No.5, May 2011, pp.1295-1301.

Author Profile

Ms. Kulkarni Laxmi G. received B.E. degree in Electronics Engineering from DKTE COE in 2010. Currently she is pursuing M.E (VLSI & ES) at Dr. D. Y. Patil College of Engineering, Ambi-Talegaon, Pune, India.