International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

REVIEW ARTICLE

ISSN: 2321-7758

REVIEW OF NETWORK SECURITY AND ITS ALGORITHMS

ROBIN MALIK[1], Prof. SUMIT RANA[2]

[1]Geeta College of Engineering,Naultha (Panipat)

[2]Geeta College of Engineering,Naultha (Panipat)

Article Received:19/05/2015 | Article Revised on:27/05/2015 | Article Accepted on:11/06/2015

ABSTRACT

Cryptography is an emerging technology, which is important for network security. Cryptology is as old as writing itself and has been used for thousands of years to safeguard military and diplomatic communications. In the past decades, we have witnessed an explosive growth of the digital storage and communication of data, triggered by some important breakthroughs such as the Internet and the expansive growth of wireless communications. These new information and communication technologies require adequate security. Cryptology is the science that aims to provide information security in the digital world. Cryptology is usually split up into two closely related fields: cryptography and cryptanalysis. Cryptography studies the design of algorithms and protocols for information security. Cryptanalysis is concerned with this study of mathematical techniques that attempt to break cryptographic primitives. Research on cryptography is still in its developing stages and a considerable research effort is still required for secured communication.

KEYWORDS:- Network security, Symmetric Algorithms,DES,IDEA,RC2,Cipher

I. INTRODUCTION

A computer network is an interconnected group of autonomous computing nodes which use a well-defined, mutually-agreed set of rules and conventions known as Protocols, interact with one-another meaningfully and allow resource-sharing preferably in a predictable and controllable manner. Study of methods of analysis of security requirements and needs of such systems and consequent design, implementation and deployment is the primary scope of the discipline named as Network Security. Although named as network security, the principles and mechanisms involved herein do apply to Internet works as well. Network security starts from authenticating any user. Once authenticated, firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective it cannot prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network. An intrusion prevention system

(IPS) helps detect and prevent such malware. IPS also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service. Communication between two hosts using the network could be encrypted to maintain privacy.

II. SYMMETRIC CRYTOGRAPHY ALGORITHM

Some of the Symmetric Cryptographic algorithms are discussed below:

2.1 Data Encryption Standard (DES)

DES is a complex block cipher. DES was designed by IBM and adopted by the U.S. government as the standard encryption method for nonmilitary and misclassified use. The algorithm encrypts a 64bit plaintext block using a 64bit key. DES has two transposition blocks (P-boxes) and 16 complex round ciphers (they are repeated). Although the 16 iteration round ciphers are conceptually the same, each using a different key derived from the original key. The initial and final permutations are keyless straight permutations are keyless straight permutations that are the inverse of each other. The permutation takes a 64bit input and permutes them according to predefined values. Each round of DES is complex round cipher. DES is the archetypal block cipher an algorithm that takes a fixed length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of DES, the block size is 64bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is usually quoted as such.

2.2 Triple DES

Critics of DES contend that the key is too short. To lengthen the key, Triple DES or 3DES has been proposed and implemented. This uses three DES blocks. Note that the encrypting block uses an encryption-decryption-decryption combination of DES'S, while the decryption block uses a encryption-decryption-decryption combination. Two different versions of 3Des are in use: 3Des with two keys and 3DES with three keys. To make the key size 112 bits and at the same time protect DES from attacks such as the man-in-the-middle attack, 3DES with two keys was designed. In this version, the first and the third keys are the same (key1=key3). This has the advantages in that a text encrypted by a single DES block can be decrypted by the new 3DES. We just set all keys equal to key1. Many algorithms use a 3DES cipher with three keys. This increases the size of the key to 168 bits.

2.3 International Data Encryption Algorithm (IDEA)

The International Data Encryption Algorithm (IDEA) is perceived as one of the strongest cryptographic algorithm. It was launched in 1990 & underwent certain changes in names & capabilities. Although it is quite strong. IDEA is not as popular as DES for two primary reasons. Firstly, it is patented unlike DES & therefore must be licensed before it can be used in commercial applications. Secondly DES has a long track record as compared to IDEA.

(a) How IDEA works

Basic Principles: Technically, IDEA is a block cipher. Like DES, it works on 64bit plaintext blocks. The key is longer and consists of 128 bits. IDEA is reversible like DES, that is, the same algorithm is used for encryption and decryption. Also, IDEA uses both diffusion and confusion for encryption. The working of IDEA can be visualized at a broad level as in figure 1.6.3.1. The 64 bit input plaintext block is divided into four portion of plaintext (each of size 16 bits), say P1 to P4.Thus P1 to P4 are the inputs to first round of algorithm. There are eight such rounds. In each round, six sub-keys are generated from the original key. Each of sub-keys consists of 16 bits. These six sub-keys are applied to the four input blocks P1 to P4. Thus, for the first round, having six keys K1 to K6. For the second round, having keys K7 to K12. Finally, for the eighth round, keys K43 to K48. The final step consists of an Output Transformation, which uses just four keys K49 to K52. The final output is output produced by Output transformation step, which is four blocks of ciphertext named C1 to C4 (each consists of 16 bits). These are combined to form the final 64-bit cipher text block.

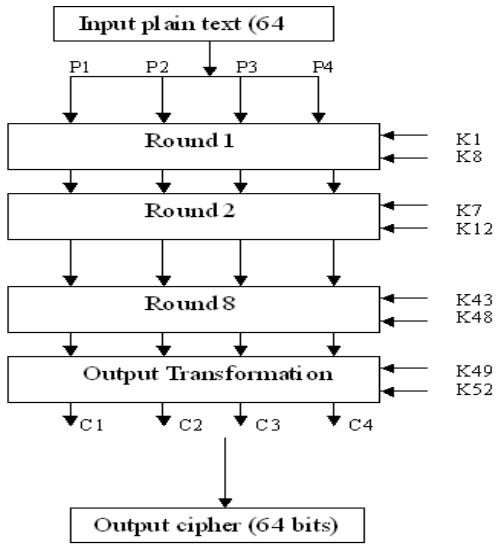

Figure 1.6 Broad level steps in IDEA

(b) Rounds: There are 8 rounds in IDEA. Each round involves a series of operations on the four data blocks using six keys. At a broad level, these steps can be described as in figure 1.6.3.2 these steps perform a lot of mathematical actions. There are multiplication, additions and XOR operations. Sub key generation for a round: As each of eight rounds makes use of six sub-keys (so, 8*6=48 sub keys are required for rounds) and the final output transformation uses four sub keys (making a total of 48 +4=52 sub-keys overall). From input keys of 128 bits, how are these 52 sub keys generated? Let us understand this with explanation for the first two rounds. First round we know the initial key consists of 128 bits, from which 6 sub keys K1 to K6 are generated for the first round. Since K1 to K6 consists of 16 bits, the first 96 bits (6 sub- key * 16 bits per sub key) are used for first round. Thus, at the end of first round, bits 97-128 of the original key is unused Second round in this round first the 32 unused bits of first round are used.

Thus for second round, we require (92–32=64) more bits. However we already exhausted all the 128 bits of original key. How we get the remaining 64 bits? For this, IDEA employs the technique of key shifting**.** At this stage the original key do 25 bits leave shifting circularly. That is 26th bit of original key moves to the first position and becomes the first bit after the shift and the 25th bit of original key moves to the last bit position and becomes the 128th bit after the shift. The second round uses the bits 97-128 of the first round, and after 25-bit shift bits 1-64. For the third round, we then use the remaining bits, i.e. bits 65-128 (i.e. a total of 64 bits). Again shift on 25 bits occurs, and post this shifting, bits 1-32 are used in third round, and so on. Thus in every round, 96 bits are obtained in the same manner, and this is how 128 bits key is divided into 96-bit sub keys. At the end of the last round, we have no unused bits. They are used in the Output Transformation.

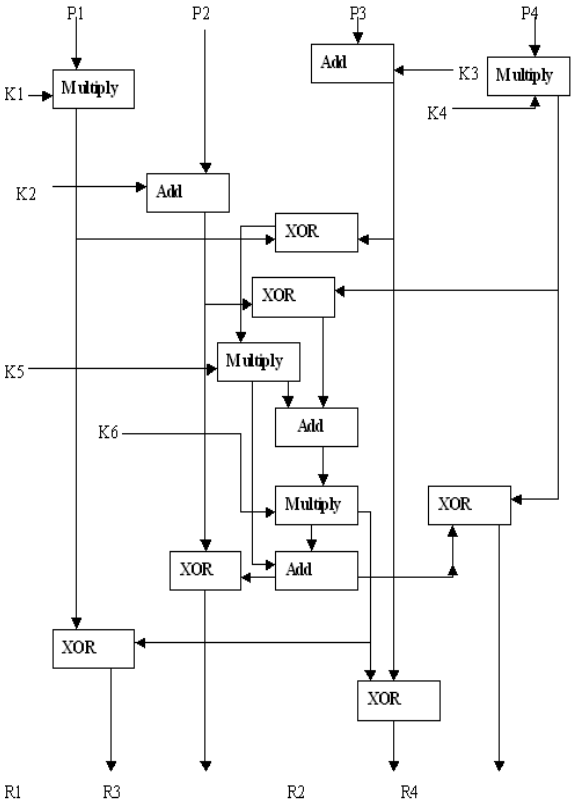

Figure 1.7 one round in IDEA

Output Transformation**:** The Output Transformation is a onetime operation. It takes place at the end of the 8th round. The input to Output Transformation is, of course, the output of the 8th round. This is, as usual, a 64-bit value divided into four sub-blocks (say R1 to R4, each consisting of 16 bits). Also, four sub-keys are applied here and not six. We assume that four 16-bit sub-keys K1 to K4 are available to the Output transformation.

(c) Sub Key Generation for the Output Transformation: The process for the Sub Key Generation for the Output Transformation is exactly similar to the sub-key generation process for the eight rounds. Recall that at the end of eighth and final round, the key was exhausted. Hence, 25 bits again shift the key. Post this shift operation, the first 64 bits of the key are taken, and are called as sub-

key K1 to K4 for the final output Transformation round.

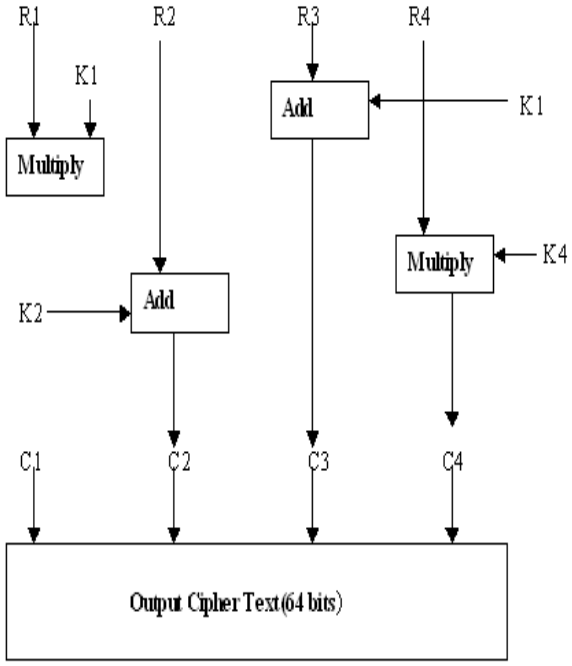

Figure 1.8 Output Transformation process

(d) IDEA Decryption**:** The decryption process is exactly the same as the encryption process. There are some alterations in the generation and pattern of sub-keys. The decryption sub keys are actually inverses of the encryption sub-keys.

(e) The Strength of IDEA**:** IDEA uses the 128 bits key, which is double than the key size of DES.Thus to break in to IDEA, 128 (i.e. 10) encryption operation would be required. As, if we obtain the correct key, only half of the possible keys (i.e. the half of the key space) need to examined, a single computer performing one IDEA encryption per microsecond would require more than 5400000000000000000000000 years to break IDEA.

2.4 RC2

In cryptography, RC2 is a block cipher designed by Ron Rivest in 1987. "RC" stands for "Ron's Code" or "Rivest Cipher"; other ciphers designed by Rivest include RC4, RC5 and RC6. The development of RC2 was sponsored by Lotus, who were seeking a custom cipher that, after evaluation by the NSA, could be exported as part of their Lotus Notes software. The NSA suggested a couple of changes, which Rivest incorporated. After further negotiations, the cipher was approved for export in 1989. Along with RC4, RC2 with a 40-bit key size was treated favourably under US export regulations for cryptography. A 64-bit block cipher using variable-sized keys designed to replace DES. Its code has not been made public although many companies have licensed RC2 for use in their products RC2 is a symmetric encryption algorithm with variable key length. It was developed by Ron Rivest (RC stands for Ron,s Code or Rivest Cipher). Its speed does not depend on the key length. The algorithm itself has never been published; RC2 is integrated in the CBC mode.

2.5 RC4

RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA Security. It is a variable key-size cipher with byte-oriented operations. The algorithm is based on the use of random permutation. Eight to sixteen machine operations are required per output byte, and the cipher can be expected to run very quickly in software. RC4was kept as a trade secret by RSA security. In September 1994, the RC4 algorithm was anonymously posted on the Internet on the Cypherpunks anonymous mailers list. The RC4 algorithm is remarkably simply and quite easy to explain. A variable length key of from 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256 byte state vector S, with elements S[0], S[1],…….,S[255]. At all times, S contains a permutation of all 8 bits numbers from 0 through 255. For encryption and decryption, a byte k is generated from S by selected one of the 255 entries in the systematic fashion. As each value of k is generated, the entries in S are once again permuted. For our analysis we will take with 8-bit key.

(a) Strengths of RC4

1. The difficulty of knowing where any value is in the table.
2. The difficulty of knowing which location in the table is used to select each value in the sequence.
3. A particular RC4 key can be used only once.
4. Encryption is about 10 times faster than DES

(b) Weakness of RC4:

1.The RC4 algorithm is vulnerable to analytic attacks of the state table.

2. One in every 256 keys can be a weak key. These keys are identified by cryptanalysis that is able to find circumstances under which one of more generated bytes are strongly correlated with a few bytes of the key.

3. Weak Keys: these are keys identified by cryptanalysis that is able to find circumstances under which one or more generated bytes are strongly correlated with small subset of the key bytes. These keys can happen in one out of 256 keys generated.

2.6 Advanced Encryption Standard (AES)

In cryptography, the Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor the Data Encryption Standard (DES). AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a 5-year standardization process. It became effective as a standard May 26, 2002. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography. It is available by choice in many different encryption packages.The cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted to the AES selection process under the name "Rijndael", a portmanteau of the names of the inventors. Unlike DES, its predecessor, Rijndael is a substitution-permutation network, not a Feistel network. AES is fast in both software and hardware, is relatively easy to implement, and requires little memory. As a new encryption standard, it is currently being deployed on a large scale. Strictly speaking, AES is not precisely Rijndael (although in practice they are used interchangeably) as Rijndael supports a larger range of block and key sizes; AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with key and block sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits.Due to the fixed block size of 128 bits, AES operates on a 4×4 array of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field.

(a) Operation

The basics of Rijndael are in a mathematical concept called as Galois field theory. Similar to the way DES functions, Rijndael also uses the basic techniques of substitution and transposition (i.e. permutation). The key size and plain text block size decide how many rounds need to be executed. The minimum number of rounds is 10 (when key size and plaintext block size are each 128 bits) and the maximum number of rounds is 14. One key differentiator between DES and Rijndael is that all the Rijndael operation involves entire byte and not individual bits of a byte. This provides for more optimized hardware and software implementation of the algorithm.

C.*PROBLEM Definition*

Cryptography is an emerging technology, which is important for network security. Research on cryptography is still in its developing stages and considerable research efforts are still required for secured communication. My objective is devoted to the security and attack aspects of cryptographic techniques, particularly to Modern Cipher techniques such as DES, 3DES in both the modes i.e. ECB and CBC. Other algorithms under consideration are IDEA, RC2, RC4, and AES. I will study the dominant issues of security, attack and various information theory characteristics of ciphertexts. The simulation based information theory tests such as Entropy, Floating Frequency, Digram, Trigram, Fourgram, Autocorrelation and Periodicity on ciphertext will be done. Also the Modern cipher techniques will be evaluated on the basis of its keylength.

1.Review of Modern Ciphers.

2.Analysis of Modern Block Cipher Techniques.

3.Comparison of Modern Block Cipher Techniques

D. *Methodology*

CrypTool simulator is a freeware program, which enables you to apply and analyze cryptographic mechanisms. It has the typical look-and-feel of a modern Windows application. CrypTool contains exhaustive online help, which can be understood without extensive knowledge of cryptography. CrypTool is available in English, German and Polish. CrypTool has implemented almost all state-of-the-art crypto functions and allows you to learn about and use cryptography within the same environment. A summary of all the encryption algorithms implemented in CrypTool is available in the online help page for the Crypt/Decrypt menu. Both, the included CrypTool presentation as well as the CrypTool web site, contain many screen shots.

REFERENCES

[1]. Carl e. landwehr and David m. goldschlag, "Security Issues in Networks with Internet Access", Proceedings of the IEEE, Vol. 85, No. 12, 1997 pp2034-2051.

[2]. Alfred O. Hero, "Secure Space–Time Communication", IEEE transactions on information theory, Vol. 49, No. 12, 2003 pp 3235-3249.

[3]. Wilhelm burger, "Networking: of Secure Systems", IEEE journal on selected areas in communications, Vol. 7, No 2. 1989 pp312-318.

[4]. Kou Yanan, Li Zengzhi and Liao Zhigang.," A prototype of security for active networks" IEEE International Conference on Algorithms and Architectures for Parallel Processing, 2002 pp 338- 341.

[5]. 5.Sakalli, M.T. Bulus, E. Buyuksaracoglu, F ," Cryptography education for students" IEEE International Conference on: Information Technology Based Higher Education and Training, 2004, pp 621- 626.

[6]. Shafi Goldwasser, "New Directions in Cryptography: Twenty Some Years Later", 38th IEEE Annual Symposium on Foundations of Computer Science, 20-22 Oct 1997 pp314-324.

[7]. Luca Breveglieri, Israel Koren and Paolo Maistri ," An Operation-Centered Approach to Fault Detection in Symmetric Cryptography Ciphers", IEEE transactions on computers, Vol. 56, No. 5, 2007 pp 635-649.

[8]. Kim, Donnie H., Rajeev and Norseman, "Exploring Symmetric Cryptography for Secure Network Reprogramming", IEEE 27th International Conference on Distributed Computing Systems Workshops, ICDCSW '07 June 2007 pp 17-27.

[9]. Dr. Eng. Sattar B. Sadkhan, "Cryptography: current status and future trends", International Conference on Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 pp 417- 420.

[10]. Raphael C., W. Phan and Mohammad Umar Siddiqi, "A Framework for Describing Block Cipher Cryptanalysis", IEEE transactions on computers, Vol. 55, No. 11, 2006 pp 1402-1409.

[11]. CHRISTOPHE DE CANNIÈRE, et al, "An Introduction to Block Cipher Cryptanalysis", Proceedings of the IEEE, Vol. 94, No. 2, 2006 pp 346-355.

[12]. Wei Li Dawu Gu,"A First Step to Provable Security in Block Ciphers against Side Channel Attacks", International Conference on Communications and Networking in China, Aug.2007 pp 408-412.

[13]. Ho Yean Li Samsudin and A. Belaton, "Heuristic cryptanalysis of classical and modern ciphers", 13th IEEE International Conference on Networks, 2005 Malaysia International Conference on Communication, 2005 Vol. 2 pp6-10.

[14]. Zi-Bin Dai, Xiao-Hui Yang and Qiao Ren Xue-Rong Yu," The research and design of reconfigurable cipher processing architecture targeted at block cipher", 7th International Conference on ASIC, Oct. 2007 pp814-817.

[15]. Seung-Jo Han Heang-Soo Oh Jongan Park , "The improved data encryption standard (DES) algorithm", IEEE 4thInternationalSymposiumonSpreadSpectrumtechniques,1996vol.3pp1310-314.

[16]. Guang Gong Golomb, S.W," Transform domain analysis of DES" IEEE Transactions on Information Theory 1999 vol.45 pp 2065-2073.

[17]. Penzhorn, W.T. ," Algebraic attacks on cipher systems", 7th AFRICON Conference Sept. 2004 Vol.2 pp 969- 974.

[18]. Nadehara, K. Ikekawa, M. Kuroda, I., "Extended instructions for the AES cryptography and their efficient implementation", IEEE Workshop on Signal Processing Systems, 2004 pp 152-157.

[19]. Chih-Chung Lu Shau-Yin Tseng ," Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter", The IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2002. pp 277-285.

[20]. Jingmei Liu Baodian Wei Xiangguo Cheng Xinmei Wang, "An AES S-box to

increase complexity and cryptographic analysis", IEEE International conference on Advanced Information Networking and Applications, 2005, Vol.1 pp 724-728.

[21]. Ocheretnij, V. Kouznetsov, G. Gossel, M. Karri, R Wang," On-line error detection and BIST for the AES encryption algorithm with different S-box implementations", 11th IEEE International On-Line Testing Symposium, 2005. IOLTS 2005.pp141-146.

[22]. Chih-Pin Su Chia-Lung Horng Chih-Tsun Huang Cheng-Wen Wu ," A configurable AES processor for enhanced security", IEEE Asia and South Pacific Design Automation conference, 2005 Vol.1 pp361-366.

[23]. Hodjat, A. Verbauwhede," Minimum area cost for a 30 to 70 Gbits/s AES processor" IEEE Computer society Annual Symposium on VLSI, Feb. 2004 pp 83- 88.

[24]. Sarker, Mohammad Zakir Hossain Parvez, Md," A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount of Data" IEEE INMIC 2005 pp 1-6.

[25]. Creighton T. R. Hager, Scott F. Midkiff, Jung-Min Park, Thomas L. Martin, "Performance and Energy Efficiency of Block Ciphers in Personal Digital Assistants", Proceedings of the 3rd IEEE Int'l Conf. on Pervasive Computing and Communications (PerCom2005), 2005 pp 127-136.

[26]. Kofahi, N.A. Turki Al-Somani Khalid Al-Zamil , "Performance evaluation of three encryption/decryption algoriithms", 46th IEEE International Midwest Symposium on Circuits and Systems, 2003 Vol. 2 pp790-793.

[27]. Yudhvir Singh, Dr. Yogesh Chaba, "Performance Analysis of proposed KK' Cryptographic Techniques", IEEE conference on AIS, 2008 pp267-276.

[28]. NETWORK SECURITY by Charlie Kaufman, Pearson Education Asia.

[29]. INTERNET CRYPTOGRAPHY by Richard E. Smith, Pearson Education Asia.

[30]. CRYPTOGRAPHY & NETWORK SECURITY by William Stallings, Pearson Education Asia.

[31]. CRYPTOGRAPHY & NETWORK SECURITY by Atul Kahate, Tata McGraw-Hill. .

[32]. DATA COMMUNICATIONS & NETWORKING by Behrouz A Forouzan, Tata McGraw-Hill.

[33]. DATA COMMUNICATIONS by William Stallings, Pearson Education Asia.