COMPARATIVE STUDY OF SELECTIVE ENCRYPTION ALGORITHM FOR WIRELESS ADHOC NETWORK

Pranay Meshram*

Pratibha Bhaisare**

S.J.Karale***

ABSTRACT

Information Security has become an important issue in data communication. Encryption has come up as a solution, and plays an important role in information security system. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. These algorithms consume a significant amount of computing resources such as CPU time, memory and battery power and computation time. This paper performs comparative study of three algorithm; Full encryption algorithm, Toss-a-coin selective encryption algorithm and Probabilistic selective encryption algorithm considering certain parameters such as encryption time percentage time, encryption time, overall time and encryption proportion. Eventually, we carry out an extensive set of simulation experiments based on ns2 simulator, and our simulation indicates that the technique of selective algorithms can indeed improve the efficiency of message encryption.

Keywords: *Wireless Security, Data Confidentiality, Selective Cryptographic Algorithm, Symmetric Key Encryption, Wireless Ad hoc Networks.*

*Department of Computer Technology, Yeshwantrao Chavan College of Engineering, RTM Nagpur University, Nagpur, India

**Lecturer, Department of Computer Science & Engineering, Yeshwantrao Chavan College of Engineering, RTM Nagpur University, Nagpur, India.

***Assistant Professor, Department of Computer Technology, Bhausaheb Mulak College of Engineering, RTM Nagpur University, Nagpur, India.

I. INTRODUCTION

Encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Asymmetric keys, two keys are used: private and public keys. Public key is used for encryption and private key is used for decryption (E.g. RSA and Digital Signatures). However, public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [1]. *Asymmetric encryption* techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [2].

A fundamental method of data protection in the area of information and network security is cryptography, which has been widely accepted as a traditional platform of data protection for decades. The application of cryptography is particularly prevalent in nowadays' information technology era, and typical examples include the use of cryptographic techniques to homeland security, military communications, financial transactions, and so on [3]. Through the data encryption and decryption, the protection of data confidentiality and integrity are achieved. However, based on the features of wireless devices, a wireless ad hoc network has special security and efficiency requirements for conventional cryptographic algorithms. At present, there are a variety of methodologies to provide protection for data confidentiality and integrity. As one of mainstream cryptographic methods, symmetric key algorithms are widely used due to its efficiency and its capability of data protection. Typically, a symmetric key cryptosystem employs a secret key for both encryption and decryption purposes. This secret key is only shared by the sender and receiver of the communicating parties and kept confidential to other irrelevant entities. The secrecy of the message will be protected well, when the secret key is kept confidential and distributed securely. Strength of Symmetric key encryption depends on the size of the key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. There are many examples of strong and weak keys of cryptography algorithms. Figure 1 illustrates the schematic diagram of symmetric key encryption and decryption procedure. Protection against unwanted eavesdropping is essential for the viability of wireless multimedia services. Furthermore, in many wireless applications, network resources, such as bandwidth, and node resources, such as battery power, must be conserved.

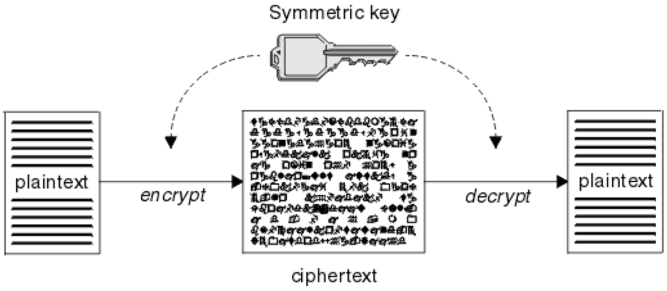

Figure1: symmetric key encryption and decryption procedure.

For a wireless and mobile network, since wireless devices are usually equipped with batteries as their power supply, they have limited computational capability and the issue of energy saving is one of the most important concerns. As a result, an efficient selective encryption algorithm is a potential solution to save considerable power for wireless devices, and at the same time, to provide sufficient protection for data communication. In this article, we study the issue of selective encryption for wireless and mobile networks

II. RELATED WORK

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources. *It was concluded in [5]* that AES is faster and more efficient than other encryption algorithms. When the transmission of data is considered there is insignicant difference in performance of different symmetric key schemes *A study in [6]* is conducted for different popular secret key algorithms such as DES, 3DES, AES, and Blowsh. They were implemented, and their performance was compared by encrypting input less of varying contents and sizes. The results showed that Blowsh had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data. *A study in [4]* is conducted for different popular secret key algorithms such as RC4, AES, and XOR. They were implemented, and their performance was compared by encrypting for real time video streaming of varying contents. The results showed; encryption delay overhead using AES is less than the overhead using RC4 and XOR algorithm. Therefore, AES is a feasible solution to secure real time video transmissions. *It was shown in [1]* that energy consumption of different common symmetric key encryptions on hand-held devices. It is found that after only 600 encryptions of a 5 MB le using Triple-DES the remaining battery power is 45% and subsequent encryptions are not possible as the battery dies rapidly. Using H.264 to compress and encrypt, videos can solve the speed and security problems in mobile application. Protecting the video information by encrypting selective data.[8] The FSET

Encryption algorithm, is a direct mapping algorithm using matrix and arrays. Consequently, it is very fast and suitable for high speed encryption applications. The matrix based substitution resulting in poly alphabetic cipher text generation followed by multiple round arrays based transposing and XOR logic based translations give strength to this encryption algorithm.[9]. While several studies of selective encryption for video and image compression have been performed and documented [10, 11, 12], very few results on selective encryption of coded speech have been presented. Servetti and De Martin [13] investigated partial encryption of G.729 at 8 kbps with respect to what bits should be encrypted to provide security with respect to several factors, including intelligibility, gender identification, plain-text identification, and speech/non-speech discrimination. They demonstrate that partial encryption of about 45% of the bit stream provides protection equivalent to full encryption, and that encryption of as little as 30% of the bit stream precludes intelligibility.SNR scalable speech coding addresses both the bandwidth efficiency and the resource conservation problems by allowing the nodes to prune the enhancement layers when wireless channels become congested, or in the case of MANETs, in order to conserve mobile node battery power, by avoiding excessive transmissions of enhancement layer bit streams [14].

III. THE SELECTIVE ENCRYPTION ALGORITHM (SEA)

AES-Rijndael with 128/192/256 bit keys and 16 byte data treats data in 4 groups of 4 bytes, operating an entire block in every round. At that time, AES are considered not suitable for visual data such as digital image because of long computation process. Recent advances in hardware capability and improvement in software have led to achieve the optimal execution rate when we can find the size of input state by implementing our SEA algorithm system. The result shows that the size of input state among 20 × 20 to 30 × 30 can get the least execution time. In this paper, we proposed a novel encryption algorithm called SEA which is selective and improves the AES algorithm. The Architecture of SEA is shown in Figure 2. The Architecture allows one to perform core idea of our algorithm is an optional manner implemented by Selector component given in Figure 2. The digital visual data have some different types, like video, audio, Image, text file, and so on. As we known, many kinds of platforms from many kinds of devices are over the wire/wireless network. Protection against unwanted eavesdropping is essential for the viability of wireless multimedia services. Furthermore, in many wireless applications, network resources, such as bandwidth, and node resources, such as battery power, must be conserved. Since full encryption of transmitted data streams can place a heavy signal processing burden on originating and receiving nodes, one is led to consider the concept of partial encryption of the data streams.

In partial encryption only a percentage of the transmitted data stream is processed by an encryption algorithm, with the remainder of the data stream being sent in the clear. The questions to be addressed in partial encryption are:

(i) What data must be encrypted to provide the needed level of security

(ii) What is the percentage of the data stream that must be protected? Clearly, the data chosen to be protected must be the "most important" bits in terms of reconstruction of the content from the overall data stream, and this idea has lead partial encryption to sometimes be denoted as selective encryption, which is the terminology that we adopt in this paper.

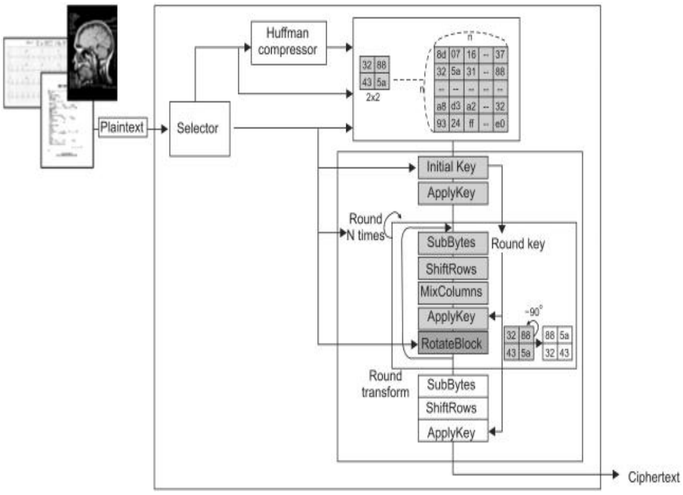

Figure2: Architecture of SEA

IV. THE ISSUES OF SELECTIVE ENCRYPTION AGLORITHMS

As we stated above, selective encryption are widely accepted in energy-aware contexts, due to the fact that they can reduce the overhead spent on data encryption/decryption, and improve the efficiency of the network. Selective encryption can be measured in a number of different ways and optimized for a number of different objectives. Key factors and metrics in selective encryption include:

Security Criterion – selective encryption is proposed both in applications where it is sufficient to damage an attacker's "degraded" – and in applications where it is hoped that an attacker can gain no useful information at all about the content – a level we will call "secret." Obviously, it is not particularly damning to show that a system only intended to degrade content fails to make it secret. It is true, however, that "degraded" is vague as a metric as it will vary by particular attacker and be affected by the cost of the alternative purchase. A further complication is that in some applications the intention is to both degrade the content to make it desirable to purchase yet leave enough fidelity that the degraded content can serve as an advertisement for the purchased content.

Security Validation – in some cases researchers validate security by feeding a selectively encrypted stream to a standard decoder implementation and observing resulting reconstructions. In others, researchers use a cryptanalytic approach, playing the role of an active attacker able to work with a modified decoder and other available information to defeat the selective encryption.

Complexity – one common goal of selective encryption is a reduction in the fraction of material that needs to be encrypted. This reduction needs to be measured and be offset against increases in complexity in, say, additional parsing operations necessary to implement selective encryption.

Algorithmic Constraints – some selective encryption systems limit themselves to working with fixed compression algorithms (e.g., standard MPEG), while others allow some variation in the compression algorithm to enhance selective encryption

V. FULL ENCRYPTION ALGORITHM

In order to protect the confidentiality of communicated messages, selective encryption algorithm takes advantage of major categories of cryptographic techniques, symmetric and asymmetric key algorithms, to guarantee the security of exchanged information. Nevertheless, due to the constrained computational power of wireless devices, it is not realistic to encrypt all information always using the public key algorithms (PKI). Hence, all official data communication between two nodes will be encrypted through symmetric key, and in the meantime, these symmetric keys will be distributed by public key encryption algorithm. In a network, when a node wants to communicate with another node, a secret key (symmetric key) will be generated for their communication [16]. Let us denote the initiating node as *S* and receiving node as *R*. If an initiating node *S* moves into the neighborhood of node *R*,

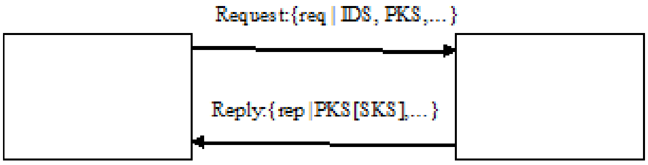

Figure3:The schematic diagram of key distribution

The above figure illustrates the procedure of secret key distribution between a pair of nodes. The message's sender composes a communicating request message *req* which contains not only its identifier *IDS* , but also its public key *PKS* , for the purpose of their later mutual authentication. Once the receiver gets such a communication request, a secret key (symmetric key) *SKS* will be generated by the receiver and encrypted using the public key *PKS* of the requester, which is included in the communicating request message. Later, the receiver composes a communicating reply *rep* message and replies it to the communicating sender, in order to indicate that their communication has been successfully established. After the sender obtains the response from the receiver, it will use its corresponding private key *PRS* to decrypt the secret key *SKS* issued from the receiver.

VI. A TOSS-A-COIN SELECTIVE ENCRYPTION ALGORITHM

Since the toss-a-coin algorithm is a basic approach, little uncertainty is involved. For all transmitted messages, we divide them to two groups: the odd number messages and the even number messages. For instance, messages *M1, M3, M5*, … *M*(*2n-1*) represent the odd number messages; messages; *M2, M4, M6*, … *M*(*2n*) represent the even number messages. When the sender needs to decide which group should be encrypted, it makes use of a toss-a-coin method to determine whether the even number messages or odd number messages are encrypted. As an example, we consider the following scenario, in which the even number messages are encrypted. After the method of toss-a-coin is applied, the sender makes the decision that only the even number messages *M2*, *M4*, … *M*(*2n*) are encrypted. Thus, half of the whole messages are chosen to be encrypted and this approach shows a basic selective encryption algorithm with a semi-determined encryption pattern. As we described before, the more data are encrypted, the more secure the communication is, but the more overhead is spent. Hence, the value of encryption ratio here is tentatively determined to be 0.5, which means that 50 percents of the communicated data will be encrypted.

VII. PROBABILISTIC SELECTIVE ENCRYPTION ALGORITHM

In this section, we will present the design of a probabilistic selective encryption algorithm step by step. Specifically, our algorithm aims to involve sufficient uncertainty into the encryption process, while providing satisfactory security protection to communicating nodes. In the ad hoc network we discuss, the links between wireless nodes are always bidirectional and every wireless node has enough computational power to finish these operations. Here, a probabilistically selective encryption algorithm, which uses the advantages of the probabilistic methodology, aiming to obtain sufficient uncertainty. During the process of sending messages, the sender will randomly generate a value to indicate the encryption percentage, which represents how many messages will be encrypted among the transmitted messages. Then, the sender uses a probabilistic function to choose the already deterministic amount of messages to encrypt them. We can see that more uncertainty is included to the probabilistic encryption algorithm, in comparison to the toss-a-coin approach, since the encryption ratio is randomly decided and the encryption pattern is not pre-determined. Moreover, this selective algorithm is comprised of the following three phases:

1) The sender of communicating parties *S* will first apply a random generator *RNG* to randomly obtain an encryption ratio *er*, which determines the percentages of encrypted messages among all messages. Here, in order to ensure that enough data are able to be encrypted so as to provide sufficient security protection, the generated encryption ratio should be higher than a pre-determined value of security requirement *SR* (*SR* means that data communication is secure if there is *SR* or more percents of messages are encrypted).

$$S \quad RNG \quad er \;|\{er >=SR\} \longrightarrow \quad (1)$$

2) Then the sender *S* will employ a probabilistic function *PF* to generate an encryption probability *pi* to determine if one message *Mi* will be encrypted or not.

$$S \quad PF(mi) \qquad Pi \qquad \longrightarrow \quad (2)$$

3) Eventually, the sender selects the messages to encrypt based on the above pre-determined encryption ratio *er*. For example, once *S* finds out that the encryption probability *pi* is less than or equal to the encryption ratio *er*, it will encrypt the message *Mi* using its secret key *SK*; otherwise, this message will not be encrypted accordingly

$$\begin{array}{ll} S & \multirow{2}{*}{$\begin{cases} SK[Mi] \xrightarrow{Pi<=er} \\ \\ Mi \xrightarrow{Pi<=er} \end{cases}$} \\ & \\ S & \end{array} \qquad (3)$$

Thus, the probabilistic selective encryption algorithm integrates both the probabilistic method and stochastic strategy, in order to increase the uncertainty in the process of message selection. As we discussed in the theory of selective encryption, the more uncertain the encryption algorithm is, the secure data communication is, based on the assumption that sufficient data is encrypted to provide reliable security.

Performance analysis of the selective encryption scheme is divided into four parts, described as follows:

i. Encryption Time Percentage: The percentages of the total time spent on encryption and decryption of selected messages to the total time encrypted all messages.

ii. Encryption Time: The overall time is spent on message encryption and decryption.

iii. Overall Time: The overall time is spent on the encryption for all message and communication.

iv. Encryption Proportion: The ratio of encrypted messages to the messages that are not encrypted.

VIII. CONCLUSION AND FUTURE WORKS

Theoretical analysis shows that the probabilistic selective encryption algorithm is one of the most promising solutions to reduce the cost of data protection in wireless and mobile networks. The probabilistic techniques the security for data communications between the messages' sender and receiver. The factor of encryption probability involves the uncertainty to data encryption. The first approach will encrypt all messages without any selective encryption, and the second approach is the toss-a-coin approach. For the purpose of simplification, we use "full" to represent the first approach, "toss-a-coin" to represent the second approach, and "probabilistic" to represent probabilistic approach. First of all, we compare the performance and efficiency of these approaches. The comparison of encryption percentages and time based on three approaches. We can learn that both toss-a-coin and probabilistic have an obvious lower encryption time percentage than full encryption, which is caused due to the fact that selective encryption takes effect and the overhead is greatly saved. The time spent on encryption/decryption is compared to show that full encryption takes a longer time than toss-a-coin and probabilistic encryption. This means that data transmission can be speeded up by virtue of toss-a-coin and probabilistic encryption. Hence, selective encryption is more efficient than full encryption and it is able to better utilize the computational resource of a wireless device. We compare the overhead spent on toss-a-coin and probabilistic encryption respectively, based on their encryption efficiency and effects. The probabilistic encryption has a little lower encryption proportion than toss-a-coin encryption but it is more flexible than toss-a-coin encryption. Because probabilistic encryption does not fix the encryption probability, the encryption proportion fluctuates in a relatively larger range. Thus, probabilistic encryption owns more uncertainty than toss-a-coin encryption, which matches with our expectation. Our comparison focuses on their efficiency and the factor of saving time is taken into account. Probabilistic encryption has a higher saving time when compared to toss-a-coin encryption, indicating that it is more efficient and spends less time on encryption/decryption. Therefore, through the comparison of their efficiency, we learn that the selective encryption does help reducing the encryption overhead and improving the efficiency of encryption.

Although an important and rich variety of selective encryption algorithms have been proposed in the literature, we believe that many research areas remain open in this field.

(i) Our future work, we will study the distribution of different packets sizes .

(ii) The algorithm should handle various kinds of data like images, videos, PDF etc We believe it will be fruitful to extend this type of analysis to other algorithms in the hope of motivating widespread application of selective encryption.

REFERENCES

1. N. Ruangchaijatupon and P. Krishnamurthy, \Encryption and power consumption in wireless LANs N," *The Third IEEE Workshop on Wireless LANs*, pp. 148-152, Newton, Massachusetts, Sep. 27-28, 2001.
2. Hardjono, *Security in Wireless LANS and MANS*, Artech House Publishers, 2005.
3. Boukerche, “Handbook of Algorithms for Wireless and Mobile Networks and Computing”, CRC Chapman Hall, 2005.
4. W. S. Elkilani and H. M. Abdul-Kader, \Perfor- mance of encryption techniques for real time video streaming," *IBIMA Conference*, pp. 1846-1850, Jan. 2009.
5. S. Hirani, Energy Consumption of Encryption Schemes in Wireless Devices Thesis, University of Pittsburgh, Apr. 9, 2003,
6. Retrieved October1,2008.(http://portal.acm.org/citation.cfm?id=383768)
7. Nadeem and M. Y. Javed, \A performance com- parison of data encryption algorithms," *Information and Communication* Technologies, ICICT 2005, pp. 84-89, 2005.
8. S. Z. S. Idrus, S. A. Aljunid, and S. M. Asi, \Performance analysis of encryption algorithms text length size on web browsers," IJCSNS International Journal of Computer Science and Network Security, vol. 8 no.1, pp. 20-25, Jan. 2008.
9. Saranya.P and Varalakshmi.L.M “H.264 based Selective Video Encryption for Mobile” International Journal of Computer Applications (0975 – 8887) Volume 17– No.4, March 2011 .

10. Shaik Rasool, Md. Ateeq-ur-Rahman, G.Sridhar and K. Hemanth Kunar "Enhanced fast and secure hybrid encryption algorithm for message communication" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 9, No. 7, July 2011.
11. M. Alattar and G. I. Al-Regib, "Evaluation of selective encryption techniques for secure transmission of MPEG-compressed bit-streams," *IEEE Int. Symp. on Circuits and Systems*, pp. 340–343, 1999.
12. H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Trans. on Signal Processing*, vol. 3, pp. 2439–2451, Aug. 2000.
13. T. Lookabaugh, I. Vedula, and D. C. Sicker, "Selective encryption and MPEG-2," *ACM Multimedia*, 2003.
14. Servetti and J. C. De Martin, "Perception-based partial encryption of compressed speech," *IEEE Trans. on Speech and Audio Processing*, vol. 10, pp. 637–643, 2002.
15. H. Dong, *SNR and bandwidth scalable speech coding*, Ph.D. thesis, Southern Methodist University, Dallas, Texas, December 2002.
16. Sooksan Panichpapiboon , Gianluigi Ferrari, and Ozan K. Tonguz "Optimal Transmit Power in Wireless Sensor Networks"IEEE Transactions on mobile computing ,vol,5,No.pp.1432-1447 10 October
17. White, Gregory,. Cisco Security+ Certification: Exam Guide, McGraw-Hill.,2003.
18. Christian Boesgaard,"A Short Introduction to AES",October 9,2003.http:// www.itu.dk/courses/DSK/E2003/DOCS/aes_introduction. pdf.
19. Boukerche, "Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks", Wiley & Sons, 2008.
20. Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud" Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types " *International Journal of Network Security, Vol.11*, No.2, PP.78{87, Sept. 2010
21. M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan." Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard" International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010 1793-8201.
22. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater Review Article " Overview on Selective Encryption of Image and Video: Challenges and

Perspectives ” EURASIP Journal on Information Security Volume 2008 (2008), Article ID 179290,18 pages doi:10.1155/55/2008/179290

23. Jiang-Lung Liu “Efficient selective encryption for JPEG 2000 images using private initial table” *Department of Electrical* Engineering, Chung Cheng Institute of Technology, National Defense University, Tahsi, Taoyuan 33509, Taiwan 8 February 2006 Pattern Recognition 39 (2006) 1509 – 1517
24. D.Jena, S. K. Panigrahy, and S. K. Jena, “A novel and efficient cryptosystem for long message encryption”, *Proceedings of* Int’l Conference on Industrial and Information Systems, pp. 7–9, 2009.
25. N. M. Thamrin, G. Witjaksono, and A. Nuruddin, *Eds.*, “An Enhanced Hardware-based Hybrid Random Number Generator for Cryptosystem”, Proceedings of International Conference on Information Management and Engineering, pp. 152–156, 2009.
26. R. Küsters, and M. Tuengerthal, “Computational soundness for key exchange protocols with symmetric encryption”,Proceedings of 16th Conf. on Computer and communications security, pp. 91–100, 2009
27. U. Potdar, K. T. Talele, and S. T. Gandhe, “Comparison of MPEG video encryption algorithms”, *Proceedings of Int’l* Conference on Advances in Computing, Communication and Control, pp. 289–294, 2009.
28. Lala Krikor, Sami Baba, Thawar Arif and Zyad Shaaban “Image Encryption Using DCT and Stream Cipher” European Journal of Scientific Research ISSN 1450-216X Vol.32 No.1 (2009), pp.47-57
29. Anoop MS, “Public key Cryptography (Applications Algorithm and Mathematical Explanations)”
30. Marshall D.Abrams, Harold J.podell on Cryptography.