View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 30 (2012) 45 – 52

Procedia Engineering

www.elsevier.com/locate/procedia

International Conference on Communication Technology and System Design 2011

Increasing Robustness of RC4 Family for Automated Selection of Ciphersuites

Arun Kumar Singh[a], Shefalika Ghosh Samaddar[b], Swagat Ranjan Sahoo[c], Glitto Mathew[d], a*

[a,b,c,d] *Department of Computer Science and Engineering*
Motilal Nehru National Institute of Technology,
Allahabad, Uttar Pradesh, 211004 India

Abstract

Information security is dependent on various access control mechanism governed by cryptography or the art of encryption and decryption. Cryptography is the largely built in computer hardware or in software using various discrete structure. Security is, thus, merging in network with cryptography to provide secure communication between trusted and/or untrusted network. Efficient mechanism of encryption process is a primary method of protecting valuable electronic information. The encryption process also needs to be dynamic in order to face new hazards and advance methods used by cryptanalysts. RC4 is one of the most popular and efficient stream ciphers [1]. Stream ciphers are often used in applications where high speed and low delay are a requirement. This paper proposes to identify the security requirements for data stream systems; according to the increasing order of robustness. Various security circumstances demand various degree of security robustness. This paper suggests to develop a family of cryptographic algorithm based on the RC4 and checks on the performance of each one to analyze the robustness so that the particular algorithm becomes readily applicable to a circumstance. The applicability of algorithm is totally governed by the requirement of robustness for the security concern of the circumstance. The security concern of robustness of circumstances is matched against the designed ciphersuites where such family of algorithms is available. The process of selection of ciphersuites and hence the cryptographic algorithm is automated in order to ensure appropriate circumstantial robustness. This analysis shows that, the full-size RC4 remains secure against known attacks [2]. The family of algorithm considered here is based on RC4. The basic RC4 algorithm and its variants suggested by different authors like RC4 KSA [3], RC4-PRGA are included in the family. In order enhance the degree of security robustness, two new algorithm S-RC4$_1$ and S-RC4$_2$ are proposed. Addition of variants of RC4 increases the range of automatic selection ensuring further enhancement in security. RC4 family is analyzed for encryption, decryption and algorithm strength is analyzed. Robustness is determined considering both the factors; speed of encryption/decryption or performance and algorithm strength. It is proposed to evaluate the effect of existing RC4 changing different parameters.

© 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of ICCTSD-2011
Open access under CC BY-NC-ND license.

Keywords: Ciphersuite, RC4, Secure Socket Layer, S-RC4;

* Arun Kumar Singh. Tel.: +91- 9455689918.
E-mail address: singh_arun7@yahoo.com.

1877-7058 © 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2012.01.832

1. Introduction

While shopping online or logging into web banking account or even checking emails, it is preferred to use a secure connection to communicate passwords and other vital information [4]. Sensitive information should remain secured and such security should be transparent and ubiquitous whenever sensitive information is shared. Cryptography plays a major role in helping to prevent eavesdropping of personal information. One of the most widespread protocols used for secure communication on the Internet is the Transport Layer Security (TLS) protocol, previously known as the Secure Socket Layer (SSL) protocol. In most cases, the https protocol is used for secure communication which is indicated at the URL. Typical lock symbol represents secure browsing. Https is, in fact, an implementation of the TLS protocol for secure communication on the Internet [5]. It is interesting and relevant to explore this layered security provisions in more detail because it greatly enhances secured business application.

1.1. Research Objectives

The objective of this study is to obtain a network security solution through automated selection of ciphersuites using cryptography. This has been achieved by evaluating the existing protocols comparing with the proposed ones in real-time at wire speeds, and its proposed flexibility to be deployed at any point in the network. The development of theoretically-sound, practical and scalable security-based packet analysis of designed cipher, including security-induced packet marking at wire-speeds at different points of deployments; studying the impact of attack mitigation techniques on network throughput and development of new attack mitigation technique using the proposed cipher is one of the objectives. This part of the study is out of the scope of the paper. Studying the impact of proposed solution on other protocols, for their efficiency, robustness and optimization is the part of this complete study of designed ciphers for automated selection and is not taken up in this paper. Implementation of both patching and clean-slate [6] versions of the proposed solution of designed ciphersuites is another ambitious study project to be conducted on the basis of experimental observation of the proposed ciphers. This paper only concentrates for building up a family of ciphers with different degree of robustness and setting a comparison between the different algorithm of the same family, namely, RC4.

1.2. Proposed Research Methodology

The proposed algorithms are based on the all previous improvement with respect to the RC4 algorithm. Major challenges of secured, reliable and flexible encryption would be evaluated. RC4 is an announced stream cipher. RC4 is used in SSL at transport layer security, S/MIME, WEP and others. The experiments would be designed on RC4 by taking care of various optimization techniques that are application specific, preparing a database of cipher and automated selection of cipher. Performance analysis occupies a major part of such evaluations methods. The proposed algorithms are based on RC4, called S-RC4, which contain two Substitution boxes S1 and S2. The algorithms like FJ-RC4, RC4A, RC4*, RC4+ are studied in depth for their proper utilization in designed cipher. Variants of RC4, S-RC4 is slow as compared to original RC4. But it ensures robustness and takes care of all the important security issues like confidentiality, integrity, and authentication. FJ-RC4 is compared to S-RC4 to prove the point of robustness.

S-RC4 is even considered for its variants. One variant is shown by varying the initialization vector over a predefined algorithm. Variation of initialization vector in introduced first time in this algorithm. Not only an algorithm of ciphers is chosen even the initialization vector used inside the algorithm is also selected either manually or automatically. Going for a lower level of automated selection of parameter definitely increase security robustness.

The rest of the paper is organized as follows, section II presents an extensive prior art in RC4 by considering its strength, weakness, enhancement in the variants of RC4 etc. Section III presents the proposed algorithm S-RC4 and its variants. This section also contains the variant algorithm of RC4 by different authors to showcase the strength of S-RC4. Section IV presents the experimental observation for this family of algorithm and a performance analysis is conducted. Section V enumerates contribution to the discipline made through this study and the resulting motivation. This section also presents the limitation of the present study in the light of the complete research work on automated selection of ciphersuites at this point of time.

2. Background

SSL (Secure Socket Layer) is one of the security protocols to achieve secure communications over a TCP/IP network. SSL has two types of authentication modes, Server Authentication mode and Client Authentication mode. The SSL security protocol provides data encryption, server authentication, message integrity check, and optional client authentication for a transmission control protocol (TCP)/IP connection [6].

The communication using HTTPS is triggered when a client send a request to the server by specifying an URL on HTTPS protocol using port number 443. The web server, providing a service for HTTPS, responds the client by sending the certificate to the client side. The web browser signifies a public key of the web server, packed in the certificate. The key is used to encode the information that the client sends consecutively to the web server. Technically, the initial information that the client sends to the web server is a session key, which would be utilized for further data transmission between the client and the web server. Consequently, web server uses its private key to decode the information (session key) transmitted by the client. As a consequence, only either the web server or the client understands the session key and that the further transmission remains secured [7]. RC4 has a secret internal state [8] which is a permutation of all the N = 2n possible n bits words, along with two indices in it. In practical applications n = 8, and thus RC4 has a huge state of log2(28! x (28)2) = 1700 bits of solution space.

If the internal state of a cipher from the RC4 family is uniformly distributed, such ciphers are not very secure. When the internal state is non-uniformly distributed then the real bias would more likely be larger rather than smaller, and the complexity of the attack would be lower, The effect may be observed on the example of RC4A-n. The security level of such constructions depends more on the degree of the recursive relations between output symbols and internal states, rather than on the length of the permuter(s). One of the solutions to protect against of such distinguishing attacks is to increase the number of accesses to the permuter(s) in the loop. This solution will increase the relational complexity between adjacent outputs. Another solution is to discard some output symbols before accepting one. Unfortunately, both the suggestions significantly decrease the speed of these ciphers making it a non-obvious choice [2].

The first weakness in RC4 is the existence of large classes of weak keys, in which a small part of the secret key determines a large number of bits of the initial permutation (KSA output). In addition, the Pseudo Random Generation Algorithm (PRGA) translates these patterns in the initial permutation into patterns in the prefix of the output stream. The second weakness is a related key vulnerability, which applies when part of the key presented to the KSA is exposed to the attacker. It consists of the observation that when the same secret part of the key is used with numerous different exposed values, an attacker can receive the secret part by analyzing the initial word of the key streams with relatively less effort.

RC4 Key Scheduling Algorithm (KSA) [9] is theoretically studied to reveal non-uniformity in the expected number of times for each value of the permutation touched by the indices i, j. Based on results available in literature regarding the existing weaknesses of RC4, few additional layers over the RC4 KSA and RC4 Pseudo-Random Generation Algorithm (PRGA) are proposed. Analysis of the modified cipher (RC4+) shows that this new strategy avoids existing weaknesses of RC4 [8]. Running time of the KSA+ is around three times that of RC4 KSA, there are three similar scrambling layers instead of one, each having N iterations Key scheduling and is run only once. The performance of the cipher is not much affected. A new algorithm RC4A [10], based on RC4's exchange shuttle model, offers increased resistance against most attacks that apply to RC4. RC4A uses fewer operations per output byte and offers the prospect of implementations that can exploit its inherent parallelism to improve its performance further. However, RC4A is designed in order to solve the weakness of the distribution of the first two output bytes of RC4. FJRC4 [11], that turned out to resemble RC4 to a great extent, has several important differences on Key scheduling, FJ-RC4 is built from a KSA, which uses the key stream in three stage processes and shares PRGA structures with RC4. One major difference between PRGA and FJ-RC4 is, in all stages of encryption, FJ-RC4 is involved in three stage encryption. The key mechanism in FJ-RC4 dictates that key needs to be initialized. The proposed mechanism of ciphersuites based on various modification of RC4 in order to improve upon robustness, is designed to prevent attacks through key scheduling. In FJ-RC4, the main key is divided also into three equal portions to make three different sub-keys. If the length of main key is not divisible by three, zero padding is used to make it divisible by three. Finding a key in the proposed FJ-RC4 algorithm takes more time than RC4. The key

schedule in FJ-RC4 by contrast is slower than RC4. This is attributed to three stages of sub-key process. The papers authored by Prasithsangaree and Krishnamurthy provides results of experiments with AES and RC4, two symmetric key algorithms. The results show that RC4 is more suitable for large packets when compared to AES for small packets.

The energy cost of the SSL record [4] stage is mainly determined by the amount of data that is transmitted securely. Analysis of the cipher suites shows that careful choices of cryptographic algorithms need to be made, in order to optimize energy during the record stage. The energy analyses of the SSL protocol and cryptographic algorithms allow to explore various options for optimizing the energy consumption of the SSL protocol. Usually, applications which require a high degree of security need client authentication. In case of applications, where security requirements are not stringent, further energy savings can be obtained by switching to smaller keys. Energy savings can also be obtained in the SSL record protocol, by choosing a symmetric algorithm depending on the size of the data to be transacted, such that the overall energy consumption is reduced. The energy costs of the handshake and record stages of the SSL protocol vary depending on parameters like functionality desired in the handshake, size of bulk data transacted, etc. These conditions reveal the opportunity for making the execution of security protocols dynamic in nature. The protocol execution can be altered depending on the input conditions, such that security of transactions is provided with optimal energy consumption. These optimization are suitably adopted in the proposed design of ciphers and consequently later in the ciphersuites.

RC4 remains a secure cipher for practical applications [2]. Several theoretical attacks exist but none have been successful against commonly used key lengths in a real world application Nonetheless, tracking analysis substantially reduce the complexity of cryptanalysis compared to the maximum key length which could be user specified. Tracking analysis would show promise if it was possible to use knowledge of the actual key length to limit the state space to be searched for optimized solutions. RC4's resilience is mainly due to the fact that the key schedule effectively prevents partial knowledge of the S-box state from providing information about the key. This contributes to the robustness of the security system.

The existence of differential characteristics and differentials in the stream cipher has several implications with respect to the security of stream ciphers [13]. Thus, stream cipher designers may consider these issues when designing new stream ciphers. Stream ciphers with high probability differentials are susceptible to many attacks: distinguishing and key recovery in the related-key/IV model, faster exhaustive key searches, and fault analysis. Stream ciphers that also offer authenticated encryption are also susceptible to repeated nonce attacks, as well as forging of the tags in case there exist good differentials. Even characteristics that deal with the evolution of internal state differences (without considering their affect on the output) can be used for analysis. These characteristics are especially useful for exhaustive key search or time-memory tradeoff attack which aim the internal state of the cipher rather its key space. Thus, we conclude that differential cryptanalysis is a versatile and important tool in the crypt analyzer toolbox, for testing and optimization.

RC4 and related six attacks: the Branch and Bound attack [14], the Second Word Bias, Predictive States, the Derailing Related Keys attack, the Special Exact Keys and the Initialization Vector Weakness are described. Overall, RC4 is still considered secure in case a hash function is used to form session keys from secret keys and Initialization Vectors. It is designed to discard the first 2n words of output before using where the value of n that remain unknown to the attacker. The performance of the RC4 [15] based on the processing time under certain conditions is analyzed. However, this may vary according to the processor and the software used to implement the system. Hence, a comparison with another encryption algorithm may be used. Analysis of the RC4 parameters has shown that the speed of encryption or decryption time is directly related to the encryption key length and to the data file size if the data is large enough. Data type is also important since image data requires larger time to be processed than text or sound data mainly due to the larger file size. This relationship had been converted into formal equations to model these relationships and may be used to predict the performance of the RC4 under different conditions. VMPC [2] is a generalization of the stream cipher RC4, whereas RC4A is an attempt to increase the security of RC4 by introducing an additional permuter in the design.

Analyzing the RC4 parameters have shown that the speed of encryption or decryption time is directly related to the encryption key length and to the data file size if the data is large enough. Data type is also important since image

data requires [17] larger time to be processed than text or sound data mainly due to the larger file size [1]. This relationship had been converted into equations to model these relationships and so may be used to predict the performance of the RC4 under different conditions.

3. Proposed Algorithms of RC4 family

This section presents the formulation of family of algorithms of RC4; some are prior art; some are enhancement and two are prepared by the authors of this paper. The proposed algorithm, Secured RC4 or S-RC4 is presented preferred here having two variants; one with fixed initialization vector (IV) and the other with variables initialization vector. The collected algorithm are presented in figure 1to figure 5 before presenting proposed S-RC4.

The outline of the proposed methodology of S-RC4 is presented here depicting the method of encryption and decryption separately.

3.1. Method of Encryption of S-RC4

Algorithm:

Step 1: Detect the upcoming slot in terms of the block size, and then divide each block size in way of slots (the member is dependent on the size of the slot).

Step 2: Each slot may be subjected to independent algorithm; size of the input slot is always less than the block, makes the block partitioned for a number of slots. In case the block is not properly divided by a number, say n, of slots (given in algorithm) then blank characters or zero will be padded in the last slot to get an integer value of slots.

Step 3: Convert each block into equivalent bit streams and corresponding to algorithm's chosen initialization vector (IV). The length of the stream may vary depending on the size, so IV may remain flexible.

Step 4: Each block computation for cipher is executed by the key which may vary with each slot as well as the substitution box. The stream resulted is a combination of permutation and substitution applied in the fixed or flexible mode.

Step 5: Cipher of the complete block has been computed by the designated key as well as substitution boxes (S1 and S2), Key may vary for each slot and also substitution box is unique for different size of the slot as per block to which it belong to.

Step 6: Repeat steps 2 to 4 until all characters of plain text, after exhausting the plaintext stream, are converted into cipher text.

3.2. Method of Decryption

Step 1: Group the cipher text into blocks of n digits of the slots of a block.

Step 2: Convert each formulated block into equivalent bit streams, permutation computation will go on as per substitution box as designed and used in the method of encryption.

Step 3: Decrypted block has been computed by computing the position of key as per algorithm containing the design of substitution boxes S1 and S2, slot numbers, formed blocks and resulting stream.

More specifically, the methodology in the proposed algorithm allows the packets to be encrypted in accordance to sensitivity in applications. The proposed network-embedded security solution will include:

(a) Comparative evaluation of existing security protocols and predetermines the application specificity.
(b) Development of an real-time efficient and optimization protocols [If needed] for designed cipher.
(c) Security-induced in-network packet and handling methods.
(d) Impact on Existing encryption and security mechanism on robustness vis-à-vis other security issues.
(e) Patching and clean-slate implementations of the proposed solutions to various applications. The algorithms with thematic and theoretic detail are presented here one with IV fixed and the other with IV varying. It may be noted that IV selection can be automated as per design of the secured algorithm of S-RC4.

Present S-RC4 (IV fixed) and S-RC4 (IV Varying) in the box captioned figure 6: Proposed S-RC4 (IV fixed) of RC4 family: Proposed (IV varying) of RC4 family.

4. Experimental Observation and Performance Analysis

4.1. Performance Analysis

Performance analysis is conducted on the basis of the experimental observations, as collected in the previous subsection 4.1. The observations are presented graphically during certain conclusions visually and analytically in figure 1.

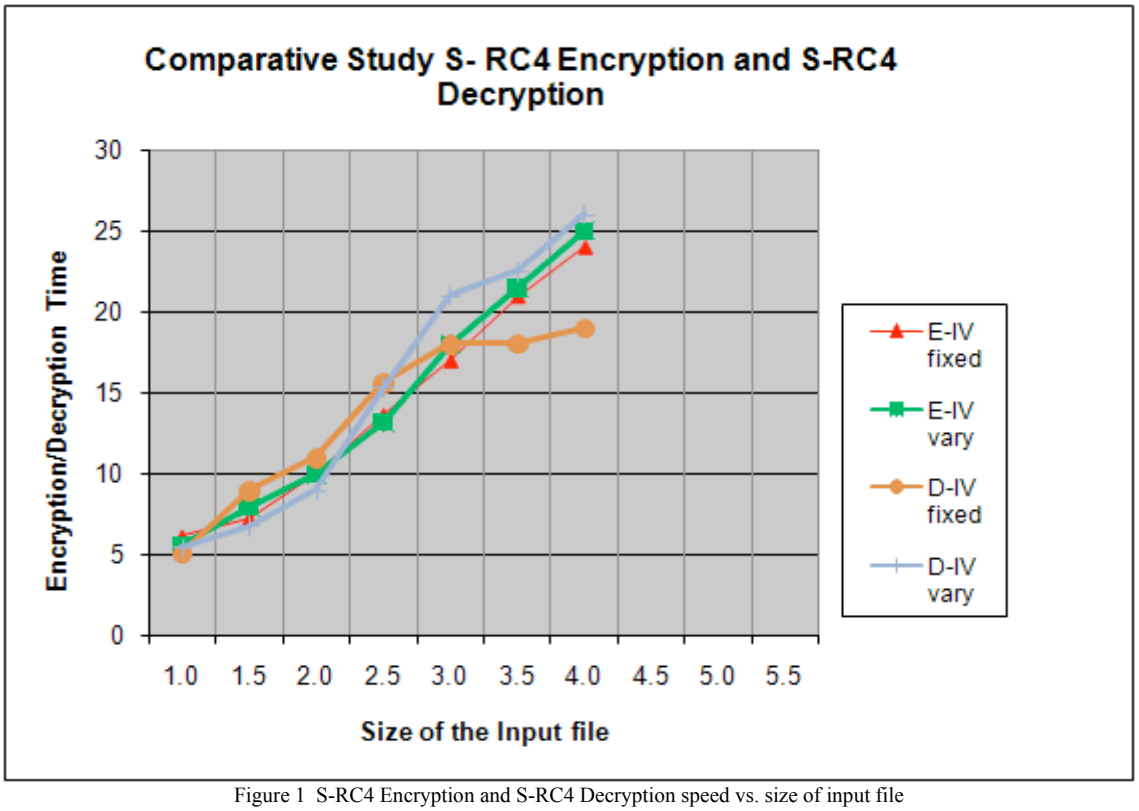

Figure 1 S-RC4 Encryption and S-RC4 Decryption speed vs. size of input file

Based on these observations following conclusion may be drawn prime facie:

- Encryption speed vs. the size of the dataset is similar in pattern to decryption speed vs. the size of the dataset though the scale may be different.

- For certain file size, the behaviors of S-RC4 may be considered different from rest of the family of algorithm.

5. Contribution to the discipline

A major contribution of this research undertaken will be the development of abstract framework that can facilitate development and deployment of security protocols in real time packet traffic at client side as well as in communication. Furthermore, several case studies will be studied to determine appropriate robustness of designed ciphersuite for the purpose of application specific automated selection. Deployment of ciphersuites will be considered to justify the proposed security framework. These frameworks will pick up security protocols, efficient in various test simulation for the network packet. Unlike the existing security studies that are based purely on various modification of encryption/decryption algorithm for addressing security and network related issues, this effort will pave the way towards generalization of cipher techniques resulting in security framework applicable in any situation. The proposed low-complexity implementations of the protocols, services and applications that are required by the framework will enhance the security robustness of application. Evaluation of the advantages and limitations of these existing and designed protocols will deliver results for elimination of the weakness. A secure framework provides better application specific security and efficient complexity rates are also considered for determination of circumstantial robustness that is required for ready on-the-fly application of automated selection of ciphers and hence of a ciphersuites. All implementations, experimental results and collected data will be shared with scientific and research communities on global basis for further growth and enhancement of information security research.

5.1. Limitation

The cipher suite rollback attack is an attack that simulates an interception of 'Hello' message to modify the list of cipher suite from a client and substitute it for an algorithm that the attacker wants. It happens because the Hello message between a client and a server is transmitted in a plaintext. This attack can be protected by including a hash value for all the messages during the Handshake protocol in the 'Finished' messages and verifying the messages and the hash value. Version 3.0 of SSL was designed to correct the flaw of the cipher suite rollback attack. Figure 6 shows the cipher suite rollback attack thematically. In Key exchange algorithm rollback attack, an attacker intercepts 'hello' message in a plaintext and replaces an algorithm of cipher suite that a client transmitted with a randomly selected key exchange algorithm of his own. In addition, he intercepts a message from a server to the client with the same method, and also replaces the algorithm with a randomly selected key exchange algorithm of his own. To prevent this kind of attack, it should inhibit the attacker from replacing the algorithm by transmitting digitally signed parameters of key exchange [3].

5.2. Resulting Motivation of the Concept Presented

Computer networks and cryptography have been the research interest of community continuously striving for enhancement of security. It has been a low complexity, low-delay higher throughput, higher speed environment to achieve against all security odds. The present study undertaken in this paper is a fillip to go further in that direction. However, the optimum combination formulation of ciphers, hashes and other security mechanism is yet to be determined and the methodology is still elusive. Fellow researchers may consider it for future direction of work. This study motivates to walk in the direction of optimal point in security space.

References

[1] Subhamoy Maitra and Goutam Paul, "Analysis of RC4 and Proposal of Additional Layers for Better Security Margin", INDOCRYPT 2008, LNCS 5365, pp. 27–39, 2008. Springer-Verlag Berlin Heidelberg 2008.

[2] S. Mister , S. E. Tavares,S. Tavares and H. Meijer (Eds.), SAC'98, LNCS 1556, pp. 131{143, 1999. Springer-Verlag Berlin Heidelberg 1999, Cryptanalysis of RC4-like Ciphers.

[3] Prasithsangaree, P.; Krishnamurthy, P., "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs", *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE.*

[4] Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan‡ and Niraj K. Jha†Analyzing the Energy Consumption of Security Protocols, ACM.

[5] Yunyoung Lee, Soonhaeng Hur, Dongho Won, and Seungjoo Kim* Information Security Group, Department of Electrical and Computer Engineering Sungkyunkwan University Suwon 440-746, South Korea {yylee, shhur, dhwon, skim}@security.re.kr, Cipher Suite Setting Problem of SSL Protocol and It's Solutions, 2009 International Conference on Advanced Information Networking and Applications Workshops IEEE]

[6] Takamichi SAITO Ryosuke HATSUGAI Toshiyuki KIT0, Meiji University, JAPAN, Toshiba Corporation, JAPAN.

[7] Thawatchai Chomsiri Faculty of Informatics, Mahasarakham University, Mahasarakham 44150, Thailand. thawatchai@msu.ac.th, HTTPS Hacking Protection.

[8] Scott Fluhrer, Itsik Mantin, and Adi Shamir 2002, Weaknesses in the Key Scheduling Algorithm of RC4, Springer-Verlag London, UK 2001.

[9] Subhamoy Maitra1 and Goutam Paul Analysis of RC4 and Proposal of Additional Layers for Better Security Margin, IEEE 2008.

[10] Jian Xie, Xiaozhong Pan, 2010, An Improved RC4 Stream Cipher International Conference on Computer Application and System Modeling (ICCASM 2010), RC4A.

[11] Fahime Javdan Kherad Mohammad V. Malakooti, A New Symmetric Cryptography Algorithm to Secure E-Commerce Transactions, 2010 International Conference on Financial Theory and Engineering

[12] Paul D. Kundarewich and Steven J.E. Wilton, , Alan J. Hu , A CPLD-based RC-4 Cracking System , IEEE

[13] Eli Biham Orr, Dunkelman, National, Differential Cryptanalysis in Stream Ciphers,

[14] Rick Wash, Lecture Notes on Stream Ciphers and RC4

[15] Allam Mousa and Ahmad Hamad , Evaluation of the RC4 Algorithm for Data Encryption, IJ CA, June 2006 Volu3 ,No 2

[16] Alexander Maximov, Two Linear Distinguishing Attacks on VMPC and RC4A and Weakness of RC4 Family of Stream Ciphers,

[17] Allam Mousa and Ahmad Hamad, Evaluation of the RC4 Algorithm for Data Encryption June 2006

[18] Abd-ElGhafar, A. Rohiem, A. Diaa, F. Mohammed, 13th International Conference on Aerospace Sciences & Aviation Technology, Generation of AES Key Dependent S-Boxes using RC4 Algorithm

[19] Arun Kumar Singh, Lokendra Kumar Tiwari, Shefalika Ghosh Samaddar and C.K Dwivedi, Security Policy & Its Scope in Research Area, accepted in International Conference on Strategy and Organization, ICSO 2010 on 14 & 15 May-2010, Institute of Management Technology, Ghaziabad, Uttar Pradesh, India.

[20] Lokendra Kumar Tiwari, Arun Kumar Singh, Shefalika Ghosh Samaddar and C.K Dwivedi , Recovery Evidentiary files using Encase Ver 6.0, accepted and presented in National conference & Workshop on High Performance & Applications, 08-10 February, Banaras Hindu University, Varanasi, Utter Pradesh, India, pp-8.

[21] Lokendra Kumar Tiwari, Arun Kumar Singh, Shefalika Ghosh Samaddar and C.K Dwivedi , Evidentiary Usage of E-mail Forensics: Real Life Design of a Case, First International Conference on Intelligent Interactive Technologies and Multimedia (IITM-2010) on Dec 28-30, 2010, Indian Institute of Information Technology Allahabad, Uttar Pradesh, India.

[22] Arun Kumar Singh, Pooja Tewari, Shefalika Ghosh Samaddar and A.K.Misra , Communication Based Vulnerabilities and Script based Solvabilities, International Conference on Communication, Computing & Security (Proceedings by ACM with ISBN-978-1-4503-0464-1) on 12-14 Feb-2011, National Institute of Technology Rourkela Orissa, India.

[23] Arun Kumar Singh, Pooja Tewari and Shefalika Ghosh Samaddar, A. K. Misra , Vulnerabilities of Electronics Communication: solution mechanism through script, International Journal of Computer Science Issues (IJCSI), Volume 8, Issue 3, 2011.

[24] Arun Kumar Singh, Lokendra Tiwari , Vulnerability Assessment and penetration Testing, National Conference on Information & Communication Technology (NCICT–2011), ISBN: 978-93-80697-77-2, 5th–6th March, 2011, Centre for Computer Sciences Ewing Christian College Allahabad–211003 Utter Pradesh, India.

[25] Lokendra Kumar Tiwari, Arun Kumar Singh, Shefalika Ghosh Samaddar and C.K Dwivedi, An Examination into computer forensic tools, accepted and to be presented in 1st International Conference on Management of Technologies and Information Security (ICIMS 2010) on 21-24 of January 2010, Indian Institute of Information Technology Allahabad, Uttar Pradesh, India. (http:// icmis.iiita.ac.in/TOOL_FORENSIC.ppt), page-75.