Asian Journal of Information Technology 5 (4) : 358-361, 2006

Stream Ciphers for Message Confidentiality

[1]M. Ismail Jabiullah and [2]M Lutfar Rahman
[1]Department of Computer Science and Engineering University of Dhaka,
Institute of Science and Technology, Affiliated to National University of Bangladesh
[2]Department of Computer Science and Engineering, University of Dhaka, Bangladesh

Abstract: Computer communication needs to protect data during their transmission for secure transactions. Secure electronic transactions are essential step on the road to electronic commerce and are thus in high demand. Modern cryptography uses the basic ideas as traditional cryptography, transpositions and substitution, but its emphasis is different. The technique of traditional cryptography deals with simple algorithms and relied on very long keys. With conventional encryption, two parties share a single encryption and decryption key. The principal challenge with conventional encryption is the distribution and protection of keys. The advantage of stream ciphers over block ciphers is that it can easily implemented in hardware with relatively few components and is much faster. The fact that bits are encrypted individually means that, individual bit errors in a ciphertext do not propagate and the only corresponding plaintext bits are destroyed. Here, four stream cipher algorithms: Onetime pad, RC4, SEAL and A5 are implemented in C programming language. Compared these algorithms with each other and then the integrated software combining all of stream ciphers. The principal challenge of conventional encryption is the distribution and the protection of the keys. Integrated software has been developed combining all the four algorithms of stream ciphers. One of these stream cipher algorithms can be selected for security and message transactions with confidentiality.

Key words: Encryption, decryption, stream cipher, cryptography and cryptanalyst

INTRODUCTION

Secret writing was probably the first widely used method for secure communication via insecure channel. The secret text, known as ciphertext, was visible to an unsuspicious reader. The method of secure communication was rather weak if the document found its way to an attacker who was an expert in secret writing. The advent of computers gave both the designer and the cryptanalysts a new powerful tool for fast computation[1]. New cryptographic algorithms were designed and new attacks were developed to break them. New impetus of cryptology was not by new designing tools but rather by new emerging applications of computer and new requirements for protection of information. Distributed computations and sharing information in computer network are among those new applications, sometime very dramatically, the necessity of providing tools for reliable and secure information delivery. Now-a-days message confidentiality is an important security issue and so stream ciphers are in high demand. Stream ciphers are an important class of encryption algorithms[2]. Here, individual characters of plaintext message are encrypted one at a time, using an encryption transformation, which varies with time. Stream ciphers are generally faster than block ciphers in hardware and have fewer complexes in hardware circuitry. They are also more appropriate and in some cases mandatory, when buffering is limited or when character must be individually processed as they are received. Because they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable. Confidentiality is the protection of transmission data from passive attacks[3]. With respect to the release of message contents several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. Another aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequently, length or other characteristics of the traffic on

Corresponding Author: M. Ismail Jabiullah, Department of Computer Science and Engineering, Institute of Science and Technology, National University of Bangladesh

a communications facility. An approach is proposed which can encrypt a message into a stream ciphertext in confidential form where an intruder cannot decode the original message from the encode one[4].

STREAM CIPHER TECHNIQUES

Selected stream cipher generation techniques one-time pad, RC4, SEAL and A5 are discussed in the following subsections.

One time pad: A one-time pad, sometimes called Vernam Cipher, uses a string of bits that is generated completely at random. The key stream is the same length as the plaintext message and the random string is combined using bit wise XOR with the plaintext to produce the ciphertext. Since the entire key stream is random, an opponent with infinite computational resources can only guess the plaintext if she/he sees the ciphertext. Such a cipher is said to offer perfect secrecy and the analysis of the one-time pad is seen as one of the cornerstone of the modern cryptography. As with all symmetric ciphers, the sender must transmit the key to the recipient via some secure and tamperproof channel, otherwise the recipient won't be able to decrypt the ciphertext[1].

RC4: RC4 is the stream cipher designed by Ron Rivest in 1987. This cipher is extremely fast and exceptionally simple, which makes it ideal for protecting network traffic. In RC4, the keystream is independent of the plaintext. The internal state consists of a permutation on numbers from 0 to 255 represented as an array of length 256 and two indices in this array. The size of the key K is available and typically rages from 40 to 256 bits. The RC4 cipher initializes the permutation S with the identity permutation.

Software-optimized Encryption Algorithm (SEAL): SEAL is a software efficient stream cipher designed at IBM by Phil Rogaway and Don Coppersmith. This is a binary additive stream cipher that was proposed in 1993. Since it is relatively new, it has not yet received much scrutiny from the cryptographic community. It was optimized for 32-bit processors. To run it well it needs eight 32-bit registers and caches of few kilobytes. Using a relatively slow operation, SEAL preprocesses the key operation into a set of Tables that are used to speed up encryption and decryption.

A5: A5 is the stream cipher used to encrypt Group Special Mobile (GSM), which is the non-American standard for digital cellular mobile telephone. It is used to encrypt the link from the telephone to the base station. The rest of the link is unencrypted the telephone company can easily snoop on your company. A GSM conversation is sent as a sequence of frames every 4.6 milliseconds. Each frame contains 114 bits representing the digitized A to B communication and 114 bits representing the digitized B to A communication. Each conversion can be encrypted by a new session-key K[5]. For each frame, K is mixed with a publicly known frame counter F_n and the result serves as the initial state of the generator, which produces 228 pseudorandom bits. These bits are XORed by the two parties with the 114+114 bits of the plaintext to produce the 114+114 bits of the ciphertext.

ENCRYPTION/DECRYPTION ALGORITHMS

The encryption processes of the selected stream ciphers are mentioned in the following subsections.

One time pad: One-time pad is a stream cipher defined on the alphabet A = {0,1}. A binary message m = $\{m_1, m_2, .. ., m_t\}$ is operated on by binary keystream k = $\{k_1, k_2,..., k_t\}$ of the same length to produce the ciphertext c = $\{c_1, c_2,..., c_t\}$[6].

Encryption algorithm

Step 1: m = $\{m_1, m_2, ..., m_t\}$
Step 2: Generate k = $\{k_1, k_2, ..., k_t\}$ of random bits as of the length of m.
Step 3: Produce the ciphertext c_i = m_i XOR k_i.

Decryption algorithm

Step 1: Received c = $\{c_1, c_2, ..., c_t\}$
Step 2: Received k = $\{k_1, k_2, ..., k_t\}$
Step 3: Produce plaintext m_i = c_i XOR k_i.

RC4: RC4 stream cipher encryption/decryption algorithms are performed by the following procedures KeySched and PseudoRand.

Procedure key sched

```
for i: = 0 to n-1 do S[i]: = i
j: = 0
for I: = 0 to n-1 do
j: = j+S[i]+k[i mod l]
Swap (S[i],S[j])
i,j: = 0
```

Procedure pseudo rand

```
i: = i+1
j: = j+S[i]
Swap(S[i],S[j])
Output z: = S[S[i]+S[j]]
```

Encryption algorithm

```
State0: = KeySched(K)
For i: = 1 to L do
(Statei, Zi): = PseudoRand(Statei-1)
ci: = Zi XOR Mi
```

There is no decryption function to produce plaintext from the ciphertext. The program for encryption process will work for the decryption process. That is, if the ciphertext is the input of the program with the same key used in encryption, the plaintext will be produced.

SEAL: In SEAL, the first generator uses a routine depending on the k-derived Tables R and T. It maps the 32-bit string n and 6-bit counter l to four 32-bit words A°, B°, C°, D° and another four 32-bit words n_1, n_2, n_3, n_4. These eight words are to be used by the second generator. The second generator uses a routine depending on the K-derived Tables. There are 64 iteration of these routine, indexed by i= 1 to 64. A°, B°, C°, D0°and serves as an input to the first iteration, producing an A_1, B_1, C_1, D_1 blocks[7].

Encryption algorithm: Here R, S and T are the pseudorandom Tables. The encryption algorithm is consists of the following four steps:

Step 1: Compute internal Tables under Secret Key K

Step 2: Compute first generator: A°, B°, C°, D°, n_1, n_2, n_3, n_4 from n,l and Table R

Step 3: Compute second generator: A^i, B^i, C^i, D^i; block from which the values are derived.

$$Y_1^i = A^i \text{ XOR } S_1^i \quad Y_2^i = B^i \text{ XOR } S_2^i$$
$$Y_3^i = C^i \text{ XOR } S_3^i \quad Y_4^i = D^i \text{ XOR } S_4^i$$

A5: A5 stream cipher is composed of three small linear feedback shift registers R1, R2 and R3 that have 19, 22 and 23 bits, respectively and a 22-bit frame counter Fn. Each shift register is shifted right to left, using clock cycles that are determined by a majority system. The majority system is determined using three bits C1, C2 and C3 where C1 is the 8the bit of R1, C2 is the 9th bit of R2 and C3 is the 10th bit of R3 and the bit are numbered from right to left starting at 0. Between the bits C1, C2, C3 if two or more of them are 0 then the majority m = 0, similarly if two or more of them are 1 then the majority m = 1. If C1 = m then R1 is shifted, if C2 = m then R2 is shifted and if C3 = m then R3 is shifted.

Encryption process

Step 1: All the registers are zeroed out. Then bit by bit starting from the least significant bit of Kc, each of the 64 bits is fed into the three registers in parallel, ignoring the majority system. During each cycle the bit from Kc is fed in by doing an XOR with bit 0 of each register.

Step 2: The 22 bits of the frame counter Fn are fed in using the same process Kc was fed in step 1.

Step 3: 100 additional cycles are performed using the majority system, but without any output.

Step 4: Another 228 cycles are performed to get the 228 pseudorandom bits.

COMPLEXITY ANALYSIS

The complexities of the mentioned stream cipher generation techniques have been discussed below.

One time pad: A key of same length of the plaintext is needed to encrypt and produces the same length ciphertext. If an intruder did an exhaustive search of possible keys, it would be ended up with many legible plaintext, with no way of knowing which was the intended plaintext. The security of one-time pad is entirely unbreakable due to the randomness of the key. If stream of characters that constitutes the key is truly random, then the stream of characters that constitutes ciphertext is truly random. Thus there is no pattern of regularities that a cryptanalyst can use to attack the ciphertext[8].

RC4: Number of initial state permutations: $(v2^n)!$, Complexity is $O(v2^n!)$, for n = 5, complexity of state Table is too high for computing power available. failure rate may be below 50%.

SEAL: SEAL requires about five elementary machine operations to encrypt each byte of text. It runs at 58 megabits per second on a 50 MHz 486 machine. On the other hand SEAL must preprocess its key into internal Tables. These Tables total roughly 3 KB in size and their calculation takes about 200 SHA computations.

A5: The A5 algorithm was designed to be efficient in hardware and its straightforward software implementation

	Calculated		Experimental			
		Compl		Compl	Total	
N	K	exity	K	exity	Com.	$v2^n!$
3	0	2^8	0	2^8	2^8	2^8
4	0	2^{21}	0	2^{20}	2^{20}	2^{22}
5	0	2^{58}	7	2^{21}	2^{55}	2^{58}
6	0	2^{132}	20	2^{23}	2^{138}	2^{148}
7	0	2^{324}	45	2^{26}	2^{302}	2^{538}
8	0	2^{779}	100	2^{30}	2^{797}	2^{842}

n	k = 1	k = 2	k = 3	k = 4	k = 5	$v2^n!$
4	2^{21}	$2^{20.5}$	$2^{19.9}$	$2^{19.4}$	$2^{18.9}$	2^{22}
5	2^{53}	2^{51}	$2^{50.5}$	2^{49}	2^{48}	2^{58}

is quite slow. To execute the preprocessing stage, one has to run it on a distributed network of PC's up to 248 times and thus one need an extremely efficient way to compute the effect of one clock cycle on the three registers[9].

CONCLUSION

Conventional stream ciphers are the most important factors in the use of cryptographic systems for the use of secure network communications. As a fundamental, the versatility of the selected stream ciphers allows constructions of Pseudorandom Number Generators (PNG), block ciphers, MACs and hash functions. They serve as a central component in message authentication techniques, data integrity mechanisms and entity authentication protocols and symmetric-key digital signature schemes. No encryption technique is suitable for all purposes. With the increased demand of speed and advance technology of computers, brute force attacks are becoming stronger. The techniques once considered unbreakable become worthless today. New techniques are being invented to protect messages from the brute force attacks. Popular encryption techniques are modified. So, no technique can be considered as classic, it will change with the need of security. In the current practical survey, all the stream cipher methods of message transmission along with necessary fields have been studied. The available security for the message transmission is reviewed. Selected four stream cipher algorithms: onetime pad, RC4, SEAL and A5 have been studied and implemented using the programming language C. Their performances have been reviewed and analyzed and are shown in tabular forms. It can help the user to select the proper stream cipher generation techniques in the perfect use of secure electronic communications and secure electronic transactions online or offline. The performances of these encryption techniques is also helpful for interested persons to understand the development of stream cipher's encryption techniques with the development of computer systems.

REFERENCES

1. Andrew, S. and Tanenbaum, 1999. Computer Networks, 3rd Edn., Prentice-Hall of India Pvt. Ltd., New Delhi.
2. Menezes, A., P.V. Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press., Inc.
3. Camenisch, Jan Leonhard, Ph.D. Thesis, Group signature schemes and payment systems based on the discrete logarithm problem, Nachdruck Der Diss. ETH No. 12520.
4. Stallings, W. Cryptography and Network Security, Principles and Practice, 2nd Ed., Prentice Hall, Upper Saddle River, New Jersey 07458.
5. Goldwasser, S. and B. Mihir. Lecture Notes on Cryptography, MIT laboratory of Computer Science, 545 Technology Square, Cambridge, MA 02139, USA.
6. Refayat Hossain Mina, M.d., 2003. Stream ciphers for message confidentiality A senior project for the degree of bachelor of science in computer science, Independent University, Bangladesh.
7. Goldwasser, S. and B. Mihir. Lecture notes on cryptography, MIT laboratory of computer science, 545 Technology Square, Cambridge, MA 02139, USA.
8. Stallings, W. Data and computer communications, 6th Edn., Prentice Hall International Inc., ISBN: 0-13-086388-2.
9. Kaufman, C., P. Radia and S. Mike, 2003. Network security private communication in a Public World, 2nd Edn., Pearson Education, ISBN: 81-7808-790-1.