PARALLEL KEY SEQUENCE GENERATORS BASED SECURITY SYSTEM TO PREVENT COMMON SECURITY ATTACKS

Neha. D. Mistri[1], Nilesh. K. Modi[2]
[1]Research Scholar, Karpagam University, Coimbatore, India
Assistant Professor, S.V. Institute. of Computer Studies, Kadi, Gujarat – India
[2]Professor & Head of the Department, S V Institute of Computer Studies,
Kadi- 382 715, Gujarat - India
drnileshmodi@yahoo.com
nehamistry27@rediffmail.com

ABSTRACT

Cryptography is an important building block used in communication systems to provide confidentiality and authenticity. Stream ciphers, which encrypt data one bit or byte at a time have been used in applications where low delay and high speed are essential requirements. In this paper, we have proposed a cipher system based on binary stream cipher in which we use binary key sequence generators. Such n encryptions are done in parallel, where n is the word length (in case if plain text is considered as a single word). This work mainly concentrates on time consumption for encryption and decryption. In this work we try to reduce the time for the encryption and decryption algorithm, also to enhance the security aspects in comparison with the existing standard stream cipher systems like A5/1. This stream cipher system uses n number of binary key sequence generators operating in parallel. We select binary random key sequence generators which will provide immunity to several types of attacks and other properties which are suitable to the use of cryptographic applications. We found that the system we propose will have high throughput, and less time consumption for the encryption and decryption process and also no implementation cost for the conversion from n bit information to binary bits and immunity to several types of common security attacks.

1. INTRODUCTION

A Symmetric Key System is divided into two categories. First one called as stream cipher system, in which words, bytes or stream of bits, are subjects to transformation, which depends upon key, with the processes of transformation as bit by bit or byte by byte or word by word at a time. Second one called as block cipher [1]. Figure 1.1 shows a basic stream cipher system consists of a source with output *r* (bits, bytes or word), called plain text. It is subjected to a key dependent transformation called encryption, to get cipher text *c*, the key *K* is kept secret. Mathematically, it is represented as $c = E_k (r)$. The intended receiver, in position of key *K* is able to invert the transformation called decryption to get back the plaintext, $r = D_k (c)$. It is assumed that eavesdropper is interested in recovering the plain text *r* without the knowledge of key *K* by brute force or any other method. Often he attempts to recover *K* by generating $K^{\wedge}$. The process of obtaining *K* or *r* is known as *cryptanalysis*. The conventional cryptography assumes that the secrecy of a system does not depend on the algorithm of the functions rather it depends on the secrecy of the key which is usually kept unknown [2]. Because of numerous benefits over block cipher system [3] like high data rate and faster. In some cases prior to encryption/decryption, long period of the key stream can be generated processing, stream ciphers are increasingly applied.

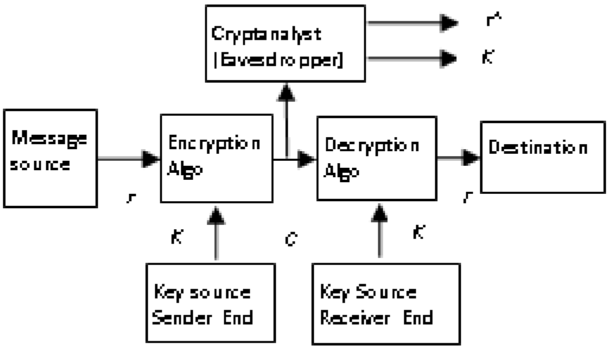

Figure 1.1 Model of basic symmetric key cipher system

Key sequence with no repetitions, statistically random, large linear complexity [4], hence we have chosen stream cipher system for this work. Generally, as said earlier [2], security of the system depends on the properties of the random key sequence generation. We propose the concept and architecture of the proposed system in section 2. Section 3 is focusing on the discussion on figure of merits and section 4 describes about results and analysis of the work. Finally, conclusion is presented in section 5.

2. PROPOSED CIPHER SYSTEM

In the proposed work the key sequence generation part is taken from already existing binary key sequence generation system. These are chosen such that property of such key sequence generators, are suitable for cryptographic applications and satisfactorily passes the tests for random sequences. The resulting cipher system gets immunity to some of the common attacks like Cipher text only attack, Known Plain text attack, Chosen plain text attack, Chosen cipher text attack, Chosen text attack for the cipher system. The new designed generators consist of multiple FSRs, uses a special clocking scheme and feedback functions. Since we use *n* such sequence generators in parallel the proposed work enhances the security, since design aspects of the key generation of this stream cipher system based on GF (2) [5] which is already in existence and proved for immunity. The proposed system takes *n*-bit plain text as an input. Each symbol of the plaintext is converted into a binary stream of *n*-bits. Theses *n*-bits are taken individually and each bit is concurrently encrypted by using keys, generated in parallel. The key sequences for *n*-bit plain text are generated by *n* known binary key sequence generators which generate *n* key sequences in parallel. After encrypting *n*-bits, in parallel these *n*-tuple cipher text is reconverted into its original *n*-bit format by just concatenating these bits. For concatenation process, we need not have to use extra hardware. The same process is used for the *n*-bit input as well as output. This reduces the extra hardware usage for conversion from *n*-bit plain text to binary or single bit, in the system.

In this paper, for the proposed system, we have taken an example of text file. For example each symbol of the plaintext, taken from a 7-bit ASCII (American Standard Code for Information Interchange) as text message, is converted into 8-bit ASCII. The binary bits of plain text ASCII is encrypted bitwise, independently. All these encryptions are handled in parallel to improve the time of encryption of the symbol. Individual encryption of single bit of ASCII is done by using separate binary key sequence generators. Each key sequence generator here is a combination of varying size FSRs with supported feedback function. After encryption of these binary bits of plain text, these are converted into an equivalent ASCII. This ASCII value is the resultant cipher text symbol. Key sequences are generated by using FSR's.

We propose three models, in the first model, Model I the 8-tuple plain text is encrypted by using the algorithm. In this 8-tuple plain text is encrypted in to 8-tuple cipher text by using eight 8 bit feedback shift registers which generates the random number. These operations are done concurrently. Next, 8-tuple plain text is encrypted by using the second model, Model II, in which 8-tuple plain text is encrypted into 8-tuple cipher text by using eight 64 bit feedback shift registers which generates the random number. The encryption and decryption operations are processed concurrently. The third model, Model III is proposed which is having the key sequence generators as same as the sequence generator of A5/1 system, so as to get the benefit of the system A5/1 as well as immunity to other types of attacks. The encryption and decryption operations are XOR operation of the binary value of individual ASCII character which is taken as plain text and key generated by the system mentioned above.

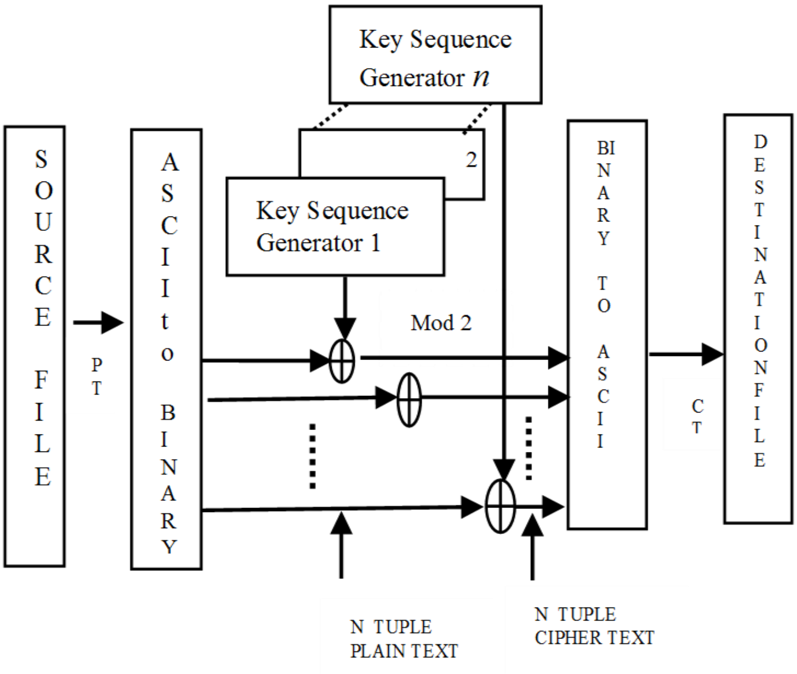

Figure 2.1: An overview of stream cipher system

3. DISCUSSION ON THE FIGURE OF MERITS

In this work, we discuss some of the figure of merits and security aspects of the proposed stream cipher system. The system we propose is simple in construction and yet powerful in avoiding attacks, in comparison with other cipher systems like a5/1, E0, RC4, etc., since they have been already undergone attacks [6] [7] [8] [9]. To prove the efficiency of proposed system, we have taken a source as input (a text file) and observed the resultant by plotting appropriate histograms of the occurrence of the plain text and cipher text and calculating the value for parameters such as Standard Deviation, Mean absolute value and the entropy as well [10], which are defined in the next section.

Standard deviation: The standard deviation of number of occurrence of cipher text element is computed as follows: Let N_i be the number of occurrences of integer i in cipher text, $0 \leq i < M$. Let N be the length of cipher text sequence. Then,

$$N = \sum_{i=0}^{M-1} N_i \qquad \ldots\ldots\ldots \qquad (3.1)$$

The mean value of number of occurrences N_i of a cipher text element is

$$\overline{N} = \lim_{N\to\infty} \frac{1}{M} \sum_{i=0}^{M-1} N_i \qquad \ldots\ldots\ldots. \qquad (3.2)$$

Then the standard deviation σ of number of occurrences of cipher text is given by

$$\sigma = \sqrt{\frac{1}{M} \sum_{i=0}^{M-1} (N_i - \overline{N})^2} \qquad \ldots\ldots\ldots. \qquad (3.3)$$

If all the cipher text integers occur equal number of times, then σ = 0. Hence minimum value of σ is zero.

Entropy: Entropy is a measure of uncertainty. Entropy of a source is maximum when all elements in the source occur with equal probability. Hence the uncertainty is the maximum when occurrence of all elements is equally likely. Let P_i be the probability of occurrence of integer i in the cipher text sequence of length N, $i = 0, 1, 2, \ldots, M - 1$

$$p_i = \underset{N\to\infty}{Lim}\frac{N_i}{N} \quad \ldots\ldots\ldots \quad (3.4)$$

And Entropy is given by

$$= \underset{N\to\infty}{Lim}\sum_{i=0}^{M-1} p_i \ \log_2\left(\frac{1}{p_i}\right)$$; average bits/cipher text element ……… (3.5)

The maximum value of entropy is $\log_2 (M)$ bits. Higher the value of entropy, higher the uncertainty and hence better is the level of security against statistical attack [10].

Mean absolute difference: Mean absolute difference $= \frac{1}{N}\sum_{j=1}^{N}\left|c_j \sim r_j\right|$ ………. (3.6)

Where c_j is cipher text integer (after recombination of parallel blocks) and r_j is plain text integer. A large value of absolute mean difference indicates very small residual information in the cipher text. The next section discusses the results and some of the security issues.

4. RESULTS AND ANALYSIS

This section of the paper covers the results obtained under various constraints for all the versions (Models) of our proposed stream cipher system. For comparison, A5/1, a standard stream cipher system is considered. A sample text is chosen as source has been taken from the text book “Network Security Essentials – Application and Standards” by William Stallings, Second Edition, chapter no. 1, page no.13, paragraph 3. This is considered as finite discrete information source. These characters are first converted to eight bit ASCII with parity. These 8 bit blocks correspond to one of the 256 characters or analog level or pixel value of an image. To study the performance of the algorithm, and to calculate the parameters discussed in Section 3, this 8-tuple plain text is encrypted by using the proposed model I, in which 8-tuple plain text is encrypted in to 8-tuple cipher text by using eight 8-bit feedback shift registers concurrently. Also we have experimented same source with Model II and Model III. It is seen that in all the cases it is not possible to guess plain text by mere observation. Further new characters which are not present in plain text are found in cipher texts obtained. Table 4.1 shows the standard deviation of the number of occurrence of the cipher text, entropy of the cipher text and mean absolute difference between cipher text and plain text. It is seen that the values obtained for three models (Model I, II, III) of our proposed system have got a gradual enhancement in terms of the parameters used for comparison with the standard A5/1 system. Hence we can say that the final design (Model III) has higher immunity towards some of the common security attacks.

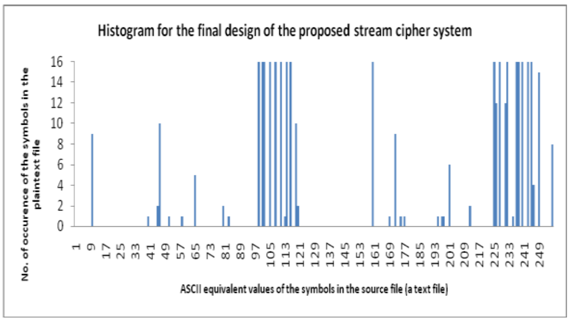

Figure 4.1 shows the histogram showing of number of occurrences of the character versus the ASCII equivalent of the above Chosen Plain Text.

The histogram shown in the figure 4.1 is the hisogram for the number of occurences of the symbols in the chosen plain text. Figure 4.2 shows the histogram for the cipher text obtained for A5/1 system. We observe from figure 4.1 and 4.3 that the occurrences of cipher text (figure 4.3) is uniformly spread in comparision with the figure 4.1, that is number of occurrences of the plain text. This shows the properties of diffusion[11].

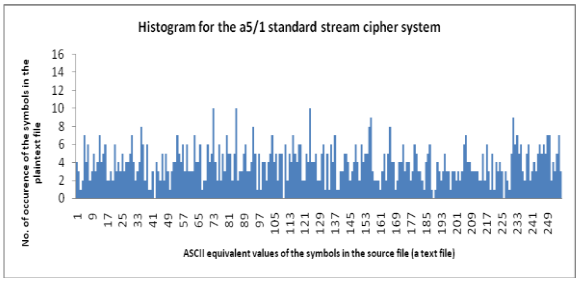

Figure 4.2 Histogram of the number of occurrence of ASCII equivalents of cipher text values obtained from the standard A5/1 stream cipher system with a single key sequence generator made of three linear feedback shift registers (19, 22, 23-bit).

From table 4.1, we observe that our initial models (Model I and II) show almost similar characteristic behavior compared to A5/1 system. But in terms of higher security they are not good enough. Plain text or deduce the key by analysis or brute force approach, trying all the possible keys for decryption. This is called attack on the system. A The third model, Model III is proposed which is having the key sequence generators as same as the sequence generator of A5/1 system, so as to get the benefit of the system A5/1 as well as immunity to other types of attacks. The standard A5/1 system has a built in immunity to algebraic attack, this advantage is extended to propose the final design (Model III) of our system since we adapt the same key sequence generator.

Table 4.1 Comparison of our proposed stream cipher system with a known standard stream cipher system, i.e.,A5/1 and all the models (I, II, III) of the proposed work.

Sl No	Type Of Stream Cipher System	Mean Absolute Difference	Standard Deviation	Entropy Value
1	Model I of the proposed stream cipher system	81.263	3.212567	7.41
2	Model II of the proposed stream cipher system	82.92	3.212567	7.44
3	Final design (Model III) of the proposed stream cipher system	83.4	2.173574	7.76
4	Standard A5/1 stream cipher system	81.599	1.940032	7.73

Security Analysis: Encrypted message is generally transmitted through the open channel which is insecure. Cryptanalyst has access to the cipher text, he taps the cipher text and without the knowledge of decrypting key tries to get plain text or deduce the key by analysis or brute force approach, trying all the possible keys for decryption.

Cipher text and relationship between the statistics of the cipher text and value of good cryptographic algorithm should withstand such attacks for short duration or long durations depending on whether it was designed for tactical or strategic applications. Security analysis deals with determining how secure the cryptographic system is against attacks. Shannon [11] stated that by making the statistical structure of plain text dissipated in to long range statistics of the encryption key as complex as possible, the task of the cryptanalyst becomes hard. The first technique is called diffusion and the second one is confusion. Further in a stream cipher system, if the period of the key sequence is larger than the length of plain text the cipher system approaches one time pad [12], which is theoretically secure.

Depending upon the amount of information known to the cryptanalyst, these attacks are generally classified as Cipher text only attack, Known Plain text attack, Chosen plain text attack, Chosen cipher text attack, Chosen text attack[13].

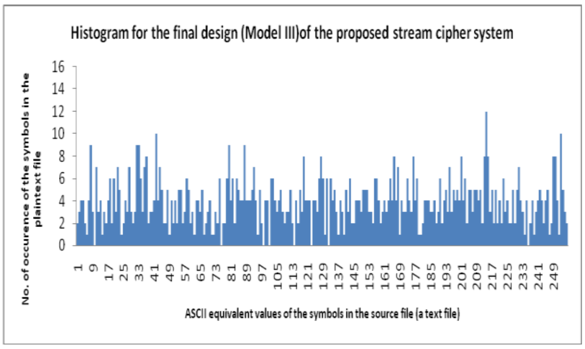

Figure 4.3 Histogram of the number of occurrence of ASCII equivalents of cipher text values obtained from the final design (Model III) of the proposed stream cipher system with eight key sequence generators, each made of three (19-, 22-, 23-bit) linear feedback shift registers, all operating in parallel.

In the proposed scheme, as a result of the running key, repeated identical plain text in general gets mapped to different cipher texts. This spreads the statistics of cipher text. Even if plain text is a sequence of repeated single character, the cipher text is a sequence of all possible elements leading to diffusion. Figure 4.5 is a histogram of the cipher text sequence for model III, for which the plain text is a sequence of repeated single character with histogram as shown in Figure 4.4. In this histogram the cipher text is diffused over all possible elements, indicating immunity to cipher text only attack. As a result of generation of running key, there is dynamic variation which impacts on the cipher text so that all symbols occur with almost equal probability. All of this leads to immunity against known plain text attack, chosen plain text attack; chosen cipher text attack and chosen text attack.

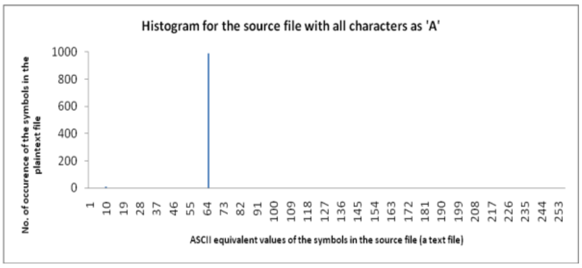

Figure 4.4 Histogram for the source file consisting of all characters as ‘A’

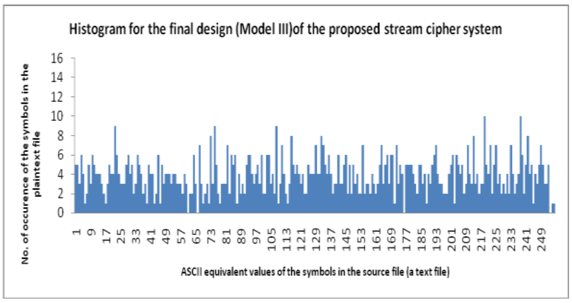

Figure 4.5 Histogram of the number of occurrence of ASCII equivalents of cipher text values (for the corresponding source file), obtained using the Model III of the proposed stream cipher system with eight key sequence generators, each made of three (19, 22, 23 bits) feedback shift registers, all operating in parallel

Algebraic attack can be foiled by using nonlinear in the generation of key sequence which uses the sequence generator of A5/1 system (Model III). Hence the proposed scheme is immune against algebraic attack.

5. CONCLUSION

We proposed three models in this paper, in the first model, the 8-tuple plain text is encrypted in parallel, by using eight 8-bit feedback shift registers which generates the random number. Model II, in which 8-tuple plain text is encrypted in to 8-tuple cipher text by using eight 64-bit feedback shift registers which generate the random number. All these 8 encryption / decryption operations are done in parallel. The third model, Model III is proposed which is having the key sequence generators as same as the sequence generator of A5/1 system is used. From table 4.1 it can be concluded that the model III of the proposed system will have better performance than A5/1 system with reference to the figure of merits - entropy and mean absolute difference. Other models (Model I and Model II) are equally better in comparison with the standard. Even though the system is a non-binary we have converted the non-binary plain text into binary *n*-tuple binary and applied the binary stream cipher key generations. This enables us to use efficient binary key generation method which has got immunity to several types of common security attacks. While converting non-binary to binary we have not used any extra hardware. The non-binary represented in computer has been taken directly as bit by bit for the encryption. Since all these encryptions can be carried out in parallel, time requirement for the encryption and decryption of the proposed system is drastically reduced, in turn the throughput of the system increases.

REFERENCES

[1] Bruce Schneier, “a self-study course in block-cipher cryptanalysis”, Published in Journal Cryptologia Taylor & Francis, Inc. Bristol, PA, USA Volume 24 Issue 1, Jan. 2000

[2] Henry Beker and Fred Piper, “Cipher Systems – The protection of Communications”, Northwood Books, London, 1982.

[3] Shepherd, S.J., “Public key stream ciphers”, Published in Security and Cryptography Applications to Radio Systems, IEE Colloquium , issue date: 1994 , On page(s): 10/1 - 10/7 , 03 Jun 1994

[4] Zeng, K. Yang, C.-H. Wei, D.-Y. Rao, T.R.N. “Pseudorandom bit generators in stream-cipher cryptography”, appeared in a journal ‘Computer’, on February, 1991, Volume 24 , Issue 2, page no. 8, 1991, IEEE

[5] Rahardja, S. Falkowski, B.J. Lozano, C.C., “Fastest linearly independent transforms over GF(2) and their properties”, Published in Circuits and Systems I: Regular Papers, IEEE Transactions , issue date : Sept. 2005 , Volume : 52 , Issue:9 , On page(s): 1832

[6] Mister and Tavares, “Cryptanalysis of RC4-like Ciphers “, in the workshop record of the Workshop on selected Areas in Cryptography (SAC ’98) Aug. 17-18 ,1999 pp.136-148

[7] E. Biham, O. Dunkelman, “Cryptanalysis of the A5/1 GSM stream Cipher”, Lecture Notes in Computer Science, vol. 1977, 2000, pp. 43–51, (Indocrypt 2000).

[8] W. Meier, and O. Staffelbach, “Fast correlation attacks on certain stream ciphers”, Journal of Cryptology, vol. 1, 1989, pp. 159–176.

[9] Yaniv Shaked and Avishai Wool, “Cryptanalysis of the Bluetooth E0 Cipher using OBDD's “, School of Electrical Engineering Systems, Tel Aviv University, Ramat Aviv 69978, ISRAEL

[10] Aithal, G. Bhat, K.N.H. Sripathi, U, “Implementation of stream cipher system based on representation of integers in Residue Number System”, This paper appears in: Advance Computing Conference (IACC), 2010 IEEE 2nd International Issue Date: 19-20 Feb. 2010 On page(s): 210 - 217 Location: Patiala Print ISBN: 978-1-4244-4790-9 INSPEC Accession Number: 11155881 Digital Object Identifier: 10.1109/IADCC.2010.5423007 Date of Current Version: 01 March 2010.

[11] Shannon, Claude (1949), "Communication Theory of Secrecy Systems". Bell System Technical Journal 28 (4): 656–715.

[12] Gilbert S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications", Journal of the IEEE, Vol 55, pp109–115 (1926).

[13] William Stallings, “Network Security Essentials – Application and Standards”, Second Edition.

AUTHORS PROFILE

Neha D Mistri has completed her B.Sc. (Physics) from Gujarat University and M.C.A. from Nirma University, Ahmedabad. Her area of interest includes Networking, Management Information System, Enterprise Resource Planning and E-commerce and Internet Security.
She is pursuing Ph.D. in the area of “Cyber Security” under the guidance of Prof. (Dr.) Nilesh Modi, from Karpagam University, Coimbatore, Tamilnadu. She has presented and published number of research papers in National/International Conferences and journals.

Nilesh K. Modi has completed M.Phil and Ph.d. He is having his active involvement as a life member of CSI, IEEE, IACSIT, laeng apart from his academic and industrial career. Dr. Modi having experience of around 8 years in academics and industry, holding Doctorate in E-Security (Computer Science and Application), continuing his research on information and communication security, presently he is pursuing post doctoral research on Wireless Communication and Security and pursuing for the Certification as an Ethical Hacker. He is working as a recognized research supervisors for Ph.D. and M.Phil. Programme from more than 03 universities of India.He has good number of research under his name and presented more than 65 research papers in International and National Journals and Conferences. He is working as a manuscript reviewer for the international journal & conference at computer science department auburn university, Alabama, USA. ofGuarat. He is also working as a reviewer for number of national and international journals. He has delivered number of expert talk on eSecuritY and hacking fi National Conferences He is also the member of board of studies and selection committee of different universities. He is working as district coordinator for SANDHAN Program initiated by Government.