EasyChair Preprint

№ 3151

Generation of Encrypted FSK RF Signals for Secured Communication Inspired with High Frequency Technique

Prashnatita Pal, Bikash Chandra Sahana, Amiya Kumar Mallick and Jayanta Poray

April 12, 2020

Generation of Encrypted FSK RF Signals for Secured Communication Inspired with High Frequency Technique

Prashnatita Pal[1] Dr.Bikash Chandra Sahana[2] Dr. Amiya Kumar Mallick[3] Dr. Jayanta Poray[4]
[1,2]Electronics & Communication Engineering
National Institute Of Technology
Patna, India
[3] Formerly Professor, Electrical Electronics & Communication Engineering
Indian Institute Of Technology
Kharagpur, India
[4]Computer Science & Engineering
Techno India University, West Bengal
Kolkata, India
Communication Email: prashnatitp@gmail.com

***Abstract*—** The paper describes a secret data transmission method using high frequency techniques. The data security system consists of two inter-related parts. One deals with encryption of binary data using RSA algorithm on software platform. Other introduces an innovative idea of transmitting the encrypted data using a single reflex klystron. Here, it requires the simultaneous generation of a pair of two independent high frequency signals with help of reflex klystron. In this scheme, the high frequency generator is biased by the repeller voltage and superimposed on a series of RSA encrypted binary data. So the system creates two high frequencies, one represent to the positive and the other one to the negative portion of the data referring in an FSK signal. The new concept have been also verified with help of simulation and experiment.

Keywords— RSA, Dual frequency generation, FSK modulation, Reflex Klystron

Introduction

The issues of privacy and security in communication network have taken on an increasingly important role as these networks continue to flourish worldwide. Cryptography techniques and tools are playing an important role in designing emerging network security technologies. Encryption is a process where important information converts into a unreadable form. Decryption is the process of restoring the information to its original form. The decrypted signal obtained at the receiver end with the input baseband signal. The input signal is encrypted using RSA algorithm. In this paper we have done a mathematical modeling of asymmetric key cryptography system using RSA algorithm by using Matrix laboratory software. Encryption of the binary data must be followed by some sort of modulation technique for the purpose of exchange of data over networks. Among the huge number of modulation techniques, frequency shift keying (FSK) plays an important role. In the paper further describes an innovative method of FSK modulation of the encrypted binary data by using a single reflex klystron.

After an introduction in first section, literature survey has been done in next. Afterwards, an overview of RSA algorithm has been described, and subsequent implementation has been done using MATLAB platform. Then the theoretical concepts of FSK generator using a Reflex klystron has been considered. Finally, the Experimental setup and simulation code is described in next section, followed by both simulation and experimental results. The paper concludes with some highlighting points regarding secure communication and future scopes to extend the model.

Literature survey

With the rapid growth of the internet and the network applications, data security becomes more important than ever before. Encryption algorithms play a crucial role in information security systems. The encryption algorithm DES has been studied and over viewed the base functions and analyzed the security for this algorithm. It is a symmetric-key algorithm for the encryption of electronic data and has a relatively short key length of 56 bits (+8 parity bits) of the symmetric key block cipher design. Its performance is evaluated in execution speed based on different memory sizes, which show the relationship between functions speed and the memory size [1]. Then we studied 3DES or the Triple Data Encryption Algorithm (TDEA) which was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data

Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is 168 bits (3 times 56). TDEA involves using three 64-bit DEA keys (K1,K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3. In 3-DES the 3-times iteration is applied to increase the encryption level and the average time. It is known fact that 3DES is slower than other block cipher methods [2].

As the encryption algorithms are known to be computationally intensive. They consume a significant amount of computing resources such as CPU time, memory, and battery power. A wireless device, usually with very limited resources, especially battery power, is subject to the problem of energy consumption due to encryption algorithms. Designing energy efficient security protocols first requires an understanding of and data related to the energy consumption of common encryption scheme, which are commonly suggested or used in WLANs. Also, RC4 encryption is more suitable for large packets[3]. Depending on the performance matrices were throughput, CPU process time, memory utilization, encryption and decryption time and key size varies. Here plaintext digits are combined with a ciphertext digit stream. So RC4 is fast and energy efficient scheme for encryption and decryption of data as it takes less time to encrypt files with respect to AES [4].

The digital signature methodology provides cryptographic services like entity authentication, authenticated key transmission and authenticated key agreement. A Digital Signature is used to provide authentication, non-repudiation integrity over the digital data in data exchanged and to validate the recipient for the authorized identity over open network. The goal of a Digital signature algorithm is to provide security for message or data. The paper focuses on a comparative study of some existing algorithms of digital signature on the basis of many hard problems[5]. We also have seen in the introduction to the fast encryption algorithm-FEA, which serves well for voice data and describes how the modification has helped in reducing the number of instructions executed. Security issues are integrated here [6].

Proceeding towards our goal, we came across another paper we have seen that data must be encrypted to make it secured by using encryption algorithm. Also there must be a key technology for encryption of data in which the delay must be lower than the other schemes [7]. Furthermore, in paper we have found out that multiple cryptographic algorithms which are applied dynamically so that our system becomes more secured and strongly protected. Less amount of CPU energy will be used [8]. According to a novel approach to decipher short mono-alphabetic ciphers, it combines both character level and word level language models. Decipherment is formulated as Tree search, used by Monte-Carlo Tree search. Both ciphers, that is, without spaces and ciphers with noise, are handled efficiently which allows us to explore its applications to unsupervised transliteration and deniable encryption [9].

As we proceed further, we came across Deffie-Hellman protocol, is to enable two users to exchange a secret key securely, used for subsequent encryption of messages. It is limited to exchange of the keys. But because of having no entity authentication mechanism, this protocol is easily attacked by the man-in-the middle and impersonation attack in practice. Key exchange scheme based on hash function which improves the security and practicality of Deffie-Hellman protocol [10]. Motivated by the several encryption standards the RSA algorithm [14] has been used in our work. The brief overview of this algorithm describes in next section.

Overview Of RSA

1. *Origin of RSA*

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys – the public key and the other is the private key. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978 [14].

2. *Structure of RSA*

The level of security provided by Message Digest Algorithms is considered to be sufficient for implementing very high security hybrid digital signature schemes When using RSA, a 1024-bit key is considered suitable both for generating digital signatures and for key exchange when used with encryption, while a 2048-bit key is recommended when a digital signature must be kept secure for an extended period of time such as a certificate authority's key. Better Key length will provide better symmetric algorithm implementation and security. Signatures can be added across databases of multiple IDS systems based on the level of threat to the network.

ALGORITHMIC SPECIFICATION OF RSA

I.Key Generation

i. Choose two distinct large random prime numbers p & q such that $p \neq q$.

ii. Compute $n = p \times q$.

iii. Calculate: $\Phi(n) = (p-1)(q-1)$.

iv. Choose an integer e such that $1 < e < \Phi(n)$ and GCD of $\Phi(n)$ and e equals 1.

v. Compute d to satisfy the congruence relation $d \times e = 1 \bmod \Phi(n)$; d is kept as private key exponent.

vi. The public key is (n, e) and the private key is (n, d)

2. RSA encryption

Plaintext : P

Ciphertext : $C = P^e \bmod n$.

3). RSA Decryption

Ciphertext: C

Plaintext: $P = C^d \bmod n$.

4)Implementation

We have implemented the overall RSA cryptographic process by using MATLAB. The flowcharts for encryption and decryption are shown in figures 5.

FSK GENERATION USING REFLEX KLYSTRON

a. Frequency-shift keying (FSK)

Frequency-shift keying (FSK)[16] is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier signal. The technology is used for communication systems such as amateur radio, caller ID and emergency broadcasts. The simplest FSK is binary FSK (BFSK). BFSK uses a pair of discrete frequencies to transmit binary (0s and 1s) information. With this scheme, the "1" is called the mark frequency and the "0" is called the space frequency.

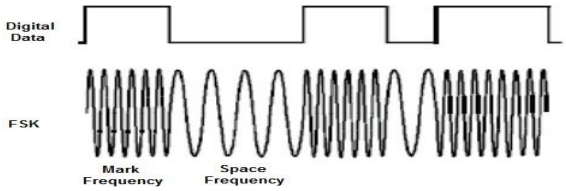

Fig-1-Pattern of Frequency shift key

b).Reflex klystron

A reflex klystron is a type in which the electron beam was reflected back along its path by a high potential electrode, used as an oscillator.

In the reflex klystron the electron beam passes through a single resonant cavity. The electrons are fired into one end of the tube by an electron gun. After passing through the resonant cavity they are reflected by a negatively charged reflector electrode for another pass through the cavity, where they are then collected. The electron beam is velocity modulated when it first passes through the cavity. The formation of electron bunches takes place in the drift space between the reflector and the cavity. The voltage on the reflector must be adjusted so that the bunching is at a maximum as the electron beam re-enters the resonant cavity, thus ensuring a maximum of energy is transferred from the electron beam to the RF oscillations in the cavity. The reflector voltage may be varied slightly from the optimum value, which results in some loss of output power, but also in a variation in frequency. This effect is used to good advantage for automatic frequency control in receivers, and in frequency modulation for transmitters. The level of modulation applied for transmission is small enough that the power output essentially remains constant. At regions far from the optimum voltage, no oscillations are obtained at all. In this procedure the klystron is suitable biased on the repeller terminal and superimposed on a train of RSA encrypted binary data so as to create two RF frequencies one corresponding to negative pick and the other one to the positive side of the data resulting in FSK signal. Next, the digital data modulates the reflex klystron the way explained in figure 2.

The mechanism of generation of two frequencies from a reflex klystron for FSK system described in reference[13]. As shown in Figure 2 a suitable mode of oscillation is chosen in V_R vs P_0 characteristics of a reflex klystron. It is found that the peak power occurs at $V_R=V_P$ and the corresponding frequency f_c. Normally fc is the resonant frequency of the cavity and the frequency of oscillation generated by klystron. The repeller voltage V_R is adjusted at V_a for lower half power point and V_b for upper half point. The RSA encrypted digital data signal connected to the external modulation mode of klystron power supply so this digital signal represented here as a train of periodic rectangular pulse only is superimposed on the repeller voltage clamped at its negetive levels at V_x. The amplitude of the digital signal is further adjusted to the repeller voltage level V_y. The frequency deviation, thus obtained is found to be f_1-f_2=δf_c.

The data signal (one) will be transmitted at frequency levels of f_1 and the zeros of the data signal at f_2 level.

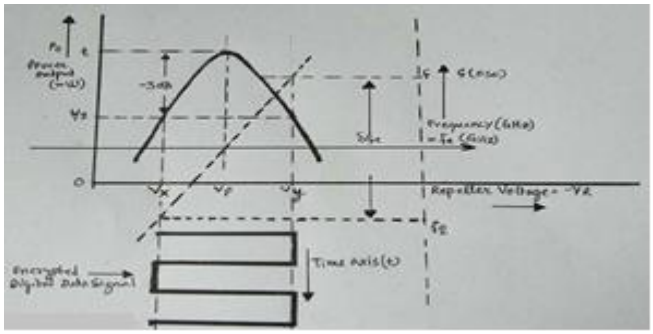

figure 2.

It may be useful to understand the electronic tuning sensitivity of the klystron that is defined as the rate of change of oscillator frequency per 1 volts of change of the repeller voltage.

Discussion: In several works the encryption algorithm has been implemented using FPGA hardware platforms [15, 13]. Our experimental framework for RSA algorithm is mainly developed using MATLAB platform.

EXPERIMENTAL SETUP

Figure 3 describes the schematic block of a transmitter in which FSK system is implemented. At first, a generator produced digital data that is encrypted in a predetermined way by using RSA algorithmic simulating environment.

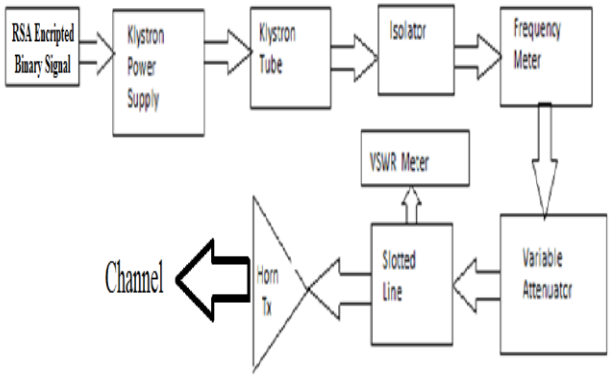

Fig-3 : Schematic Block Diagram of FSK Transmitter

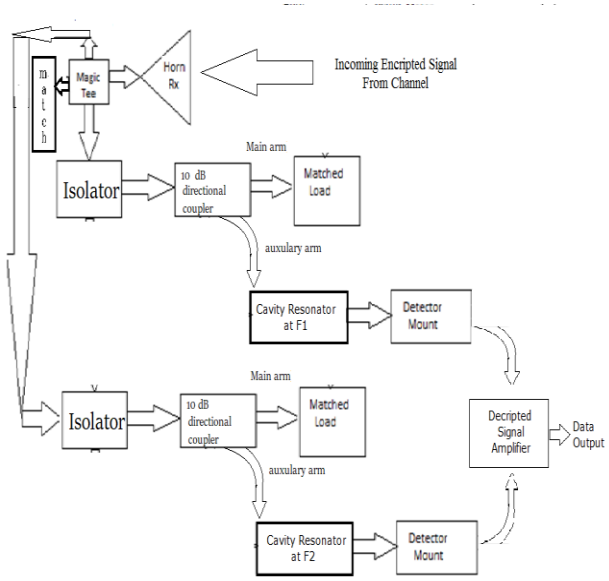

Fig-4 : Schematic Block Diagram of FSK Receiver

In next level, the digital data modulates the reflex klystron the way explained in Figure 4. Here mainly X band microwave test bench is used for experimental purpose. So rest of the block is same as that of a standard microwave bench carrying two microwave frequencies, namely f_1(9.85GHz) and f_2(9.95GHz).

RESULTS

i) Simulation data: Output of the RSA algorithm:

The experimental results for RSA algorithm is shown below:

```
Enter the prime no. for p: 7
Enter the prime no. for q: 11
  Enter the message: hello
ASCII equivalent of message
  104   101   108   108   111

The encrypted message is
      76 76 76 76 76
The decrypted message in ASCII is
      104 101 108 108 111
 The decrypted message is: hello
```

ii) Klystron Data

Beam voltage = 225volts. The mode of oscillation having largest peak power is selected for operation. The repeller voltage is adjusted at -75 volts so as to obtain maximum peak power of 13.54 mW. The corresponding frequency of oscillation as obtained in wave meter is 9.95 GHz. The half-power point s where the power is 6.77mW are obtained by adjusting the repellar voltages at - 71volts (lower one) and -81volts (upper one) respectively. At lower half-power point the frequency of operation as observed in the wave meter is 9.85GHz. The amplitude of the encrypted data will be suitably adjusted and properly placed so as to have its lower peak clamed at -71 volts level and its upper peak at -81volts level as illustrated in fig … It may , therefore be written that beam voltage V0 = 250volts.

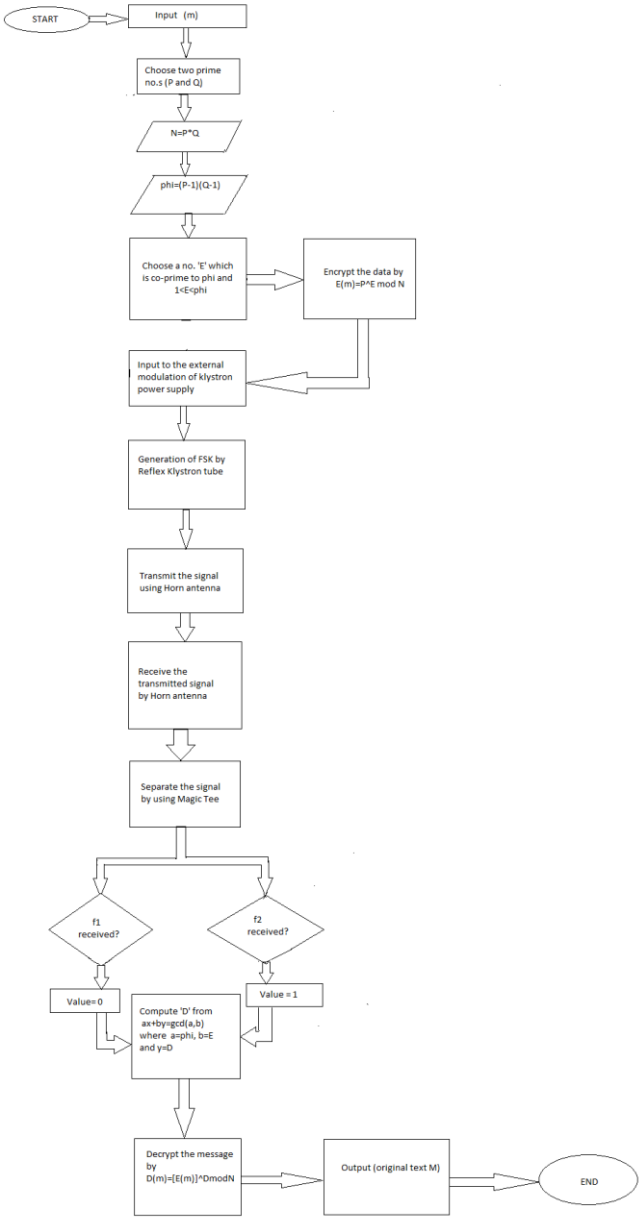

Fig-5: Flow chart for RSA encrypted FSK

ii) Klystron Data

Repeller voltage for peak power V_R = -76volts.
Half power repeller voltages V_A= -71 volts , V_B= -81 volts
Corresponding frequencies are F_c=9.92GHz.
F_1 = 9.85GHz, F_2 = 9.95GHz
Frequency deviation (δf_c) =9.95-9.85=100MHz.
Cavity data at receiver circuit:
(All other passive RF components used are standard X-band components.)

Cavity	cut off frequency	BW
1	9.95 GHz	<50 MHz.
2	9.85 GHz	<50 MHz.

On experimentation, it has been found that the output signal obtained is the exact replica of the input signal before the stage of encryption having all the superior features of FSK system.

CONCLUSION

The main objective of this paper is to secure a message signal when it is transmitted at high frequency by FSK technique for long distance communication. We have done the encryption part using RSA algorithm. Here, an experimental set-up is done to verify the importance of security and communication together. The MATLAB software suite is used for encryption and decryption. Later FSK is used to modulate the signal to support the long distance communication using microwave tube. Furthermore, this paper also confirms the feasibility and strength of cryptography using RSA algorithm, highlighting the scope of secure communication for high frequency transmission.

REFERENCE

1. T. Nie and T. Zhang, "A study of DES and Blowfish encryption algorithm," *TENCON 2009 - 2009 IEEE Region 10 Conference*, Singapore, 2009, pp. 1-4. doi: 10.1109/TENCON.2009.5396115

2. Gurpreet Singh, Supriya and G Singh "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security " - International Journal of Computer Applications, 2013 - pdfs.semanticscholar.org

3. P. Prasithsangaree and P. Krishnamurthy, "Analysis of energy consumption of RC4 and AES algorithms in wireless LANs," *GLOBECOM '03. IEEE Global Telecommunications Conference (IEEE Cat. No.03CH37489)*, San Francisco, CA, 2003, pp. 1445-1449 vol.3.

4. E Thambiraja, G Ramesh, Dr. R Umarani , E Thambiraja, G Ramesh and DR Umarani " A Survey on Various Most Common Encryption Techniques" - … of advanced research in …, 2012 - academia.edu

5. Dimple Bansal, Manish Sharma and Ayushi Mishra. "Analysis of signature based algorithm for authentication and privacy in digital data" Erschienen in: Health Policy and Planning ; 31 (2016), suppl 1. - S. i3-i16

6. P. Prasithsangaree and P. Krishnamurthy, "Analysis of energy consumption of RC4 and AES algorithms in wireless LANs," GLOBECOM '03. IEEE Global Telecommunications Conference (IEEE Cat. No.03CH37489), San Francisco, CA, 2003, pp. 1445-1449 vol.3.

7. Lin Shaofeng, Guo Chaoping, Ni Lin, Kou Wanli, and Zeng Minjiao. "The Research of Encryption algorithm for voice communucation of the mobile station " International Conference on Intelligent Transportation, Big Data and Smart City (ICITBS 2015)

8. R. Y. Hou and Y. Leung, "Dynamic encryption protocol for secure multimedia communication," 2013 IEEE 2nd Global Conference on Consumer Electronics (GCCE), Tokyo, 2013, pp. 284-285. doi: 10.1109/GCCE.2013.6664828

9. Bradley Hauer, Ryan Hayward, and Grzegorz Kondrak. "Solving substitution ciphers with combined language models"

10. Nan Li, "Research on Diffie-Hellman key exchange protocol," 2010 2nd International Conference on Computer Engineering and Technology, Chengdu, 2010, pp. V4-634-V4-637. doi: 10.1109/ICCET.2010.5485276

11. Samual Y Liao, " Microwave Devices and Circuits",4th edition ,Pearson Education Pvt. Ltd,New Delhi,2003,pp.380.

12. I. Lebedev, " Microwave Electronics " Mir Publishers, Moscow,1974,pp.214-215.

13. Mohuya Chakraborty and Amiya Kumar Mallick " AES Encrypted FSK at X-band Frequency using a Single Reflex Klystron"

14. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. Commun. of the ACM, 21:120 - 126, 1978.

15. Tahir, Ari. (2015). Design and Implementation of RSA Algorithm using FPGA. International Journal of Computers & Technology. Vol 14. 6361-6367.

16. Richard W. Middlestead, "FREQUENCY SHIFT KEYING (FSK) MODULATION, DEMODULATION, AND PERFORMANCE," in Digital Communications with Emphasis on Data Modems: Theory, Analysis, Design, Simulation, Testing, and Applications , , Wiley, 2017, pp.207-225