RSA Encrypted FSK RF Transmission Powered by an Innovative Microwave Technique for Invulnerable Security

Prashnatita Pal

February 3, 2021

RSA ENCRYPTED FSK RF TRANSMISSION POWERED BY AN INNOVATIVE MICROWAVE TECHNIQUE FOR INVULNERABLE SECURITY

Prashnatita Pal[1]

Member, IEEE

Abstract The paper mainly concerns with the generation of two high frequencies in the X-Band range with the help of a single Reflex Klystron tube, which is suitably adjusted with a train of DC pulses connected across the repeller terminals of the tube. These two predetermined frequencies innovatively created are used for a secret data transmission, in which encryption of binary data using RSA algorithm on software platform has been incorporated. One of these RF frequencies corresponds to the “1”s of the binary number and the other represents “0”s of the same. Thus, the transmission of secret digital data has been successfully put into operation utilizing FSK modulation at microwave frequency. This will, certainly ensure further improvement of security level of the system. This novel concept of data transfer proposed in this paper has also been corroborated with suitable simulation as well as laboratory experimentation.

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

I. Introduction

THE issues of privacy and security in communication networks 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 an 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 the RSA algorithm. In this paper, we have done mathematical modelling of asymmetric key cryptography system using RSA algorithm by using Matrix laboratory software and also experimentally verified these mathematical modelling. Encryption of the binary data must be followed by some sort of modulation technique for the exchange of data over networks. Among the huge number of modulation techniques, frequency shift keying (FSK) plays an important role. The paper further describes an innovative method of FSK modulation of the encrypted binary data by using a only one reflex klystron.

After an introduction in the first section, literature survey has been done next. Afterward, an overview of the RSA algorithm has been described, and subsequent implementation has been done using the MATLAB platform. Then the theoretical concepts of FSK generator using a Reflex klystron have been considered. Finally, the Experimental setup and simulation code is described in the 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.

II. Literature survey

With the rapid growth of the internet and 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 overviewed the base functions and analysed the security for this algorithm. It is a

[1] Prashnatita Pal was with St Thomas College of Engineering & Technology, Kolkata, India. He is now with the Department of Electronics & Communication Engineering, National Institute of Technology, Patna, India (e-mail: prashnatitap.phd19.ec@nitp.ac.in).

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 function speed and 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 a 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 require an understanding of and data related to the energy consumption of a common encryption scheme, which is 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 cipher text digit stream. So RC4 is a fast and energy-efficient scheme for encryption and decryption of data as it takes less time to encrypt files concerning 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 an open network. The goal of a digital signature algorithm is to provide security for messages or data. The paper focuses on a comparative study of some existing algorithms of digital signature based on 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 an encryption algorithm. Also, there must be a key technology for encryption of data in which the delay must be lower than the other schemes [11]. Furthermore, in the paper, we have found out that multiple cryptographic algorithms are applied dynamically so that our system becomes more secure and strongly protected. Less amount of CPU energy will be used [14]. 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 [15].

As we proceed further, we came across Diffie-Hellman protocol, is to enable two users to exchange a secret key securely, used for subsequent encryption of messages. It is limited to the exchange of 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 a hash function which improves the security and practicality of Diffie-Hellman protocol [7]. Motivated by the several encryption standards the RSA algorithm [10] has been used in our work. The brief overview of this algorithm describes in the next section.

III. Overview of Cryptography

A. 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 [10].

B. 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 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.

IV. FSK GENERATION USING REFLEX KLYSTRON

A. *Frequency-shift keying (FSK)*

Frequency-shift keying (FSK) [12] 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.

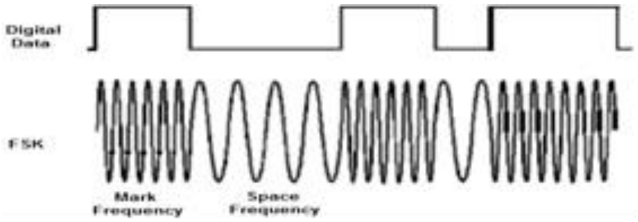


Fig-1-Pattern of Frequency shift key

B. *Reflex klystron*

Reflex klystron is basically a microwave generator where velocity modulation technique has been utilize to from a high energy density bunch of electron which suitably reflected to generate high frequency RF oscillation with in a re-entered cavity[8]

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 based on the repeller terminal and superimposed on a train of RSA encrypted binary data 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 the FSK system described in reference [9]. As shown in Figure 2 a suitable mode of oscillation is chosen in V_R (Repeller voltage) vs P_0 (output power of reflex klystron) characteristics of a reflex klystron. It is found that the peak power occurs at $V_R=V_P$ and the corresponding frequency Fc. 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 Va for the lower half PowerPoint and V_b for the upper half point. The RSA encrypted digital data signal connected to the external modulation mode of the klystron power supply so this digital signal represented here like a train of periodic rectangular pulse only is superimposed on the repeller voltage-clamped at its negative levels at Vx. The amplitude of the digital signal is further adjusted to the repeller voltage level Vy. The frequency deviation, thus obtained is found to be f_1-f_2=δfc. [13]

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

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 volt of change of the repeller voltage.

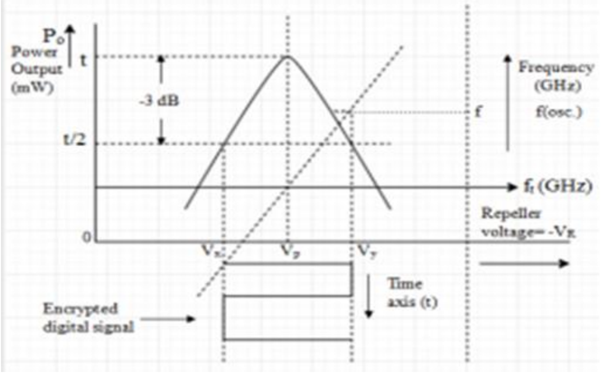


Figure 2

C. *Discussion:*

In several works, the encryption algorithm has been implemented using FPGA hardware platforms [11]. Our experimental framework for the RSA algorithm is mainly developed using MATLAB platform [13]. Here we show that entire simulation result verified with help of experiment.

V. EXPERIMENTAL DETAILS

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

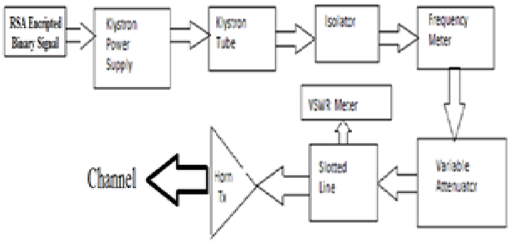


Fig-3: Schematic Block Diagram of FSK Transmitter

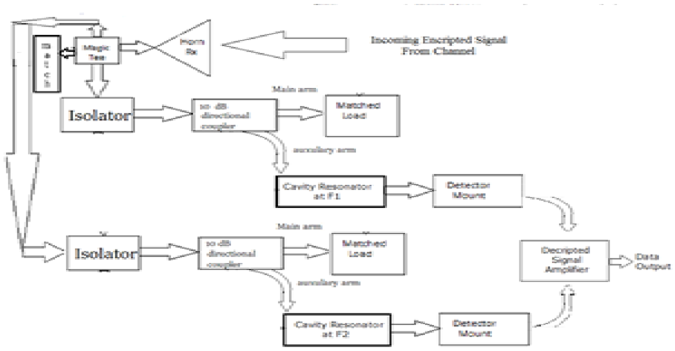


Fig-4: Schematic Block Diagram of FSK Receiver

In the 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 purposes. So the rest of the block is the same as that of a standard microwave bench carrying two microwave frequencies cavity resonators., One tuned with f1(9.85GHz) and other f2(9.95GHz). Later details discussion on designing procedure of these two cavity resonators.

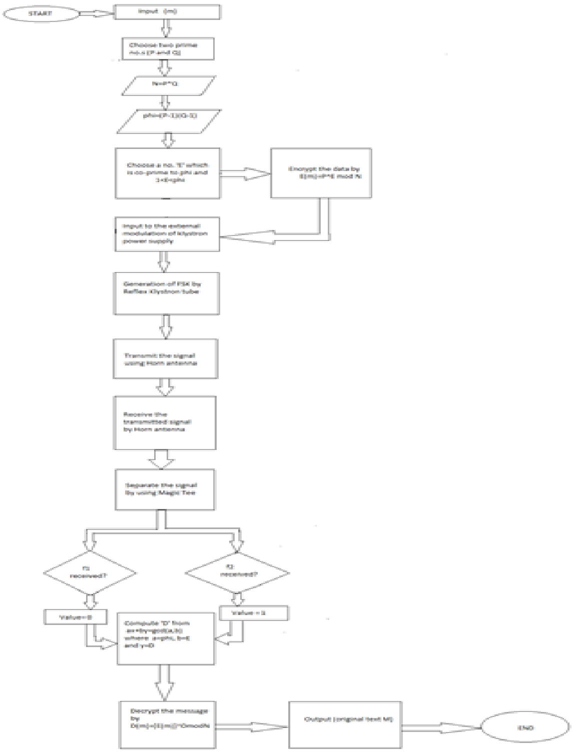

START
Input (m)
Choose two prime no.s (P and Q)
N=P*Q
phi=(P-1)(Q-1)
Choose a no. 'E' which is co-prime to phi and 1<E<phi
Encrypt the data by E(m)=P^E mod N
Input to the external modulation of klystron power supply
Generation of FSK by Reflex Klystron tube
Transmit the signal using Horn antenna
Receive the transmitted signal by Horn antenna
Separate the signal by using Magic Tee
f1 received?
f2 received?
Value=0
Value =1
Compute 'D' from ax+by=gcd(a,b) where a=phi, b=E and y=D
Decrypt the message by D(m)=(E(m))^DmodN
Output (original text M)
END

Fig-5: Flow chart for RSA encrypted FSK

VI. RESULT ANALYSIS

A. *Simulation data*

1. The simulation output for the RSA algorithm are shown below:

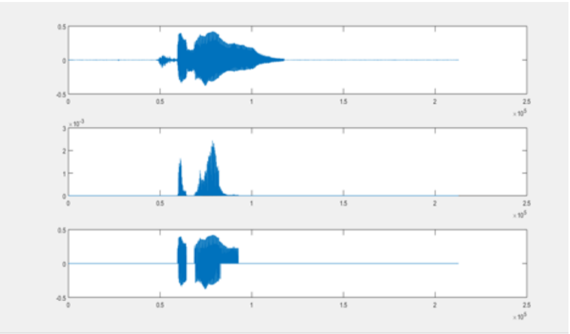


Fig.6. Time domain representation of i) encrypted signal, ii) chipper signal, iii) decrypted signal

2. The Simulation result for RSA algorithm are 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”

B. *Cavity Design*

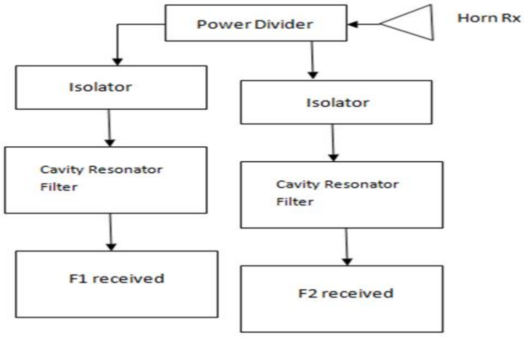


Fig 7: Cavity block diagram

1. Design using HFSS :

The cylindrical cavity resonator is designed for TM010 mode. Theoretically, the radius and height of the cylindrical cavity for the given frequencies are as follows:

Theoretically, For 9.95 GHz, radius =1.154 cm and height = 2.308 cm and for 9.855 GHz, radius = 1.165cm and height=2.3cm.

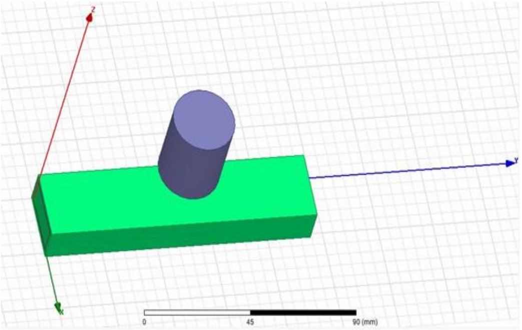


Fig:8 Cylindrical cavity resonator design

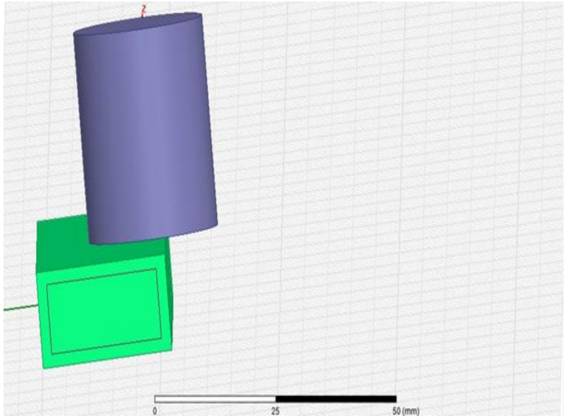


Fig: 9 Side view of cylindrical cavity resonator

2. Design layout:

The waveguide is designed is HFSS by designing a vacuum rectangular box which is surrounded by a copper rectangular box. The length, breadth and height of the rectangular vacuum box and rectangular copper box were measured physically from the waveguide present in the laboratory.

Vacuum box, length = 12cm
Breadth = 2.32 cm
Height = 1.06 cm

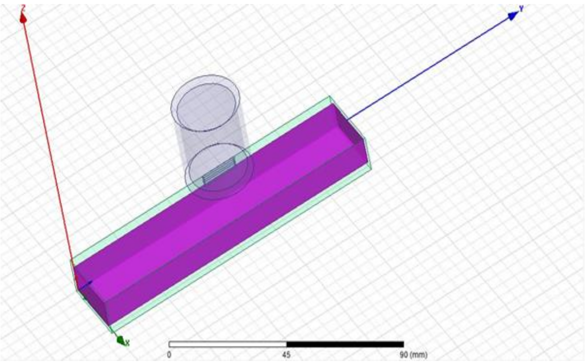


Fig: 10 Vacuum rectangular box of waveguide

Copper box, length = 12 cm, breadth = 2.52 cm
Height = 1.26 cm

The next step was the design of a vacuum cylinder which is surrounded by a solid copper cylinder placed above the waveguide with a vacuum opening between the two which is known as resonator aperture. Theoretically,

For 9.95GHz, Radius of vacuum cylinder = 1.154 cm Radius of copper cylinder= 1.354 cm

Height of vacuum cylinder = 2.308 cm Height of copper cylinder =2.708 cm

For 9.855GHZ, Radius of vacuum cylinder =1.165 cm Radius of copper cylinder = 1.365 cm

Height of vacuum cylinder =2.33 cm
Height of copper cylinder = 2.73 cm

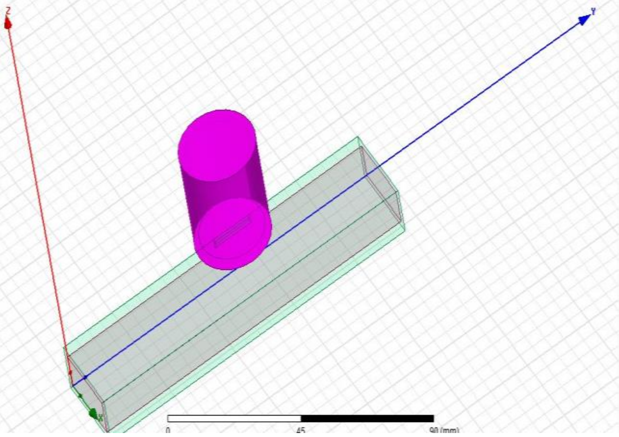


Fig: 11 Solid cylinder of the cavity resonator

Coupling holes are designed in a waveguide which is used as the feeding transmission line, the aperture, is the natural coupling device. Depending on the location of the aperture in the waveguide, the tangential magnetic field or normal electric field will penetrate the aperture and couple to the resonance mode. The strength of the coupling (the electric or magnetic dipole moment) is proportional to the third power of the radius of the aperture. The coupling depends, of course, on the location of the aperture with respect to the field of the resonance mode and the direction of the field lines in the case of magnetic coupling. The coupling hole is placed exactly at the mid-point of the cylindrical cavity resonator. The height of the vacuum coupling hole is such that it connects the waveguide with the cylindrical cavity. The width of the coupling hole is 0.1 cm and the length is. $\lambda/2$.

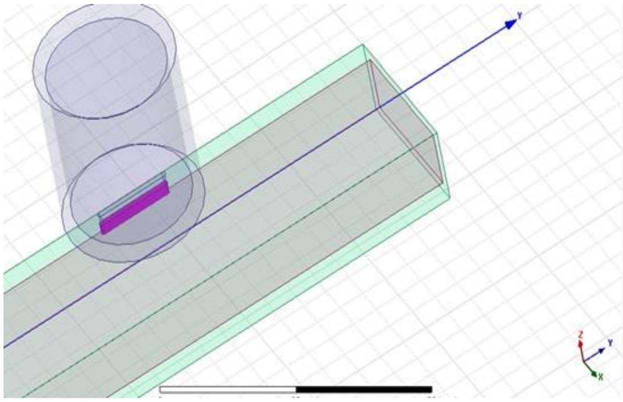


Fig:12 Coupling hole of the cavity resonator

The following results are obtained while simulating for achieving 9.95 GHz resonant frequency:

Cavity mode	a(cm)	d(cm)	Aspect Ratio	Resonant freq.
TM_{010}	1.154	1.731	1.33	10.86 GHz
TM_{010}	1.154	2.308	1	9.58 GHz
TM_{010}	1.154	2.636	0.875	9.95 GHz
TM_{010}	1.154	2.885	0.8	9.3 GHZ

Hence, we obtain the resonant frequency of 9.95 GHz at aspect ratio of 0.875.

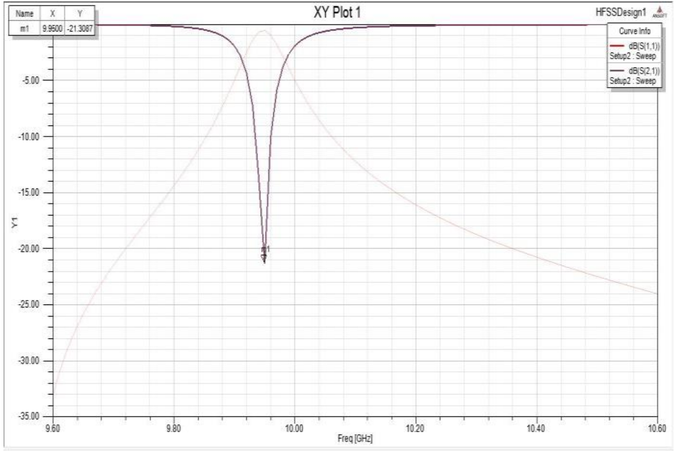


Fig 13 S21 and S11 obtained for the cylindrical cavity resonator resonating at 9.95 GHz

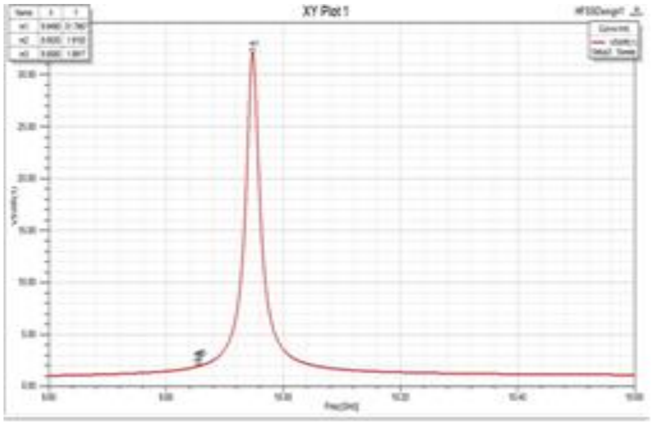


Fig:14 VSWR vs. frequency graph obtained from the simulated results

VSWR for 9.95 GHz = 31.7957

9.855 GHz =1.9153

Hence, we obtain the resonant frequency of 9.855 GHz at aspect ratio of 0.833.

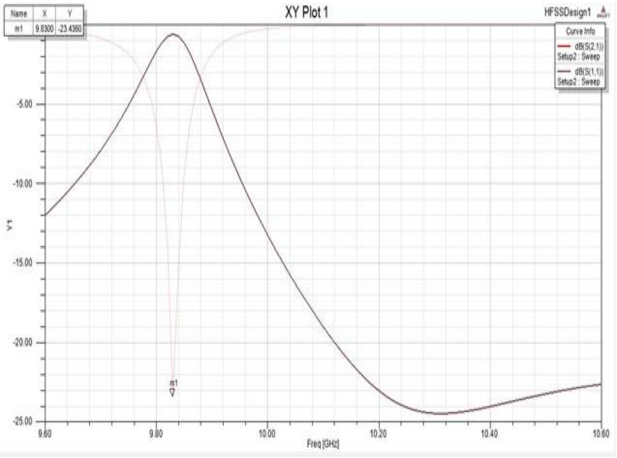


Fig: 15 S21 and S12 obtained for the cylindrical cavity resonator at 9.855 GHz

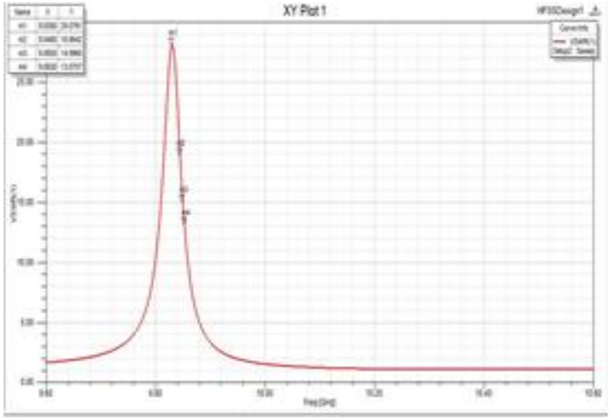


Fig:16 VSWR vs. frequency graph obtained from the simulated results

VSWR for 9.855 GHz = 13.07

9.95 GHz = 1.9811

Cavity mode	a(cm)	d(cm)	Aspect Ratio	Resonant frequency
TM_{010}	1.165	2.33	1	9.925 GHz
TM_{010}	1.165	2.679	0.869	9.469 GHz
TM_{010}	1.165	2.795	0.833	9.831 GHz
TM_{010}	1.165	3.029	0.769	9.101 GHz

C. *Reflex Klystron Data analysis from Microwave test Bench*

Beam voltage = 225volts. The mode of oscillation having the largest peak power is selected for operation. The repeller voltage is adjusted at -75 volts to obtain maximum peak power of 13.54 mW. The corresponding frequency of oscillation as obtained in the wavemeter is 9.95 GHz. The half-power point s where the power is 6.77mW is obtained by adjusting the repeller voltages at - 71volts

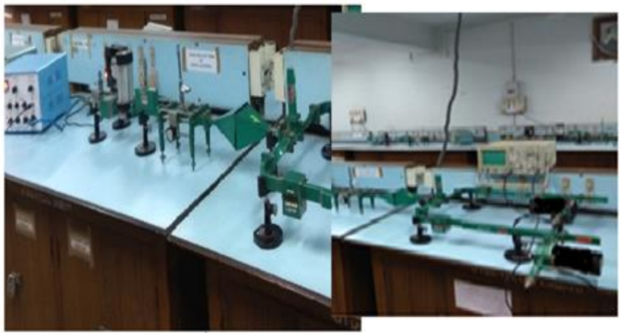
(lower one) and -81volts (upper one) respectively. At lower half-power point the frequency of operation as observed in the wavemeter is 9.85GHz. The amplitude of the encrypted data will be suitably adjusted and properly placed to have its lower peak claimed at -71 volts level and its upper peak at -81volts level as illustrated in fig … It may, therefore, be written that beam voltage V0 = 250volts. Repeller voltage for peak power V_R = -76volts.Half power repeller voltages V_A= -71 volts, V_B= -81 volts and corresponding frequencies are Fc=9.92GHz.

F_1 = 9.85GHz, F_2 = 9.95GHz. Frequency deviation (δfc) =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



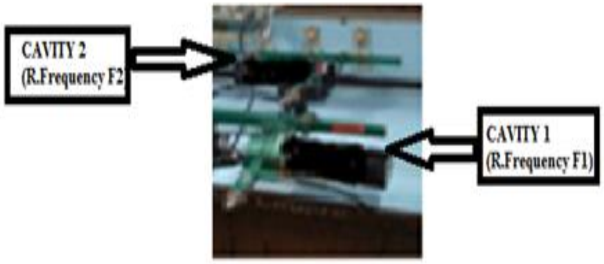


Fig.17. Setup of klystron characteristics using external modulation

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

VII. CONCLUSION

The main objective of this paper is to secure a message signal when it is transmitted at high frequency by the FSK technique for long-distance communication. We have done the encryption part using the 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 long-distance communication using a microwave tube. Furthermore, this paper also confirms the feasibility and strength of cryptography using the RSA algorithm, highlighting the scope of secure communication for high-frequency transmission.

REFERENCES

[1] T.Nie and T. Zhang, "A study of DES and Blowfish encryption algorithm," IEEE Region 10 Conference, Singapore, 2009, pp. 1-4.

[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

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

[4] 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

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

[6] R. Y. Hou and Y. Leung, "Dynamic encryption protocol for secure multimedia communication," IEEE 2nd Global Conference on Consumer Electronics (GCCE), Tokyo, 2013, pp. 284-285.

[7] 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.

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

[9] Chakraborty Mohuya & Mallick, Amiya. AES Encrypted FSK Generation at X-Band Frequency using a Single Reflex Klystron. Wireless Communication over ZigBee for Automotive Inclination Measurement. China Communications. 2010, 7. 1-9.

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

[11] Tahir, Ari. . Design and Implementation of the RSA Algorithm using FPGA. International Journal of Computers & Technology.2015 Vol 14. 6361-6367.

[12] 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

[13] Pal Prashnatita ,Sahana Bikash Chandra ,Mallick Amiya Kumar and Poray Jayanta, Generation of Encrypted FSK RF Signals for Secured Communication Inspired with High Frequency Technique . International conference on Recent Trends in Artificial Intelligence, IOT, Smart Cities & Applications (ICAISC-2020),Available at SSRN: https://ssrn.com/abstract=3610690

[14] Wang, Z.; Yao, Y. Tong, X. Luo, Q. Chen, X. "Dynamically Reconfigurable Encryption and Decryption System Design for the Internet of Things Information Security". Sensors 2019,

[15] Hannan, Shaikh Abdul; Asif, Ali Mir Arif Mir. "Analysis of Polyalphabetic Transposition Cipher Techniques used for Encryption and Decryption International Journal of Computer Science and Software Engineering; Vol. 6, Iss. 2, (Feb 2017): 41-46.