ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Cryptographic Key Exchange using Dual Tone Multi Frequency Generator

Alex Chirayath[1], Shyam Padia[2], Alfred Gonsalves[3], Prof. Monali Shetty[4]

[1] B.E. Student, Dept. of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering, Maharashtra, India
[2] B.E. Student, Dept. of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering, Maharashtra, India
[3] B.E. Student, Dept. of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering, Maharashtra, India
[4] Assistant Professor, Dept. of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering, Maharashtra, India

ABSTRACT: This paper presents a new cryptographic technique for secure key exchange. For information resource transactions cryptosystem plays an important role in encrypting and decrypting the messages which are sent on secure communication channels for protecting from eavesdroppers. In this research study, the DTMFG key exchange (a new cryptographic key exchange technique) has been introduced for secure network communication. The DTMFG key exchange depends primarily on DTMFG (Dual Tone Multi Frequency Generator) for both key generation and key exchange.
Every telephone key has a unique frequency associated with it. Thus, every key generates a specific sound note and this tone can be used to identify the value of the key. The telephone key generator used in this project works exactly in the same way. Written in Python language, the DTMFG replicates the exact unique tone associated with the key. The DTMFG generates the tone and stores it in a .wav file which can then be decoded later. The idea is use to these frequency tones (which can be set) to use in the field of cryptography in key exchange.

KEYWORDS: Dual tone, Cryptography, Key Exchange, Multi frequency, telephone, high-frequency, frequency generator

I. INTRODUCTION

Key exchange is a technique in cryptography by which the secret keys are exchanged between senders and receivers for the purposes of encryption and decryption of messages respectively. In the communication world, various key exchange techniques are being used for secure key exchange to protect from eavesdroppers. If encryption of messages is vulnerable, then eavesdroppers can gain full information over communication channels. In this research study, a new approach is introduced for efficient and secure key exchange which is named as DTMFG key exchange technique.DTMF (dual tone multi frequency) is the signal to the phone company that you generate when you press an ordinary telephone's touch keys. DTMF was first developed in the Bell System in the United States where it's known as "Touchtone" phone (formerly a registered trademark of AT&T). DTMF has generally replaced loop disconnect ("pulse") dialing.

DTMF is standardized by ITU-T Recommendation. With DTMF, each key you press on your phone generates two tone of specific frequencies. So that a voice can't imitate the tones, one tone is generated from a high-frequency group of tones and the other from a low frequency group. These signals are used in touch-tone telephone call signaling as well as many other areas such as interactive control applications, telephone banking, and pager systems. Each of these tones is composed of two pure sine waves of the low and high frequencies superimposed on each other. These two frequencies explicitly represent one of the digits on the telephone keypad.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

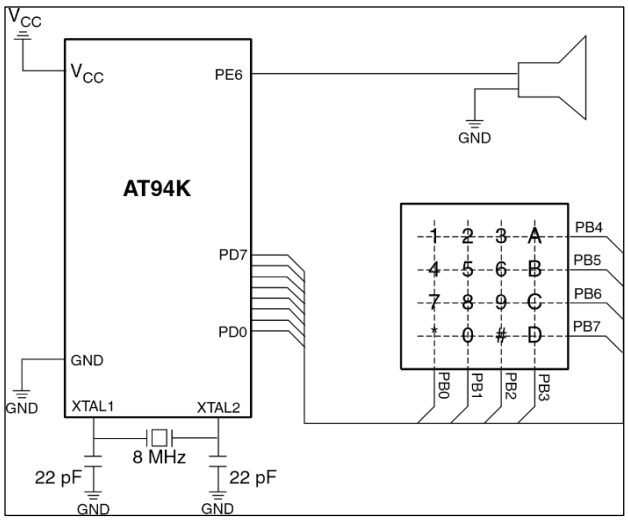

Fig.1a-DTMF Generator Circuit

The generated signal can be expressed mathematically as follows:

f (t) = AH sin(2π fH t) + AL sin(2π fL t) … (1)

Where AH, AL are the amplitudes & fH, fL are the frequencies of high & low frequency range.

Properties of DTMF tone frequencies are:

- No frequency is an integer multiple of another
- The difference between any two frequencies does not equal any of the frequencies
- The sum of any two frequencies does not equal any of the frequencies

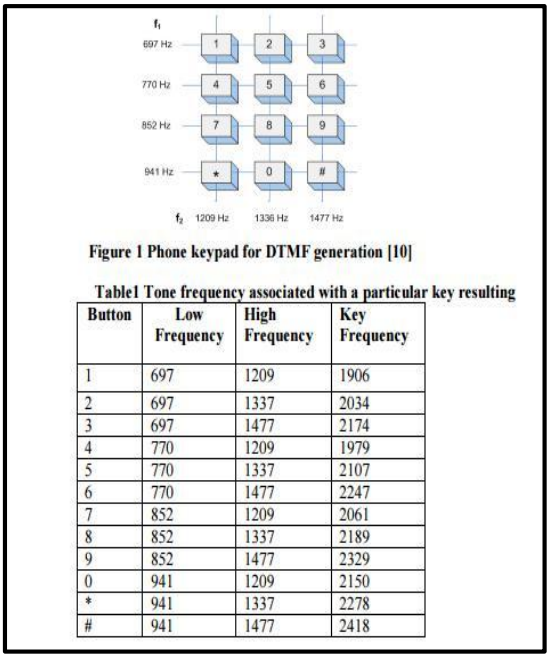

Figure 1 Phone keypad for DTMF generation [10]

Table1 Tone frequency associated with a particular key resulting

Button	Low Frequency	High Frequency	Key Frequency
1	697	1209	1906
2	697	1337	2034
3	697	1477	2174
4	770	1209	1979
5	770	1337	2107
6	770	1477	2247
7	852	1209	2061
8	852	1337	2189
9	852	1477	2329
0	941	1209	2150
*	941	1337	2278
#	941	1477	2418

Fig 1a - Phone Keypad Frequencies of AT&T

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

II.LITERATURE SURVEY

Key-exchange protocols are mechanisms by which two parties that communicate over an adversarially-controlled network can generate a common secret key. Key exchange protocols are essential for enabling the use of shared-key cryptography to protect transmitted data over insecure net works. As such they are a central piece for building secure communications or secure channels, and are among the most commonly used cryptographic protocols (contemporary examples include SSL, IPSec, SSH, among others).

The design and analysis of secure key exchange protocols has proved to be a non-trivial task, with a large body of work written on the topic, including [1,2,3,4,5,6] and many more. In fact, even today, after two decades of research, some important issues remain without satisfactory treatment. One such issue is how to guarantee the adequacy of key exchange protocols for their most basic application: the generation of shared keys for implementing secure channels. Providing this guarantee (with minimal requirements from key exchange protocols) is the main focus and objective of this work.

A. Diffie –Hellman Session Key Agreement

Diffe-Hellman session key agreement is the first key exchange protocol, proposed by Diffie and Hellman [7]. Diffie-Hellman key exchange by itself achieves perfect forward secrecy because no long-term keying material exists at the end of the session to be disclosed. However, it does not provide authentication of the communicating parties; hence it is vulnerable to a man-in-the-middle attack.

B. Station-To-Station (STS) Protocol

In order to fix the security flaw in the Diffie-Hellman protocol, the Station-To-Station (STS) protocol was proposed in [8]. To add authentication, the STS protocol requires both the parties to have a pair of public keys for signature generation and verification, and to know a publicly released symmetric key encryption. In contrast, note that the Diffie-Hellman protocol does not have these assumptions. These assumptions can be included into the protocol by sending public key certificates if the keys are not known in advance. In the STS protocol, STS protocol uses signatures to authenticate the communicating parties. It encrypts the signatures with the session key subsequently to show the knowledge of this session key. However, signatures and certificates cause the messages to increase considerably in size.

C. Secure Socket Layer (SSL)

SSL [9] involves negotiating and establishing secure connections, and securing the data transmission. SSL handshake uses certificates and PKI [10] for mutual authentication and key exchange. PKI binds public keys with particular user identities by means of a certificate authority (CA). The CA is the trusted entity that signs and issues digital certificates [11] to other parties. A digital certificate contains a public key and the identity of the owner and the validity period of the certificate. Therefore, authentication is performed through sending and verifying certificates which involve a great overhead. SSL key exchange can use an RSA algorithm, an asymmetric technique for session key exchange which encrypts the session key from the client to the server. A Diffie-Hellman key exchange can also be used which is more secure since both parties agree on the session key without having to send the key across the wire.

D. ID-based Authenticated Key Agreement

Many protocols were proposed for ID-KEX [12] [13]. Paterson and Price[14] noted that the aim in designing a good ID-KEX protocol is to achieve all the properties of the best usual key agreement protocols while trying to maximize efficiency. The public key can be chosen by any client in the system as it is generated from public information (email address or network address). Each party, then contacts the trusted authority (TA) once to authenticate and get the required private key. Therefore, there is no earlier distribution of keys between individual participants. Yuan and Li [15] proposed an efficient ID-KEX Protocol. A key agreement protocol is said to be authenticated if it offers the guarantee that only the participating parties of the protocol can compute the agreed key. Therefore, this ID-KEX protocol is authenticated because it uses public and private keys to generate a shared secret.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

III.RELATED WORK

In [1, 2, 3, 4, 5, 6] The design and analysis of secure key exchange protocols with a large body of work is written on the topic. In [7] it is mentioned that Diffe-Hellman session key agreement is the first key exchange protocol, proposed by Diffie and Hellman. In [8] to fix the security flaw in the Diffie-Hellman protocol, the Station-To-Station (STS) protocol was explained. In [9, 10, 11] it is explained how SSL connection is established and how the handshake is made along with details about the security certificates. In [12, 13, 14] Paterson and Price proposed a new ID-KEX protocol to maximize the efficiency and in [15] Yuan and Li did the same to increase the efficiency further. In [16, 17, 18, 19] as explained by Ylonen and Lonvick SSH is a secure transmission and user authentication protocol and its working is explained. In [28, 29] it is explained how the DTMF tones and their frequencies could be generated and how it can be implemented.

II. METHODOLOGY

A. HISTORY OF KEYS

The engineers had envisioned telephones being used to access computers, and automated response systems. They consulted with companies to determine the requirements. This led to the addition of the number sign (#, "pound" or "diamond" in this context, "hash", "square" or "gate" in the UK, and "octothorpe" by the original engineers) and asterisk or "star" (*) keys as well as a group of keys for menu selection: A, B, C and D. In the end, the lettered keys were dropped from most phones, and it was many years before the two symbol keys became widely used for vertical service codes such as *67 in the United States of America and Canada to suppress caller ID.

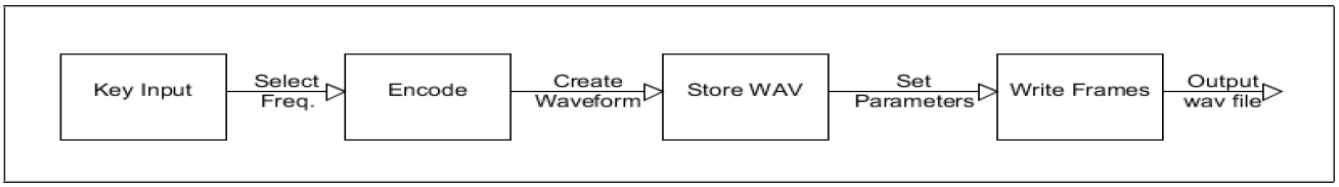

Fig 2a – Flowchart of the Encoding Program

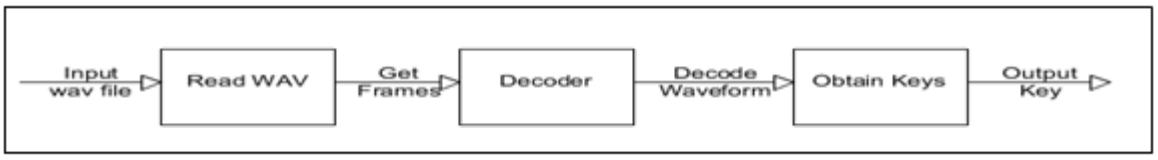

Fig 2b – Flowchart of the Decoding Program

Public payphones that accept credit cards use these additional codes to send the information from the magnetic strip.

Present-day uses of the A, B, C and D signals on telephone networks are few, and are exclusive to

network control. For example, the A key is used on some networks to cycle through different carriers at will. The A, B, C and D tones are used in radio phone patch and

repeater operations to allow, among other uses, control of the repeater while connected to an active phone line.

The *, #, A, B, C and D keys are still widely used worldwide by amateur radio operators and commercial two-way radio systems for equipment control, repeater control, remote-base operations and some telephone communications systems.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Fig 3c -16 keys- Keypad Frequencies used in the project

B. SIGNAL GENERATION

The DTMF signal for a key is the sum of two sinusoidal waves, one at each frequency. The rows of the matrix shown in Table 1 represent the low frequencies while the columns represent the high frequency values. For example, this matrix shows that digit 5 is represented by a low frequency of f_b = 770 Hz and a high frequency of f_a = 1336 Hz. The two frequencies are transformed to a DTMF signal using equation 1:

$$f(t) = Aa * \sin(2\pi fat) + Ab * \sin(2\pi fbt)) \quad \ldots(1)$$

where the ratio between the two amplitudes should be:

$$Ab / Aa = K \quad ; \quad 0\ 7 < K < 0\ 9 \quad \ldots(2)$$

III. FUNCTIONALITY

The DTMF generation code for encoding and decoding is prepared in the python script by importing the wave package. The inbuilt as well as custom made functions used in the project are explained in this paper.

encoder( )

Function is used for encoding the key tones. It checks which key is selected from the key matrix and apply it to the frequency equation scaled to the frame rate of 44000 and store in the .wav file. The encoder( ) gives a call to the store_wav( ) function in which the Most significant bit and the Least Significant Bit are updated and the updated values are written into audio frames. We create data for every 44000 frames and store it in the audio .wav format file using the following equation:

```
data -> scale+(sin(p*f1*PI2)+sin(p*f2*PI2))/2*scale
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

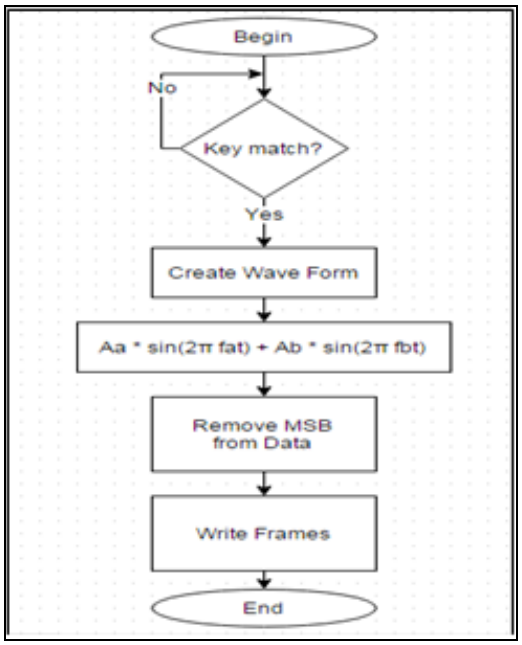

Fig 4a-Flow chart of the Encoding Algorithm

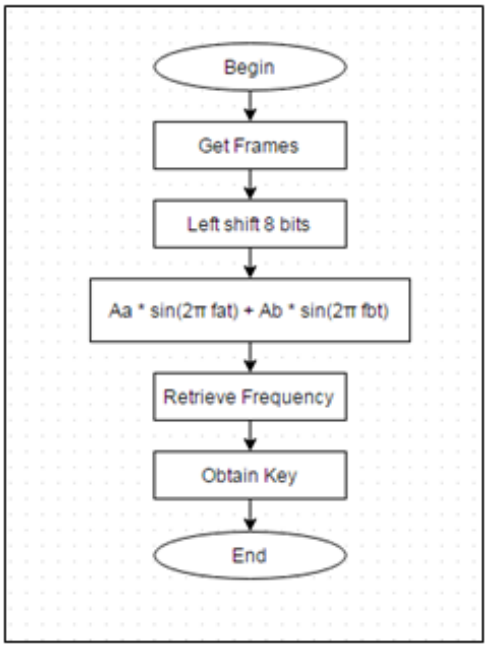

Fig 4b-Flow chart of the Decoding Algorithm

decoder( )

Function is used for decoding the audio signal to key values. The read_wav( ) function calculates the number of frames in the file and reads the data for each frame. It gets the MSB and LSB from the file and returns the data obtained from 44000 frames.

S -> scale+scale*(sin(p*f1*PI2)+sin(p*f2*PI2))/2

The above equation is used to scale the frequency and match it with the frequency ranges to get appropriate key value.

IV. DTMF KEY EXCHANGE

For a simple illustration, let us consider a very basic encryption technique.

Encryption

1) Input key which will be stored in abc.wav
2) Null byte is appended at the end
3) Length of the new file is calculated
4) d = length / n
5) Get random numbers R[]
6) for i=0 to n-1
   Calculate inverse of R[i] mod 16
   Put key[i] on R[i]
7) Send inverse(R[i]) AND abc.wav
8) Receiver can then decode

V. RESULTS

The figure 7a shows the voltage to time graph of the keytone '1'. The key '1' is assigned the higher frequency as 1209 Hz and lower frequency as 697 Hz. Similarly, we can see that for different keys, unique keytone frequencies generate a unique graph. The figure 7b shows the graph for the keys '3', '#' and 'B' respectively.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

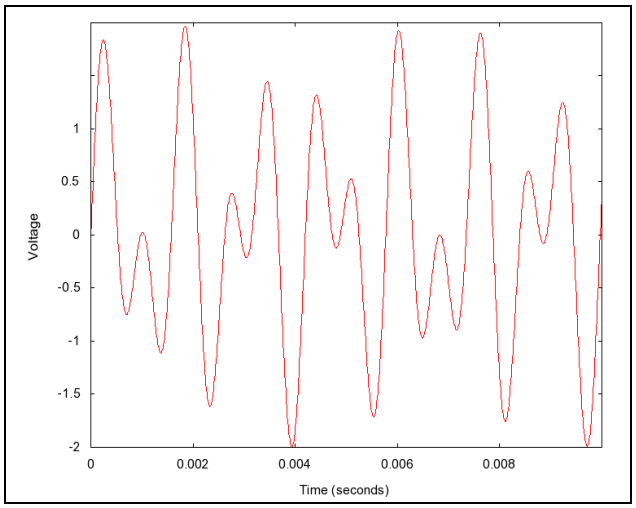

Fig 7a-1209 Hz on 697 Hz to make the '1' tone

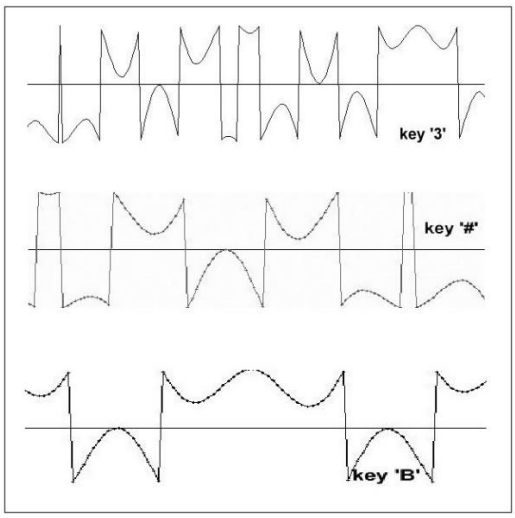

Fig 7b-O/P generated by the DTMFG

Thus, we can observe that each key generates its own unique assigned tone.

VI. CONCLUSION

In this research study, a new key exchange technique, DTMFG key exchange, has been introduced for efficient and secure key exchange between two parties. The DTMFG key exchange technique used the DTMF for the purpose of key generation. Powers of accepted frequency components were theoretically set as if they were a pure sine function. Actually, the generated signals contain noise: as a result, DTMF components would be less powerful. Thus, there are approximate calculations made for the wave generation. However, DTMFG can be used for various different fields. The distinct unique tone associated with each key allows for development of various applications in cryptography itself. This paper gives a very basic example of key exchange using DTMF. However, when applied with the new modern techniques, DTMF can prove very useful in the field of cryptography leading to stronger encryption techniques as it adds one more level of security to the current techniques used in key exchange.

REFERENCES

[1] W. Diffie and M.Hellman, "New directions in cryptography ", IEEE Trans.Info. Theory IT-22, November 1976, pp. 644-654.
[2] R.Needham and M.Schroeder, "Using encryption for authentication in large networks of computers," Communications of the ACM ,Vol.21, No. 12, December 1978, pp. 993-999.
[3] M.Bellare and P.Roga way, "Entity authentication and key distribution", Advances in Cryptology,-CRYPTO'93, Lecture Notes in Computer Science Vol.773,DStinson ed,Springer-Verlag,1994,pp.232-249
[4] M.Bellare,R.Canetti and H.Krawczyk,"Amodular approach to the design and analysis of Authentication and key-exchange protocols",30th STOC,1998
[5] M.Bellare and P.Rogaway,"Provably secure session key distribution-the three party case," Annual Symposium on the Theory of Computing (STOC) , 1995
[6] H.Krawczyk,"SKEME: A Versatile Secure Key Exchange Mechanism for Internet,", Proceedings of the 1996 Internet Society Symposium on Network and Distributed System Security ,Feb. 1996, pp.114-127.
[7] Diffie W. Hellman, M.E. 1976 "New directions in cryptography".
[8] Diffie W. Van Oorschot, P.C., Wiener, M.J.1992, "Authentication and authenticated key exchanges. Des. Codes Cryptography 2(2)" ,107-125
[9] Frier, A., K.P., Kocher, P.1996, "The secure socket layer", Technical report, Netscape Communications Corp.
[10] Younglove, R.2001,"Public key infrastructure, how it works", Computing & Control Engineering Journal 12, 99-102.
[11] Feghhi, J., Feghhi, J., Williams, P.1999, "Digital Certi_cates: Applied Internet Security", Addison Wesley Long man.
[12] Chen, L., Kudla, C.2002," Identity based authenticated key agreement protocols from pairings", In: In: Proc. 16th IEEE Security Foundations Workshop. pp. 219-233. IEEE Computer Society Press.
[13]Choie, Y. J., J.E., Lee, E. 2005," Efficient identity -based authenticated key agreement protocol from pairings", Applied Mathematics and Computation 162, 179-188.
[14] Paterson, K., Price, G.2003, "A comparison between traditional public key infrastructures and identity -based cryptography", Information Security 8(16), 57-72.
[15] Yuan, Q., Li, S.2005, "A new efficient id-based authenticated key agreement protocol.Cryptology", ePrint Archive: Report 2005/309

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

[16] Lee, H.K., Malkin, T., Nahum, E.2007, "Cryptographic strength of ssl/tls servers: current and recent practices", In: IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. pp. 83-92. ACM, New York, NY, USA.
[17] Ylonen, T., Lonvick, C.E.2006, "The secure shell (ssh) transport layer protocol", rfc 4253
[18] Ylonen,T., Lonvick, C.E.2006."The secure shell (ssh) authentication protocol", rfc 4252
[19] Ylonen, T., Lonvick, C.E.2006.The secure shell (ssh) connection protocol, rfc 4254.
[20] Canetti, R., Krawczyk, H.2002,"Security analysis of ikes signature-based key-exchange Protocol", In: In: Proc. CRYPTO02, Springer LNCS 2442. pp. 143-161. Springer –Verla.
[21] Smart, N.P.2002,"An id-based authenticated key agreement protocol based on the weil Pairing", Electronics Letters 38(13), 630-632.
[22] Shim, K.2003,"Efficient id-based authenticated key agreement protocol based on the weil Pairing", Electronics Letters 39(8), 653-654.
[23] Lee, H.K., Malkin ,T. Nahum, E.2007, "Cryptographic strength of ssl/tls servers: current and recent practices", In: IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. pp. 83-92. ACM, New York, NY, USA.
[24] Castelluccia, C. Mykletun, E. Tsudik, G.2005, "Improving secure server performance by re-balancing ssl/tls handshakes", In: in Proceedings of the 10th Annual USENIX Security Symposium. pp. 26-34
[25] chun Kuo , F.Tschofenig, H. Meyer, F., Fu, X.2006,"Comparison studies between pre-shared and public key exchange mechanisms for transport layer security", In: 25th IEEE International Conference on Computer Communications. pp. 1-6
[26] Tim Massey and Ramesh Iyer, "DSP Solutions for Telephony and Data/Facsimile Modems", Application Book, Texas Instruments Inc. 1997
[27] Wikipedia Contributors, Dual tone multi frequency signalling.
[28] Atmel Corporation, "DTMF Generator", Educypedia, 2002
[29] "DTMF Code Generation. An Implementation using the TMS320C2xx", Texas Instruments Europe, 1997
[30] Github Contributors, Available at https://github.com/hfeeki/dtmf/
[31] StackOverflow Contributors, Available at http://stackoverflow.com/questions/3244876/can-we-generate-dtmf-tones-using-python