Pelita Informatika : Informasi dan Informatika, Volume 9, Nomor 2, Oktober 2020
ISSN 2301-9425 (Media Cetak)
Hal: 86-91

Implementasi Teknik Enrkipsi Algoritma Tweakable Block Cipher Untuk Pengamanan Voice Chat Pada Perancangan Aplikasi Chatting

Mahadi Suwanda[1]

Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Sumatera Utara, Indonesia
Email: [1*]mahadisuwanda1@gmail.com

Abstrak

Voice chat adalah suatu pesan suara di sebuah teknologi jaringan komputer yang mengijinkan pemakainya untuk mengirimkan pesan suara ke pengguna lain yang tersambung dalam sebuah jaringan komputer atau jaringan internet. Saluran komunikasi yang digunakan kurang aman, maka penyerang akan mudah membobol saluran yang ada dan menyadap semua komunikasi yang terjadi. Teknik kriptografi dapat digunakan untuk pengamanan file yang bersifat rahasia dengan menggunakan proses enkripsi dan dekripsi data sehingga file tidak dapat dipahami artinya. Algoritma kriptografi yang dapat digunakan untuk melakukan proses enkripsi adalah algoritma Tweakable Block Cipher. Algoritma Tweakable Block Cipher adalah turunan dari mode CBC (Cipher Block Chaining) dimana algoritma Tweakable Block Cipher akan melakukan teknik penyandian dengan cara mode block yang membutuhkan dua input yaitu ciphertext dan kunci. Penelitian ini mengggunakan algoritma Tweakable Block Cipher untuk proses enkripsi dan dekripsi. Sebuah file yang berisikan voice chat dengan tipe berekstensi .ogg yang akan di enkripsi menggunkan algoritma Tweakable Block Cipher sehingga menghasilkan ciphervoice. Proses ini dapat meningkatkan keamanan voice chat dan mempresulit pihak-pihak yang tidak bertanggung jawab memahami voice chat tersebut.

Kata Kunci : Kriptografi, Algoritma Tweakable Block Cipher, Voice Chat

1. PENDAHULUAN

Kriptografi adalah ilmu yang mempelajari mengenai bagaimana cara mengamankan suatu informasi/data. Pengamanan ini dilakukan dengan mengenkripsi informasi/data tersebut dengan suatu kunci khusus. Informasi/data ini sebelum dienkripsi dinamakan plaintext. Setelah dienkripsi dengan suatu kunci dinamakan ciphertext [1].

Aplikasi chatting adalah aplikasi yang digunakan untuk komunikasi melalui jaringan lokal atau internet. Dapat digunakan untuk membuat komunikasi menjadi efektif dan mudah digunakan tetapi ada beberapa kekurangan dalam proses pengiriman informasi adalah keamanan data voice chat ketika komunikasi sedang berlangsung [2]. Voice Chat adalah suatu pesan suara di sebuah teknologi jaringan komputer yang mengijinkan pemakainya untuk mengirimkan pesan suara ke pengguna lain yang tersambung dalam sebuah jaringan komputer atau jaringan internet [3].

Aplikasi chatting umumnya digunakan untuk saling bertukar pesan suara maupun saling menjaga keaslian data antara pengguna komputer. Bila saluran komunikasi yang digunakan kurang aman, maka penyerang akan mudah membobol saluran yang ada dan menyadap semua komunikasi yang terjadi. Untuk menyelesaikan masalah yang telah diuraikan diatas, maka digunakan metode kriptografi. Metode kriptografi digunakan untuk mengamankan file yang bersifat rahasia agar file tersebut tidak diketahui oleh orang lain yang tidak berkepentingan. Salah satu metode kriptografi yang dapat digunakan adalah metode Tweakable Block Cipher. Pada metode kriptografi terdapat dua proses yaitu enkripsi dan dekripsi. Enkripsi fungsinya adalah mengubah pesan suara yang berisi plaintext atau pesan suara biasa yang dirubah menjadi chipertext atau teks acak yang tidak bisa dibaca.

Algoritma Tweakable Block Cipher adalah salah satu algoritma yang dapat digunakan untuk mewujudkan teknik kriptografi. Algoritma Tweakable Block Cipher adalah teknik penyandian yang dilakukan dengan cara mode block, dimana Tweakable Block Cipher adalah turunan dari mode CBC (Cipher Block Chaining). Algoritma Tweakable Block Cipher membutuhkan dua input – tunggal - ciphertext $C \in \{0,1\}^n$. Dengan demikian untuk tanda tangan blok sandi [4].

Pengenalan Tweakable Block Cipher ini adalah konstruksi DESX yang diperkenalkan oleh M. Liskov, R. L. Rivest dan D. Wagner," Tweakable Block Cipher", Advances In Cryptology, vol. 24, pp.31-46, 2002 (tidak dipublikasikan). Alasan untuk memperkenalkan DESX adalah untuk memberikan informasi kunci tambahan untuk DES dengan murah. Keamanan DESX telah dianalisis oleh Kilian dan Rogaway. Mereka menunjukkan bahwa DESX dengan input n-bit (dan tweak dan kunci k-bit memiliki panjang kunci efektif k + n – 1 – lgm dimana musuh terbatas pada panggilan oracle [4].

Adapun penelitian yang lain yang dilakukan oleh S. Halevi dan P. Rogaway," A Tweakable Enciphering Mode", Advances In Cryptology, pp.482-499, 2003, menerangkan bahwa membayangkan serangan-model adalah serangan plaintext / ciphertext yang dipilih yang versary ad- dapat mempelajari ciphertext C untuk setiap plaintext P dan tweak T,dan dapat mempelajari plaintext P untuk setiap ciphertext C dan tweak T. Secara informal, kita ingin tweakable, kuat, pseudorandom permutasi (PRP) yang beroperasi pada Blocksize lebar (seperti 512 bytes) [5].

2. TEORITIS

A. Kriptografi

Kriptografi dibagi menjadi 2 kata yaitu *Crypto* yang berarti rahasia dan *Graphy* yang berarti tulisan. Para pelaku atau praktisi kriptografi disebut *cryptographers*. Sebuah algoritma kriptografik (*cryptographic algorithm*) disebut *cipher* yang merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya

kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat [8].

B. Algoritma Tweakable Block Cipher

Algoritma tweakable block cipher adalah sebuah teknik penyandian yang dilakukan dengan cara mode block, dimana algoritma tweakable block cipher adalah turunan dari metode CBC (Cipher Block Chaining). Algoritma tweakable block cipher melakukan proses enkripsi dengan membutuhkan dua input yaitu kunci ($K \in \{0,1\}^k$) dan pesan atau plaintext ($M \in \{0,1\}^n$) sehingga menghasilkan output berupa ciphertext ($C \in \{0,1\}^n$). Dengan demikian rumus dari proses enkripsi algoritma tweakable block cipher adalah sebagai berikut:

$E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ [4].

C. Voice Chat

Voice Chat adalah suatu pesan suara di sebuah teknologi jaringan komputer yang mengijinkan pemakainya untuk mengirimkan pesan suara ke pengguna lain yang tersambung dalam sebuah jaringan komputer atau jaringan internet [3].

3. ANALISA

A. Analisa Masalah

Tahapana Analisa yang dilakukan pada sub bab ini menjelaskan mengenai pengumpulan data dan informasi yaitu bagaimana Teknik penerapan algoritma lucifer dalam mengamankan voice chat pada aplikasi yang dirancang dan dibangun.

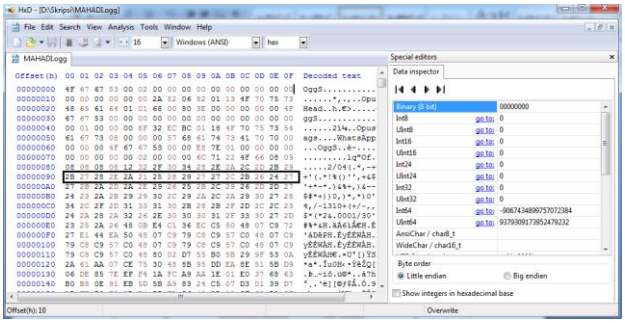
Proses enkripsi algoritma Tweakable dilakukan dengan memberikan nilai input sebesar128 bit, yang kemudian dilakukan proses pembentukan kunci dengan panjang bernilai sama dengan nilai input yaitu 128 bit. Objek pada penelitian ini yang akan dienkripsi adalah voice chat sementara ini didapatkan dari aplikasi whatsapp. Selanjutnya pada objek voice chat dilakukan ekstrasi nilai dengan bantuan aplikasi HxD. Berikut skema proses ekstrasi nilai hexadecimal dari file voice cha tmenggunakan aplikasi HxD. Setelah didapat nilai hexadecimal selanjutnya proses penerapan algoritma Tweakable

B. Penerapan Algoritma Tweakable Block Cipher

Tweakable merupakan algoritma block cipher pertama yang menggunakan feistel cipher yang terdiri dari 16 round. Sehingga awalnya block akan dibagi dua menjadi left block dan right block. Kemudian left block dan subkey pada round itu akan dimasukkan ke F-Function, setelahnya di XOR kan dengan right block yang hasilnya menjadi setengah bagian block untuk round berikutnya. Setiap akhir round left block dan right block akan ditukar kecuali pada round terakhir. Setelah itu left block dan right block dikombinasikan untuk mendapatkan ciphertext yang diinginkan. Maka yang akan dilakukan yaitu dari sebuah jenis pesan *voice chat* yang digunakan sebagai contoh untuk menerapkan algoritma Tweakable Block Cipher, penulis menggunakan jenis voice chat dari aplikasi Whatsapp, Berikut spesifikasi:

Nama File : MAHADI.ogg
Tipe File : OGG Audio File (.ogg)
Ukuran File : 485 KB (496,992 bytes)
Waktu : 30/07/2019 6:32 PM

Proses selanjutnya adalah melakukan pengambilan nilai hexadecimal dari file *voicechat* yang akan digunakan, dalam hal ini penulis menggunakan aplikasi HxD.



Gambar 1. Proses Ekstrasi Nilai Hexadecimal menggunakanHxD

Setelah dilakukan proses ekstrasinilai hexadecimal dari file voice, berikut nilai hexadecimal *plainvoice* yang digunakan dalam penelitian ini sebagai berikut:**2B 27 28 2E 2A 21 25 28 29 27 27 2C 2B 26 24 27**, kemudian akan dikonversi dalam bentuk biner seperti berikut ini:

Tabel 1. Konversi *Plainvoice* Ke Biner

Konversi Hexadesimal Ke Biner					
2B		**00101011**	29		**00101001**
27		**00100111**	27		**00100111**
28		**00101000**	27		**00100111**
2E	=	**00101110**	2C	=	**00101100**
2A		**00101010**	2B		**00101011**
21		**00100001**	26		**00100110**
25		**00100101**	24		**00100100**
28		**00101000**	27		**00100111**

Kemudian bagi dua *bloc k*awal menjadi *leftblock* (L) dan *rightblock* (R).

L_0 = 00101011001001110010100000101110001010100010000100100101001010000

R_0 = 00101001001001110010011100101100001010110010011000100100001000111

Setelah itu lakukan proses pengenkripsian sebanyak 16 *round* dengan menggunakan rumus berikut ini :

Rumus mencari nilai L adalah$L_1 = R_0$

Rumus mencari nilai R adalah$R_1 = L_0 \oplus F(R_0, K_0)$

Putaran1 :

L_1 = 00101011001001110010100000101110001010100010000100100101001010000

$R_1 = L_0 \oplus F(R_0, K_0)$

01001001010001000100000101010010010011010100000100110001001100000⊕
01000100010010010100000101001110010111110100000101001110001000111
=00001101000011010000000000011100000100100000000000111111101110111
01010011010101000100110101001001010010110100001001010101000100
R_1 =
01011110010110010100110101010101010101100101000010001010100011001 1
Putaran2 :
L_2 =
01011110010110010100110101010101010101100101000010001010100011001 1
$R_2 = L_1 \oplus F(R_1, K_1)$
01011110010110010100110101010101010101100101000010001010100011001 1⊕
01000111010001110100000101010010010000010011000100111100100110001
=00011001000111100000110000000111000110000011100110001001100000010
01001001010001000100000101010010010011010100000100110001001100000
R_2 =
01010000010110100100110101010101010101010011001001000100011001 0
Putaran3 :
L_3 =
01010000010110100100110101010101010101010011001001000100011001 0
$R_3 = L_2 \oplus F(R_2, K_2)$
01010000010110100100110101010101010101010011001001000100011001 0⊕
00110001001100000100010001001001010000010100111001011111101000001
=01100001011010100000100100011100000101000011111001111111101110111
01011110010110010100110101010101010101100101000010001010100011001 1
R_3 =
00111111001100110100010001001001010011010011111001010111010000000
Putaran4 :
L_4 =
00111111001100110100010001001001010011010011111001010111010000000
$R_4 = L_3 \oplus F(R_3, K_3)$
00111111001100110100010001001001010011010011111001010111010000000⊕
01000001010011100100011101000111010000010101001001000100110001
=01111110011111010000001100001110000011000110110100000101100111000 1
01010000010110100100110101010101010101010011001001000100011001 0
R_4 =
00101110001001110100111001011011010110011010111100011010001000011
Putaran5 :
L_5 =
00101110001001110100111001011011010110011010111100011010001000011
$R_5 = L_4 \oplus F(R_4, K_4)$
00101110001001110100111001011011010110011010111100011010001000011⊕
00110001001110010011000100110000010001000100101001010000101001110
=00011111000111100111111101101011000111010001011101111010100001101
00111111001100110100010001001001010011010011111001010111010000000
R_5 =
00100000001011010011101100100010010100000010100100100001001101
Putaran6 :
L_6 =
00100000001011010011101100100010010100000010100100100001001101
$R_6 = L_5 \oplus F(R_5, K_5)$
00100000001011010011101100100010010100000010100100100001001101⊕
01001110010111110100000101001110010001110100011101000000101010010
=01101110011100100111101001101100000101110110111001100001100111111
00101110001001110100111001011011010110011010111100011010001000011
R_6 =
01000000010101010011010000110111010011100011000001010111010111100
Putaran7 :
L_7 =
01000000010101010011010000110111010011100011000001010111010111100
$R_7 = L_6 \oplus F(R_6, K_6)$
01000000010101010011010000110111010011100011000001010111010111100⊕
01010010010000010011000100111001001100010011000001000100100100101
=00010010000101000000010100001110011111110000000000001001100010101
00100000001011010011101100100010010100000010100100100001001101
R_7 =
00110010001110010011111000101100001011110010100100110001011000
Putaran8 :
L_8 =
00110010001110010011111000101100001011110010100100110001011000
$R_8 = L_7 \oplus F(R_7, K_7)$
00110010001110010011111000101100001011110010100100110001011000⊕

01001001010000010100111001011111010000010100111001000111101000111
=01111011011110000111000001110011011011100110011101111011000011111
01000000010101010011010000110111010011100011000000101011101011100
R_8 =
00111011001011010100010001000100001000000101011100100000101000011
Putaran9 :
L_9 =
00111011001011010100010001000100001000000101011100100000101000011
$R_9 = L_8 \oplus F(R_8, K_8)$
00111011001011010100010001000100001000000101011100100000101000011⊕
01000111010000010101001001000001001100010011100100110000100110000
=01111100011011000001011000000101000100010110111100000100001110011
00110010001110010011111000101100001011110010100100110000101011000
R_9 =
01001110010101010010100000101001001111100100011100100000100101011
Putaran10 :
L_{10} =
01001110010101010010100000101001001111100100011100100000100101011
$R_{10} = L_9 \oplus F(R_9, K_9)$
01001110010101010010100000101001001111100100011100100000100101011⊕
00110000010001000100100101000001010011100101111101000000101001110
=01111110000100010110000101101000011100000000110000011000001100101
00111011001011010100010001000100001000000101011100100000101000011
R_{10} =
01000101001111000010010100101100010100000100111101000000100100110

Putaran11 :
L_{11} =
01000101001111000010010100101100010100000100111101000000100100110
$R_{11} = L_{10} \oplus F(R_{10}, K_{10})$
01000101001111000010010100101100010100000100111101000000100100110⊕
01001110010001110100011101000001010100100100000101100010011100100
=00001011011110110110001001101101000000100000111100110000000011111
01001110010101010010100000101001001111100100011100100000100101011
R_{11} =
01000101001011100100101001000100001111000100100101010000100100110100

Putaran12 :
L_{12} =
01000101001011100100101001000100001111000100100101010000100100110100
$R_{12} = L_{11} \oplus F(R_{11}, K_{11})$
01000101001011100100101001000100001111000100100101010000100100110100⊕
00111001001100010011000001000100010010010100000101001110011111100
=01111100000111110111101000000000011101010000100000111101101011
01000101001111000010010100101100010100000100111101000000100100110
R_{12} =
00111001001000110101111100101100001001010100011101011111001001101
Putaran13 :
L_{13} =
00111001001000110101111100101100001001010100011101011111001001101
$R_{13} = L_{12} \oplus F(R_{12}, K_{12})$
00111001001000110101111100101100001001010100011101011111001001101⊕
01011111010000010100111001000111010001110100000101001001000001
=01100110011000100001000101101011011000100000011000000110000001100
01000101001011100100101001000100001111000100100101010000100100110100
R_{13} =
00100011010011000101101100101111010111100100111101011111001001110
Putaran14 :
L_{14} =
00100011010011000101101100101111010111100100111101011111001001110
$R_{14} = L_{13} \oplus F(R_{13}, K_{13})$
00100011010011000101101100101111010111100100111101011111001001110⊕
01000001001100010011100100110001001100000100010001001000001
=01100010011111101011000100001111001101110000010100010001111001
00111001001000110101111100101100001001010100011101011111001001101
R_{14} =
01011011010111100011110100110010010010110100110001001010100110100
Putaran15 :
L_{15} =
01011011010111100011110100110010010010110100110001001010100110100
$R_{15} = L_{14} \oplus F(R_{14}, K_{14})$
01011011010111100011110100110010010010110100110001001010100110100⊕
01000001010011100101111101000001010011100100011101000011101000001

=0001101000010000011000100111001100000101000010110000110101110101
0010001101001100010110110010111101011110010011110101110100111000
R_{15} =
0011100101011100001110010101110001011011010001000101000001001101
Putaran16 :
L_{16} =
0011100101011100001110010101110001011011010001000101000001001101
$R_{16} = L_{15} \oplus F(R_{15}, K_{15})$
0011100101011100001110010101110001011011010001000101000001001101⊕
0100000101010010010000010011000100111001001100001001100000100100
=0111100000001110011110000110110101100010011101000000000001001
0101101101011110001111010011001001001011010011000100101000110100
R_{16} =
0010001101010000010001010101111100101001001110010010101000111101

Berdasarkan perhitungan di atas, maka *ciphervoice* yang dihasilkan dalam bentuk biner adalah sebagai berikut:
0010001101010000010001010101111100101001001110010010101000111101001110010101110000111001010111000101101001000100010100000010011011 *Ciphervoice* yang di konversi dari biner ke huruf hexadesimal, **2B27282E2A2125282927272C2B262427**

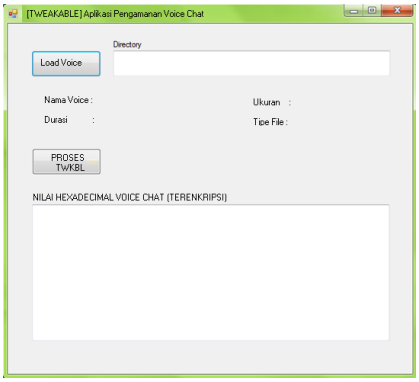
4. IMPLEMENTASI

Spesifikasi sistem atau perangkat yang digunakan untuk medukung kegiatan proses pengujian terhadap algorimta Tweakable dalam proses pengamanan file voice chat, sebagai berikut:

1. Spesifikasi Perangkat Keras
   a. Merek perangkat tidak dibatasi, namun dalam penelitian ini penulis menggunakan perangkat Laptop merek Asus.
   b. Minimal Processor Intel Pentium 4
   c. Minimal Memory 1 GB
   d. Minimal Harddisk 40 GB
   e. VGA Card 8 MB, Printer, Mouse, dan Keyboard
2. Spesifikasi Perangkat Lunak
   a. Microsoft Windows XPProfesional atau diatasnya.
   b. Microsoft Visual Basic .NET 2008.
   c. Binary View.

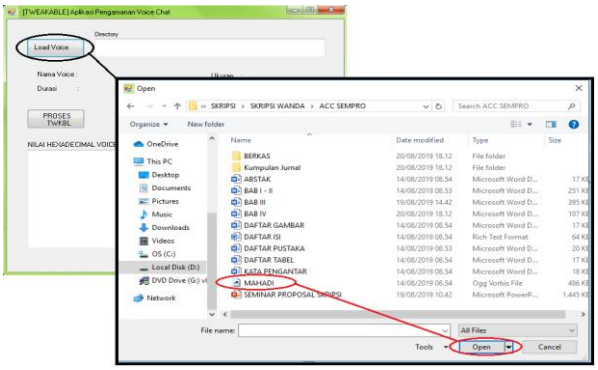
A. Tampilan Pengujian

Proses pengujian pada penelitian ini menggunakan aplikasi yang telah dibanggun menggunakan Microsoft Visual Basic Net 2008. Proses pengujian dilakukan untuk menguji algoritma Tweakable dalam mengamankan file voice chat, informasi yang ada pada file voice chat tidak dapat diakses oleh orang tidak berkepentingan. Berikut tampilan form pengamanan file voice chat,



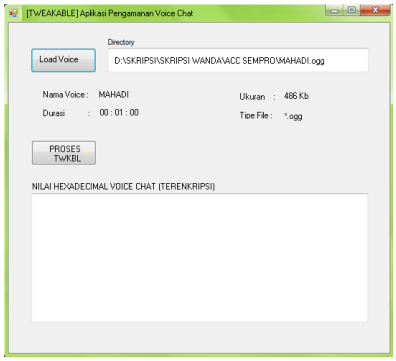
Gambar 2. Tampilan Aplikasi PengamananFile voice chat

Langkah selanjutnya adalah melakukan proses akses terhadap file voice chat yang telah disimpan dalam direktori penyimpanan untuk diproses, dengan mengklik tombol "Load File voice chat" atau lebih jelas dapat dilihat pada gambar berikut ini.



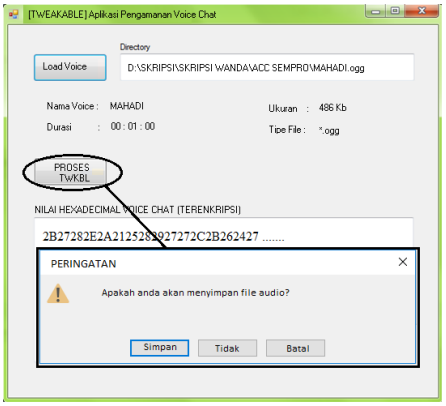
Gambar 3. Proses Load File voice chat

Setelah proses load file voice chat dilakukan maka tampil spesifikasi file voice chat, seperti pada tampilan gambar berikut ini



Gambar 4. Spesifikasi File voice chat

Selanjutnya klik tombol "PROSES TWKBL" untuk melakukan proses pengamanan terhadap file voice chat sehingga menghasilkan voice chatyang terenkripsi.Pada penelitian ini ditampilkan dalam bentuk nilai hexadecimal, serta akan muncu pertanyaan untuk proses penyimpanan file voice chat. Lebih jelas dapat dilihat pada gambar berikut ini



Gambar 5. Tampilan Form untuk Menyimpan File Voice Chat Terenkripsi

5. KESIMPULAN

Dari hasil penelitian yang dilakukan terhadap pengamanan voice chat pada perancangan aplikasi chatting menggunakan algoritma Tweakable Block Cipher, maka terdapat beberapa kesimpulan berdasarkan uraian yang telah tercantum pada bab-bab sebelumnya. Adapun kesimpulan dari hasil penelitian ini voice chat dengan format ogg dapat diamankan pada teknik kriptografi dengan melakukan pengambilan nilai hexadecimal dari file voicechat dengan menggunakan aplikasi HxD. Algoritma Tweakable Block Cipher dapat melakukan proses enkripsi terhadap voice chat dengan merubah nilai-nilai yang terdapat di dalam voice chat menjadi nilai Hexadecimal sehingga voice chat tidak mudah untuk di pahami. Aplikasi yang dirancang menggunakan Microsoft Visual Basic 2008 berdasarkan tahap-tahap proses enkripsi dari algoritma Tweakable Block Cipher sehingga dapat mempermudah proses pengamanan voice chat.

REFERENCES

[1] M. Liskov, R. L. Rivest, and D. Wagner, “Tweakable block ciphers,” J. Cryptol., 2011.
[2] S. Halevi and P. Rogaway, “A Tweakable Enciphering Mode,” 2003.
[3] W. Pan, F. Luo, and L. Xu, “Research and design of chatting room system based on Android Bluetooth,” in 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings, 2012.Sora, (2019,Feb.18). Pengertian Audio dan Media Audio Secara Lengkap [online]. Available: http://www.pengertianku.net/2014/11/pengertian-audio-dan-media-audio-secara-lengkap.html.
[4] M. Muttaqin, H. Sajati, and N. D. Retnowati, “PENERAPAN SISTEM KEAMANAN MENGGUNAKAN CRYPTOGRAPHY PADA APLIKASI CHATTING DENGAN MEMODIFIKASI ALGORITMA RIVEST SHAMIR ADLEMAN (RSA),” Compiler, 2014.