Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 4, August 2021, Page 288-294
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)
DOI 10.47065/josyc.v2i4.819

Implementasi Pisanc Chiper Untuk Autentikasi Voice Chat

Muhammad Fajar Rizky, Muhammad Syahrizal, Soeb Aripin

Fakultas Ilmu Komputer dan Teknologi Informasi, Prodi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: [1]mhd.frizky27@gmail.com, [2]msyahrizal86@gmail.com
Submitted: **26/07/2021**; Accepted: **22/08/2021**; Published: **31/08/2021**

Abstrak−Dalam melakukan pengamanan pesan suara informasi yang dikirimkan melalui jaringan internet tersebut harus diautentikasi keasliannya, isi datanya, waktu pengiriman, dan lain-lain. Untuk mencegah terjadinya manipulasi data oleh pihak-pihak yang tidak bertanggung jawab maka, terciptanya suatu kebocoran data yang berdampak negatif. Terjadinya kebocoran data yang kini masih kurang diwaspadai oleh kebanyakan pengguna. Hal ini bisa saja terjadi dikarenakan kurangnya keamanan pesan itu sendiri yang mengakibatkan masalah yang timbul dan juga kerugian oleh pihak otoriter tertentu. Solusi dalam pengamanan pesan suara tersebut menggunakan teknik kriptografi modern yang telah di kombinasikan dari pengkodean enkoding NRZI dan jaringan feistel oleh Pisanc Cipher, merupakan cara untuk menjaga keaslian dan keakuratan data atau autentikasi pada pesan suara. Berguna untuk mencari karekteristik enkripsi yang baik yaitu kebingungan dan difusi. Sehingga didapatkan keamanan dengan tingkat yang lebih tinggi. Dengan menggunakan metode Pisanc Cipher untuk mengamankan pesan suara, dapat menghasilkan suatau keamanan dan mengautentikasikan suatu data untuk mencegah terjadinya kebocoran data. Selain itu manfaat lain dari pengunaan metode Pisanc Cipher dapat menjaga suatu keaslian pesan suara.

Kata Kunci: Pengamanan; Pesan Suara; Kriptografi; Pisanc Cipher

Abstract−In securing voice messages, information sent through the internet network must be authenticated for its authenticity, data content, delivery time, and so on. To prevent data manipulation by irresponsible parties, the creation of a data leak that has a negative impact. The occurrence of data leaks that most users are still not aware of. This can happen due to the lack of security of the message itself which results in problems that arise and also losses by certain authoritarian parties. The solution in securing voice messages using modern cryptographic techniques that have been combined with NRZI encoding and the Feistel network by Pisanc Cipher, is a way to maintain the authenticity and accuracy of data or authentication in voice messages. It is useful to look for the characteristics of good encryption, namely confusion and diffusion. This results in a higher level of security. By using the Pisanc Cipher method to secure voice messages, it can generate security and authenticate data to prevent data leakage. In addition, another benefit of using the Pisanc Cipher method is to maintain the authenticity of voice messages.

Keywords: Security; Voicemail; Cryptography; Pisanc Cipher

1. PENDAHULUAN

Perkembanganteknologi dan informasi kini semakin memudahkan manusia dalam menyelesaikan pekerjaannya dengan cepat dan praktis. Dunia teknologi dan informasi yang kini jugabanyak di butuhkan dalam bidang militer, perkantoran juga personaldan lain sebagainya yangbisa dirasakan manfaatnya. Seperti halnya teknologi informasi yang berbasis pesan suara merupakan teknologi yang sedang berkembang pesat saat ini, dan juga memepengaruhi kemajuan dalam aspek kehidupan yang didukung oleh kemajuan teknologi tersebut untuk memepermudah mengakses data atau informasi. Dari manfaat yang dihasilkan oleh pesan suara, kini manusia lebih mudah terhubung dan berkomunikasi dengan cepat. Akan tetapi harus kita waspadai juga apabila pesan yang kita anggap penting bisa diketahui oleh pihak-pihak yang tidak bertanggung jawab yang akan menimbulkan kerugian bagi pemlilik dan pengguna pesan suara tersebut.

Terjadinya percakapan di dalam sebuah aplikasi menggunakan layanan pesan suara dimaksud dengan komunikasi. Komukasai merupakan proses pertukaran informasi yang dimana hasil dari komunikasi tersebut menghasilkan data atau informasi.Pesan suara yang terhubung dengan jaringan internet adalah (VoIp) *Voice Over Internet Protocol*yaitu pesan suara yang menggunakan suatu aplikasi yang menggunakan jaringan internet dimana pesan suara tersebut menggunakan suatu jaringan yang harus terhubung ke internet. Dalam hal ini harus kita perhatikan dengan cermat dikarenakan pesan yang dikirim dan yang dierima harus terhubung ke suatu jaringan internet. Pesan suara tersebutdiubah menjadi kode digital dan dialirkan melalui jaringan yang mengirimkan paket-paket data, dan bukan melalui sirkuit analog telepon biasa.

Informasi yang dikirimkan melalui jaringan internet tersebut harus diautentikasi keasliannya, isi datanya, waktu pengiriman, dan lain-lain. Untuk mencegah terjadinya manipulasi data oleh pihak-pihak yang tidak bertanggung jawab maka, terciptanya suatu kebocoran data yang berdampak negatif. Misalnya pada saat pengiriman pesan ke pihak tertentu ternyata isi dari pesan tersebut sudah tidak asli lagi ataupun sudah diketahui isi datanya dengan kata lain sudah dalam pengupingan atau pengawasan oleh orang ketiga. Terjadinya kebocoran data yang kini masih kurang diwaspadai oleh kebanyakan pengguna. Hal ini bisa saja terjadi dikarenakan kurangnya keamanan pesan itu sendiri yang mengakibatkan masalah yang timbul dan juga kerugian oleh pihak otoriter tertentu.

Konsep kriptografi klasik lebih rentan untuk di pecahkan oleh *cryptanalysis* untuk diambil data maupun informasinya. Berbeda dengan kriptografi modern yang dimana menggunakan pengamanan dengan tingkat kerumitan yang lebih tinggi sehingga dapat menjaga keaslian dan kerahasiaan pesan dengan baik. Maka dari itu *voice chat* yang diekripsi lebih susah untuk dipecahkan oleh *cryptanalysis*. Oleh karena itu lebih aman apabila menjaga keaslian ataumengautentikasi*voice chat* dengan menggunakan teknik kriptografi modern yang telah di

Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 4, August 2021, Page 288-294
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)
DOI 10.47065/josyc.v2i4.819

kombinasikan dari pengkodean enkoding NRZI dan jaringan feistel oleh Pisanc Chiper. Pisanc Chiper merupakancara untuk menjaga keaslian dan keakuratan data atau autentikasi pada pesan suara. Disini penulis menggunakan algoritma Pisanc Chiper yang dimana algoritma tersebut menggunakan kombinasi anatara NRZI dan juga jaringan feistel berguna untuk mencari karekteristik enkripsi yang baik yaitu kebingungan dan difusi.Sehingga didapatkan keamanan dengan tingkat yang lebih tingi.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptograf (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi dikarenakan setiap software pasti memiliki kelebihan dan kelemahannya masing-masing [2].

2.2 Algoritma Pisanc Chiper

Algoritma PISANC adalah algoritma yang mencari karakteristik enkripsi yang baik yaitu kebingunggan, difusi, dan jaringan feistel. Karakteristik-karakteristik ini dipenuhi dengan pengokodean NRZI yang biasa ditemukan dilapisan OSI dan ekstensi lapisan feistel yang disebut triple feistel. Gabungan kedua ide dasar ini sudah dapat memenuhi karakteristik kebinggungan. Sehingga proses enkripsi tidak mudah di kenali oleh pihak yang tidak bertanggug jawab.

Enkripsi PISANC secara keseluruhan bekerja dengan terlebih dahulu mengenkripsi plainvoice dengan cara menggunakan enkoding NRZI dan kemudian diteruskan dengan mengenkripsi hasilnya dengan perputaran triple feistel. Sedangkan fungsi dari triple feistel disini bertujuan agar plainvoice yang telah di enkripsikan menjadi kode oleh NRZI menjadi berhamburan dan menyebabkan kebingungan dan difusi apabila cryptanalis ingin memecahkan dan membuka kunci tersebut. Enkripsi PISANC menggunakan kunci yang sama mulai dari 1 bit hingga 1 GB. Yang dimana pengkodean NRZI hanya membutuhkan satu kunci dengan perlulangan hingga 5 kali putaran sedangkan triple feistel membutuhkan kunci sebanyak dua kali putaran [5].

2.3 Voice Chat

Cara bahasa pengertian chatting adalah suatu pesan instan dalam teknologi jaringan komputer untuk mengirimkan informasi ke pengguna lain yang terhubung melalui koneksi internet. Saat ini, istilah chatting tidak hanya ditemukan pada pengguna email messenger saja, karena sudah banyak aplikasi chatting yang tersedia untuk pengguna smartphone. *Voice Chat* merupakan suatu program di Internet untuk berkomunikasi langsung sesama pengguna internet yang sedang *online* / yang sedang sama-sama menggunakan Internet. Komunikasi ini dapat berupa teks (*text chat*) ataupun suara (*voice chat*). Atau definisi *chatting* adalah suatu pesan instant ataupun instant messaging di sebuah teknologi jaringan komputer yang mengijinkan pemakainya untuk mengirimkan pesan ke pengguna lain yang tersambung dalam sebuah jaringan komputer ataupun internet [10].

3. HASIL DAN PEMBAHASAN

Sebuah pesan suara yang bersifat rahasia sangat rentang terhadap pengambilan data oleh pihak yang tidak berhak akan pesan tersebut demi keuntungan pribadinya ataupun kelompok. Kurangnya tingkat keamanan seperti penyandian dan penyembunyian terhadap pesan suara tersebut memudahkan pihak-pihak yang tidak tekait mengambilnya, terutama pada pesan suara yang belum disandikan.

Pesan suara rahasia yang belum disandikan jika berada ditangan yang salah, maka dengan sangat mudah dianalisa dan diambil datanya sehingga dapat merugikan pihak yang memiliki pesan suara rahasia tersebut. Maka hal ini dapat di minalisir dengan teknik kriptografi.

Berdasarkan rumusan masalah pada bab sebelumnya, masalah yang terjadi adalah bagaimana sebuah pesan suara yang belum disandikan dapat diamankan dan disandikan dengan teknik kriptografi. Teknik kriptografi akan mengacak data suara rahasia menjadi data yang tidak dapat dipahami ketika pihak yang tidak bertanggung jawab atau *cryptanalis*.

Maka metode yang digunakan dalam pembahasan ini adalah sebuah algoritma kriptografi Pisanc Cipher. Pisanc Cipher akan melakukan enkripsi terhadap pesan suara yang akan diamankan menggunakan pengkodean NRZI terdahulu dan proses selanjutnya menggunakan metode triple feistel. Dimana metode tersebut akan di enkripsikan oleh algoritma Pisanc Cipher.

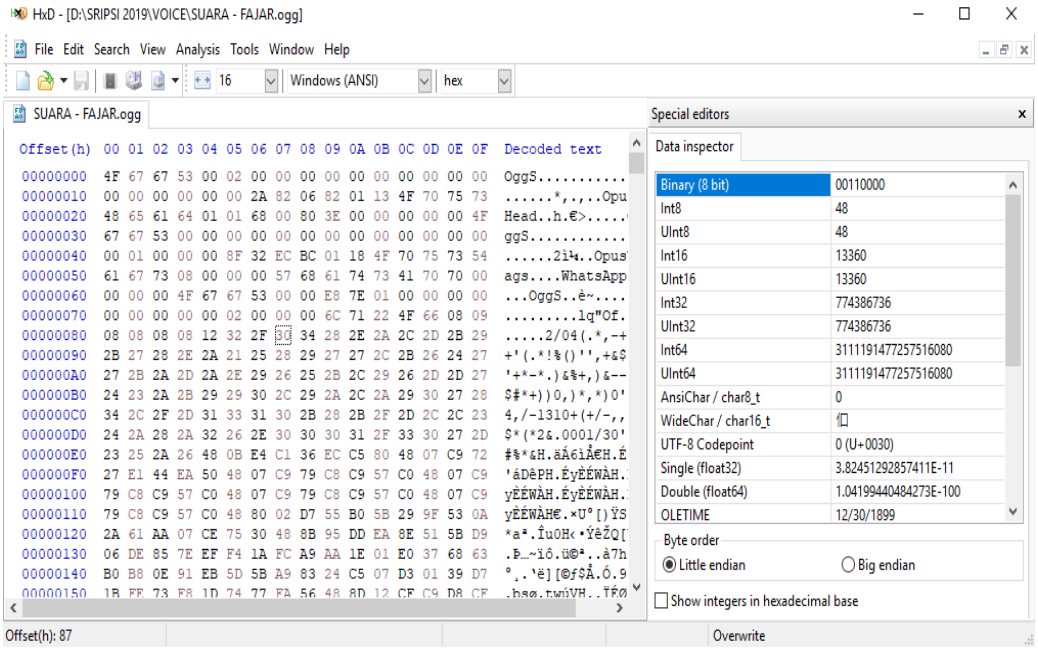
3.1 Penerapan Algoritma Pisanc Cipher

Proses penerapan algoritma Pisanc Cipher adalah proses yang menggabungkan anatara NRZI dan triple feistel yang dimana dengan mengkodekan terdahulu suara dengan NRZI kemudian dilanjukan mengenkripsi hasil

Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 4, August 2021, Page 288-294
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)
DOI 10.47065/josyc.v2i4.819

hasilnya dengan triple feistel. Triple fiestel melakukan putaran yang membuat kebingungannya dengan penerapan yang dimana melakukan putaran sampai 10 kali putaran. Maka yang akan dilakukan yaitu dari sebuah jenis pesan *voice chat* yang digunakan sebagai contoh untuk menerapkan algoritma Pisanc Cipher, penulis menggunakan jenis voice chat dari aplikasi

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

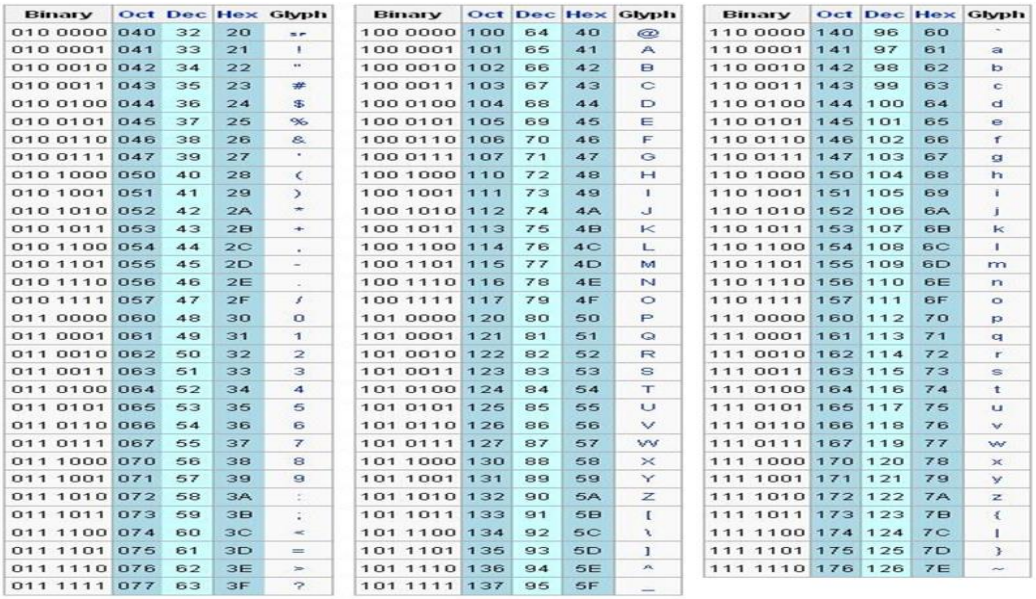


Gambar 1. Tampilan aplikasi HxD

Selanjutnya nilai yang akan digunakan untuk penerapan algoritma PISANC sebagai landasan dasar untuk mengenkripsi *voicechat* nantinya sebagai mana yang telah di tentukan nilai biner dari *voicechat* tersebut, penulis menggambil nilai sampel, sebagai berikut:

[2B 27 28 2E 2A 21 25 28 29 27 27 2C 2B 26 24 27 27 2B 2A 2D 2A 2E 29 26]

Maka Proses selanjutnya adalah menubah bilangan nilai bentuk biner kedalam betuk hexa desimal dengan menggunakan tabel ascii, aapun tabel ascii sebagai berikut;



Binary	Oct	Dec	Hex	Glyph
010 0000	040	32	20	sp
010 0001	041	33	21	!
010 0010	042	34	22	"
010 0011	043	35	23	#
010 0100	044	36	24	$
010 0101	045	37	25	%
010 0110	046	38	26	&
010 0111	047	39	27	'
010 1000	050	40	28	(
010 1001	051	41	29	)
010 1010	052	42	2A	*
010 1011	053	43	2B	+
010 1100	054	44	2C	,
010 1101	055	45	2D	-
010 1110	056	46	2E	.
010 1111	057	47	2F	/
011 0000	060	48	30	0
011 0001	061	49	31	1
011 0010	062	50	32	2
011 0011	063	51	33	3
011 0100	064	52	34	4
011 0101	065	53	35	5
011 0110	066	54	36	6
011 0111	067	55	37	7
011 1000	070	56	38	8
011 1001	071	57	39	9
011 1010	072	58	3A	:
011 1011	073	59	3B	;
011 1100	074	60	3C	<
011 1101	075	61	3D	=
011 1110	076	62	3E	>
011 1111	077	63	3F	?

Binary	Oct	Dec	Hex	Glyph
100 0000	100	64	40	@
100 0001	101	65	41	A
100 0010	102	66	42	B
100 0011	103	67	43	C
100 0100	104	68	44	D
100 0101	105	69	45	E
100 0110	106	70	46	F
100 0111	107	71	47	G
100 1000	110	72	48	H
100 1001	111	73	49	I
100 1010	112	74	4A	J
100 1011	113	75	4B	K
100 1100	114	76	4C	L
100 1101	115	77	4D	M
100 1110	116	78	4E	N
100 1111	117	79	4F	O
101 0000	120	80	50	P
101 0001	121	81	51	Q
101 0010	122	82	52	R
101 0011	123	83	53	S
101 0100	124	84	54	T
101 0101	125	85	55	U
101 0110	126	86	56	V
101 0111	127	87	57	W
101 1000	130	88	58	X
101 1001	131	89	59	Y
101 1010	132	90	5A	Z
101 1011	133	91	5B	[
101 1100	134	92	5C	\
101 1101	135	93	5D	]
101 1110	136	94	5E	^
101 1111	137	95	5F	_

Binary	Oct	Dec	Hex	Glyph
110 0000	140	96	60	`
110 0001	141	97	61	a
110 0010	142	98	62	b
110 0011	143	99	63	c
110 0100	144	100	64	d
110 0101	145	101	65	e
110 0110	146	102	66	f
110 0111	147	103	67	g
110 1000	150	104	68	h
110 1001	151	105	69	i
110 1010	152	106	6A	j
110 1011	153	107	6B	k
110 1100	154	108	6C	l
110 1101	155	109	6D	m
110 1110	156	110	6E	n
110 1111	157	111	6F	o
111 0000	160	112	70	p
111 0001	161	113	71	q
111 0010	162	114	72	r
111 0011	163	115	73	s
111 0100	164	116	74	t
111 0101	165	117	75	u
111 0110	166	118	76	v
111 0111	167	119	77	w
111 1000	170	120	78	x
111 1001	171	121	79	y
111 1010	172	122	7A	z
111 1011	173	123	7B	{
111 1100	174	124	7C	|
111 1101	175	125	7D	}
111 1110	176	126	7E	~

Gambar 2. Kode ASCII

Nilai Hexadecimal : **Kelompok A = 2B 27 28 2E 2A 21 25 28**
Kelompok B = 29 27 27 2C 2B 26 24 27
Kelompok C = 27 2B 2A 2D 2A 2E 29 26

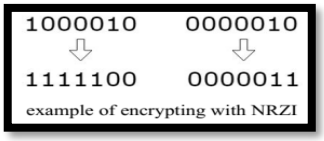
Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 4, August 2021, Page 288-294
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)
DOI 10.47065/josyc.v2i4.819

Nilai Biner:
A = 00101011001001110010100000101110001010100010000100100101001010000
B = 00101001001001110010011100101100001010110010011000100100 00100111
C = 00100111001010110010101000101101001010100010111000101001001001110

Proses pembangkitan kunci pada setiap fungsi pada algoritma Pisanc Cipher dilakukan berdasarkan karakter yang dimasukan oleh pengguna sebagai kata atau kalimat kunci. Sebagai contoh pembangkit kunci menggunakan karakter "**FAJAR RIZKY**". Adapun jumlah panjang kunci yaitu sebesar 64 bit, jika melebihi maka yang digunakan hanya 64 bit saja untuk bit selanjutnya tidak dianggap. Jika kurang dari 64 bit maka dilakukan penambahan bit nol hingga mencukupi jumlah 64 bit. Pada penelitian ini penulis menggunakan karater kunci yaitu:

Karakter : **FAJAR RIZKY**
Nilai Hexadecimal : **46 41 4A 41 52 20 52 49 5A 4B 59**
NilaiBiner : **01000110 01000001 01001010 01000001 01010010 00110010 01010010 01001001**
01011010 01001011 01011001
Dari nilai biner diatas maka biner yang digunakan hanya 64 bit yaitu :
01000110 01000001 01001010 01000001 01010010 00110010 01010010 01001001

Selanjutnya melakukan proses encoding NRZI dengan cara jika biner kiri bernilai satu maka lakukan perubahan terhadap masing-masing biner disebelah kanannya, jika sebelah kiri bernilai nol maka lakukan perubahan terhadap biner setelah menemukan angkat satu disebelahkanannya, lebih jelasnya dapat dilihat pada gambar berikut ini



Gambar 3. Enkoding NRZI

Berikut hasil perubahan nilai blok biner sesuai dengan metode NRZI.
A = 00101011001001110010100000101110001010100010000100100101001010000
Menjadi
00110100110110001101011111010001110101011100111011010111010111
B = 00101001001001110010011100101100001010110010011000100100 00100111
Menjadi
00110110110110001101100011010011110101001101100111011011011000
C = 00100111001010110010101000101101001010100010111000101001001001110
Menjadi
00111000110101001101010111010010110101011101000111010110011011001

Berdasarkan penerapan NRZI diatas maka didapatkan nilai biner *Plainvoice*, yang dimana nilai biner tersebut akan dilakukan ekstrasi lagi dengan triple feistel yang akan melakukan proses perputaran dengan dibagi tiga feistel setiap putaran. Putaran tersebut maka yang akan dihasilkan pengamanan hingga tingkat kebingungan dan difusi, adapun nilai dari proses NRZI tersebut yaitu sebagai berikut:

A_0 = 00110100 11011000 11010111 11010001 11010101 11001110 11011010 11010111
B_0 = 00110110 11011000 11011000 11010011 11010100 11011001 11011011 11011000
C_0 = 00111000 11010100 11010101 11010010 11010101 11010001 11010110 11011001

Setelah dilakukan proses penerapan pada NRZI maka di dapatkanlah hasil binernya. Dimana nilai biner tersebut akan melakukan ekstrasi menggunakan teknik triple feistel yang memelakukan proses penerapannya dibagi menjadi tiga blok setiap putarannya. Dan putaran tersebut akan di XOR kan Maka selanjutnya akan dilakukan proses pemutaran nilai biner sampai 10 x putaran. Adapun proses penerapannya sebagai berikut :

1. Putaran Pertama (1)
   a. Mencari Nilai Kunci *Function 1* (**F_1**): Proses **XOR** biner "B_0" dengan biner "Kunci"
   $B_0 \oplus$ Kunci = F1
   00110110110110001101100011010011111010100110110011101101111011000
   01000110010000010100101001000001010100100011001001010010010001 ⊕
   01110000100110011001001010010010100001101110101110001001100100001
   b. Mencari Nilai **A_0'** dengan melakukan proses **XOR** biner "A_0" dengan biner "Function 1"
   $A_0 \oplus F_1$ = **A_0'**
   00110100110110001101011111010001110101011100111011011010111010111
   01110000100110011001001010010010100001101110101110001001100100001 ⊕
   01000100010000010100010101000011010100110010010101010011010000110

Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 4, August 2021, Page 288-294
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)
DOI 10.47065/josyc.v2i4.819

c. Mencari Nilai Kunci *Function 2* (**F_2**): Proses **XOR** biner "C_0" dengan biner "Kunci"
$C_0 \oplus$ Kunci = **F_2**
00111000110101001101010111010010110101011101000111010110110011001
01000110010000010100101001000001010100100011001001010010010010001 ⊕
01111110100101011001111110010011100001111110001110000100100100000

d. Mencari Nilai **B_0'** dengan melakukan proses **XOR** biner "B_0" dengan biner "Function 2"
$B_0 \oplus F_2 = B_0$'
00110110110110001101100011010011110101001101100111011011110110000
01111110100101011001111110010011100001111110001110000100100100000 ⊕
01001000010011010100011101000000010100110011101001011111010010000 0011101001011111 01001000

e. Mencari Nilai **C_0'** masih bernilai sama dengan C_0
C_0'= C_0
C_0'=00111000110101001101010111010010110101011101000111010110110011

f. Hasil Proses Putaran Pertama (1)
A0'= 01000100010000010100010101000011010100110010010101010011010001110
B0' = 01001000010011010100011101000000010100110011101001011111010010000
C0' = 00111000110101001101010111010010110101011101000111010110110011001

2. Putaran Kedua (2)
a. Tentukan nilai **A_1, B_1, C_1** dengan format sebagai berikut
A0' = B1
B0' = C1
C0' = A1
Berdasarkan format diatas maka nilai **A1, B1, C1,** sebagai berikut:
A1 = 00111000110101001101010111010010110101011101000111010110110011001
B1 = 01000100010000010100010101000011010100110010010101010011010001110
C1 = 01001000010011010100011101000000010100110011101001011111010010000

b. Mencari Nilai Kunci *Function 1* (**F_1**): Proses **XOR** biner "B_1" dengan biner "Kunci"
$B_1 \oplus K =$ **F_1**
01000100010000010100010101000011010100110010010101010011010001110
01000110010000010100101001000001010100100011001001010010010010001 ⊕
00000010000000000000111100000010000000010001011100000000100001111

c. Mencari Nilai **A_1'** dengan melakukan proses **XOR** biner "A_1" dengan biner "Function 1"
$A_1 \oplus$ F1 = **A_1'**
00111000110101001101010111010010110101011101000111010110110011001
00000010000000000000111100000010000000010001011100000000100001111 ⊕
00011010110101001101101011010000110101001100011011010111110101 10

d. Mencari Nilai Kunci *Function 2* (**F_2**): Proses **XOR** biner "C_1" dengan biner "Kunci"
$C_1 \oplus K =$ **F_2**
01001000010011010100011101000000010100110011101001011111010010000
01000110010000010100101001000001010100100011001001010010010010001 ⊕
00001110000011000000110100000001000000010000100000001101000000001

e. Mencari Nilai **B_1'** dengan melakukan proses **XOR** biner "B_1" dengan biner "Function 2"
$B_1 \oplus F_2 =$ **B_1'**
01000100010000010100010101000011010100110010010101010011010001110
00001110000011000000110100000001000000010000100000001101000000001 ⊕
01001010010011010100100001000011010100100010110101010111100100 0111

f. Mencari Nilai **C_1'** masih bernilai sama dengan C_1
C_1'= C_1
C_1'= 01001000010011010100011101000000010100110011101001011111010010000

g. Hasil Putaran Kedua (2)
A_1'= 00011010110101001101101011010000110101001100011011010111110101 10
B_1'= 01001010010011010100100001000011010100100010110101010111100100 0111
C_1'= 01001000010011010100011101000000010100110011101001011111010010000

Lakukan proses tersebut berulang hingga pada proses ke – 10 (sepuluh). Dari proses XOR yang telah dilakukan sampai mencapai 10 x putaran tersebut, Maka nilai yang dihasilkan oleh *ciphervoice chat* pada algoritma Pisanc adalah :

01001001 01001101 01000111 01000000 01010010 00101010
01011111 01001000 00011011 11010100 11011010 11010000
11010100 11000110 11010100 11010110 01001011 01001101
01001000 01000011 01010010 00101101 01011110 01000111

Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 4, August 2021, Page 288-294
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)
DOI 10.47065/josyc.v2i4.819

Dari hasil XOR yang dilakukan, maka menghasilkan nilai Ciphervoice. Dan selanjutnya akan di rubah menjaadi nilai hexadesimal. Adapun nilai yang di hasilkan yaitu sebagai berikut:

49 4D 47 40 52 2A 4F 48 1B D4 DA D0 D4 C6 D4 D6 4B 4D 48 43 52 2D 5E 47

3.2 Proses Pengujian

Proses pengujian dalam penelitian ini dilakukan terhadap beberapa file video yang berbeda, berikut tabel hasil pengujian yang telah dilakukan:

Tabel 1. Hasil Pengujian

No.	Spesifikasi File Video Asli	Kode Hash File Video Asli	Perubahan yang dilakukan	Spesifikasi File Video Palsu	Kode Hash File Video Asli
1	NamaFile: ALDO Ukuran: 654 Kb Durasi: 01:00 Jenis: *.mpg	E4A40F15AE54AA E07B72B2E0611AD CFA	Memotong durasi video	NamaFile: ALDO Ukuran: 580 Kb Durasi: 00:55 Jenis: *.mpg	A4E40F15AE54 2AE32B723450 611A5CCB
2.	NamaFile: aldo1 Ukuran: 693 Kb Durasi: 00:57 Jenis: *.mpg	0C00D49F80EFA78 5DDCAD01A0FFFF 700	Menambah kontras video	NamaFile: aldo1 Ukuran: 720 Kb Durasi: 00:57 Jenis: *.mpg	BA2DDA481FD D08EDDC8AF0 EA00A1FCA7
3.	NamaFile: aldo2 Ukuran: 820 Kb Durasi: 01:20 Jenis: *.mpg	DD0AC7F9C00E1A AF5CD4AE0DAC0 ABB2E0	Menambah watermark didalam video	NamaFile: aldo2 Ukuran: 898 Kb Durasi: 01:20 Jenis: *.mpg	0C00D49F80EF A785DDCAD01 A0FFEE700

4. KESIMPULAN

Dari hasil penelitian yang dilakukan penulis, maka dihasilkan suatu kesimpulan yang memberikan terobosan baru pada pengguna layanan pesan suara atau *voice chat* pada Whattshapp, yang dimana nantinya dapat memberikan kontribusi bagi kenyamanan pengguna layanan *voice chat*. adapun kesimpulan Teknik autentikasi *voice chat* merupakan teknik yang bertujuan untuk membutikan keaslian suatu pesan suara dengan merubah bilangan biner kedalam menjadi bentuk digital. Teknik algoritma Pisanc Cipher merupakan teknik yang digunakan untuk mengautentikasi *voice chat* yang menggabungkan antara NRZI dan triple feistel.

REFERENCES

[1] Usman, "https://www.pengertianmenurutparaahli.net/pengertian-implementasi/," Pengertian Implementasi menurut para ahli, 2002. [Online].
[2] D. N. Novi and E. W. Anang, "PENERAPAN TEKNIK KRIPTOGRAFI STEAM - CHIPER UNTUK PENGAMANAN BASIS DATA," Jurnal Basis Data, vol. Vol. 6, no. No.1, pp. 2-22, 201.
[3] L. Mokh. and A. Putra, "https://docplayer.info/50630911-Enkripsi-dan-dekripsi-pesan-suara-dengan-metode-algoritma-serpent-menggunakan-visual-basic-6-0.html," ENKRIPSI DAN DEKRIPSI PESAN SUARA DENGAN METODE ALGORITMA SERPENT MENGGUNAKAN VISUAL BASIC 6.0. [Online].
[4] P. Arif and N. Nurdin , "ANALISA DAN IMPLEMENTASI KRIPTOGRAFI PADA PESAN RAHASIA MENGGUNAKAN ALGORITMA CIPHER TRANSPOSITION," Jurnal Elektronik Sistem Informasi dan Komputer, vol. Vol.3, no. No.1, pp. 2-11, Januari-Juni 2017.
[5] F. Lazuadi, "http://informatika.stei.itb.ac.id," Kriptografi PISANC CHIPER, 05. 2018-2019. [Online]. [Accessed 01-2019/makalah1 Kriptografi-2019-05.].
[6] E. H. R. D. W. U. d. R. R. S. C. A. Sari, "Penyembunyian Data Untuk Seluruh Ekstansi File Mengguanakan Kriptografi Vernam Cipher dan Bit Shiffing," Journal of Applied Intelligent System, vol. vol.1, pp. 179-190, 2016.
[7] S. M. Melwin Syafrizal, "https://journal.amikom.ac.id/index.php/KIDA/article/download/4475/2170," journal.amikom.ac, pp. 2-13.
[8] s. Fharis , "http://harissitumeangdetektif.apa-itu-cipher-code.html," blogspot.com, 07 2013. [Online].
[9] jakfar, "https://www.scribd.com/document/389239727/Pengertian-Autentikasi," [Online].
[10] "https://www.maxmanroe.com/vid/teknologi/pengertian-chatting.html," Pengertian Chatting dan Contohnya, Fungsi, Serta Manfaatnya. [Online].
[11] S. N, "http://www.pengertianku.net/2015/02/pengertian-chatting-dan-fungsinya-secara-lebih-jelas.html," pengertian-chatting-dan-fungsinya-secara-lebih-jelas., 02 2015. [Online].
[12] D. P. 2, "https://www.dosenpendidikan.com," pengertian-chatting-fungsi-manfaat-dampak/, 10 02 2019.
[13] E. Sutanta, Pengantar Teknologi Informasi, Graha Ilmu., Yogyakarta, 2005.

Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 4, August 2021, Page 288-294
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)
DOI 10.47065/josyc.v2i4.819

[14] K. L.V. , "Available:http://www.vbtutor.net/index.php/visual-basic-2010-tutorial/," Visual Basic 2010 Tutorial [online], 6 oktober 2012. [Online].
[15] HEADER AKIB, "Haedar Akib/ Jurnal Administrasi Publik," IMPLEMENTASI KEBIJAKAN:, vol. Volume 1 , no. No. 1 , pp. 2-11, Thn. 2010.