Jurnal Teknologi Komputer dan Informasi (JUTEKINF)
Vol. 14, No. 1 Januari - Juni 2026, Hal. 25-36

Analisa Kriptografi Metode *Word Auto Key Encryption* (WAKE) Terhadap Keamanan Pesan *Chatting*

Lisda Juliana Pangaribuan*[1], Catra Indra Cahyadi [2], Sakaria Efrata Ginting[3]
[1,3]Program Studi Rekayasa Perangkat Lunak, Universitas Mandiri Bina Prestasi [2]Program Studi Teknik Navigasi Udara Poltekbang Medan
*e-mail: lisdajuliana@gmail.com[1], catraindracahyadi@gmail.com[3], sakariaginting1983@gmail.com[3]

Abstract

One of internet facilities widely used by the public is chatting. However, information hacking often occurs when sending or forwarding information through chat applications, making people often receive hoax information. This study aims to analyze the security of chat messages using the Word Auto Key Encryption (WAKE) Cryptography Method using a 128-bit key, 32-bit plaintext. The results show that S-Box Table of the WAKE algorithm is flexible and different for each round, the keys formed are also different, depending on the number of rounds (N) so that messages encrypted with the same key are also different. If cryptanalyst knows the encrypted message, the original message cannot be known because the keys used are different. For 10-round chat message encryption, binary and hexadecimal numbers remain the same, but the 20-round encryption is different. Even if a cryptanalyst knows the encrypted message, the original message cannot be detected because the keys used are different. This makes WAKE cryptography safe for sending chat messages on social media. Besides being secure, encryption and decryption process is also fast, taking only 0.1 seconds.

***Keywords**: Stream_Cipher, Substitution_Box, WAKE_Algorithm, XOR_Operation, Chatting*

Abstrak

Salah satu fasilitas internet yang banyak digunakan oleh masyarakat adalah *chatting*. Namun peretasan informasi sering terjadi pada saat mengirim atau meneruskan informasi melalui aplikasi *chat* membuat masyarakat sering menerima informasi *hoax*. Penelitian ini bertujuan menganalisa keamanan pesan *chatting* menggunakan Kriptografi Metode *Word Auto Key Encryption* (WAKE) menggunakan kunci 128 bit, plaintext 32 bit. Hasil penelitian menunjukkan Tabel S-Box algoritma WAKE bersifat fleksibel dan berbeda-beda untuk setiap putaran, kunci yang dibentuk juga berbeda beda, tergantung pada jumlah putaran (N) sehingga pesan yang dienkripsi dengan kunci yang sama juga berbeda. Untuk enkripsi pesan chat 10 putaran untuk bilangan biner dan hexadesimal tetap sama, namun untuk 20 putaran enkripsi yang dibentuk berbeda. Jika *cryptanalyst* mengetahui pesan yang telah dienkripsi, pesan asli belum dapat diketahui karena kunci yang digunakan berbeda beda.Hal ini membuat kriptografi Metode WAKE aman digunakan untuk pengiriman pesan *chatting* pada media sosial. Selain aman proses enkripsi dan dekripsi juga cepat, hanya 0,1 detik.

Kata Kunci: *Stream_Cipher, S_Box*, Algoritma_WAKE, Operasi_XOR, *Chatting*

1. PENDAHULUAN

Perkembangan teknologi internet yang dapat menyajikan dan mempersatukan berbagai jenis data digital, media foto, adalah citra atau image (Azzura & Pratiwi, 2023). Salah satu aplikasi *Internet Of things* (IoT) yang dinikmati oleh masyarakat adalah *chatting.*

Chatting merupakan aplikasi yang digunakan untuk bertukar informasi antar sesama *user* melalui internet menggunakan beberapa jejaring social seperti *Facebook, Yahoo Massenger* maupun media *Chatting* lainnya (Arifin & Mufti, 2018). Masalahnya, pengiriman informasi melalui internet mempunyai risiko di bidang keamanan. Peretasan informasi pada *chatting* sering terjadi pada saat mengirim atau meneruskan informasi melalui aplikasi *chat* membuat masyarakat sering menerima informasi *hoax*. (Pangaribuan & Sitanggang, 2022). Kasus

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887

kebocoran data pada Instagram di 2019 sekitar 49juta, *Database* yang berisi 49 juta informasi influencer, selebritas, dan merek di platform Instagram telah tersebar secara daring, Tahun 2023 ada sekitar 235 juta informasi pengguna *Twitter* terekspos di forum *hacker online*. *CyberNews* pada *page* pertama menginformasikan kebocoran data, ada sekitar 63GB database diekspos. Kebocoran data meliputi nama pengguna, email, dan nomor telepon dengan harga USD 200.000 (Putri Nugroho et al., 2024). Untuk melindungi informasi tersebut agar tidak dirusak,diubah atau dicuri oleh pihak yang tidak berkewenangan dikembangkanlah algoritma keamanan informasi (Panjaitan & Pangaribuan, 2021). Keamanan informasi harus memenuhi 4(empat) aspek utama yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), Nir-penyangkalan (*non-repudiation*) dan otentikasi(*authentication*) (Juliana Pangaribuan et al., 2023) (Febrianto & Zulianto, 2024). Keamanan pengiriman informasi melallui internet terletak pada distribusi kunci, jika kunci sudah diketahui oranglain maka seluruh informasi yang dikirim dapat diketahui (Pangaribuan & Simbolon, 2017). Selain kekuatan kunci, hal yang perlu dipertimbangkan dalam keamanan pengiriman pesan adalah kecepatan. Metode yang sering digunakan untuk pengamanan data adalah steganografi dan kriptografi(Andara et al., 2022). Steganografi adalah salah satu teknik untuk menyembunyikan informasi ke dalam suatu data tanpa menampakkan keberadaan informasi tersebut dan menimbulkan kecurigaan bahwa data yang disisipi dengan informasi tersebut telah berubah. Implementasi steganografi saat ini telah menggunakan media digital sebagai media penampung atau penyembunyi pesan, salah satunya media gambar (citra digital). Umumnya pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial(Azzura & Pratiwi, 2023).

Sedangkan Kriptografi merupakan seni untuk mengamankan informasi supaya hanya penerima aslinya yang dapat membaca dan memahaminya sehingga informasi yang bersifat rahasia dan dikirim melalui jaringan internet tidak dapat diketahui serta dimanfaatkan oleh pihak yang tidak berkepentingan(Juliana Pangaribuan et al., 2023). Kriptografi dengan algoritma yang memiliki komputasi rendah perlu diterapkan untuk menjaga keamanan data pada pengaplikasian IoT untuk menjaga keamanan proses transaksi data dan menjaga keaslian asal suatu data (Febrianto & Zulianto, 2024). Beberapa penelitian menggunakan algoritma Kriptografi dalam *chatting* adalah *Caesar Cipher*, dimana pesan *chat* dapat dienkripsi menggunakan teknik proses end-to-end yang membuktikan enkripsi dan deskripsi pesan dapat dilakukan saat *chatting* (Andrea et al., 2023).

Semetara menurut penelitian "Integrasi Algoritma RSA dan Teknologi Kriptografi Kuantum dalam Keamanan Aplikasi Web *Chatting*", pemakaian minimum RSA 2048-bit memberikan margin keamanan yang memadai terhadap serangan *brute force*, sementara AES-GCM memastikan kerahasiaan sekaligus integritas/perotentikasian pesan pada lapisan simetris sehingga menghasilkan rancangan sistem yang efektif, kompatibel dengan tumpukan web modern, dan tangguh terhadap skenario serangan yang diuji (Okario et al., 2026). Penelitian lain mengatakan Keamanan data dalam komunikasi daring merupakan isu krusial, karena menyimpan data chat pribadi pengguna di basis data *Firebase* di *Cloud* (Darmawan & Windarto, 2018). Algoritma RC4+ berhasil mengenkripsi dan dekripsi data *chat* dengan waktu rata-rata enkripsi 0,30 ms dan dekripsi 0,19 ms. Selain itu, *Avalanche Effect* yang dihasilkan sebesar 3,009%, menunjukkan efektivitas algoritma dalam menjaga integritas data.(Kumala et al., 2025).

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887

Dalam penelitiannya terhadap pesan chat aplikasi whatsapp, Lisda Juliana Pangaribuan mengatakan Aloritma GOST sangat baik karena proses enkripsi dan dekripsi cukup panjang dan rumit karena melalui 32 putaran yang memproses 64 bit pesan, namun algoritma ini memiliki kelemahan yaitu proses pembentukan kunci sangat sederhana (Pangaribuan & Sitanggang, 2022).Walaupun informasi chat yang dikirim melalui media sosial udah di enkripsi menggunakan metode *END TO END*, tetapi masih dapat disadap, itulah sebabnya dalam penelitian ini digunakan kriptografi dengan algoritma WAKE untuk keamanan pesan *chatting*. WAKE adalah salah satu algoritma stream cipher yang cepat implementasinya dalam perangkat lunak menggunakan kunci 128 bit, plaintext 32 bit dan sebuah tabel 256 x 32 bit. Dalam algoritmanya, metoda ini menggunakan operasi XOR, AND, OR dan Shift Right (M. D. Sinaga et al., 2019). Keunikan metode WAKE terletak pada proses pembentukan tabel S-Box dan proses pembentukan kunci. Proses enkripsi dan dekripsi diperoleh melalui operasi XOR dari plaintext dan kunci untuk menghasilkan ciphertext dan operasi XOR dari *ciphertext* dan kunci untuk menghasilkan plaintext (Eddy & Pahlevi, 2014). Metode WAKE merupakan cukup rumit dan sulit untuk dikerjakan secara manual karena algoritmanya yang cukup panjang dan kompleks(Jaya & Juanita, 2018). Beberapa peneliti sudah melakukan penelitian menggunakan algoritma WAKE yang menyatakan bahwa algoritma WAKE cocok dalam mengenkripsi semua teks karakter(Silalahi & Ginting, 2020).

Stream Cipher adalah algoritma kriptografi dari *symetric key* digunakan untuk melakukan ekripsi dan deskrispi menggunakan XOR dan XNOR sehingga meghasilkan ciphertext. *Stream Cipher* melakukan proses ekripsi dan deskripsi lebih cepat dibandingkan block cipher. Kelebihannya panjang plainteks tak terbatas tetapi masih memiliki kelemahan pada pengacakan KSA (Key Scheduling Algorithm)(Milian & Sulistyo, 2023).

2. METODE

Penelitian ini bersifat deskriptif yang dilakukan dengan studi literatur dan ekperimen dengan pesan chat menggunakan metode *Word Auto Key Encryption* (WAKE) untuk mengetahui hasil enkripsi dan dekripsi pesan *chatting*. Jenis data yang digunakan hanya pesan dalam bentuk teks.

Tahapan Penelitian

Penelitian ini dimulai dengan identifikasi masalah yaitu dengan mengirim pesan chat, kemudian pengumpulan data, analisis data, lalu membangun sistem kemudian melakukan pengujian terhadap sistem (Panjaitan & Pangaribuan, 2021). Pada penelitian ini algoritma Kriptografi yang digunakan adalah algoritma WAKE dengan melakukan langkah-langkah: Proses pembentukan Tabel S-Box, Proses pembentukan Kunci, Proses Enkripsi dan Proses Dekripsi.(Silalahi & Ginting, 2020). (Prasetyo & Ariyani, 2018).

a. Proses Pembentukan Tabel S-Box (N. Sinaga, 2019).

1. Inisialisasi nilai TT[0] … TT[7] :

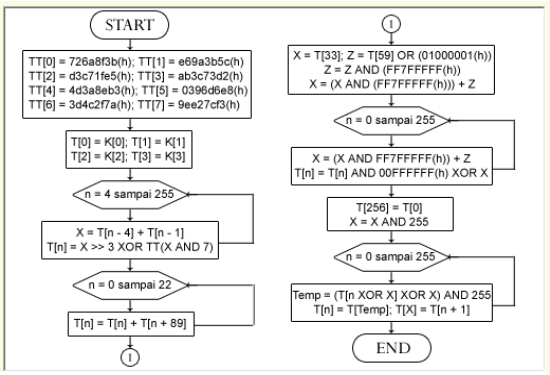
TT[0] : 726a8f3b (dalam heksadesimal)	TT[4] : 4d3a8eb3 (dalam heksadesimal)
TT[1] : e69a3b5c (dalam heksadesimal)	TT[5] : 0396d6e8 (dalam heksadesimal)
TT[2] : d3c71fe5 (dalam heksadesimal)	TT[6] : 3d4c2f7a (dalam heksadesimal)
TT[3] : ab3c73d2 (dalam heksadesimal)	TT[7] : 9ee27cf3 (dalam heksadesimal)

2. Inisialisasi nilai awal untuk T[0] … T[3] :

   T[0] = K[0]
   T[1] = K[1]
   K[0], K[1], K[2], K[3] dihasilkan dari kunci yang dipecah menjadi 4 bagian yang sama panjang.

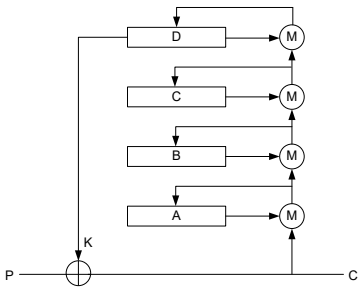
E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887

3.Untuk T[4] sampai T[255], lakukan proses berikut :
X = T[n-4] + T[n-1]
T[n] = X >> 3 XOR TT(X AND 7)
4.Untuk T[0] sampai T[22], lakukan proses berikut :
T[n] = T[n] + T[n+89]
5.Set nilai untuk beberapa variabel di bawah ini :
X = T[33]
Z = T[59] OR (01000001h)
Z = Z AND (FF7FFFFFh)
X = (X AND FF7FFFFFh) + Z
6. Untuk T[0] … T[255], lakukan proses berikut :
X = (X AND FF7FFFFFh) + Z
T[n] = T[n] AND 00FFFFFFh XOR X
7. Inisialisasi nilai untuk beberapa variabel berikut ini :
T[256] = T[0] X = X AND 255
8. Untuk T[0] … T[255], lakukan proses berikut :
Temp = (T[n XOR X] XOR X) AND 255
T[n] = T[Temp]
T[X] = T[n+1]



Gambar1. Proses Pembentukan Tabel S-Box

b. Proses Pembentukan Kunci(Prasetyo & Ariyani, 2018).
Proses pembentukan kunci membutuhkan kunci dengan panjang 128 bit biner atau 16 karakter ascii. Pertama, input kunci dipecah menjadi 4 kelompok dan di-set sebagai nilai awal dari variabel A0, B0, C0, D0. Kemudian isi variabel A, B, C dan D dan ulangi sebanyak n-putaran yang di-input. Fungsi M(X, Y) = (X + Y)>>8 XOR T[(X + Y) AND 255].) Selanjutnya dilakukan langkah Ai+1= M(Ai, Di), Bi+1= M(Bi, Ai+1), Ci+1= M(Ci, Bi+1), Di+1= M(Di, Ci+1) sehingga nilai Di adalah nilai kunci K (Ndruru & Ramadhani, 2019).
Proses Pembentukan kunci dapat dilihat pada Gambar1.



Gambar2 . Proses Pembentukan Kunci

c. Proses Enkripsi (Ndruru & Ramadhani, 2019).

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887

Proses enkripsi metode WAKE adalah dengan melakukan operasi perhitungan XOR pada plaintext dengan kunci untuk menghasilkan chipertext.

$$P \text{ XOR } K = C \quad [1]$$

Dimana: P =

Plaintext K = Kunci C = Chipertext

d. Proses Dekripsi (Prasetyo & Ariyani, 2018).
Proses dekripsi dalam metode WAKE diperoleh dengan melakukan operasi perhitungan XOR pada chipertext dengan kunci dan 32 bit kunci yang dihasilkan dari proses pembentukan kunci untuk mendapatkan plaintext.

$$C \text{ XOR } K = P \quad [2]$$

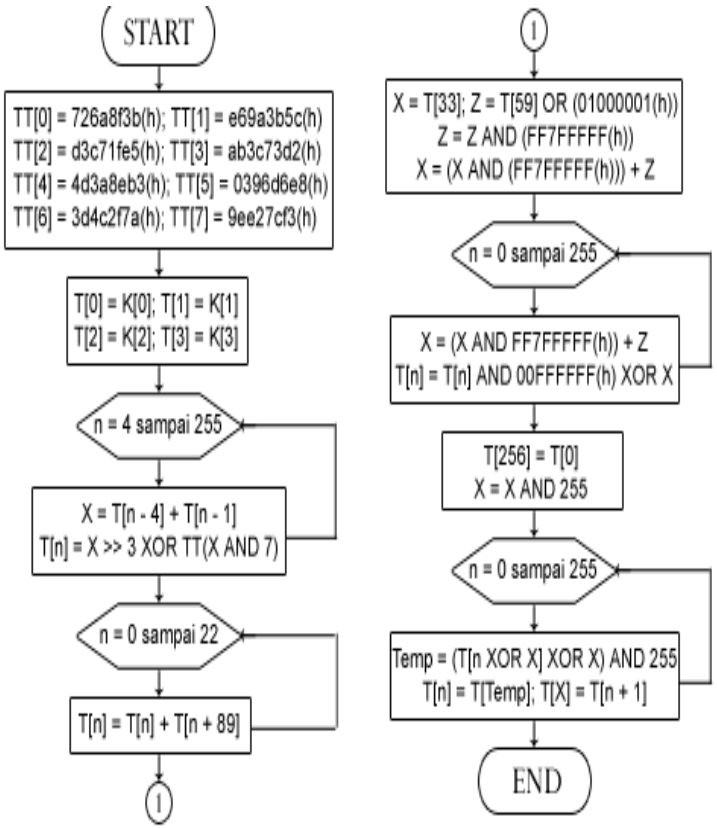
Dimana : C = Chipertext K = Kunci P = Plaintext

3. HASIL DAN PEMBAHASAN

Setelah dilakukan ujicoba menggunakan sistem informasi Kriptografi Algoritma WAKE diperoleh hasil enkripsi dan dekripsi pesan *chatting*.

Proses Pembentukan Tabel S-Box

Proses pembentukan tabel S-Box memerlukan input kunci 16 karakter ascii atau 128 bit biner.
Input kunci (16 karakter) = Lisda Juliana P.
Flowchart Pembentukan Tabel S-BOX dengan Kunci Lisda Juliana P. dapat dilihat pada gambar2. Sedangkan Tabel S-Box dengan Kunci Lisda Juliana P. dapat dilihat pada Tabel1.



Gambar2. *Flowchart* Pembentukan Tabel S-BOX dengan Kunci Lisda Juliana P

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887

Tabel 1. Tabel S-BOX dengan Kunci Lisda Juliana P

S-BOX / T[N]	BINER	HEXA
T[0]	11110010101100001011100000000110	F2B0B806
T[1]	10101110000101000111000011011011	AE1470DB
T[2]	00110100000100110100001100011110	341344C6
T[3]	11101111010010100111000000010010	EF4A7012
T[4]	10100001101010001000100100110011	A1A88933
T[5]	10101011111100101110101111011000	ABF2EBB8
T[6]	11100001000111001100000111011111	E11CC1DF
T[7]	01010111010011110111010000111011	574F743B
T[8]	01000000110111101001011001110001	40DE9671
T[9]	01111111011100000100110011111101	7F704CFD
T[10]	00101101110101111111010000101001	2DD7EA29
T[11]	10000110110101100111011001011111	86D66CAF
T[12]	10011110010001010010010001111100	9E45247C
T[13]	11011001011001001100011111000010	D964C7C2
T[14]	11001111011001101101011000110001	CF66D631
T[15]	10011110010001010010010001111100	9E45247C
T[16]	01111000011100111000011010101111	787386AF
T[17]	11111010111100101011010101110011	FB795753
T[18]	00011000011010111001100001011111	186B985F
T[19]	00100010011100001001100001111101	2270987D
T[20]	01100000111100010101011010110010	60F156B2
T[21]	11011001011001001100011111000010	D964C7C2
T[22]	00001111100011110010000100000100	0F8F2104
T[23]	01100000111100010101011010110010	60F156B2
T[24]	01111000011100111000011010101111	787386AF
T[25]	10000011110010011001111111000100	83C99FC4
T[26]	10010000101110010100100000011100	90B9481C
T[27]	01100101110000011101110010101000	65C1DCA8
T[28]	10010100110101101101100001001000	94D6D848
T[29]	10100001101010001000100100110011	A1A88933
T[30]	10110101100010000011000010110011	B58830B3
T[31]	10101001000000000011110001010111	A90078AF
T[32]	01111110111000001001100111111101	7F704CFD
T[33]	11110100010001011100001001111100	F445C27C
T[34]	10100011010010000111010010101010	A34874AA
T[35]	01101101000001111010110110100001	6D07ADA1
T[36]	10101101010101111010111110011010	AD57AF3A
T[37]	11010100011000101000011011011101	D46286DD
T[38]	00001000100110100101111100010011	089A5F13
T[39]	11000110111101000010011100001000	C6F42708
T[40]	01111101011111110010100010101110	7D7F28AE
T[41]	10010101101001100110011001100101	95A66665
T[42]	10000011110010011001111111000100	83C99FC4
T[43]	01111110111000001001100111111101	7F704CFD
T[44]	11100100101101111011110111100010	E4B7BDE2
T[45]	01100111000111101110010001100111	671EE467
T[46]	10001101100010100010100100000011	8D8A2903
T[47]	00110100000100110100010011000110	341344C6
T[48]	11110100010001011100001001111100	F445C27C
T[49]	'00000011111010110110000010010110	03EB6096
T[50]	11110001001111110001100011001000	F13F18C8
T[51]	'01011001010001011000000001011100	5945805C
T[52]	'10110011001110101111100011011001	B33AF8D9
T[53]	'00101111010111010101100110110011	2F5D59B3
T[54]	'01001100111100100000011000100111	4E720627
T[55]	11010111010010100001100010010111	D74A1897
T[56]	10000001101100010011110010111111	81B13CBF
T[57]	11100101000101101111110000010010	E516FC12
T[58]	01111111011100000100110011111101	7F704CFD
T[59]	'10001110000010101011111000111000	8E0ABE38
T[60]	'00100011011111111101100010111100	237FD8BC
T[61]	'00101110000110000011000001111110	2E18307E
T[62]	01111011101101000101111000000101	7BB45E05
T[63]	'01011101101111001000001111110111	5DBC87F7
T[64]	10000011110010011001111111000100	83C99FC4
T[65]	10000011110010011001111111000100	83C99FC4
T[66]	10100011010010000111010010101010	A34874AA
T[67]	11110111101000101000110001101011	F7A28C6B
T[68]	11000001101001010111100100000000	C1A57900
T[69]	00101110000011000001100000111110	2E18307E
T[70]	00101111010111010101100110110011	2F5D59B3

S-BOX / T[N]	BINER	HEXA
T[71]	'11010101111111010010000101010001	D5FA4291
T[72]	10011110010001010010010001111100	9E45247C
T[73]	'10011110010001010010010001111100	9E45247C
T[74]	00101000000000001001011010110000	28012D60
T[75]	01111111011100000100110011111101	7F704CFD
T[76]	'00101111010111010101100110110011	2F5D59B3
T[77]	11010110101010111110011101001100	D6ABE74C
T[78]	'01111110111100011010101011011100	7EF1AADC
T[79]	10100011010010000111010010101010	A34874AA
T[80]	00011010000111101100011100101000	1A3D8F28
T[81]	'01101100100110110110000110100000	6C9B6340
T[82]	'00001001101001011011110000100101 0	09A5B84A
T[83]	'10000011110010011001111111000100	83C99FC4
T[84]	'01110011000110011101010011111000	7319D4F8
T[85]	11011001011001001100011111000010	D964C7C2
T[86]	'00011011000101000011110001110111	1B143C77
T[87]	'11111010100100101001011010101101	FA9296AD
T[88]	'10110110000001010111111001000111	B6057E47
T[89]	01111100100001011011111000100010	7C85BE22
T[90]	10100100101011111011001110101101	A4AFB3AD
T[91]	11001000010111110111010110010000	C85F7590
T[92]	00111100110100101001010101111010	3E694ABA
T[93]	'11110001001111110001100011001000	F13F18C8
T[94]	'10000000111111101000111100110001	80FE8F31
T[95]	11000110111101000010011100001000	C6F42708
T[96]	'00111111000111011100011110100001	3F1DC7A1
T[97]	01111111011100000100110011111101	7F704CFD
T[98]	01001101011000101000101100000011	4D628B03
T[99]	'00011011000101000011110001110111	1B143C77
T[100]	10000011110010011001111111000100	83C99FC4
T[101]	00101111010111010101100110110011	2F5D59B3
T[102]	11001111011001101101011000110001	CF66D631
T[103]	'11000000100001000001101101100010	C0841B62
T[104]	01000000110111101001011001110001	40DE9671
T[105]	01111101011111111001010001010110	7D7F28AE
T[106]	00111001101000011110110101000000	39A1ED40
T[107]	11101011010111001011110001100001	EB5CBC61
T[108]	10100011010010000011010010101010	A34874AA
T[109]	00111111000111011100011110100001	3F1DC7A1
T[110]	'01111111011100000100110011111101	7F704CFD
T[111]	'10011110010001010010010001111100	9E45247C
T[112]	01001011000110110010100010100101	4B1B28A5
T[113]	11100101000101101111110000010010	E516FC12
T[114]	'01110010001101111101101011100100	7237DAE4
T[115]	'11001001111010111100111011100000	C9EBCEE0
T[116]	'11010111010010100001100010010111	D74A1897
T[117]	'00111101100000001101010011011001	3D80D4D9
T[118]	'10110011001110101111100011011001	B33AF8D9
T[119]	'10100100101011111011001110101101	A4AFB3AD
T[120]	00010111010011010011111000110001	174D3E31
T[121]	'01001101011000101000101100000011	4D628B03
T[122]	11101001011011111111110000101011	E96FFC2B
T[123]	'10001101100010100010100100000011	8D8A2903
T[124]	11101000010111010011001110010100	E85D3394
T[125]	' 00111110011010010100101010111010	3E694ABA
T[126]	'11101000010111010011001110010100	E85D3394
T[127]	' 11010111010010100001100010010111	D74A1897
T[128]	11010111010010100001100010010111	D74A1897
T[129]	00111110011010010100101010111010	3E694ABA
T[130]	'11110100010001011100001001111100	F445C27C
T[131]	'11110100010001011100001001111100	F445C27C
T[132]	11101000010111010011001110010100	E85D3394
T[133]	01011101101111001000001111110111	5DBC87F7
T[134]	01111111011100000100110011111101	7F704CFD
T[135]	'11010111010010100001100010010111	D74A1897
T[136]	'11010111010010100001100010010111	D74A1897
T[137]	' 00111101100000001101010011011001	3D80D4D9
T[138]	'10000001101100010011110010111111	81B13CBF
T[139]	'10000011110010011001111111000100	83C99FC4
T[140]	'10000011110010011001111111000100	83C99FC4

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887

S-BOX / T[N]	BINER	HEXA
T[141]	'10100100101011111011001110101101	A4AFB3AD
T[142]	01011100111100000000010100111111	5CF00D3F
T[143]	'10000011110010011001111111000100	83C99FC4
T[144]	'00111111000111011100011110100001	3F1DC7A1
T[145	]' 00101111010111010101100110110011	2F5D59B3
T[146]	'11110111101000101000110001101011	F7A28C6B
T[147]	'11010111010010100001100010010111	D74A1897
T[148]	10010100110101101101100001001000	94D6D848
T[149]	10100100101011111011000110101101	A4AFB3AD
T[150]	01111111011100000100110011111101	7F704CFD
T[151]	'10010100110101101101100001001000	94D6D848
T[152]	'10111000000111111111010000100000	B81FF420
T[153]	11110111010000101000110001101011	F7A28C6B
T[154]	10000000111111101000111100110001	80FE8F31
T[155]	10000001101100010011110010111111	81B13CBF
T[156]	'01011101101111001000011111110111	5DBC87F7
T[157]	01111111011100000100110011111101	7F704CFD
T[158]	'11010101111110100100001010010001	D5FA4291
T[159]	'11100101000101101111110000010010	E516FC12
T[160]	'11000110111101000010011100001000	C6F42708
T[161]	10000001101100010011110010111111	81B13CBF
T[162]	00101111010111010101100110110011	2F5D59B3
T[163]	'11000110111101000010011100001000	C6F42708
T[164]	10101101010101111010111100111010	AD57AF3A
T[165]	01110010000110111110110101100100	7237DAE4
T[166]	' 01111111011100000100110011111101	7F704CFD
T[167]	'10011110010001010010010001111100	9E45247C
T[168]	'10010100110101101101100001001000	94D6D848
T[169]	11001111011001101101011000110001	CF66D631
T[170]	'00011010001111011000111100101000	1A3D8F28
T[171]	10110100010000100100100101000010	B4424942
T[172]	' 10000011110010011001111111000100	83C99FC4
T[173]	'01111111011100000100110011111101	7F704CFD
T[174]	00001001101001011011100001001010	09A5B84A
T[175]	10011110010001010010010001111100	9E45247C
T[176]	01001110011100100000011000100111	4E720627
T[177]	11101011010111001011110001100001	EB5CBC61
T[178]	00111110011010010100101010111010	3E694ABA
T[179]	00101111010111010101100110110011	2F5D59B3
T[180]	11101001011011111111110000101011	E96FFC2B
T[181]	11001001111010111100111011100000	C9EBCEE0
T[182]	10000001101100010011110010111111	81B13CBF
T[183]	10000000111111101000111100110001	80FE8F31
T[184]	00101111010111010101100110110011	2F5D59B3
T[185]	10010100110101101101100001001000	94D6D848
T[186]	11110001001111110001100011001000	F13F18C8
T[187]	11100101000101101111110000010010	E516FC12
T[188]	00101111010111010101100110110011	2F5D59B3
T[189]	00101110000110000011000001111110	2E18307E
T[190]	10000011110010011001111111000100	83C99FC4
T[191]	'00111111000111011100011110100001	3F1DC7A1
T[192]	'11101001011011111111110000101011	E96FFC2B
T[193]	'11110001001111110001100011001000	F13F18C8
T[194]	00101111010111010101100110110011	2F5D59B3
T[195]	'01000000110111101001011001110001	40DE9671
T[196]	'10100011010010000111010010101010	A34874AA
T[197]	' 00011010001111011000111100101000	1A3D8F28
T[198]	'11001111011001101101011000110001	CF66D631
T[199]	'00111111000111011100011110100001	3F1DC7A1
T[200]	'01001110011100100000011000100111	4E720627
T[201]	'01100000111100010101011010110010	60F156B2
T[202]	'11000110111101000010011100001000	C6F42708
T[203]	00111110011010010100101010111010	3E694ABA
T[204]	'00111111000111011100011110100001	3F1DC7A1

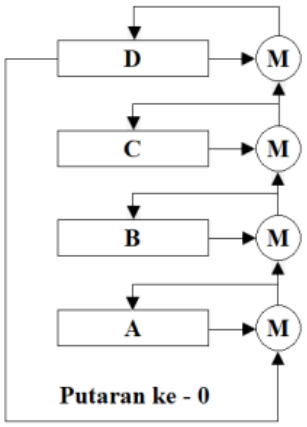
S-BOX / T[N]	BINER	HEXA
T[205]	'10100100101011111011001110101101	A4AFB3AD
T[206]	11011001011001001100011111000010	D964C7C2
T[207]	'00101111010111010101100110110011	2F5D59B3
T[208]	'10010100110101101101100001001000	94D6D848
T[209]	10010100110101101101100001001000	94D6D848
T[210]	'01000000110111101001011001110001	40DE9671
T[211]	'00101111010111010101100110110011	2F5D59B3
T[212]	'01111111011100000100110011111101	7F704CFD
T[213]	'01111111011100000100110011111101	7F704CFD
T[214]	11000001101001010111100100000000	C1A57900
T[215]	'11110001001111110001100011001000	F13F18C8
T[216]	'00111110011010010100101010111010	3E694ABA
T[217]	'00111110011010010100101010111010	3E694ABA
T[218]	11110001001111110001100011001000	F13F18C8
T[219]	'10010101101001100110011001100101	95A66665
T[220]	'00011100110100111110011000011111	1CD3E61F
T[221]	'01110010001101111101101011100100	7237DAE4
T[222]	' 01111111011100000100110011111101	7F704CFD
T[223]	'01111111011100000100110011111101	7F704CFD
T[224]	'11001111011001101101011000110001	CF66D631
T[225]	'10000001101100010011110010111111	81B13CBF
T[226]	' 00101111010111010101100110110011	2F5D59B3
T[227]	'10000001101100010011110010111111	81B13CBF
T[228]	'10011110010001010010010001111100	9E45247C
T[229]	10100011010010000111010010101010	A34874AA
T[230]	'10011110010001010010010001111100	9E45247C
T[231]	'10011110010001010010010001111100	9E45247C
T[232]	00101110000110000011000001111110	2E18307E
T[233]	'10000001101100010011110010111111	81B13CBF
T[234]	'11101000010111010011001110010100	E85D3394
T[235]	'00010111010011010011111000110001	174D3E31
T[236]	'10011110010001010010010001111100	9E45247C
T[237]	'10000011110010011001111111000100	83C99FC4
T[238]	'10000011110010011001111111000100	83C99FC4
T[239]	'00101111010111010101100110110011	2F5D59B3
T[240]	'10000001101100010011110010111111	81B13CBF
T[241]	'01001110011100100000011000100111	4E720627
T[242]	'00111110011010010100101010111010	3E694ABA
T[243]	'00101111010111010101100110110011	2F5D59B3
T[244]	'11110001001111110001100011001000	F13F18C8
T[245]	'11100101000101101111110000010010	E516FC12
T[246]	'00101111010111010101100110110011	2F5D59B3
T[247]	10011110010001010010010001111100	9E45247C
T[248]	'11100101000101101111110000010010	E516FC12
T[249]	'00101111010111010101100110110011	2F5D59B3
T[250]	10000001101100010011110010111111	T 81B13CBF
T[251]	'00101111010111010101100110110011	2F5D59B3
T[252]	'00111110011010010100101010111010	3E694ABA
T[253]	'01111111011100000100110011111101	7F704CFD
T[254]	11001111011001101101011000110001	CF66D631
T[255]	10000001101100010011110010111111	81B13CBF
T[256]	10111000000111111111010000100000	B81FF420

Berdasarkan tabel S-BOX dapat dilihat bahwa Tabel S-Box algoritma WAKE bersifat fleksibel dan berbeda-beda untuk setiap putaran.

Proses Pembentukan Kunci

Kunci diinput dengan panjang 128 bit biner atau 16 karakter ascii. Kunci yang diinput sepanjang 16 karakter akan terbentuk menjadi kunci baru dalam bentuk biner atau heksa decimal. Kunci yang terbentuk tergantug pada jumlah putaran (n).

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887



Gambar3. *Flowchart* Putaran Pembentukan Kunci

Setelah dilakukan ujicoba sampai 20 putaran, adapun kunci yang terbentuk adalah :
Kunci 'Lisda Juliana P.' diubah dalam bentuk heksa = 4C69736461204A756C69616E6120502E
Pecah kunci menjadi 4 kelompok dan masukkan ke A(0), B(0), C(0) dan D(0).
A(0) = 4C697364
B(0) = 61204A75
C(0) = 6C69616E
D(0) = 6120502E

KUNCI PUTARAN 1

FungsiM(A[0],D[0]) = FungsiM(4C697364,6120502E) = (4C697364 + 6120502E)>>8 XOR T[(4C697364 + 6120502E) AND 255(10)] = AD89C392>>8 XOR T[146] = 00AD89C3 XOR F7A28C6B = F70F05A8
A[1] = F70F05A8
FungsiM(B[0],A[1]) = FungsiM(61204A75,F70F05A8) = (61204A75 + F70F05A8)>>8 XOR T[(61204A75 + F70F05A8) AND 255(10)] = 582F501D>>8 XOR T[29] = 00582F50 XOR A1A88933 = A1F0A663
B[1] = A1F0A663
FungsiM(C[0],B[1]) = FungsiM(6C69616E,A1F0A663) = (6C69616E + A1F0A663)>>8 XOR T[(6C69616E + A1F0A663) AND 255(10)] = 0E5A07D1>>8 XOR T[209] = 000E5A07 XOR 94D6D848 = 94D8824F
C[1] = 94D8824F
FungsiM(D[0],C[1]) = FungsiM(6120502E,94D8824F) = (6120502E + 94D8824F)>>8 XOR T[(6120502E + 94D8824F) AND 255(10)] = F5F8D27D>>8 XOR T[125] = 00F5F8D2 XOR 3E694ABA = 3E9CB268

D[1] = 3E9CB268

Dengan cara yang sama diperoleh **kunci putaran D[n]** adalah : D[2] = C1B159BF, D[3] = 7FE1C6F8, D[4] = 9E5B74D8, D[5] = B3E4D4E9, D[6] = 08789FD6, D[7] = 3E2E578D, D[8] = 7FACD7D5, D[9] = AE710AE7, D[10] = B308F9CF, D[11] = EB96A321, D[12] = AE790BD7, D[13] = 9E09F8EC, D[14] = 2E594E9F, D[15] = 2FA9D98C, D[16] = C1099A25, D[17] = 393BF90B, D[18] = 7FAE58EE, D[19] = D9140278, KUNCI = D[20] = D788880.

Berdasarkan hasil ujicoba dapat dilihat bahwa kunci yang dibentuk berbeda beda, tergantung pada jumlah putaran (N), sehingga kunci terbentuk lebih sulit ditebak daripada kunci pada algoritma GOST,

Proses Enkripsi

a. Enkripsi Biner 10 putaran

Input Plaintext : **'Berikut disertakan dokumen'**

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887

Kode ascii dari 'B' = 01000010
Kode ascii dari 'e' = 01100101
Kode ascii dari 'r' = 01110010
Kode ascii dari 'i' = 01101001
Kode ascii dari 'k' = 01101011
Kode ascii dari 'u' = 01110101
Kode ascii dari 't' = 01110100
Kode ascii dari ' ' = 00100000
Kode ascii dari 'd' = 01100100
Kode ascii dari 'i' = 01101001
Kode ascii dari 's' = 01110011
Kode ascii dari 'e' = 01100101
Kode ascii dari 'r' = 01110010
Kode ascii dari 't' = 01110100
Kode ascii dari 'a' = 01100001
Kode ascii dari 'k' = 01101011
Kode ascii dari 'a' = 01100001
Kode ascii dari 'n' = 01101110
Kode ascii dari ' ' = 00100000
Kode ascii dari 'd' = 01100100
Kode ascii dari 'o' = 01101111
Kode ascii dari 'k' = 01101011
Kode ascii dari 'u' = 01110101
Kode ascii dari 'm' = 01101101
Kode ascii dari 'e' = 01100101
Kode ascii dari 'n' = 01101110
Maka Plaintext (dalam biner) =
01000010011001010111001001101001011010111011101010111010000100000011001000110100101
11001101100101011100100111010001100001011010110110000101101110001000000110010001101
11110110101101110101011011010110010101101110
Kunci dari proses pembentukan kunci = **10110011000010001111100111001111**
Ciphertext = Plaintext XOR Key
01000010 XOR 10110011 = 11110001 = 'ñ'
01100101 XOR 00001000 = 01101101 = 'm'
01110010 XOR 11111001 = 10001011 = '‹'
01101001 XOR 11001111 = 10100110 = '¦'
01101011 XOR 10110011 = 11011000 = 'Ø'
01110101 XOR 00001000 = 01111101 = '}'
01110100 XOR 11111001 = 10001101 = '•'
00100000 XOR 11001111 = 11101111 = 'ï'
01100100 XOR 10110011 = 11010111 = '×'
01101001 XOR 00001000 = 01100001 = 'a'
01110011 XOR 11111001 = 10001010 = 'Š'
01100101 XOR 11001111 = 10101010 = 'ª'
01110010 XOR 10110011 = 11000001 = 'Á'
01110100 XOR 00001000 = 01111100 = '|'
01101011 XOR 11001111 = 10100100 = '¤'
01101110 XOR 00001000 = 01100110 = 'f'
00100000 XOR 11111001 = 11011001 = 'Ù'
01100100 XOR 11001111 = 10101011 = '«'
01101111 XOR 10110011 = 11011100 = 'Ü'
01101011 XOR 00001000 = 01100011 = 'c'
01110101 XOR 11111001 = 10001100 = 'Œ'
01101101 XOR 11001111 = 10100010 = '¢'
01100101 XOR 10110011 = 11010110 = 'Ö'
01101110 XOR 00001000 = 01100110 = 'f'
Hasil proses enkripsi 10 putaran = **ñm‹¦Ø}•ï×aŠªÁ|˜¤ÒfÙ«ÜcŒ¢Öf**

b. Enkripsi Hexadecimal 10 putaran

Plain Text (dalam heksa) =
426572696B7574206469736572746 16B616E20646F6B756D656E
Kunci dari proses pembentukan kunci = B308F9CF
Hasil proses enkripsi 10 putaran = **ñm‹¦Ø}•ï×aŠªÁ|˜¤ÒfÙ«ÜcŒ¢Öf**

c. Enkripsi *Biner* 20 putaran
   Kunci dari proses pembentukan kunci = 11010111100010001000100000001101
   Hasil proses enkripsi 20 putaran = •íúd¼ýü-³áûh¥üéf¶æ¨i¸ãý`²æ
d. Enkripsi *Hexadecimal* 20 putaran
   Kunci dari proses pembentukan kunci = D788880D
   Hasil proses enkripsi 20 putaran = •íúd¼ýü-³áûh¥üéf¶æ¨i¸ãý`²æ

Dari hasil proses enkripsi dapat diketahui bahwa hasil enkripsi untuk berbeda, tergantung pada kunci yang dibentuk.

Proses Dekripsi

a. Dekripsi Biner 20 putaran

Cipher Text : '•íúd¼ýü-³áûh¥üéf¶æ¨i¸ãý`²æ'

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887

Cipher Text (dalam biner) =
11110001011011011000101110100110110110000111110110001101111011111101011101100001100010
10101010101100000101111100100110001010010011010010011001101101100110101011110111000 1
10001110001100101000101101011001100110

Kunci dari proses pembentukan kunci 20 putaran = 10110011 00001000 11111001 11001111
Plain Text = CipherText XOR Key
11110001 XOR 10110011 = 01000010 = 'B' 01111100 XOR 00001000 = 01110100 = 't'
01101101 XOR 00001000 = 01100101 = 'e' 10011000 XOR 11111001 = 01100001 = 'a'
10001011 XOR 11111001 = 01110010 = 'r' 10100100 XOR 11001111 = 01101011 = 'k'
10100110 XOR 11001111 = 01101001 = 'i' 11010010 XOR 10110011 = 01100001 = 'a'
11011000 XOR 10110011 = 01101011 = 'k' 01100110 XOR 00001000 = 01101110 = 'n'
01111101 XOR 00001000 = 01110101 = 'u' 11011001 XOR 11111001 = 00100000 = ' '
10001101 XOR 11111001 = 01110100 = 't' 10101011 XOR 11001111 = 01100100 = 'd'
11101111 XOR 11001111 = 00100000 = ' ' 11011100 XOR 10110011 = 01101111 = 'o'
11010111 XOR 10110011 = 01100100 = 'd' 01100011 XOR 00001000 = 01101011 = 'k'
01100001 XOR 00001000 = 01101001 = 'i' 10001100 XOR 11111001 = 01110101 = 'u'
10001010 XOR 11111001 = 01110011 = 's' 10100010 XOR 11001111 = 01101101 = 'm'
10101010 XOR 11001111 = 01100101 = 'e' 11010110 XOR 10110011 = 01100101 = 'e'
11000001 XOR 10110011 = 01110010 = 'r' 01100110 XOR 00001000 = 01101110 = 'n'
Hasil proses dekripsi = **Berikut disertakan dokumen**

b. Dekripsi Hexadesimal 20 putaran

Cipher Text : '•íúd¼ýü-³áûh¥üéf¶æ¨i¸ãý`²æ'
Cipher Text (dalam heksa) =
F1 6D 8B A6 D8 7D 8D EF D7 61 8A AA C1 7C 98 A4 D2 66 D9 AB DC 63 8C A2 D6 66
Kunci dari proses pembentukan kunci 20 putaran = B308F9CF
Plain Text = CipherText XOR Key
Hasil proses dekripsi = **Berikut disertakan dokumen**

c. Dekripsi Biner 10 putaran

Cipher Text : 'ñm‹¦Ø}•ï×aŠªÁ|˜¤ÒfÙ«ÜcŒ¢Öf'
Cipher Text (dalam biner) =
11110001
01101101100010111010011011011000011111011000110111101111110101110110000110001010101 01
01011000001011111001001100010100100110100100110011011011001101010111101110001100011 1
00011001010001011010110011001 10
Kunci dari proses pembentukan kunci 10 putaran = 10110011000010001111100111001111
Plain Text = CipherText XOR Key
Hasil proses dekripsi = **Berikut disertakan dokumen**

d. Dekripsi Hexa 10 putaran

Cipher Text : 'ñm‹¦Ø}•ï×aŠªÁ|˜¤ÒfÙ«ÜcŒ¢Öf'
Cipher Text (dalam heksa) =
95 ED FA 64 BC FD FC 2D B3 E1 FB 68 A5 FC E9 66 B6 E6 A8 69 B8 E3 FD 60 B2 E6
Kunci dari proses pembentukan kunci 10 putaran= D7 88 88 0D
Hasil proses dekripsi = Berikut disertakan dokumen

Dari hasil ujicoba dekripsi untuk bilangan biner dan hexadecimal dengan kunci 10 putaran dan 20 putaran, pesan *chatting* yang telah di enkripsi dapat dikembalikan ke pesan semula. Hasil enkripsi pesan chat 10 putaran untuk bilangan biner dan hexadesimal tetap sama,

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887

namun untuk 20 putaran enkripsi yang dibentuk berbeda. Proses enkripsi dan dekripsi juga cepat, hanya 0,1 detik.

4. PENUTUP

Dari hasil ujicoba analisa terhadap Kriptografi Metode *Word Auto Key Encryption* (WAKE) disimpulkan bahwa Tabel S-Box algoritma WAKE bersifat fleksibel dan berbeda-beda untuk setiap putaran, kunci yang dibentuk juga berbeda beda, tergantung pada jumlah putaran (N) sehingga pesan yang dienkripsi dengan kunci yang sama juga berbeda. Jika cryptanalyst mengetahui pesan yang telah dienkripsi, pesan asli belum dapat diketahui karena kunci yang digunakan berbeda beda. Hal ini membuat kriptografi Metode WAKE aman digunakan untuk pengiriman pesan *chatting* pada media social, selain aman penggunaan algoritma ini juga memberi kenyamanan pada pengguna karena proses enkripsi yang cepat yaitu 0,1 detik. Karena pada penelitian ini planteks hanya berupa teks sepanjang 32 bit, maka disarankan untuk mengkombinasikan dengan algoritma yang lain supaya dapat mengenkripsi dan dekripsi pesan dalam bentuk image, suara dan video.

DAFTAR PUSTAKA

Andara, H., Damayanti, F., & Khairunnisa. (2022). Implementasi Kriptografi Hybrida Algoritma RSA dan Vernam Cipher Dalam Pengamanan File Text. *Jurnal Ilmu Komputer Dan Informatika*, *6*(1), 8–15.

Andrea, K., Wardana, A., Wanandi, B. S., & Ikhwan, A. (2023). Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp. *Januari*, *2*(1), 6. https://doi.org/10.47233/jppie.v2i1.660

Arifin, M., & Mufti. (2018). Implementasi Kriptografi Chatting Menggunakan Metode Vigenere dan AES 128 Berbasis Web. *Skanika*, *1*(1), 102–109.

Azzura, C. M., & Pratiwi, M. (2023). *Implementasi Watermarking Desain Citra Menggunakan Metode Modifikasi End Of File (MEOF). 11*(1), 11–19.

Darmawan, M. R., & Windarto. (2018). Implementasi Algoritma Kriptografi Vigenere Cipher dan Affine Cipher untuk Mengamankan Pesan pada Aplikasi Chatting Berbasis Android. *Skanika*, *1*(2), 583–590.

Eddy, & Pahlevi, M. R. (2014). Pembelajaran Enkripsi Metode Word Auto Key Encryption. *Sisfotenika*, *4*(1), 23–32.

Febrianto, R. W., & Zulianto, A. (2024). Kriptografi Ringan dengan Menggunakan Algoritma di Internet Of Things (IoT). *Journal of Informatics Management and Information Technology*, *4*(3), 81–91.

Jaya, P., & Juanita, S. (2018). Aplikasi Pengamanan Basis Data dengan Algoritma RSA dan WAKE Berbasis Desktop. *Skanika*, *Vol 1*(1), 352–358.

Juliana Pangaribuan, L., Indra Cahyadi, C., Banjarnahor, J., Barus, B., & Siahaan, B. N. (2023). KLIK: Kajian Ilmiah Informatika dan Komputer Strategi Otentikasi Dokumen Pada Email Menggunakan Digital Signature dengan Algoritma Schnorr. *Media Online*, *3*(4), 384–392. https://djournals.com/klik

Kumala, J., Zaman, B., & Bahri, S. (2025). Implementasi Algoritma Rc4+ Pada Keamanan Sistem Komunikasi Chatting Pada Website Saheb. *KHARISMA Tech*, *20*(1), 44–56. https://doi.org/10.55645/kharismatech.v20i1.528

Milian, Y. C., & Sulistyo, W. (2023). Model Pengembangan Keamanan Data dengan Algoritma ROT 13 Extended Vernam Cipher dan Stream Cipher. *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)*, *7*(2), 208–216. https://doi.org/10.35870/jtik.v7i2.716

Ndruru, K., & Ramadhani, P. (2019). Penerapan Metode Segitiga Pascal Aljabar Untuk Memaksimalkan Teknik Penyandian Algoritma Word Auto Key Encryption (Wake). *KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer)*, *3*(1), 150–154. https://doi.org/10.30865/komik.v3i1.1582

Okario, A., Gede, I. P., Suputra, H., Ayu, G., Mastrika, V., & Widhi, I. M. (2026). *Integrasi Algoritma RSA dan Teknologi Kriptografi Kuantum dalam Keamanan Aplikasi Web Chatting*. *14*(3), 459–468.

Pangaribuan, L. J., & Simbolon, F. H. (2017). Kriptografi Hybrida Menggunakan Algoritma Hill Cipher dan Algoritma RSA untuk Keamanan Pengiriman Informasi pada Email. *KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer)*, *I*, 1–11.

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887

Pangaribuan, L. J., & Sitanggang, D. (2022). *KEAMANAN PESAN WHATSAPP MENGGUNAKAN KRIPTOGRAFI ALGORITMA GOVERNMENT STANDARD (GOST)*. *2*(1), 210–217.

Panjaitan, C. H. P., & Pangaribuan, L. J. (2021). Analisis Pola Identifikasi Zero Knowledge Proof Dengan Algoritma Feige Fiat Shamir Menggunakan Blum Blum Shub. *MEANS (Media Informasi Analisa Dan Sistem)*, *6*(1), 7–12. https://doi.org/10.54367/means.v6i1.1203

Prasetyo, A. I., & Ariyani, P. F. (2018). Dengan Algoritma Affine Cipher Dan Wake Berbasis Web. *Skanika*, *1*(3), 1176–1181.

Putri Nugroho, F. N., Listanto, M. F., Amelia, N., & Annisa, S. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. *Fibonacci : Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *1*(2), 58–65. https://doi.org/10.63217/fibonacci.v1i2.70

Silalahi, S. D., & Ginting, G. L. (2020). Penerapan Algoritma Kriptografi Word Auto Key Encryption Dalam Untuk Pengamanan Soal Ujian Berbasis Komputer. *Journal of Computer System and …*, *2*(1), 91–106. https://ejurnal.seminar-id.com/index.php/josyc/article/view/467

Sinaga, M. D., Sembiring, N. S. B., Tambunan, F., & Sianturi, C. J. M. (2019). Hybrid Cryptography WAKE (Word Auto Key Encryption) and Binary Caesar Cipher Method for Data Security. *2018 6th International Conference on Cyber and IT Service Management, CITSM 2018*, (Citsm), 5–9. https://doi.org/10.1109/CITSM.2018.8674346

Sinaga, N. (2019). Perancangan Aplikasi Pengamanan Pesan Teks dengan Menggunakan Metode Wake (Word Auto Key Encryption). *Jurnal Teknik Informatika Unika St. Thomas (JTIUST)*, *04*(01), 76–88.

E-ISSN : 2830 – 7879 || P-ISSN : 2355 - 1887