MEANS (Media Informasi Analisa dan Sistem)
p-ISSN: 2548-6985, e-ISSN:2599-3089

Penerapan Algoritma Salsa20 Untuk Mengamankan Sandi Akun Virtual

Muhammad Abdul Rasyid Hasibuan
Universitas Budidarma, Sisingamangaraja, Sumatera Utara, Indonesia
E-Mail : abdulrasyid077077@gmail.com

Sinar Sinurat
Universitas Budidarma, Sisingamangaraja, Sumatera Utara, Indonesia
E-Mail : sinurat.sin@gmail.com

ABSTRACT
The application of the SALSA20 algorithm in securing virtual account passwords aims to increase the security of users' personal data in an increasingly complex digital era. The SALSA20 algorithm, which is known as one of the efficient and secure stream cipher algorithms, has superior characteristics in terms of speed and resistance to cryptanalysis attacks. This research explores the implementation of SALSA20 in a virtual account password security system, testing the performance of this algorithm under various conditions and comparing it with other commonly used cryptographic algorithms, such as AES (Advanced Encryption Standard). The research results show that SALSA20 is able to provide a high level of security with a faster execution time compared to several other algorithms. Testing includes analysis of encryption and decryption speed, system resource usage, as well as resistance to various types of attacks, such as brute force and differential analysis attacks. In addition, the integration of SALSA20 in real applications shows that this algorithm is easy to implement and provides significant protection against attempts to steal user passwords and personal data.

Keywords: Security, Account, Virtual, Salsa20

PENDAHULUAN

Akun virtual merupakan jenis akun yang hanya ada dalam bentuk digital atau elektronik, tanpa wujud fisik seperti akun bank konvensional. Biasanya, akun ini digunakan untuk berbagai aktivitas online, seperti transaksi e-commerce, pembayaran tagihan, dan transfer dana secara elektronik. Pengelolaan dan akses akun virtual dilakukan melalui platform online atau aplikasi perbankan digital. Banyak perusahaan menawarkan fleksibilitas dan kemudahan dalam penggunaannya, serta menjamin tingkat keamanan tinggi dalam transaksi daring. Akun virtual juga bisa terhubung dengan akun bank fisik untuk memfasilitasi transfer dana atau layanan perbankan lainnya [1].

Keamanan akun virtual sangat penting, terutama melalui penggunaan kata sandi yang diperlukan untuk transaksi, mengakses informasi akun, atau mengubah pengaturan. Akun virtual rentan terhadap ancaman seperti peretasan, pencurian identitas, dan penipuan online. Oleh karena itu, perlindungan akun virtual menjadi esensial guna menjaga data pengguna, aset finansial, dan privasi. Pendekatan menyeluruh diperlukan untuk mengamankan akun ini, mencakup penggunaan kata sandi yang kuat, otentikasi dua faktor, enkripsi data, serta pemantauan aktivitas transaksi yang mencurigakan.

Kelemahan pada kata sandi akun virtual yang digunakan pengguna membuatnya rentan diambil alih oleh pihak yang tidak berwenang melalui teknik seperti phishing atau menebak kata sandi yang lemah, yang dapat merugikan pemilik akun virtual. Untuk mengatasi masalah ini, perlu dilakukan pengamanan kata sandi akun virtual dengan menerapkan teknik kriptografi menggunakan algoritma Salsa20.

Keamanan kata sandi merupakan faktor penting dalam melindungi akun perbankan, sehingga pembobolan rekening nasabah dapat dicegah. Proses pembuatan kata sandi harus melibatkan kombinasi karakter, termasuk angka, huruf (baik huruf besar maupun kecil), serta simbol, agar sulit ditebak. Semakin beragam dan panjang karakter yang digunakan, semakin tinggi tingkat keamanan kata sandi tersebut[2][3].

BAHAN METODE

2.1 Kriptografi

Kriptografi adalah cabang ilmu yang memanfaatkan persamaan matematis untuk

melakukan enkripsi dan dekripsi data. Teknik ini digunakan untuk mengubah data menjadi kode tertentu, sehingga informasi yang disimpan atau dikirim melalui jaringan yang tidak aman, seperti internet, tidak dapat dibaca oleh pihak yang tidak berwenang [4][5]. Kriptografi bertujuan menciptakan komunikasi yang aman, yang hanya bisa dipahami oleh pihak yang berhak. Kriptografi tidak sekadar mempelajari pengacakan data elektronik dengan bantuan program komputer, melainkan memastikan bahwa hanya pihak tertentu yang dapat mengaksesnya. Manfaat kriptografi meliputi [6]:

1. Kerahasiaan (Privacy) : Mencegah pihak yang tidak berwenang membaca pesan.
2. Keaslian (Authenticity) : Memastikan pengirim dan penerima pesan dapat memverifikasi identitas satu sama lain.
3. Keutuhan (Integrity) : Menjamin pesan tidak diubah atau dipalsukan oleh pihak yang tidak berhak selama pengiriman.
4. Tidak Ada Penolakan (Non-Repudiation) : Mencegah pengirim atau penerima menyangkal telah mengirim atau menerima pesan.

2.2 Pengamanan Sandi

Pengamanan kata sandi adalah praktik dan teknologi yang digunakan untuk melindungi data sensitif melalui penggunaan kata sandi atau frasa sandi (passphrase). Tujuan utamanya adalah mencegah akses tidak sah ke akun, sistem, atau data yang dilindungi. Peran penting pengamanan kata sandi meliputi perlindungan informasi sensitif, pencegahan akses ilegal, menjaga privasi, menghindari pemalsuan identitas, serta memberikan perlindungan dari serangan [7][8].

2.3 Algoritma Salsa20

Algoritma Salsa20 merupakan salah satu algoritma kriptografi simetris yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma ini dikembangkan oleh Daniel J. Bernstein sebagai bagian dari proyek eSTREAM. Salsa20 termasuk dalam jenis stream cipher, yaitu algoritma kriptografi yang bekerja pada setiap bit dari plaintext atau ciphertext, sehingga enkripsi dan dekripsi dilakukan secara individu pada setiap bit pesan. Tahapan pada algoritma Salsa20 meliputi [9][10]:

1. Inisialisasi
   Pilih kunci enkripsi, yang akan diulang hingga panjangnya sama dengan panjang teks asli.
2. Enkripsi
   Untuk setiap karakter dalam teks asli, gunakan tabel untuk menemukan karakter enkripsi yang sesuai dengan mencocokkan kunci dan huruf dalam teks asli, lalu pilih baris yang cocok dengan huruf kunci.
3. Deskripsi
   Pilih kunci yang sama dengan yang digunakan untuk enkripsi. Untuk setiap karakter dalam teks terenkripsi, gunakan tabel untuk menemukan huruf asli, dan pilih baris yang sesuai dengan huruf kunci.

HASIL DAN PEMBAHASAN

Keamanan data atau informasi yang menggunakan teknik kriptografi tidak hanya bergantung pada kompleksitas algoritma, tetapi juga pada kesulitan dalam memecahkan kunci yang digunakan selama proses enkripsi dan dekripsi. Pengamanan kata sandi akun virtual dengan kriptografi memerlukan kunci. Dalam implementasinya, sistem yang dibangun pada penelitian ini bertujuan untuk melindungi sandi akun virtual. Prosesnya dimulai dengan mengenkripsi plaintext menggunakan algoritma Salsa20, sehingga menghasilkan ciphertext atau pesan yang terlindungi dan tidak bisa dibaca. Untuk mengembalikan kata sandi akun virtual yang telah dienkripsi, dilakukan proses dekripsi menggunakan algoritma yang sama. Algoritma ini menerima input berupa 64 byte, yang terdiri dari 32 byte kunci, 8 byte nonce, 8 byte block counter, dan 16 byte konstanta, yang direpresentasikan dalam bentuk matriks.

1. Proses Enkripsi
   Enkripsi adalah tahap mengubah data menjadi bentuk yang tidak dapat dipahami oleh orang lain. Dalam penelitian ini, data yang dienkripsi berupa pesan sandi akun virtual. Sebelum proses enkripsi menggunakan algoritma Salsa20, pesan dalam file teks dikonversi terlebih dahulu ke bentuk desimal sesuai tabel ASCII.
   Plainteks : ABDURRASYID
   Kunci : kriptografi

Tabel 1. Proses Mengubah Plainteks Menjadi Desimal

Plainteks (M_i)	A	B	D	U	R	R	A	S	Y	I	D
Desimal	65	66	68	85	82	82	65	83	89	73	68
Kunci (K_i)	k	r	i	p	t	o	g	r	a	f	i
Nilai Desimal	107	114	105	112	116	111	103	114	97	102	105

Untuk karakter (M_1) = *k* dan kunci (K_1) = A
$C_1 = (K_1\text{-}M_1) \bmod 26 = (k\text{-}A) \bmod 26 + 97$
$= (107\text{-}65) \bmod 26 + 97$
$= 113$ (huruf “q” dalam tabel ASCII)
Untuk karakter (M_2) = *k* dan kunci (K_2) = B
$C_2 = (K_2\text{-}M_2) \bmod 26 = (r\text{-}B) \bmod 26 + 97$

= (114-66) mod 26+ 97
= 119 (huruf "w" dalam tabel ASCII)

Untuk karakter (M_3) = *k* dan kunci (K_3) = D
$C_3 = (K_3-M_3)$ mod 26 = (i- D) mod 26 + 97
= (105-68) mod 26+ 97
= 134 (huruf "ƭ" dalam tabel ASCII)

Untuk karakter (M_4) = *k* dan kunci (K_4) = U
$C_4 = (K_4-M_4)$ mod 26 = (P-u) mod 26 + 97
= (112-85) mod 26+ 97
= 98 (huruf "b" dalam tabel ASCII)

Untuk karakter (M_5) = *k* dan kunci (K_5) = R
$C_5 = (K_5-M_5)$ mod 26 = (t-R) mod 26 + 97
= (116-82) mod 26+ 97
= 131 (huruf "ƒ" dalam tabel ASCII)

Untuk karakter (M_6) = *k* dan kunci (K_6) = R
$C_6 = (K_6-M_6)$ mod 26 = (o-R) mod 26 + 97
= (111-82) mod 26+ 97
= 100 (huruf "d" dalam tabel ASCII)

Untuk karakter (M_7) = *k* dan kunci (K_7) = A
$C_7 = (K_7-M_7)$ mod 26 = (g-A) mod 26 + 97
= (103-65) mod 26+ 97
= 109 (huruf "m" dalam tabel ASCII)

Untuk karakter (M_8) = *k* dan kunci (K_8) = S
$C_8 = (K_8-M_8)$ mod 26 = (r-S) mod 26 + 97
= (114-83) mod 26+ 97
= 102 (huruf "f" dalam tabel ASCII)

Untuk karakter (M_9) = *k* dan kunci (K_9) = Y
$C_9 = (K_9-M_9)$ mod 26 = (a-Y) mod 26 + 97
= (97-89) mod 26 + 97
= 105 (huruf "i" dalam tabel ASCII)

Untuk karakter (M_{10}) = *k* dan kunci (K_{10}) = I
$C_{10} = (K_{10}-M_{10})$ mod 26 = (f-I) mod 26 + 97
= (102-73) mod 26+ 97
= 100 (huruf "d" dalam tabel ASCII)

Untuk karakter (M_{11}) = *k* dan kunci (K_{11}) = D
$C_{11} = (K_{11}-M_{11})$ mod 26 = (i- D) mod 26 + 97
= (105-68) mod 26+ 97
= 108 (huruf "l" dalam tabel ASCII)

Berdasarkan perhitungan di atas maka diperoleh hasil enkripsi = **qwƭbƒdmfidl**

2. Proses Dekripsi

Proses dekripsi melibatkan penggunaan nilai kunci dengan menghitung jumlah karakter dalam ciphertext, kemudian membaginya dengan nilai kunci enkripsi. Berikut adalah ciphertext dan kunci yang digunakan dalam proses dekripsi:

Tabel 2. Proses Mengubah Cipherteks Menjadi Desimal

Cipherteks (C_i)	q	w	ƭ	b	ƒ	d	M	f	i	d	l
Nilai Desimal	113	119	134	98	131	100	109	102	105	100	108
Kunci (K_i)	k	r	i	p	t	o	g	r	a	f	i
Nilai Desimal	107	114	105	112	116	111	103	114	97	102	105

Untuk karakter (C_1) = *c* dan kunci (K_1) = *q*
$M_1 = (K_1-C_1)$ mod 26 = (k-q) mod 26 + 97
= (107-113) mod 26+ 97
= 65 (A)

Untuk karakter (C_2) = *c* dan kunci (K_2) = w
$M_2 = (K_2-C_2)$ mod 26 = (r-w) mod 26 + 97
= (114-119) mod 26+ 97
= 66 (B)

Untuk karakter (C_3) = *c* dan kunci (K_3) = ƭ
$M_3 = (K_3-C_3)$ mod 26 = (i-ƭ) mod 26 + 97
= (105-134) mod 26+ 97
= 68 (D)

Untuk karakter (C_4) = *c* dan kunci (K_4) = *b*
$M_4 = (K_4-C_4)$ mod 26 = (p-b) mod 26 + 97
= (112-98) mod 26 + 97
= 85 (U)

Untuk karakter (C_5) = *c* dan kunci (K_5) = ƒ
$M_5 = (K_5-C_5)$ mod 26 = (t-ƒ) mod 26 + 97
= (116-131) mod 26+ 97
= 82 (R)

Untuk karakter (C_6) = *c* dan kunci (K_6) = d
$M_6 = (K_6-C_6)$ mod 26 = (o-d) mod 26 + 97
= (111-100) mod26 + 97
= 82 (R)

Untuk karakter (C_7) = *c* dan kunci (K_7) = m
$M_7 = (K_7-C_7)$ mod 26 = (g-m) mod 26 + 97
= (103-109) mod26 + 97
= 65 (A)

Untuk karakter (C_8) = *c* dan kunci (K_8) = f
$M_8 = (K_8-C_8)$ mod 26 = (r-f) mod 26 + 97
= (114-102) mod26 + 97
= 83 (S)

Untuk karakter (C_9) = *c* dan kunci (K_9) = i
$M_9 = (K_9-C_9)$ mod 26 = (a-i) mod 26 + 97
= (97-105) mod 26 + 97
= 89 (Y)

Untuk karakter (C_{10}) = *c* dan kunci (K_{10}) = d
$M_{10} = (K_{10}-C_{10})$ mod 26 = (f-d) mod 26 + 97
= (102-100) mod 26+ 97
= 73 (I)

Untuk karakter (C_{11}) = *c* dan kunci (K_{11}) = l
$M_{11} = (K_{11}-C_{11})$ mod 26 = (i-l) mod 26 + 97
= (105-108) mod 26+ 97
= 68 (D)

Berdasarkan perhitungan di atas maka diperoleh hasil dekripsi = ABDURRASYID

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan terkait pengamanan pesan teks, dapat disimpulkan beberapa hal sebagai berikut:

1. Keamanan kata sandi akun virtual dapat ditingkatkan secara signifikan, yang membantu melindungi akun dari berbagai ancaman siber.

2. Penggunaan algoritma Salsa20 untuk pengamanan kata sandi akun virtual dapat melindungi data selama proses transmisi.
3. Sistem yang dikembangkan mampu memberikan perlindungan yang efektif, sehingga pesan teks tidak dapat diakses atau dilihat oleh pihak yang tidak berwenang.

UCAPAN TERIMAKASIH

Penulis mengucapkan terimakasih ke pembimbing yang telah banyak memberikan masukan dalam penyelesaian penelitian ini. Ucapan terima kasih juga penulis ucapkan ke program studi yang telah memberikan kesempatan untuk melakukan penelitian ini serta ucapan terimakasih juga penulis ucapkan kepada orangtua yang telah memberikan dukungan.

DAFTAR PUSTAKA

[1] Tuti Nurhaeni, et.al, 2016, "Rancangan Virtual Account Sebagai Media Pembayaran Pada Perguruan Tinggi Raharja", Vol. 2, No. 2, ISSN : 2356-5195
[2] Dani Indra Junaedi, 2018, "Peluang Keamanan Password Dalam Transaksi Perbankan", Jurnal ilmu Informatika dan Manajemen STMIK", Vol. 12, No. 1, ISSN : 1978-3310
[3] Muhammad Thareq Parsaulian, et.al, 2020, "Implementasi Algoritme Salsa20 Untuk Pengamanan Search Keyword Dokumen Terenkripsi", Jurnal Pengembangan Teknologi Informasi, Vol. 4, No. 10, e-ISSN : 2548-964X
[4] Rapli Maulana Aji, et.al, 2023, "Implementasi Algoritme Salsa20 Untuk Mengamankan Data GPS Menggunakan Perangkat Raspberry Pi 3", Jurnal Teknik Informatika Dan Sistem Informasi", Vol. 10, No. 2, E-ISSN : 2503-2933
[5] Paulus Lucky Tirma Irawan, et.al, 2014, "Implementasi Kripto-Steganografi Salsa20 dan BPCS Untuk Pengamanan Data Citra Digital", Jurnal EECCIS, Vol. 8, No. 2.
[6] Alif Khamsyar, 2022, "Aplikasi Enkripsi Gambar Menggunakan Metode (Rivest Shamir Adleman) RSA", Jurnal Sintaks Logika, Vol. 2, No. 3.
[7] Tamado Ramot Sitohang, et.al, 2019, "Kriptosistem Gabungan S-ECIES dan RSA, Jurnal Eurekamatika", Vol. 7, No. 1
[8] Hilda Dwi, et.al, 2023, "Implementasi Kriptografi Advanced Encryption Standard 128 Bit Dalam Pengamanan Data Keuangan Kas", Jurnal Jukomtek, Vol. 01, No. 02
[9] Julieta Adhelia Pratiwi, 2022, "Penggunaan QR Code Berbasis Kriptografi Menggunakan Algoritma Elliptic Curve Cryptography", JINACS, Vol. 3, No. 4
[10] SB. Sinaga, 2018, "Pengamanan Pesan Komunikasi Menggunakan Algoritma RSA, Rabbin Miller dan Fungsi SHA-1 Serta Penanganan Man In The Middle Attack Dengan Interlock Protocol", Jurnal Teknik Informatika Unika St. Thomas, Vol. 03, No. 01, ISSN : 2548-1916
[11] Angger Ramadhan, et.al, 2021, "Implementasi Algoritme Enkripsi Salsa20 Untuk Pengamanan data Video Surveilans Secara Real-Time", Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, Vol. 5, No. 2
[13] Fery Fernando, et.al, 2022, "Implementasi Super Enkripsi Menggunakan Metode Rail Fence Cipher dan Metode Caesar Cipher Pada data Pasien Klinik Eka Karigas", Jurnal J-SAKTI, Vol. 6, No. 2, ISSN: 2584-9771