Implementasi Enkripsi Data MD5 dan SHA-256 pada Sistem Informasi Peminjaman Buku Tanah

Implementation of MD5 and SHA-256 Data Encryption in the Land Book Lending Information System

Hajra Rasmita Ngemba[1], Ifandi[2], Syaiful Hendra[3], I Gusti Ngurah Agung Kade Dwi Arsana[4]
[1,2,3,4]Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Tadulako
E-mail: [1]hajra.rasmita@gmail.com, [2]ifandiifan@gmail.com,
[3]syaiful.hendra.garuda@gmail.com, [4]ngurahagung543@gmail.com

Abstrak

Setiap lapisan masyarakat harus memperhatikan keamanan sistem informasi untuk menghindari kejahatan dunia maya. Keadaan ini menimbulkan risiko yang harus dikelola untuk melindungi aset dari kejahatan dunia maya. Oleh karena itu diperlukan kriptografi. Tujuan dari penelitian ini adalah mengimplementasikan algoritma MD5 dan SHA-256. Data password pengguna sistem informasi peminjaman buku tanah ATR/BPN Kota Palu dienkripsi. Dengan menggunakan kolaborasi kedua algoritma tersebut, sistem dapat memanfaatkan kecepatan MD5 untuk menghitung hash dari input, serta keamanan dari SHA-256 untuk mengamankan hash tersebut. Selain itu, menggunakan dua algoritma sekaligus, kemungkinan terjadinya tabrakan (collision) akan menjadi lebih kecil. Metode pengembangan sistem untuk penelitian lanjutan adalah metode waterfall. Hasil penelitian disimpulkan bahwa kolaborasi fungsi MD5 dan SHA-256 dapat mengenkripsi data password pengguna dengan tingkat keamanan yang baik sehingga aman untuk digunakan setelah dilakukan pengujian rainbow table attack, timing attack safe dan avalanche effect. Setelah pengujian tersebut, menunjukkan bahwa fungsi sistem dapat dijalankan tanpa masalah dengan diimplementasikannya kedua kolaborasi fungsi tersebut.

Kata kunci: Enkripsi, MD5, SHA-256, Sistem, Keamanan

Abstract

Every level of society must pay attention to the security of information systems to avoid cyber crimes. This situation creates risks that must be managed to protect assets from cybercrime. Therefore cryptography is needed. The purpose of this research is to implement the MD5 and SHA-256 algorithms. Password data for users of the Palu City ATR/BPN land book lending information system are encrypted. By using the collaboration of the two algorithms, the system can take advantage of the speed of MD5 to calculate the hash of the input, as well as the security of SHA-256 to secure the hash. In addition, using two algorithms at the same time, the possibility of collisions will be smaller. The system development method for further research is the waterfall method. The results of the study concluded that the collaboration of the MD5 and SHA-256 functions can encrypt user password data with a good level of security so that it is safe to use after testing the rainbow table attack, timing attack safe and avalanche effect. After the test, it shows that the system functions can be run without problems with the implementation of the two collaboration functions.

Keywords*: Encryption, MD5, SHA-256, System, Security*

1. PENDAHULUAN

Dengan renstra 2020-2024, Kementerian Komunikasi dan Informatika menargetkan pembangunan infrastruktur digital nasional yang lebih terstruktur dan berskala besar. Dari sisi pemerintahan dan pelayanan publik, Kementerian Komunikasi dan Informatika telah melaksanakan transformasi digital pemerintah, antara lain melakukan percepatan pembangunan

dan pemanfaatan pusat data nasional untuk satu data nasional, dan percepatan implementasi sistem pemerintahan berbasis elektronik (SPBE)[1]. Ada beberapa strategi dan faktor yang perlu diperhatikan dalam menghadapi transformasi digital, salah satunya adalah keamanan. Dengan banyaknya ancaman yang terbukti dari pelanggaran data digital dan kejahatan dunia maya, keamanan data yang baik dan efektif sangat diperlukan untuk proses transformasi digital[2]. Salah satu instansi pemerintahan yang melaksanakan transformasi digital yaitu kantor ATR/BPN kota Palu.

Berdasarkan jumlah penduduk kota Palu 373.857 jiwa dengan kepadatan penduduk 1.049 jiwa/km^2 [3]. Mayoritas penduduk kota Palu telah terdaftar tanahnya pada kantor ATR/BPN kota Palu. Dengan data pertanahan berjumlah ratusan ribu di ruang warkah membuat pekerjaan petugas warkah dalam pengelolaan data pertanahan tidak efisiensi secara tenaga dan waktu dikarenakan pendataan peminjaman buku tanah masih bersifat manual (tulis tangan). Selain itu, ada banyak kasus di mana data pertanahan seperti surat ukur dan buku tanah hilang. Hal ini semakin memperumit pekerjaan yang harus dilakukan ketika data pertanahan sengaja atau tidak sengaja dihilangkan oleh pihak yang tidak bertanggung jawab karena tidak adanya manajemen peminjaman yang sistematis. Untuk itu diperlukan pengelolaan data tanah dengan menggunakan teknologi informasi. Hal ini berkaitan dengan karakteristik data pertanahan itu sendiri yang bersifat *multidimensional* dan terkait dengan persoalan ekonomi, politik, pertahanan dan keamanan, serta sosial budaya. Data pertanahan, seperti data yang disimpan dalam surat ukur dan buku tanah, memiliki utilitas dan nilai arsip yang luar biasa karena sifatnya yang sangat dinamis [4]. Untuk itu, perlunya dibuatkan sistem informasi dalam pengelolaan data pertanahan.

Mengenai sistem informasi tentunya tidak lepas dari keamanan. Sistem informasi yang rentan dapat menjadi ancaman bagi infrastruktur penting perusahaan. Kerentanan adalah segala jenis kerentanan yang memungkinkan penyerang masuk ke sistem secara ilegal dan mengambil tindakan yang tidak diinginkan.[5]. Oleh karena itu , diperlukan kriptografi. Tujuan enkripsi adalah untuk melindungi kerahasiaan data sehingga orang yang tidak berwenang tidak dapat dengan mudah melihat informasi tersebut. Enkripsi mengubah data asli (sering disebut *plaintext*) dengan data yang dihasilkan (data sensitif disebut *ciphertext*).[6]. Enkripsi data memiliki fungsi terkenal yang disebut *hashing*. Fungsi *hash* satu arah adalah untuk mengambil panjang data acak dan mengubahnya menjadi nilai *hash* ukuran tetap (tetap)[7].

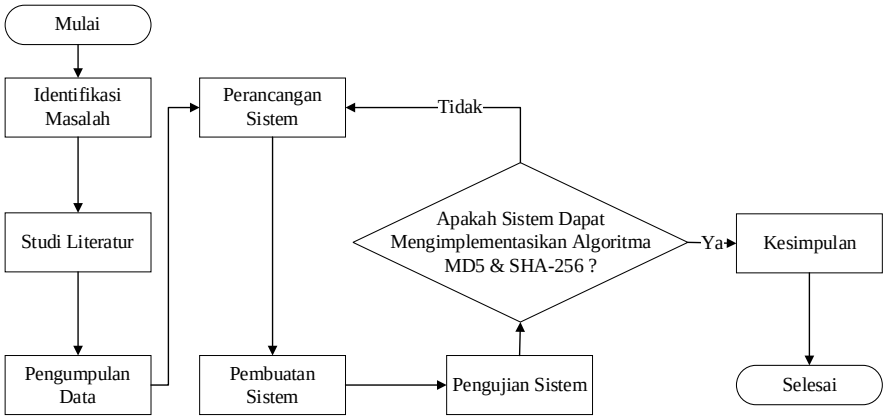
Ada dua jenis fungsi *hash* yaitu fungsi *hash* satu arah dan dua arah. Fungsi *hash* satu arah hasil *hash* (*hash value*) sangat sulit dikembalikan ke nilai *hash* awal. MD5 dan SHA-256 merupakan diantara berbagai macam fungsi *hash* yang ada. MD5 adalah fungsi matematika yang memodifikasi variabel data yang berukuran besar kemudian disederhanakan. Sebaliknya SHA-256 adalah fungsi *hash* satu arah yang dirancang oleh Institut Standar dan Teknologi Nasional (NIST) pada tahun 2002 dan versi SHA-2 [6].

Penelitian yang dilakukan oleh [6] menggunakan algoritma kolaboratif, yaitu enkripsi dengan *Message-Digest Algorithm* 5 (MD5) dan *Secure Hash Algorithm* 256 (SHA-256), untuk menguji perangkat lunak penyerang *CrackStation* dan ditunjukkan hasil *Rainbow*. Pengkodean tabel cukup aman terhadap serangan *brute force*. Hasil uji efek longsoran adalah 71% *AE*. Ini berarti bahwa hasil pengkodean sangat baik. MD5 masih sangat populer sebagai metode enkripsi data[8]. Meskipun algoritma MD5 dan SHA-256 memiliki kompleksitas yang sama ($\Theta(N)$), kita dapat melihat bahwa MD5 mengungguli SHA-256 dalam hal kecepatan eksekusi[7]. tetapi algoritma ini rentan terhadap serangan yang dapat menghasilkan *hash* yang sama dari *input* yang berbeda. Tabrakan (*Collision*) MD5 sangat jarang terjadi, tetapi bukan berarti aman[8]. Algoritma SHA-256 lebih aman dibandingkan MD5[9], tetapi membutuhkan waktu yang lebih lama untuk menghitung *hash* dari *input*. Algoritma SHA-256 adalah fungsi *hash* yang cukup aman untuk meng-*hash byte* data menjadi *string*[10]. Dengan menggunakan kolaborasi kedua algoritma tersebut, sistem dapat memanfaatkan kecepatan MD5 untuk menghitung *hash* dari *input*, serta keamanan dari SHA-256 untuk mengamankan *hash* tersebut. Selain itu, menggunakan dua algoritma sekaligus, kemungkinan terjadinya tabrakan (*collision*) akan menjadi lebih kecil.

Berdasarkan uraian permasalahan tersebut dan penelitian yang terkait, maka penulis bermaksud melakukan penelitian dengan tujuan mengimplementasikan kolaborasi antara fungsi MD5 dan SHA-256 dalam mengenkripsi data kata sandi pengguna pada sistem informasi peminjaman buku tanah ATR/BPN kota Palu. Meskipun telah ada penelitian yang menggunakan fungsi MD5 dan SHA-256 pada sistem, melalui penelitian ini dilakukan pengembangan pengujian algoritma lebih mendalam dengan menggunakan 3 metode terhadap penggunaan fungsi MD5 dan SHA-256 untuk mengetahui tingkat keamanan sistem dari serangan siber. Pengujian dilakukan untuk mengidentifikasi kelemahan dalam sistem keamanan terkait penggunaan kata sandi, mengidentifikasi kerentanan waktu dalam sistem keamanan pada otentikasi kata sandi serta mengukur sejauh mana fungsi MD5 dan SHA-256 mencapai efek *avalanche effect* . Manfaat dilakukan penelitian ini agar menghasilkan sebuah sistem informasi dengan tingkat keamanan yang baik dalam menunjang terwujudnya kinerja dan operasional yang lebih baik lagi pada kantor ATR/BPN kota Palu.

2. METODE PENELITIAN

Jenis penelitian kualitatif digunakan dalam penelitian ini. Penelitian dilaksanakan di kantor ATR/BPN Kota Palu, dengan tema penelitian implementasi kolaborasi algoritma MD5 dan algoritma SHA-256 pada sistem informasi peminjaman buku tanah ATR/BPN Kota Palu. Teknik pengumpulan data dilakukan dengan mengamati langsung objek yang diteliti, mewawancarai pihak-pihak yang terlibat dalam membantu pembuatan sistem, dan mengkaji literatur dari berbagai sumber. Untuk dapat menguraikan masalah yang akan digunakan untuk memecahkan masalah yang ada dalam penelitian ini. Metode pengembangan sistem yang digunakan dalam penelitian ini adalah metode *waterfall*. Pada penelitian ini terdapat beberapa tahap penelitian agar penelitian dapat berjalan dengan baik. Berikut tahapan-tahapan dari penelitian ini yang dapat dilihat pada gambar. 1.



Gambar. 1 *Flowchart* Tahapan Penelitian

2.1 Identifikasi Masalah

Identifikasi masalah merupakan tahapan yang dilakukan dengan menemukan, mempelajari dan memecahkan masalah dengan membangun sebuah sistem. Permasalahan yang ditemui yaitu pendataan peminjaman buku tanah yang masih bersifat manual (tulis tangan) yang dilakukan oleh petugas warkah pada kantor ATR/BPN kota Palu.

2.2 Studi Literatur

Penelitian kepustakaan merupakan tahap pertama pengumpulan bahan, informasi dan referensi yang relevan dengan topik penelitian yang dilakukan untuk memecahkan masalah.

2.3 Pengumpulan Data

Pengumpulan data merupakan langkah yang dilakukan melalui pengumpulan data yang digunakan dalam penelitian ini yaitu data laporan peminjaman buku tanah dan data buku tanah yang disimpan diruang warkah. Selama pengumpulan data, dilakukan juga wawancara data melalui sesi tanya jawab dan dialog langsung dengan pihak-pihak terkait, serta mendukung pengembangan sistem dan observasi langsung terhadap subyek penelitian.

2.4 Perancangan Sistem

Perancangan sistem merupakan tahapan yang dilakukan untuk merancang sistem yang akan dibuat. Pada tahapan perancangan sistem yang akan dilakukan yaitu perancangan desain tampilan dan basis data sistem. Metode pengembangan sistem menggunakan metode *waterfall*. Menurut [11] model *waterfall* menggunakan pendekatan yang sistematis dan berurutan. Tahapan model *waterfall* meliputi persyaratan, desain, implementasi, verifikasi, dan pemeliharaan.

2.5 Pembuatan Sistem

Pembuatan sistem adalah langkah menuju implementasi hasil desain yang dicapai sebelumnya. Tahapan ini juga mengimplementasikan fungsi *Message Digest Algorithm* (MD5) dan *Secure Hash Algorithm* (SHA-256) dalam mengenkripsi data *password* pengguna pada sistem informasi peminjaman buku tanah ATR/BPN kota Palu.

Algoritma MD5 (Message Digest 5) dirancang oleh Ron Rivest. Besarnya blok untuk MD5 adalah 512 bit sedangkan *digest size* adalah 128 bit. Karena *word size* ditentukan sebesar 32 bit, satu blok terdiri dari 16 *word* sedangkan *digest* terdiri dari 4 *word*. MD5 mengolah blok 512 bit, dibagi ke dalam 16 sub blok berukuran 32 bit. Keluaran algoritma diset menjadi 4 blok yang masing-masing berukuran 32 bit yang setelah digabungkan akan membentuk nilai *hash* 128 bit. MD5 terdiri atas 64 operasi, dikelompokan dalam empat putaran dari 16 operasi.

Fungsi *hash* SHA-256 merupakan versi SHA dengan ukuran *digest* 256 pada versi SHA-2. SHA merupakan singkatan dari *Secure Hash Algorithm* adalah fungsi *hash* satu arah yang dibuat oleh NIST (*National Institute of Standard and Technology*). SHA-256 menggunakan enam logika, di mana setiap fungsi beroperasi pada 32-bit, yang direpresentasikan sebagai x, y, dan z. Fungsi logika tersebut merupakan kombinasi dasar seperti AND, OR, XOR, pergeseran bit ke kanan (*shift right*), dan rotasi bit ke kanan (*rotate right*). SHA-256 mengubah pesan masukan ke dalam *message digest* 256 bit. Berdasarkan *Secure Hash Signature Standard*, pesan masukan yang panjangnya lebih pendek dari 264 bit, harus dioperasikan oleh 512 bit dalam kelompok dan menjadi sebuah *message digest* 256-bit [6].

2.6 Pengujian Implementasi Algoritma

a. Pengujian *Rainbow Table Attack*

Pengujian *rainbow table attack* dilakukan untuk menentukan kerentanan algoritma otentikasi kolaborasi MD5 dan SHA-256 menggunakan *hash* akun *login* pengguna. Pengujian ini menggunakan nilai *hash* pengguna yang valid untuk kemudahan pengujian. Pengujian dijalankan untuk mengambil teks biasa (*plaintext*) dengan mencari nilai *hash* yang disimpan dalam *database* tabel *hash*[12]. Perangkat lunak penyerang yang digunakan dalam pengujian adalah *RainbowCrack*, yang menggunakan *database* dari *https://crackstation.net* yang berisi

total sekitar 16,5 miliar tabel pencarian data dan *database hash* yang berisi lebih dari 1,5 miliar *hash* kata sandi. *Rainbow tables* memungkinkan mempercepat proses peretasan kata sandi dengan menyesuaikan jenis *hash* yang digunakan. Sebagian besar *rainbow tables* dapat memecahkan hampir semua *hash* kata sandi yang ada[13].

b. Pengujian *Timing Attack Safe*

Metode pengujian mengadopsi dari metode yang digunakan oleh [14] , dimana dicoba observasi buat memandang apakah terdapat perkembangan waktu pemrosesan sebanding dengan panjang *input*. Implementasi yang tahan terhadap *timing attack* bisa dikatakan *timing attack safe*. *Timing attack* sendiri merupakan serbuan yang melaksanakan eksploitasi pengukuran waktu pemrosesan algoritma ataupun tahapan dalam algoritma buat memperoleh informasi rahasia. Salah satu metode membenarkan algoritma tahan terhadap *timing attack* merupakan dengan membenarkan algoritma berjalan dengan *constant-time*, ialah membutuhkan waktu pemrosesan yang sama buat tiap eksekusi[15].

c. Pengujian *Avalanche Effect*

Avalanche effect adalah rasio jumlah bit *ciphertext* yang berubah sebagai akibat dari perubahan *plaintext* terhadap jumlah total bit. Jika perubahan bit adalah setengah (50%) dari jumlah bit dalam *ciphertext*, maka sulit dipecahkan. Pengujian ini memungkinkan untuk menguji *avalanche effect* (transformasi *plaintext*) dalam proses enkripsi, menentukan perubahan bit *plaintext*, dan mendapatkan hasil persentase yang menentukan apakah algoritma tersebut baik atau buruk. Rumus *avalanche effect* dapat dilihat pada persamaan berikut[16].

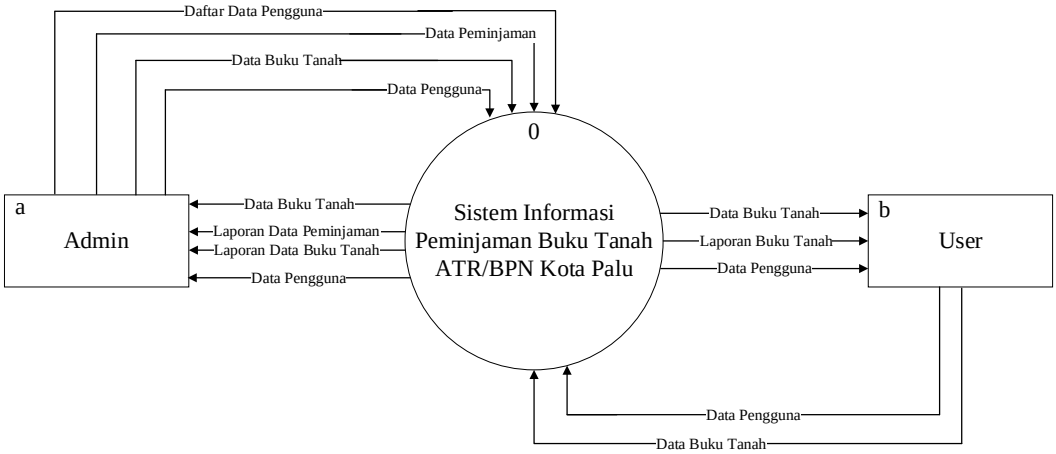
$$AE = \frac{Jumlah\ bit\ yang\ berubah}{Jumah\ bit\ total}\ X\ 100\% \quad (1)$$

3. HASIL DAN PEMBAHASAN

3.1 Pemodelan Sistem

a. Diagram Konteks

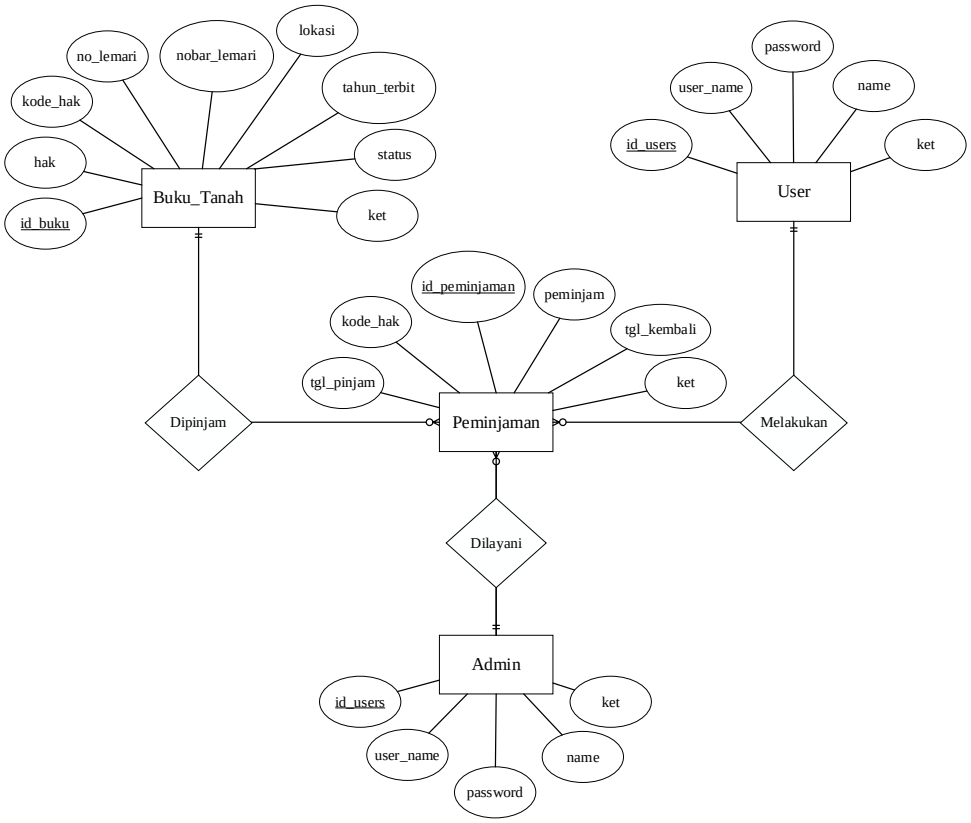
Skema diagram konteks Sistem Informasi peminjaman buku tanah ATR/BPN kota Palu dapat dilihat pada gambar. 2.



Gambar. 2 Diagram Konteks Sistem Informasi Peminjaman Buku Tanah ATR/BPN Kota Palu

b. *Entity Relationship Diagram* (ERD)

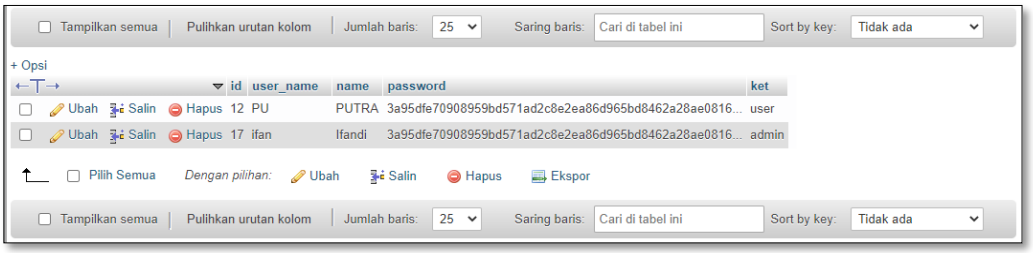
Skema *entity relationship diagram* (ERD) Sistem informasi peminjaman buku tanah ATR/BPN kota Palu dapat dilihat pada gambar. 3.



Gambar. 3 *Entity Relationship Diagram* (ERD) Sistem Informasi Peminjaman Buku Tanah ATR/BPN Kota Palu

3.2 Implementasi Algoritma

Implementasi algoritma dilakukan dengan mengacu pada beberapa literatur khusus tentang enkripsi data *password* pengguna. Salah satu referensi adalah penelitian yang dilakukan oleh[6]. Implementasi algoritma adalah proses implementasi atau pembuatan kode program dari algoritma yang telah ditentukan. Pada penelitian ini, hasil implementasi algoritma dapat dilihat pada basis data sistem di mana *password* pengguna terenkripsi. Basis data dapat dilihat pada gambar. 4.

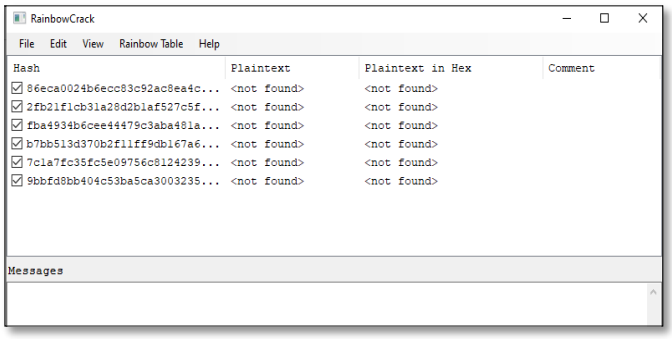


Gambar. 4 Tampilan Basis Data Tabel Pengguna

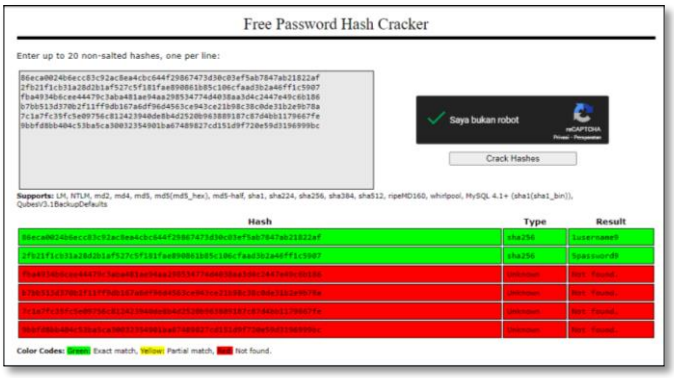
3.3 Pengujian Implementasi Algoritma

a. *Rainbow Table Attack*

Data *plaintext* yang disiapkan untuk diuji dalam penelitian ini secara berurutan yaitu “username” , “password” , “ifandi” , “kampus” , “informatika” dan “xenon”. Pengujian dilakukan menggunakan *software RainbowCrack* dan *CrackStation*. Hasil pengujian *Rainbow table attack* dengan menggunakan *software RainbowCrack* dapat dilihat pada gambar. 5 dan hasil pengujian menggunakan *CrackStation* dapat dilihat pada gambar. 6.



Gambar. 5 Hasil Pengujian *RainbowCrack*

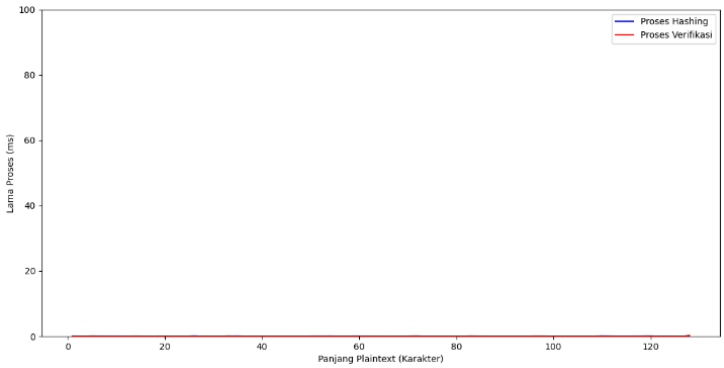


Gambar. 6 Hasil Pengujian *CrackStation*

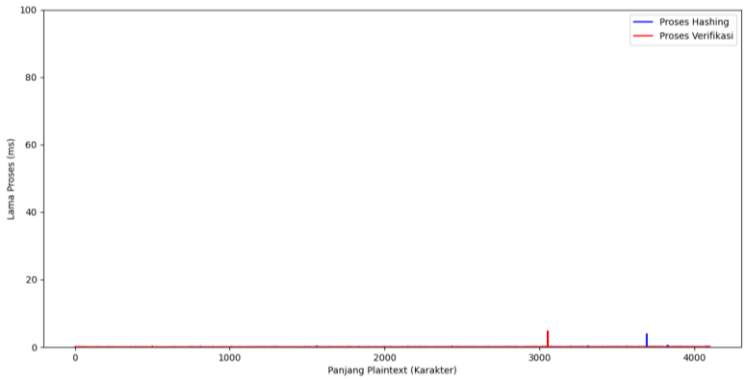
Dari hasil pengujian, dapat diketahui implementasi kolaborasi algoritma MD5 dan SHA-256 dengan pengujian menggunakan *software RainbowCrack* bahwa semua *ciphertext* yang dihasilkan tidak dapat diselesaikan atau diubah menjadi *plaintext*. Sedangkan untuk pengujian menggunakan *CrackStation* bahwa 2 dari 6 *plaintext* menghasilkan *ciphertext* yang dapat diselesaikan atau dikembalikan dalam format teks biasa (*plaintext*).

b. *Timing Attack Safe*

Pengujian dilakukan dengan membandingkan *hash* pada *input* atau *password* dari panjang 1 hingga 4096 karakter. Pada pengujian ini, beban komputasi implementasi kolaborasi algoritma MD5 dan SHA-256 (iterasi *hashing*) dikurangi agar berada dalam jangkauan yang kecil. Hasil pengujian implementasi kolaborasi algoritma MD5 dan SHA-256 dapat dilihat sebagai berikut.



Gambar. 7 Grafik Waktu Pemrosesan *Hashing* Dan Verifikasi *Hash* 1-128 Karakter Implementasi Kolaborasi MD5 & SHA-256



Gambar. 8 Grafik Waktu Pemrosesan *Hashing* Dan Verifikasi *Hash* 1-4096 Karakter Implementasi Kolaborasi MD5 & SHA-256

Berdasarkan grafik pengujian *timing attack safe*, dapat diketahui bahwa implementasi kolaborasi algoritma MD5 dan SHA-256 dengan pengujian panjang *input* atau *password* 1 sampai 128 karakter pada gambar. 7 dan panjang *input* atau *password* 1 sampai 4096 karakter pada gambar. 8 menunjukkan kedua grafik bernilai *constant-time* dalam mencapai waktu pemrosesan *hashing*.

c. *Avalanche effect*

Pengujian ini menggunakan kolaborasi algoritma MD5 dan SHA-256 untuk kata sandi. Data yang akan diuji adalah pesan (*plaintext*) dengan melihat seberapa banyak keluaran atau *hash* berubah ketika karakter diubah. Kemudian hasil *hash* dibandingkan. Mengetahui berapa bit karakter yang diubah dalam satu kali perubahan. Setelah mengetahui jumlah bit yang diubah, hal ini dihitung dengan menggunakan rumus *AE* (*avalanche effect*). Hasil tes ditunjukkan dalam bentuk tabel sebagai berikut.

Tabel. 1 Hasil Pengujian *Avalanche Effect Plaintext* Huruf

Plaintext	***Hash***	**Jumlah Bit Yang Berubah**	**Jumlah Bit**	***Avalanche Effect***
username	86eca0024b6ecc83c92ac8ea4cbc644f29867473d30c03ef5ab7847ab21822af	163	256	64%
tsername	d2fb6aae9dbad58f937a675180a36e2340f1301761a26c6b609b2fc012815452			
password	2fb21f1cb31a28d2b1af527c5f181fae890861b85c106cfaad3b2a46ff1c5907	168	256	66%
passwort	b2a1c7d008338401ada65b4a95acf34cb864d4536eccfa2a506de985a7eabb91			
ifandi	fba4934b6cee44479c3aba481ae94aa298534774d4038aa3d4c2447e49c6b186	155	256	61%
ivandi	ffb3ac14471cf5a4219b3894080d301f85cb66ef26751d49d8b8a44176223574			
kampus	b7bb513d370b2f11ff9db167a6df96d4563ce943ce21b98c38c0de31b2e9b78a	152	256	59%
kanpus	05fc6a5326293724902c2183d94f14bd066aa7437f8d6f5ef9ce04ecf94f44d7			
informatika	7c1a7fc35fc5e09756c8124239440de8b4d2520b963889187c87d4bb1179667fe	163	256	64%
informatyka	d9ee02b983c33e0fcd26ed1cb24558d05a619369c2270976cac67c6675ad9255			
xenon	9bbfd8bb404c53ba5ca30032354901ba67489827cd151d9f720e59d31996999bc	171	256	67%
senon	a7ac1eebee3b4d58299a47c34535d57dbc4bae9b0d6c4905eb0a1aa81092a153			
Mean				64%

Berdasarkan data Tabel 1 bahwa hasil pengujian dengan data *plaintext* berupa huruf memiliki nilai *avalanche effect* lebih dari 50% pada masing-masing *hashing* dari *plaintext* dan nilai rata-rata *avalanche effect* dari semua data *plaintext* yang diuji sebesar 64%.

Tabel. 2 Hasil Pengujian *Avalanche Effect Plaintext* Angka

Plaintext	***Hash***	**Jumlah Bit Yang Berubah**	**Jumlah Bit**	***Avalanche Effect***
12000323	638f4b3a36e6b67085b16c32dff128f610d4f9cedc966eeb8bc9007130bb9291	150	256	59%
12010323	17de83933c73747b85e79b144d0cf2e87b366d2dbb82123747cc0d81bc107083			
45698255	cffa9cb3880036e97e2846565f4420716ee26e0256b1feee8c54e1e84526d23c	175	256	68%
35698255	8506f9ed9443a58af3975fec2c925b58b65daabb44be09f0ec7637c047a94dcf			
7789905 2	3e459be99a6cb3eb6bef1339aa1b637d42a76112e5bcc386e26db15688f9473e	182	256	71%
7789905 1	efaf491cdd2ce95c03ec7ddc0ed13d99a3cb52e22267b1758c8c1d55d6efd9c5			
0000000 4	3c3108e4226831256b541eac272280f62b14a2dba351d3dad2133 5e21b8913a6	158	256	62%
0000000 3	6aa5dfaa6c0005793422c3719f124afb6a9b4e56608eaa44e833c75bc9a0e0be			
12345678	09eff806869c74f74df314d5883777f385767ee8eb7fcf2a212e1a8e6bd8ecf45	172	256	67%
12245678	b76ff6a3dc71f7a5be3949e3c72d486a3768666ee950ae4d1ecfd35e772b26120			
4242311 1	14dc8e5d8aac09919f2507bbc8ae2a32743a09be550e35083edbd66fabc80e1e	179	256	70%
4242316 1	227db3b38255584ee407758a996feccf67419ee14ce4c8bca7c9e90bd26b8b12			
Mean				66%

Berdasarkan data tabel. 2 bahwa hasil pengujian dengan data *plaintext* berupa angka memiliki nilai *avalanche effect* lebih dari 50% pada masing-masing *hashing* dari *plaintext* dan nilai rata-rata *avalanche effect* dari semua data *plaintext* yang diuji sebesar 66%.

Tabel. 3 Hasil Pengujian *Avalanche Effect* Kombinasi *Plaintext* Huruf Dan Angka

Plaintext	***Hash***	**Jumlah Bit Yang Berubah**	**Jumlah Bit**	***Avalanche Effect***
d1g1ta l	d8c46caedf98cbe5d66db5f8d2448ae638342d158a70225c94be8ebc14865c0e	194	256	76%
d1g1t4 l	2315153495f83789cb8ec63e3efe3899d4b669f8694b7841a5912822ff0a923e			
k0mput3r	97ab13226664ffdef3890c627077d8721030c9b9546e4c631c86519df79d2bf7	176	256	69%
c0mput3r	18d9f53b9048afbca7db9421863c2708ea3428dc1c89c5a8c6b565330e194c4c			
b1nt4n5	41db783fdb5f95e53806cb69aa094d37b0693006cb828dffc6a2f4b36aa6e177	181	256	71%
b1nt4ng	88d7dd0f7d7f5c06f14e380b57db52606ded99744daff96852834886505f561e			

Plaintext	***Hash***	**Jumlah Bit Yang Berubah**	**Jumlah Bit**	***Avalanche Effect***
1f4nd1	5bc348df54f665159ea50427bfbae0438d0a9b70e3ad507f62855c8289949c338	171	256	67%
1v4nd1	57e367730cda2e7b1cd6a7c1ee3ed47bf1e6ec9330d70cb26eb31ba1e9ca2da8			
p3n5uj1an	5007ee4ef6ac9dacafb5d9a9cccff03427f8251c2a75369386fa5d14be997811	171	256	67%
p3n6uj1an	02ff89372097d021f6365c1341013 0c848a13e9cbd03699be72e921b06ac7678			
4v4lanch3	392a7549c61f6bbba0cda6822e32e10c49526a6db75daaec5ca007e63b13fbbe	165	256	64%
8v4lanch3	2355426654f203011e2b8d2bd24c601ea2e99243b21de91d4e900cdb552dd1e9			
Mean				69%

Berdasarkan data Tabel 3 bahwa hasil pengujian dengan data *plaintext* berupa kombinasi huruf dengan angka memiliki nilai *avalanche effect* lebih dari 50% pada masing-masing *hashing* dari *plaintext* dan nilai rata-rata *avalanche effect* dari semua data *plaintext* yang diuji sebesar 69%.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan pengujian dan pembahasan implementasi kolaborasi *Message Digest Algorithm* (MD5) dan *Secure Hash Algorithm* (SHA-256) pada sistem informasi peminjaman buku tanah ATR/BPN kota Palu, hasil penelitian menghasilkan kesimpulan sebagai berikut:

a. Fungsi sistem dengan mengimplementasikan kolaborasi algoritma MD5 dan SHA-256 dapat dijalankan tanpa masalah.
b. Pengujian *rainbow table attack* menggunakan *RainbowCrack*, semua *plaintext* yang diuji menghasilkan *ciphertext* tidak dapat diselesaikan atau diubah menjadi plaintext. Untuk pengujian menggunakan *CrackStation* hasil uji yaitu 2 dari 6 *plaintext* yang diuji dapat diselesaikan atau dikembalikan dalam format teks biasa (*plaintext*).
c. Pengujian *timing attack safe* menghasilkan grafik yang menunjukkan lama waktu yang dibutuhkan untuk proses *hashing* dan verifikasi *hash* dengan nilai *constant-time*.
d. Pengujian *avalanche effect* menghasilkan nilai *avalanche effect* lebih dari 50% pada masing-masing *hashing* dari semua data *plaintext* dan nilai rata-rata *avalanche effect* dari *plaintext* berupa huruf yang diuji sebesar 64%, *plaintext* berupa kombinasi huruf dengan angka yang diuji sebesar 69% dan *plaintext* berupa angka yang diuji sebesar 66%.

4.2 Saran

Dalam menyelesaikan penelitian ini, peneliti menyadari kekurangan pada penelitian ini, dan untuk penelitian selanjutnya menyarankan beberapa perkembangan sebagai berikut:

a. Peneliti berharap keamanan sistem yang dibuat dapat dikembangkan kedepannya dengan menggunakan kolaborasi algoritma *hash* lainnya. Dikarenakan algoritma MD5 rentan terhadap serangan dan sudah tidak layak digunakan dalam keamanan sistem pada perkembangan teknologi saat ini.
b. Dalam pengujian *rainbow table attack* menggunakan *CrackStation* didapatkan hasil bahwa 2 dari 6 *plaintext* yang diuji dapat dikembalikan ke bentuk *plaintext*. Untuk itu, peneliti menyarankan pengujian dilakukan lebih mendalam. Misalnya, menggunakan *software* penyerang lain dan lebih banyak lagi *plaintext password* pengguna yang akan diuji.

DAFTAR PUSTAKA

[1] Kementerian Komunikasi dan Informatika, "Rencana Strategis 2020-2024 Kementerian Komunikasi dan Informatika," *Rencana Strateg. 2020-2024 Kementeri. Komun. dan Inform.*, 2021.

[2] A. N. Panggabean, "Memahami dan mengelola transformasi digital," *E-bus. Strateg. Implement.*, 2018.

[3] R. I. Kementerian Dalam Negeri, "Visualisasi Data Kependudukan," 2020. [Online]. Available: https://gis.dukcapil.kemendagri.go.id/peta/

[4] A. Rachman, "Badan pertanahan nasional republik indonesia sekolah tinggi pertanahan nasional yogyakarta 2012," pp. 1–85, 2012.

[5] N. Pirsa and Sumijan, "Meningkatkan Keamanan Sistem Informasi Puskesmas Terpadu dengan Metode Grey-Box Penetration Test Menggunakan Computer Assisted Audit Techniques," *J. Inf. dan Teknol.*, 2020, doi: 10.37034/jidt.v2i4.79.

[6] S. Sulastri and R. D. M. Putri, "Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan," *J. Tek. Elektro*, vol. 10, no. 2, 2018, doi: 10.15294/jte.v10i2.18628.

[7] M. Benedict, M. A. Budiman, and D. Rachmawati, "Perbandingan Algoritma Message Digest 5 (MD5) Dan GOST Pada Hashing File Dokumen," *J. Tek. Inform. Kaputama*, vol. 1, no. 1, pp. 50–61, 2017.

[8] A. Muhidin and R. Alfianto, "KELEMAHAN METODE ENKRIPSI MESSAGE DIGEST 5 TERHADAP KRIPTANALISIS MODERN," *Kaos GL Derg.*, vol. 11, pp. 161–166, 2020, [Online]. Available: https://doi.org/10.1016/j.jnc.2020.125798%0Ahttps://doi.org/10.1016/j.smr.2020.02.002%0Ahttp://www.ncbi.nlm.nih.gov/pubmed/810049%0Ahttp://doi.wiley.com/10.1002/ane.197505391%0Ahttp://www.sciencedirect.com/science/article/pii/B9780857090409500205%0Ahttp:

[9] Y. Bin Pairin, "Kode Autentikasi Hash pada Pesan Teks Berbasis Android," *Eksplora Inform.*, vol. 8, no. 1, 2018, doi: 10.30864/eksplora.v8i1.129.

[10] A. Fauzi, "Ekstraksi Citra Pada Proses Keamanan Kriptografi Memanfaatkan Algoritma Secure Hash (Sha)," *J. Inform. Kaputama*, vol. 4, no. 1, 2020.

[11] A. A. Wahid, "Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi," *J. Ilmu-ilmu Inform. dan Manaj. STMIK*, no. November, 2020.

[12] Musliy, Z. Ana, T. Y. Arif, and R. Munadi, "Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia," *J. Rekayasa Elektr.*, vol. 12, no. 1, p. 21, 2016, doi: 10.17529/jre.v12i1.2896.

[13] M. Risqi Firdaus, "Analisis Penggunaan Algoritma Bcrypt dengan Garam (Salt) untuk Pengamanan Password dari Peretasan," 2022.

[14] A. Toponce, "Aaron Toponce _ Do Not Use sha256crypt _ sha512crypt - They're Dangerous," 2018. https://pthree.org/2018/05/23/do-not-use-sha256crypt-sha512crypt-theyre-dangerous/ (accessed Dec. 21, 2022).

[15] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1996, vol. 1109. doi: 10.1007/3-540-68697-5_9.

[16] A. Aminudin, A. F. Helmi, and S. Arifianto, "Analisa Kombinasi Algoritma Merkle-Hellman Knapscak dan Logaritma Diskrit pada Aplikasi Chat," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 3, 2018, doi: 10.25126/jtiik.201853844.