Jurnal Quancom
Vol.3, No.1, Juni 2025, pp. 8~12
e-ISSN: 2988-0998
P-ISSN: 2988-1005
DOI : https://doi.org/10.62375/jqc.v3i1.627

Perbandingan Algoritma Kriptografi *Hash Sha* 256 dan *Sha* 512 Untuk Keamanan Sandi

Toras Pangidoan Batubara [1]*, Mhd Adi Setiawan Aritonang [2]
[1] Sistem Informasi, Universitas Murni Teguh
[2] Teknik Komputer, Institut Teknologi Batam
toras@murniteguhuniversity.ac.id
adi@iteba.ac.id

Article Info

Article history:

Received 13 Juni 2025
Revised 18 Juni 2025
Accepted 28 Juni 2025

Keyword:

Hash, *Sha* 256, *Sha* 512, Kriptografi.

ABSTRACT

Hash algorithms are still in great demand for use in data security but there are still many things that need to be tested Time and security of the hash algorithm. the author has tested the hash-256 algorithm and the hash-512 algorithm from testing both hash algorithms found a very unique comparison, namely the results of the hash-256 algorithm encryption of numeric characters are superior to the results of the hash-512 algorithm encryption for numeric characters when the original plaintext is returned. the conclusion is that the encryption of numeric characters from the hash-256 algorithm is safer to use than the results of the hash-512 algorithm encryption..

PENDAHULUAN

Dalam era digital yang terus berkembang pesat, data telah menjadi salah satu aset paling berharga. Hampir semua aktivitas manusia saat ini berkaitan erat dengan penggunaan teknologi informasi dan komunikasi, mulai dari transaksi keuangan, pertukaran informasi pribadi, hingga penyimpanan data penting secara daring (online) [1] Seiring dengan meningkatnya volume dan nilai data digital, tantangan terhadap keamanan data pun menjadi semakin kompleks. Salah satu ancaman terbesar adalah akses tidak sah, pencurian data, serta serangan siber yang dapat menyebabkan kebocoran data dan kerugian besar bagi individu maupun institusi[2].

Untuk mengatasi permasalahan tersebut, kriptografi menjadi teknologi inti dalam pengamanan data. Salah satu metode kriptografi yang paling banyak digunakan adalah algoritma hash. Algoritma hash berfungsi mengubah data menjadi string karakter tetap yang bersifat unik dan irreversible, sehingga sangat cocok untuk penyimpanan kata sandi (password), tanda tangan digital, dan integritas data.[3] Di antara berbagai algoritma hash yang ada, SHA-256 dan SHA-512 merupakan dua varian yang paling populer dalam keluarga SHA-2 yang dikembangkan oleh National Security Agency (NSA) dan distandarisasi oleh NIST (National Institute of Standards and Technology)[4].

Kriptografi, khususnya fungsi hash, merupakan salah satu pendekatan penting dalam menjaga integritas dan keamanan data. Fungsi hash bekerja dengan mengubah input data menjadi string karakter dengan panjang tetap, yang bersifat unik dan tidak dapat dibalik menjadi data aslinya. Oleh karena itu, algoritma hash banyak digunakan untuk menyimpan kata sandi, memverifikasi integritas file, hingga sebagai bagian dari protokol keamanan seperti TLS/SSL[5].

Dalam beberapa tahun terakhir, algoritma hash SHA-256 dan SHA-512 telah menjadi dua algoritma yang paling umum digunakan dalam berbagai aplikasi keamanan data terkhusus aplikasi wabsite[6] .

SHA-256 dan SHA-512 merupakan dua algoritma hash yang dikembangkan oleh National Security Agency (NSA) dan diterbitkan oleh NIST (National Institute of Standards and Technology)[7]. Kedua algoritma tersebut memiliki kelebihan dan kekurangan masing-masing dalam hal kinerja dan keamanan. Oleh karena itu, perlu dilakukan penelitian

untuk membandingkan kedua algoritma tersebut dalam berbagai aspek, sehingga dapat memberikan informasi yang berguna bagi pengembang sistem keamanan data dan pengguna lainnya[8]

Beberapa penelitian menunjukkan bahwa meskipun SHA-512 memiliki tingkat kerumitan yang lebih tinggi dan ukuran. hash yang lebih panjang, dalam konteks tertentu seperti efisiensi dan kecepatan pemrosesan pada perangkat tertentu, SHA-256 justru bisa lebih optimal [1] Selain itu, efektivitas algoritma hash juga sangat bergantung pada jenis data yang dienkripsi, seperti karakter abjad, angka, atau campuran.[9]

Penelitian ini bertujuan untuk membandingkan kinerja algoritma SHA-256 dan SHA-512 dalam berbagai aspek, seperti kecepatan proses, dan keamanan. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan sistem keamanan data yang lebih baik dan lebih aman[10].

Kontribusi dari penelitian ini penting, mengingat banyaknya aplikasi dan sistem yang masih belum mempertimbangkan dengan matang pemilihan algoritma hash berdasarkan jenis data yang diolah. Hasil penelitian ini diharapkan dapat menjadi referensi teknis maupun akademis dalam menentukan strategi perlindungan data yang optimal, khususnya dalam bidang pengamanan kata sandi pada sistem informasi[11].

METODE

Adapun metode yang digunakan pada penelitian ini adalah pengujian kinerja dari enkripsi algoritma hash-256 dan hash-512 kemudian pengujian hasil enkripsi algoritma hash-256 dan hash-512 berdasarkan data yang telah di buat dengan algoritma hash tersebut.

A. Pengujian Kinerja

Pengujian yang dilakukan penulis dalam mencari tahu kinerja setiap algoritma adalah denga cara mencoba berbagai kombinasi karakter dengan menggunakan 8 karakter yaitu

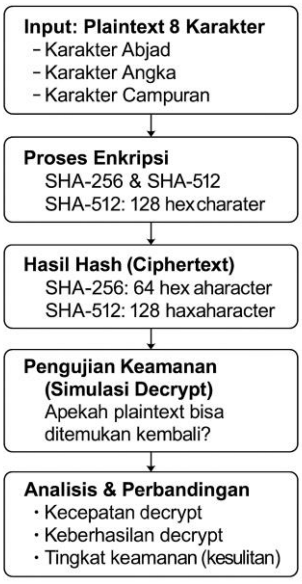
1. Karakter abjad dengan jumlah 8
2. Karakter angka dengan jumlah 8
3. Karakter campuran dengan jumlah 8

Gambar 1. Pengujian kinerja

Setiap karakter akan di uji kemampuan enkripsinya berdasarkan waktu dan keamanan setiap enkripsi hash yang di proses agar di peroleh keamanan dari setiap enkripsi karakter.

B. Pengujian Hasil Enkripsi

Hasil enkripsi algoritma hash 8 karakter akan di uji berdasarkan jenis karakter yang di lakukan untuk keamanan proses enkripsi yang di peroleh setelah di lakukan decrypt algoritma hash berdasarkan jumlah karakter.



Gambar 2. Pengujian kinerja

Pengujian Hasil Enkripsi yaitu SHA-256 dan SHA-512. Tahap pertama dimulai dengan pemberian input berupa plaintext sepanjang 8 karakter yang dibagi menjadi tiga jenis: karakter abjad, karakter angka, dan karakter campuran. Setelah input ditentukan, data kemudian diproses melalui algoritma enkripsi SHA-256 dan SHA-512. Proses ini menghasilkan hash dalam bentuk ciphertext yang bersifat unik dan irreversible, dengan hasil SHA-256 berupa 64 karakter heksadesimal dan SHA-512 menghasilkan 128 karakter heksadesimal[1].

Langkah berikutnya adalah pengujian keamanan melalui simulasi decrypt, yaitu upaya untuk mengembalikan ciphertext menjadi plaintext guna melihat seberapa mudah data dapat dipecahkan kembali. Pengujian ini tidak dilakukan dengan membalik hash secara langsung, melainkan melalui teknik pencocokan seperti brute force atau dictionary attack. Dari proses ini, dilakukan pula pengukuran waktu yang dibutuhkan untuk menemukan kembali plaintext, yang dicatat dalam satuan detik untuk setiap jenis karakter[2].

Tahap terakhir adalah analisis dan perbandingan antara kedua algoritma berdasarkan tiga aspek utama: kecepatan proses decrypt, keberhasilan dalam menemukan kembali plaintext, dan tingkat kesulitan atau ketahanan algoritma terhadap serangan. Hasil dari pengujian ini memberikan gambaran menyeluruh mengenai kekuatan dan kelemahan masing-masing algoritma, serta merekomendasikan algoritma mana yang lebih unggul dalam aspek keamanan untuk karakter tertentu.

HASIL DAN PEMBAHASAN

Setelah penulis lakukan proses enkripsi algoritma hash terhadap hash-256 dan hash-512. Penulis akan mencoba membandingkan waktu dan kemanan beberapa kemampuan hasil proses enkripsi algoritma hash-256 dan hash-512 terhadap proses decrypt yang dihasilkan untuk menghasilkan plaintext asli. Adapun pengujian karakter yang di lakukan penulis berdasarkan top karakter yang sering digunakan[8].

A. Karakter Abjad Hash-256

Proses decrypt algoritma hash-256 yang dilakukan penulis terhadap karakter abjad dengan jumlah 8 karakter mendapatkan hasil sebagai berikut:

TABEL I
DECRYPT SHA-256

No	Plaintext	Hasil Hash-256	Hasil Waktu Decrypt	Hasil Decrypt
1	password	5e884898da28047151d0e56f8dc629277360 3d0d6aabbdd62a11ef721d1542d8	0.97s	Berhasil di Temukan

B. Karakter Abjad Hash-512

Proses decrypt algoritma hash-512 yang dilakukan penulis terhadap karakter abjad dengan jumlah 8 karakter mendapatkan hasil sebagai berikut:

TABEL II
DECRYPT SHA-512

No	Plaintext	Hasil Hash-256	Hasil Waktu Decrypt	Hasil Decrypt
1	password	b109f3bbbc244eb82441917ed06d618b9008 dd09b3befd1b5e07394c706a8bb980 b1d7785e5976ec049b46df5f1 326af5a2ea6d103fd07c95385 ffab0acbc86	1.29s	Berhasil di Temukan

C. Karakter Angka Hash-256

Proses decrypt algoritma hash-256 yang dilakukan penulis terhadap karakter angka dengan jumlah 8 karakter mendapatkan hasil sebagai berikut:

TABEL III
HASIL DECRYPT SHA-256

No	Plaintext	Hasil Hash-256	Hasil Waktu Decrypt	Hasil Decrypt
1	12345678	ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f	1.05s	Berhasil di Temukan

D. Karakter Angka Hash-512

Proses decrypt algoritma hash-512 yang dilakukan penulis terhadap karakter angka dengan jumlah 8 karakter mendapatkan hasil sebagai berikut:

TABEL IV
HASIL DECRYPT SHA-512

No	Plaintext	Hasil Hash-512	Hasil Waktu Decrypt	Hasil Decrypt
1	12345678	fa585d89c851dd338a70dcf535aa2a92fee7836dd6aff1226583e88e0996293f16bc009c652826e0fc5c706695a03cddce372f139eff4d13959da6f1f5d3eabe	0.60s	Berhasil di Temukan

E. Karakter Campuran Hash-256

Proses decrypt algoritma hash-256 yang dilakukan penulis terhadap karakter campuran dengan jumlah 8 karakter mendapatkan hasil sebagai berikut:

TABEL V
HASIL DCRYPT SHA-256

.No	Plaintext	Hasil Hash-256	Hasil Waktu Decrypt	Hasil Decrypt
1	Qwerty1!	195f62edd40a1d9b0c6407104596d6c29e2b408ecc1cc964e8033769 17ab1fd0	0.58s	Berhasil di Temukan

F. Karakter Campuran Hash-512

Proses decrypt algoritma hash-512 yang dilakukan penulis terhadap karakter campuran dengan jumlah 8 karakter mendapatkan hasil sebagai berikut.

TABEL VI
HASIL DECRYPT SHA-512

No	Plaintext	Hasil Hash-512	Hasil Waktu Decrypt	Hasil Decrypt
1	Qwerty1!	7b258781f94f1065d5591935d4a87e4ca738b8940090 7c05f8d55e757a7f98058 08c419 0eef4a9d937eac5beb5a17ea0c0c0b42ec42fa2abd3358fea7fadd34a	0.93s	Berhasil di Temukan

SIMPULAN

Penelitian ini menguji waktu dan keamanan enkripsi dari dua algoritma hash, yaitu hash-256 dan hash-512. Dari hasil yang penulis peroleh berdasarkan dua algoritma hash yang di uji yaitu hash-256 dan hash-512 maka dapat diambil beberapa kesimpulan yaitu: Algoritma hash-256 dan hash-512 memiliki waktu yang berbeda dari sisi keamanan. Waktu keamanan hasil encrypt hash-256 dan hash-512 karakter abjad sangat berbeda dan lebih lama di decrypt ke plainteks asli karakter abjad hash-512. Waktu keamanan hasil encrypt hash-

256 dan hash-512 karakter angka sangat berbeda dan lebih lama di decrypt ke plainteks asli karakter angka hash-256. Waktu keamanan hasil encrypt hash-256 dan hash-512 karakter campuran sangat berbeda dan lebih lama di decrypt ke plainteks asli karakter campuran hash-512.Semua karakter yang di uji penulis bedasarkan waktu dan kemanan terkhusus algoritma has-256 dan hash-512 ada satu keunikan yaitu karakter angka hash-256 lebih unggul saat di decrypt dibandingkan hash-512 artinya algoritma hash-256 karakter angka lebih aman digunakan dibandingkan karakter angka algoritma hash-512.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dalam penyelesaian penelitian ini. Semoga hasil penelitian ini bermanfaat bagi pengembangan keamanan data terkhusus algoritma hash-256 dan algoritma hash-512. Universitas Murni Teguh dan Institut Teknologi Batam, yang telah memberikan fasilitas dan lingkungan akademik yang kondusif bagi pelaksanaan penelitian ini

DAFTAR PUSTAKA

[1] A. Yoshida, H., & Biryukov, "Analysis of a SHA-256 variant.," *Int. Work. Sel. Areas Cryptogr.*, pp. 245–260, 2005.

[2] J. Gueron, S., Johnson, S., & Walker, "SHA-512/256," *2011 Eighth Int. Conf. Inf. Technol.*, pp. 354–358, 2011.

[3] R. Bhanot, R., & Hans, "A review and comparative analysis of various encryption algorithms.," *Int. J. Secur. Its Appl.*, vol. 9, no. 4, pp. 289–306, 2015.

[4] R. Stiawan, D., Idris, M. Y., Malik, R. F., Nurmaini, S., Alsharif, N., & Budiarto, "Investigating brute force attack patterns in IoT network," *J. Electr. Comput. Eng.*, vol. 1, 2019.

[5] B. Guttman, *An introduction to computer security: the NIST handbook* . USA: US Department of Commerce, Technology Administration, National Institute of Standards and Technology., 1995.

[6] A. R. Ramalinda, D., & Raharja, "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi.," *J. Int. Multidiscip. Res.*, 2024.

[7] D. Tewksbury, "National Security Agency (NSA)," *In Encyclopedia of Big Data*. pp. 1–4, 2017.

[8] A. (2009). Fernando, H., & Boyer, "Perbandingan dan pengujian beberapa algoritma pencocokan string," *Makal. IF2251*.

[9] P. J. Chen, V. M., & Hogg, "Encryption and decryption of tissue factor," *J. Thromb. Haemost.*, vol. 11, pp. 277–284, 2013.

[10] N. Mairs, *Plaintext.* University of Arizona Press, 1992.

[11] H. Mukhtar, *Kriptografi untuk Keamanan Data.* 2018.