EVALUASI SKEMA PENGACAKAN *PASSWORD* MENGGUNAKAN KOMBINASI GERBANG LOGIKA TERHADAP TINGKAT KEAMANAN *CHIPERTEXT HASH*

Oleh:

MUHAMAD ZAKI ANBARI

22206051017

PROGRAM STUDI INFORMATIKA

PROGRAM MAGISTER FAKULTAS SAINS DAN TEKNOLOGI

UIN SUNAN KALIJAGA

YOGYAKARTA

2024

PERNYATAAN KEASLIAN

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Muhamad Zaki Anbari

NIM : 22206051017

Jenjang : Magister

Program Studi : Informatika

menyatakan bahwa naskah tesis ini secara keseluruhan adalah hasil penelitian/karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya.

Yogyakarta, 13 Mei 2024

Pernyatakan,

Muhamad Zaki Anbari

NIM: 22206051017

PERNYATAAN BEBAS PLAGIASI

PERNYATAAN BEBAS PLAGIASI

Yang bertanda tangan di bawah ini:

Nama	: Muhamad Zaki Anbari
NIM	: 22206051017
Jenjang	: Magister
Program Studi	: Informatika

menyatakan bahwa naskah tesis ini secara keseluruhan benar-benar bebas dari plagiasi. Jika di kemudian hari terbukti melakukan plagiasi, maka saya siap ditindak sesuai ketentuan hukum yang berlaku.

Yogyakarta, 13 Mei 2024

Saya yang menyatakan,

Muhamad Zaki Anbari

NIM: 22206051017

HALAMAN PENGESAHAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1006/Un.02/DST/PP.00.9/06/2024

Tugas Akhir dengan judul : EVALUASI SKEMA PENGACAKAN PASSWORD MENGGUNAKAN KOMBINASI GERBANG LOGIKA TERHADAP TINGKAT KEAMANAN CHIPERTEXT HASH

yang dipersiapkan dan disusun oleh:

Nama : MUHAMAD ZAKI ANBARI, S.Si
Nomor Induk Mahasiswa : 22206051017
Telah diujikan pada : Rabu, 15 Mei 2024
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM., ASEAN Eng.
SIGNED
Valid ID: 6667e4eba19a0

Penguji I

Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D.
SIGNED
Valid ID: 6678dce24d491

Penguji II

Prof. Dr. Ir. Shofwatul 'Uyun, S.T., M.Kom., IPM., ASEAN Eng.
SIGNED
Valid ID: 6668464466b0

Yogyakarta, 15 Mei 2024
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED
Valid ID: 667bf94da357d

PERSETUJUAN TIM PENGUJI UJIAN TESIS

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

BERITA ACARA UJIAN TUGAS AKHIR

Penyelenggaraan Ujian Tugas Akhir Mahasiswa

A. Waktu, Tempat dan Status Ujian Tugas Akhir:

1. Hari dan Tanggal : Rabu, 15 Mei 2024
2. Pukul : 07:30 s/d 08:30 WIB
3. Tempat : FST-1-101
4. Status : Utama

B. Susunan Tim Ujian Tugas Akhir:

No.	Jabatan	Nama	Tanda Tangan
1.	Ketua Sidang	Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM., ASEAN Eng.	Valid ID: 6667e48b1e11f
2.	Penguji I	Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D.	Valid ID: 6657f424010d9
3.	Penguji II	Prof. Dr. Ir. Shofwatul 'Uyun, S.T., M.Kom., IPM., ASEAN Eng.	Valid ID: 6666869bb74c8

C. Identitas Mahasiswa yang diuji:

1. Nama : MUHAMAD ZAKI ANBARI, S.Si
2. Nomor Induk Mahasiswa : 22206051017
3. Program Studi : Informatika
4. Semester : IV
5. Program : S2
6. Status Kehadiran Mahasiswa : Menghadiri Ujian

D. Judul Tugas Akhir : EVALUASI SKEMA PENGACAKAN PASSWORD MENGGUNAKAN KOMBINASI GERBANG LOGIKA TERHADAP TINGKAT KEAMANAN CHIPERTEXT HASH

E. Pembimbing/Promotor:

1. Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM., ASEAN Eng.

F. Keputusan Sidang

1. LULUS dengan Perbaikan
2. Predikat Kelulusan : 92.00 (A-)
3. Konsultasi Perbaikan a. _____

b. _____

Yogyakarta, 15 Mei 2024
Ketua Sidang/Pembimbing/Promotor,

Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM., ASEAN Eng.
SIGNED

Valid ID: 6667e48b1e11f

NOTA DINAS PEMBIMBING

Yth,
Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta

Assalamu'alaikum Wr. Wb.

Setelah melakukan bimbingan, arahan, dan koreksi terhadap penulisan tesis yang berjudul:

EVALUASI SKEMA PENGACAKAN *PASSWORD* MENGGUNAKAN KOMBINASI GERBANG LOGIKA TERHADAP TINGKAT KEAMANAN *CHIPERTEXT HASH*

Yang ditulis oleh:

Nama	: Muhamad Zaki Anbari
NIM	: 22206051017
Jenjang	: Magister
Program Studi	: Informatika

Saya berpendapat bahwa tesis tersebut sudah dapat diajukan kepada Magister Informatika UIN Sunan Kalijaga untuk diujikan dalam rangka memperoleh gelar Magister Informatika

Wassalamu'alaikum wr wb

Yogyakarta, 13 Mei 2024
Pembimbing,

Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM., ASEAN Eng.

ABSTRAK

Digitalisasi berbagai sektor kehidupan membuat isu keamanan informasi menjadi sangat krusial di era ini. Keamanan informasi mengikuti prinsip-prinsip AAA, di mana salah satu bagian terpentingnya adalah autentikasi. Metode autentikasi yang banyak digunakan adalah *username password*. Metode pengamanan data *username password* yang terbaik adalah dengan mengkonversi *plaintext* menggunakan fungsi hash. Namun, dengan perkembangan teknologi komputasi yang lebih tinggi, peretas dapat menemukan *plaintext* menggunakan metode serangan seperti serangan *brute force*, *rainbow table*, dan lain sebagainya. Penelitian ini mengusulkan algoritma pengacakan *username password* sebelum dimasukkan ke dalam fungsi *hash* untuk meningkatkan ketahanan terhadap serangan peretas. Algoritma yang diusulkan diberi nama algoritma LG (*Logical Gates*). Algoritma ini bekerja dengan cara mengubah *username password* ke dalam bentuk biner, kemudian menambahkan *salt* dan mengacak dengan serangkaian gerbang logika tertentu. Pengujian dibagi menjadi dua yaitu *time of execution test* dan *resistance of attack test*. Hasil pengujian waktu eksekusi menunjukkan LG membutuhkan waktu 0.0443432033 detik, sedangkan tanpa LG membutuhkan waktu 0.01403197646 detik. Hasil pengujian ketahanan terhadap serangan menunjukkan bahwa hash yang diperkuat dengan LG tidak dapat ditemukan sama sekali, sedangkan tanpa LG, teks biasa dapat ditemukan dalam durasi waktu tertentu.

Kata Kunci: *Hashing, Salt, Logical Gates, Binary*, Keamanan Informasi

ABSTRACT

The digitalization of various sectors of life has made information security issues very crucial in this era. Information security follows the principles of AAA, where one of the most important parts is authentication. The most widely used authentication method is username-password. The best username and password security method is to convert its plaintext using a hash function. However, with the development of higher computing technology, hackers can find the plaintext using attack methods such as brute force attacks, rainbow tables, etc. This research proposes a username-password randomization algorithm before it is entered into the hash function to increase resistance to hacker attacks. The proposed algorithm is named the LG (Logical Gates) algorithm. It works by converting the username and password into a binary form, then adding salt and scrambling it with a series of certain logic gates. Testing is divided into two categories: time execution and resistance to attack. Time execution test results show LG takes 0.0443432033 seconds, while without LG it takes 0.01403197646 seconds. The results of the resistance of attack test show that the hash reinforced by LG cannot be found at all, while without LG, plain text can be found for a certain duration of time.

Keywords: *Hashing, Salt, Logical Gates, Binary, Information Security*

MOTTO

اَلعَقلُ وَالفِكرُ مَعدِنُ ذَهَبٍ لَا يَحتَاجُ لِلطَّلَبِ عَنهُ وَشِرَائِهِ

إِذَا كُنتَ تَرغَبُ فِي اسِتخرَاجِ الثَروَةِ، يَكفِى عَلَيكَ حَفرُهَا أَكبَرُ قَدرِ مُمكِن

"Akal dan fikiran adalah tambang emas yang tidak usah dicari dan dibeli. Bila ingin menambang kekayaan cukup menggalinya sepuas mungkin."

KATA PENGANTAR

Bissmillahirahmanirrahim,
Assalamu'alaikum warahmatullahi wabarakatuh

Puji dan syukur kita panjatkan kepada Allah SWT atas nikmat dan hidayah-Nya serta telah memberikan kita kekuatan, kesehatan dan kesabaran. Sehingga penulis dapat menyelesaikan tesis dengan judul "**EVALUASI SKEMA PENGACAKAN *PASSWORD* MENGGUNAKAN KOMBINASI GERBANG LOGIKA TERHADAP TINGKAT KEAMANAN *CHIPERTEXT HASH*"**.

Dalam penyusunan dan penyelesaian karya ini, penulis mengakui banyak mendapat dorongan dan bimbingan dari berbagai pihak. Oleh karena itu, penulis ingin menggunakan kesempatan ini untuk mengucapkan terima kasih kepada:

1. Bapak Ahmad Jauhari dan Ibu Nur Azizah selaku orang tua.
2. Inayah Mumpuni Budiati, M.Si., selaku rekan seperjuangan.
3. Ibu Dr. Khurul Wardati, M,Si, selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
4. Bapak Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM., ASEAN Eng. selaku Kaprodi Magister Informatika sekaligus dosen pembimbing tesis.
5. Bapak Ir. Muhammad Taufiq Nuruzzaman, S.T., M.Eng., Ph.D., selaku dosen penguji dan dosen pembimbing akademik.
6. Ibu Prof. Dr. Ir. Shofwatul 'Uyun, S.T., M.Kom., IPM., ASEAN Eng., selaku dosen penguji.
7. Bapak K. Muhammad Nur Salafuddin Alhafidz dan Keluarga Besar Pondok Pesantren Kyai Galang Sewu.

8. Bapak K.H Abdul Mustaqim dan Keluarga Besar Pondok Pesantren Lingkar Studi Al Quran (LSQ) Ar-Rohmah.
9. Seluruh kawan-kawan Magister Informatika Angkatan 2022.

Penulis juga mengucapkan terima kasih kepada seluruh dosen program Magister Informatika yang telah memberikan banyak ilmu dan wawasan bermanfaat selama pendidikan. Semangat penulis dalam menyelesaikan naskah ini tidak lepas dari dukungan keluarga dan rekan-rekan. Oleh karena itu, penulis juga ingin memanfaatkan kesempatan ini untuk mengucapkan terima kasih kepada seluruh kerabat, terutama orang tua, yang telah mendoakan dan memotivasi hingga menyelesaikan tesis ini dengan baik.

Akhir kata, naskah ini belum sempurna, oleh karena itu penulis sangat menghargai kritik dan saran yang bersifat membangun. Semoga Allah meridhoi langkah kita, Armin. Oleh karena itu, penulis menyusun tesis ini. Semoga tesis ini dapat dikembangkan dan digunakan sesuai kemampuan masing-masing dan semoga Allah SWT selalu memberikan ilmu yang bermanfaat kepada semua orang dan membimbing mereka di jalan Allah.

Wassalamu'alaikum warahmatullahi wabarakatuh.

Yogyakarta, 13 Mei 2024

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

A. LATAR BELAKANG

Perkembangan teknologi yang kian masif menyebabkan banyak aktivitas manusia tidak bisa lepas dari teknologi digital. Misalnya dalam hal komunikasi, mayoritas orang saat ini membutuhkan teknologi seperti telepon dan internet untuk dapat saling berkomunikasi dan mengakses informasi. Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna Internet di Indonesia diperkirakan mencapai 221.563.479 jiwa pada tahun 2024 (Haryanto, 2024). Pengguna internet yang sedemikian besar juga diiringi dengan munculnya layanan-layanan digital di berbagai sektor seperti pendidikan, keuangan, bisnis, dan lain sebagainya. Digitalisasi tersebut semakin memudahkan masyarakat dalam melakukan berbagai aktivitas, namun disisi lain juga meningkatkan resiko kejahatan *cyber*. Menurut data Kaspersky Indonesia terdapat sekitar 29 juta serangan *cyber* terjadi di Indonesia pada tahun 2023 (Pribady, 2024). Oleh karena itu isu tentang keamanan data menjadi isu yang penting untuk diteliti.

Salah satu cara untuk mengamankan data adalah dengan kriptografi. Kriptografi adalah ilmu yang menggunakan matematika dan komputer untuk menyembunyikan dan mengamankan informasi dari pihak yang tidak berwenang (Rountree, 2011). Tujuan utama kriptografi adalah untuk melindungi kerahasiaan, integritas, dan keautentikan data. Dalam dunia kriptografi dikenal sebuag algoritma yang disebut hash.

Algoritma *hash* digunakan untuk mengubah sebuah teks yang biasanya berupa kata sandi menjadi *string* yang disebut *hash value* atau *chipertext*. *Hash* merupakan fungsi satu arah yang secara teoritis ketika

suatu *plain text* di *hash* dan menjadi *hash value* maka tidak dapat diterjemahkan kembali menjadi *plaintext*, sehingga *hash* diklaim lebih aman dibandingkan enkripsi. *Hash* dapat diperkuat lagi dengan menambahkan *salt* pada *password*. *Salt* berarti menambahkan *string* acak ke kata sandi pengguna sebelum melakukan *hashing* untuk meningkatkan kekuatan *hash* dan mempersulit peretas membaca *plaintext password* jika dia berhasil meretas *hash* tersebut (Karrar *et al.*, 2018). *Salt* umumnya dihasilkan setiap pembuatan *password* sehingga setiap *password* baru harus di-*hash* menggunakan *salt* yang baru (Ebanesar and Suganthi, 2019).

Penggunaan *salt* terhadap *password* dapat meningkatkan keamanan autentikasi dalam suatu aplikasi, namun tidak menutup kemungkinan *attacker* tetap dapat melakukan *cracking* terhadap nilai *hash* yang telah dihasilkan mengingat semakin banyaknya *tools cracking password* yang beredar di internet. Pada umumnya *salt* diletakan sebagai *prefix* dan *postfix password* sebelum dilakukan *hashing*. Namun cara tersebut sangat rentan terhadap serangan *attacker*, sehingga diperlukan metode pengacakan baru untuk meningkatkan keamanan password.

B. RUMUSAN MASALAH

Bagaimana pengaruh pengacakan *password* terhadap tingkat keamanan *chipertext hash* ?

C. BATASAN MASALAH

Dalam melakukan penelitian diperlukan batasan masalah untuk membatasi tema dan kaidah penelitian. Batasan masalah dalam penelitian ini adalah:

1. Menggunakan algoritma *hashing* MD5 sebagai objek pengujian.
2. Mengusulkan satu algoritma pengacakan *password* dan *salt.*

3. Mengevaluasi dua algoritma pengacakan *password* dan *salt* lain sebagai pembanding.
4. Panjang *password* dan *username* dibatasi sejumlah 6 karakter.
5. Panjang *salt* dibatasi sejumlah 2 karakter.

D. TUJUAN PENELITIAN

Tujuan penelitian ini adalah untuk mengevaluasi algoritma pengacakan *password* dan *salt,* serta mengusulkan satu algoritma baru guna meningkatkan keamanan *chipertext* suatu fungsi *hash*.

E. MANFAAT PENELITIAN

Adapun manfaat dari penelitian ini sebagai berikut.

1. Bagi pengembang sistem, dapat dimanfaatkan untuk meningkatkan keamanan autentikasi
2. Bagi pengguna informasi akan menjadi lebih aman dan dipastikan hanya dapat diakses oleh pengguna yang berhak.
3. Meminimalisir terjadinya kebocoran data pada sebuah sistem.

F. KEASLIAN PENELITIAN

Sebuah penelitian dilakukan dengan menggunakan pendekatan eksperimental untuk mengevaluasi skema pengacakan kata sandi menggunakan kombinasi gerbang logika pada tingkat keamanan *hash Chipertext*. Penelitian-penelitian tersebut tidak pernah dilakukan sepanjang observasi dilakukan mengingat penelusuran literatur.

BAB V
PENUTUP

A. KESIMPULAN

Pengacakan *password* sebelum dimasukkan kedalam fungsi *hash* dapat meningkatkan keamanan *chipertext* yang dihasilkan. Penelitian ini mengusulkan sebuah algoritma baru untuk mengacak *password*, *username*, dan *salt* menggunakan rangkaian gerbang logika tertentu. Hasil pengujian *part of execution* menunjukkan bahwa menggunakan algoritma LG membutuhkan waktu empat kali lebih lama dibandingkan tidak menggunakan algoritma LG. Namun hal tersebut tidak menjadi masalah mengingat urutan waktu eksekusi dari hasil tesnya sendiri masih kurang dari 0,1 detik. Oleh karena itu, manusia tidak terlalu memperhatikan perbedaannya. Hasil pengujian *resistance of attack* menunjukkan adanya peningkatan durasi serangan *brute force* yang cukup signifikan. Variasi *prefix* durasi serangan *brute force* naik sebesar 321,3 % dengan penerapan algoritma LG, sedangkan pada variasi *postfix* durasi serangan *brute force* naik sebesar 161,3 % dengan penerapan algoritma LG.

B. SARAN

Penelitian mendatang mengenai topik ini diharapkan dapat menemukan metode atau algoritma baru untuk meningkatkan kekuatan *chipertext hash.* Selain itu, algoritma LG dapat dikembangkan lagi kedalam bentuk hardware sehingga implementasinya untuk melindungi data bisa semakin luas.

DAFTAR PUSTAKA

Ajharie, M.A. and Sulistiyono, M. (2022) 'Implementasi Framework Mitm (Man in the Middle Attack) Untuk Memantau Aktifitas Pengguna Dalam Satu Jaringan', *Jurnal Infomedia*, 7(1), p. 45. doi:10.30811/jim.v7i1.2966.

Al-Shareeda, M.A. *et al.* (2022) 'Replay-Attack Detection and Prevention Mechanism in Industry 4.0 Landscape for Secure SECS/GEM Communications', *Sustainability (Switzerland)*, 14(23). doi:10.3390/su142315900.

Balu, D. *et al.* (2019) 'Implementation of Security in Login Page Using Salt and Pepper Algorithm', *SSRN Electronic Journal* [Preprint]. doi:10.2139/ssrn.3358813.

Chanda, K. (2016) 'Password Security: An Analysis of Password Strengths and Vulnerabilities', *International Journal of Computer Network and Information Security*, 8(7), pp. 23–30. doi:10.5815/ijcnis.2016.07.04.

Ebanesar, T. and Suganthi, G. (2019) 'Improving Login Process by Salted Hashing Password Using SHA-256 Algorithm in Web Applications', *International Journal of Computer Sciences and Engineering*, 7(3), pp. 27–32. doi:10.26438/ijcse/v7i3.2732.

Garg, B. and Kaur, S. (2019) 'a Review of Logic Gates and Its Applications', *Journal of Emerging Technologies and Innovative Research*, 6(5), pp. 124–129. Available at: www.jetir.org.

Haryanto, A.T. (2024) *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*. Available at: https://inet.detik.com/cyberlife/d-7169749/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.

Joshi, A., Wazid, M. and Goudar, R.H. (2015) 'An efficient cryptographic scheme for text message protection against brute force and cryptanalytic attacks', *Procedia Computer Science*, 48(C), pp. 360–366. doi:10.1016/j.procs.2015.04.194.

Karrar, A. *et al.* (2018) 'Enhancing Salted Password Hashing Technique Using Swapping Elements in an Array Algorithm', *IJCST Vol. 10, Issue 4 (Oct-Dec 2019)*, 8491, pp. 21–25.

Kävrestad, J. *et al.* (2020) 'Constructing secure and memorable passwords', *Information and Computer Security*, 28(5), pp. 701–717. doi:10.1108/ICS-07-

2019-0077.

Luthfansa, Z.M. and Rosiani, U.D. (2021) 'Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet', *Journal of Information Engineering and Educational Technology*, 5(1), pp. 34–39. doi:10.26740/jieet.v5n1.p34-39.

Maulid, R. (2024) *Pentingnya Python untuk Profesi Back-End Developer*. Available at: https://dqlab.id/pentingnya-python-untuk-profesi-back-end-developer.

Mohammed, S.D., Rahma, A.M.S. and Hasan, T.M. (2020) 'Maintaining the integrity of encrypted data by using the improving hash function based on GF (28)', *TEM Journal*, 9(3), pp. 1277–1284. doi:10.18421/TEM93-57.

Mohanty, R., Sarangi, N. and Bishi, S.K. (2010) 'A secured Cryptographic Hashing Algorithm', *Analysis*, (March 2010), p. 4. Available at: http://arxiv.org/abs/1003.5787.

Munir, R. (2006) *Bahan Kuliah IF5051 Kriftografi*. Departemen Teknik Informatika, Institut Teknologi Bandung.

OWASP (2014) *Splash Data's Top 100 Worst Passwords*. Available at: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf (Accessed: 27 January 2024).

Patel, P. *et al.* (2021) 'Brute Force, Dictionary and Rainbow Table Attack on Hashed Passwords', 9(4), p. 1899. Available at: www.ijcrt.org.

Pointcheval, D. (2009) 'Computational Security for Cryptography', pp. 1–46.

Polpong, J. and Wuttidittachotti, P. (2020) 'Authentication and password storing improvement using SXR algorithm with a hash function', *International Journal of Electrical and Computer Engineering (IJECE)*, 10(6), p. 6582. doi:10.11591/ijece.v10i6.pp6582-6591.

Pribady, M.L. (2024) *29 Juta Serangan Siber Diblokir di Indonesia Selama 2023*. Available at: https://inet.detik.com/security/d-7214588/29-juta-serangan-siber-diblokir-di-indonesia-selama-2023.

Python Software Foundation (2024) *secrets — Generate secure random numbers for managing secrets*, *Python Software Foundation*. Available at: https://docs.python.org/3/library/secrets.html.

Rahim, I. *et al.* (2022) 'Komparasi Fungsi Hash Md5 Dan Sha256 Dalam Keamanan Gambar Dan Teks', *Ikraith-Informatika*, 7(2), pp. 41–48.

doi:10.37817/ikraith-informatika.v7i2.2249.

Rountree, D. (2011) 'Cryptography', in *Security for Microsoft Windows System Administrators*. Elsevier, pp. 29–69. doi:10.1016/B978-1-59749-594-3.00002-8.

Sumandri (2017) 'Studi Model Algoritma Kriptografi', *Seminar Matematika Dan Pendidikan Matematika Uny*, pp. 265–272. Available at: http://seminar.uny.ac.id/semnasmatematika/sites/seminar.uny.ac.id.semnasmatematika/files/full/T-37.pdf.

Sutriman and Sugiantoro, B. (2019) 'Analysis of password and salt combination scheme to improve hash algorithm security', *International Journal of Advanced Computer Science and Applications*, 10(11), pp. 420–425. doi:10.14569/IJACSA.2019.0101158.

Tucakovic, Z. (2016) 'Technical Diagnosis of Basic Logic Gates', in *Conference: The 39th international convention on information and communication technology, electronics and microelectronics (MIPRO 2016)*.