PENGGUNAAN QR CODE DALAM AUTENTIKASI TANDA TANGAN PADA DOKUMEN DIGITAL DENGAN ALGORITMA SECURE HASH ALGORITHM-256 (SHA-256) DAN RIVEST SHAMIR ADLEMAN (RSA) YANG DITINGKATKAN

SKRIPSI

Diajukan untuk memenuhi salah satu syarat untuk memperoleh gelar
Sarjana Matematika

Oleh:
Fatimah Az-Zahra
NIM. 2005437

PROGRAM STUDI MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
BANDUNG

2024

PENGGUNAAN QR CODE DALAM AUTENTIKASI TANDA TANGAN PADA DOKUMEN DIGITAL DENGAN ALGORITMA SECURE HASH ALGORITHM-256 (SHA-256) DAN RIVEST SHAMIR ADLEMAN (RSA) YANG DITINGKATKAN

Oleh
Fatimah Az-Zahra

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia
April 2024

LEMBAR PENGESAHAN

FATIMAH AZ-ZAHRA

PENGGUNAAN QR CODE DALAM AUTENTIKASI TANDA TANGAN PADA DOKUMEN DIGITAL DENGAN ALGORITMA SECURE HASH ALGORITHM-256 (SHA-256) DAN RIVEST SHAMIR ADLEMAN (RSA) YANG DITINGKATKAN

Disetujui dan disahkan,
Pembimbing I

Dra. Hj. Rini Marwati, M.S.
NIP. 196606251990012001

Pembimbing II

Ririn Sispiyati, S.Si., M.Si.
NIP. 198106282005012001

Mengetahui,
Ketua Program Studi Matematika

Dr. Kartika Yulianti, S.Pd., M.Si.
NIP. 198207282005012001

ABSTRAK

Banyak hal didigitalisasi karena perkembangan bidang teknologi yang sangat pesat saat ini, salah satunya adalah dokumen. Tanda tangan basah telah beralih ke tanda tangan digital sebagai akibat dari adanya perubahan bentuk dokumen. Tidak ada jaminan bahwa isi dari dokumen digital tidak diubah oleh orang lain selama proses distribusi. Oleh sebab itu, diperlukan alat untuk membuat dan memastikan keaslian tanda tangan dari dokumen digital. Ilmu kriptografi, khususnya algoritma kriptografi kunci asimetri, dapat menjadi solusi dari masalah tersebut. Salah satu algoritma kriptografi asimetri adalah Rivest-Shamir-Adleman (RSA) yang keamanannya bergantung pada masalah pemfaktoran bilangan bulat. Versi yang ditingkatkan dari RSA dapat digunakan untuk mempercepat proses enkripsi dan dekripsi dengan menambahkan satu bilangan prima pada proses pembangkitan kunci. Selain kriptografi kunci asimetri, fungsi hash adalah salah satu fitur yang berguna dalam pembuatan tanda tangan digital. Menggabungkan algoritma kriptografi RSA yang ditingkatkan dan fungsi hash jenis *Secure Hash Algorithm*-256 (SHA-256) dapat menjadi salah satu cara untuk autentikasi tanda tangan dari dokumen digital. Selain itu, penambahan QR Code dapat membuat proses penandatanganan dan pemeriksaan dokumen menjadi lebih mudah. Program aplikasi autentikasi tanda tangan digital berbentuk QR Code dapat dihasilkan dengan memanfaatkan *Graphical User Interface* (GUI) Python versi 3.10 dan dapat digunakan untuk memastikan keaslian tanda tangan dari dokumen digital dengan mudah serta efisien.

Kata Kunci: Autentikasi Dokumen, Tanda Tangan Digital, RSA yang Ditingkatkan, SHA-256, QR Code.

ABSTRACT

Many things are digitized due to the rapid development of the technology field today, one of which is documents. Wet signatures have switched to digital signatures as a result of the change in the form of documents. There is no guarantee that the contents of a digital document are not altered by others during the distribution process. Therefore, a tool is needed to create and ensure the authenticity of signatures from digital documents. Cryptography, especially asymmetric key cryptography algorithms, can be a solution to this problem. One asymmetric cryptography algorithm is Rivest-Shamir-Adleman (RSA) whose security relies on the integer factoring problem. An improved version of RSA can be used to speed up the encryption and decryption process by adding one prime number to the key generation process. Besides asymmetric key cryptography, hash functions are one of the useful features in digital signature generation. Combining an enhanced RSA cryptographic algorithm and a Secure Hash Algorithm-256 (SHA-256) type hash function can be one way to authenticate signatures of digital documents. In addition, the addition of QR codes can make the process of signing and checking documents easier. The digital signature authentication application program in the form of a QR Code can be generated by utilizing the Graphical User Interface (GUI) Python version 3.10 and can be used to ensure the authenticity of signatures from digital documents easily and efficiently.

Keywords: *Document Authentication, Digital Signature, Enhanced RSA, SHA-256, QR Code.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR PUSTAKA

Atika, P. D. (2018). Digital Signature dengan Algoritma Sha-1 dan Rsa sebagai Autentikasi. *Jurnal Cendikia*, *16*(2 Oktober), 74-83.

Banoth, R., & Regar, R. (2023). Classical and Modern Cryptography for Beginners. Springer Nature.

Bienz, T., Cohn, R., & Adobe Systems (Mountain View, Calif.). (1993). *Portable document format reference manual* (p. 214). Boston^ eMA MA: Addison-Wesley.

Burton, D. (2011). *Elementary Number Theory*. McGraw Hill.

Clark, A. (2015). Pillow (pil fork) documentation. *readthedocs*.

Deineko, Z., Kraievska, N., & Lyashenko, V. (2022). QR Code as an Element of Educational Activity. *International Journal of Academic Information Systems Research (IJAISR)*, *6*(4), 26-31.

Fachrul, M., Sutardi, Tajidun, L.M., Aksara, L.M. B. (2022). Penerapan Konsep *Digital Signature* terhadap Verifikasi Keaslian Dokumen Transkrip Nilai Mahasiswa menggunakan Enkripsi *Rivest Shamir Adleman*. *semanTIK, 8*(1), 45-52.

Firdaus, J., Marwati, R., & Muhtar, S. (2018). Penyandian Pesan Menggunakan Kombinasi Algoritma Rsa Yang Ditingkatkan Dan Algoritma Elgamal. *Jurnal EurekaMatika*, *6*(1), 23-32.

Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge University Press.

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi dan Sistem Komputer*, *3*(2), 253-258.

Guerfi Sahra, G. N. E. Generate and read QR code using Python and Opencv.

Hendrawaty, H., Azhar, A., & Atthariq, A. (2016). Implementasi Algoritma RSA dan QR Code Untuk Keamanan Transkrip Nilai di Politeknik Negeri Lhokseumawe. *Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan*, *1*(2).

Hermawan, L., & Ismiati, M. B. (2020). Aplikasi Pengecekan Dokumen Digital Tugas Mahasiswa Berbasis Website. *Jurnal Buana Informatika*, *11*(2), 94-103.

Hinek, M. J. (2007). On the security of some variants of RSA.

Irwan, I. (2017). *IMPLEMENTASI KRIPTOGRAFI RSA (RIVEST-SHAMIRADLEMAN) PADA SISTEM APLIKASI FILE TRANSFER BERBASIS WEB: KRIPTOGRAFI RSA* (Doctoral dissertation, University of Muhammadiyah Malang).

Ismael, K. D., & Irina, S. (2020). Face recognition using Viola-Jones depending on Python. *Indonesian Journal of Electrical Engineering and Computer Science*, *20*(3), 1513-1521.

Kampus, K. Q. A. M. Implementasi Algoritma RSA dan Hash SHA-256 untuk Tanda Tangan Digital dalam Membangkitkan.

Melina, M., Sukono, F., Napitupulu, H., & Kusumaningtyas, V. A. (2022). Verifikasi Tanda Tangan Elektronik dengan Teknik Otentikasi Berbasis Kriptografi Kunci Publik Sistem Menggunakan Algoritma Kriptografi Rivest-Shamir-Adleman. *Jurnal Matematika Integratif*, *18*(1), 27-39.

Munir, R. (2005). Penggunaan Tanda-Tangan Digital untuk Menjaga Integritas Berkas Perangkat Lunak. In *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*.

Munir, R. (2006). Kriptografi. *Informatika, Bandung*.

Munir, R. (2015). Algoritma RSA.

Munir, R. (2017). *Tandatangan Digital Bahan Kuliah IF4020 Kriptografi*.

Nainggolan, S. (2022). Implementasi Algoritma SHA-256 Pada Aplikasi Duplicate Document Scanner. *Resolusi: Rekayasa Teknik Informatika dan Informasi*, *2*(5), 201-213.

Neumann, M., Shen, Z., & Skjonsberg, S. (2021). PAWLS: PDF annotation with labels and structure. *arXiv preprint arXiv:2101.10281*.

Pangan, A. M. S., Lacuesta, I. L., Mabborang, R. C., & Ferrer, F. P. (2022). Authenticating Data Transfer Using RSA-Generated QR Codes. *European Journal of Information Technologies and Computer Science*, *2*(4), 18-30.

Sarasvananda, I. B. G., & Iswara, I. B. A. I. (2022). Tanda Tangan Elektronik Menggunakan Algoritma Rivest Shamir Adleman (RSA) pada Sistem

Informasi Surat Menyurat LPIK INSTIKI. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *11*(2), 289-296.

Sari, I. Y., Jamaluddin, J., Simarmata, J., Rahman, M. A., Iskandar, A., Pakpahan, A. F., ... & Manullang, S. O. (2020). Keamanan Data dan Informasi.

Sebastian, A. (2007). Implementasi dan perbandingan performa algoritma hash SHA-1, SHA-256, dan SHA-512. *Skripsi, Institut Teknologi Bandung, Bandung, Indonesia*.

Shankar, T. N., & Sahoo, G. (2010). Cryptography by karatsuba multiplier with ASCII codes. *International journal on computer applications*, 53-60.

Soon, T. J. (2008). QR code. *synthesis journal*, *2008*, 59-78.

Srinath, K. R. (2017). Python–the fastest growing programming language. *International Research Journal of Engineering and Technology*, *4*(12), 354-357.

Stinson, D. R. (2005). *Cryptography: theory and practice*. Chapman and Hall/CRC.

Sulastri, S., & Putri, R. D. M. (2018). Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan. *Jurnal Teknik Elektro*, *10*(2), 70-74.

Sumandri, S. (2017). Studi Model Algoritma Kriptografi Klasik dan Modern. *Semin. Mat. dan Pendidik. Mat. UNY*, 265-272.

Van Rossum, G., & Drake, F. L. (1995). Python library reference.

Wang, X., Yin, Y. L., & Yu, H. (2005). Finding collisions in the full SHA-1. In *Advances in Cryptology–CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005. Proceedings 25* (pp. 17-36). Springer Berlin Heidelberg.