Analisis Performa dan Keamanan Algoritma HMAC-SHA-2 dan KMAC-SHA-3 dalam *Time-based One Time Password* pada *Two-Factor Authentication*

SANDY ARDANU BAGASRAGA

NIM. 1910511054

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

2026

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa, atas segala rahmat-Nya sehingga Tugas Akhir ini berhasil diselesaikan. Tugas Akhir ini dilakukan dalam bentuk skripsi. Tugas Akhir ini dilaksanakan sejak bulan April 2026 sampai bulan Mei 2026 dengan judul "Analisis Performa dan Keamanan Algoritma HMAC-SHA-2 dan KMAC-SHA-3 dalam *Time-based One Time Password* pada *Two-Factor Authentication*". Terima kasih penulis ucapkan kepada:

1. Kedua orang tua serta seluruh keluarga yang telah memberikan dukungan doa, dan kasih sayangnya.
2. Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
3. Dr. Ridwan Raafi'udin, S.Kom., M.Kom selaku Koordinator Program Studi Sarjana Jurusan Informatika Fakultas Ilmu Komputer UPN Veteran Jakarta.
4. Dr. Widya Cholil, S.Kom., M.I.T selaku Dosen Pembimbing Akademik Program Studi Informatika Fakultas Ilmu Komputer Angkatan 2019
5. Henki Bayu Seta, S.Kom, MTI. selaku Dosen Pembimbing 1.
6. Neny Rosmawarni, M.Kom selaku Dosen Pembimbing 2.

Semoga Tugas Akhir ini bermanfaat bagi pihak yang membutuhkan dan bagi kemajuan ilmu pengetahuan.

Jakarta, 22 Juli 2026

Penulis

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Judul	: Analisis Performa dan Keamanan Algoritma HMAC-SHA-2 dan KMAC-SHA-3 dalam Time-based One Time Password pada Two-Factor Authentication
Nama	: Sandy Ardanu Bagasraga
NIM	: 1910511054
Program Studi	: S1 Informatika

Disetujui oleh:

Penguji 1:

Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM

Penguji 2:

I Wayan Rangga Pinastawa, M.Kom

Dosen Pembimbing 1:

Henki Bayu Seta, S.Kom, MTI.

Dosen Pembimging 2:

Neny Rosmawarni, M.Kom

Diketahui oleh:

Koordinator Program Studi:

Dr. Ridwan Raafi'udin, S.Kom.,M.Kom

NIP. 198805022021211001

Dekan Fakultas Ilmu Komputer:

Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM

NIP. 197605082003121002

Tanggal Ujian Tugas Akhir:

14 Juli 2026

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama	:	Sandy Ardanu Bagasraga
NIM	:	1910511024
Tanggal	:	28 Juli 2026

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku

Jakarta, 28 Juli 2026

Yang Menyatakan

Sandy Ardanu Bagasraga

LEMBAR PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

LEMBAR PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama	:	Sandy Ardanu Bagasraga
NIM	:	1910511054
Fakultas	:	Ilmu Komputer
Program Studi	:	S-1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non - exclusive Royalty Free Right*) atas skripsi saya yang berjudul:

Analisis Performa dan Keamanan Algoritma HMAC-SHA-2 dan KMAC-SHA-3 dalam *Time-based One Time Password* pada *Two-Factor Authentication*

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/memformatkan, mengelola dalam bentuk pangkalan data (basis data), merawat dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya

Dibuat di: Jakarta
Pada tanggal: 28 Juli 2026
Yang Menyatakan

Sandy Ardanu Bagasraga

ABSTRAK

Penggunaan kata sandi tunggal semakin tidak memadai dalam menghadapi ancaman serangan identitas digital, sehingga penerapan *Two-Factor Authentication* (2FA) berbasis *Time-based One Time Password* (TOTP) menjadi standar keamanan yang krusial. Namun, efektivitas sistem TOTP saat ini terhalang oleh penggunaan standar lama HMAC-SHA-2 (seperti HMAC-SHA-256 dan HMAC-SHA-512) yang memanfaatkan arsitektur Merkle-Damgård. Arsitektur ini memerlukan pemrosesan fungsi *hash* secara ganda (*nested double-pass*) untuk mencegah serangan *length-extension*, sehingga menimbulkan beban komputasi yang tinggi dan penggunaan memori yang kurang efisien. Penelitian ini bertujuan untuk menganalisis, membandingkan, serta mengevaluasi performa dan tingkat keamanan algoritma HMAC-SHA-2 dengan algoritma KMAC-SHA-3 (KMACXOF128 dan KMACXOF256 berbasis *Sponge Construction* / KECCAK) dalam implementasi TOTP 2FA. Pengujian dilakukan menggunakan pendekatan eksperimental dan analisis matematis. Aspek performa diuji meliputi kecepatan *generate* dan verifikasi kode TOTP (pada skenario 1.000 *secret key* dan 1.000.000 total eksekusi), penggunaan sumber daya (CPU dan RAM), serta *throughput* dan *multi-thread*. Aspek keamanan dievaluasi melalui uji *avalanche effect*, keacakan (*randomness* menggunakan NIST *Statistical Test Suite*), serta analisis matematis pada *collision resistance, preimage resistance, dan second-preimage resistance*. Hasil analisis dan perbandingan ini diharapkan dapat memberikan referensi akademis serta panduan teknis bagi pengembang sistem keamanan digital dalam melakukan transformasi dan migrasi standar dari HMAC ke KMAC pada skema TOTP masa depan.

Kata Kunci: TOTP, 2FA, HMAC-SHA-2, KMAC-SHA-3, Performa dan Keamanan Kriptografi.

ABSTRACT

The rely on single passwords has become increasingly inadequate in mitigating digital identity threats, making the implementation of Time-based One Time Password (TOTP) within Two-Factor Authentication (2FA) a critical security standard. However, the current effectiveness of TOTP systems is constrained by the legacy standard HMAC-SHA-2 (such as HMAC-SHA-256 and HMAC-SHA-512), which relies on the Merkle-Damgård architecture. This architecture requires a nested double-pass hash execution to prevent length-extension attacks, resulting in high computational overhead and inefficient memory utilization. This study aims to analyze, compare, and evaluate the performance and security strength of HMAC-SHA-2 algorithms against KMAC-SHA-3 algorithms (KMACXOF128 and KMACXOF256 based on Keccak Sponge Construction) in TOTP-2FA implementations. The evaluation was conducted using an experimental approach combined with mathematical analysis. Performance metrics included TOTP code generation and verification latency (tested across 1,000 secret keys and 1,000,000 total executions), resource usage (CPU and RAM), as well as throughput and multi-threading capabilities. Security properties were assessed via avalanche effect testing, bit randomness (using the NIST Statistical Test Suite), and mathematical analysis of collision resistance, preimage resistance, and second-preimage resistance. The comparative findings provide academic reference and technical guidance for digital security developers transitioning from legacy HMAC to modern KMAC standards in future TOTP authentication systems.

Keywords: *TOTP, 2FA, HMAC-SHA-2, KMAC-SHA-3, Cryptographic Performance and Security.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR RUMUS

DAFTAR LAMPIRAN