

ABSTRAK

Nama : Gunawan Yuga Utama
Program Studi : Informatika
Judul : Implementasi Algoritma *TOTP SHA-3* Untuk Pengelolaan *Password Wifi* Pada Media Tempat Sampah
Pembimbing I : Dr. Ir. Winarno Sugeng, M.kom.
Pembimbing II : Theta Dinnarwaty. P, S.Kom, MT.

Algoritma *Time-Based One Time Password (TOTP)* merupakan algoritma yang berfungsi menghasilkan *password* untuk satu kali pemakaian. *Password* yang dihasilkan memiliki batas waktu tertentu dan akan selalu berubah secara dinamis dalam periode tertentu. Algoritma *TOTP* menggabungkan *secret key* dengan *current time* yang kemudian dilakukan *hashing* menggunakan algoritma enkripsi *SHA-3*. Pada penelitian ini *TOTP* diaplikasikan untuk pengelolaan *password wifi* pada media tempat sampah dimana keterkaitan *user* dan kebutuhan mengakses *wifi*, *TOTP* akan menghasilkan *password wifi* untuk *user* jika *user* melakukan kegiatan membuang sampah pada media tempat sampah. Pada *secret key* dilakukan enkripsi menggunakan algoritma *caesar* terlebih dahulu sebelum dilakukan tahap *hashing*, ini agar membuat *secret key* dinamis sehingga variasi *password* menjadi lebih banyak dan dapat meningkatkan keamanan dari *password*. Dari hasil pengujian keluaran *password* tidak muncul secara berulang namun memiliki tingkat kemiripan sebesar 0,02%.

Kata Kunci: *Internet Of Thing, TOTP, SHA-3, Tempat sampah*

ABSTRACT

Name	:	Gunawan Yuga Utama
Study Program	:	Informatic Enginering
Title	:	Implementasi Algoritma <i>TOTP SHA-3 Untuk Pengelolaan Password Wifi Pada Media Tempat Sampah</i>
Counselor I	:	Dr. Ir. Winarno Sugeng, M.kom.
Counselor II	:	Theta Dinnarwaty. P, S.Kom, MT.

The Time-Based One Time Password (TOTP) algorithm is an algorithm that produces a password for only one use. A password that is produced has a limited time and always changed dynamically in a specific period . The TOTP algorithm combines a secret key with a current time which is then hased with an encryption algorithm SHA-3. In this experiment the TOTP is applied for managing a wifi password for a user, when the user is throwing a trash at a particular bin. The secret key will be encrypted used a caesar algorithm before the hashing process, this done so that a secret key become dynamic and the password multiplied, and the security level will be higher. In this experiment the password output has not produced periodically but has a 0.02% similliarity.

Keywords: *Internet Of Thing, TOTP, SHA-3,Trashbin.*