UNIVERSITAS
GADJAH MADA
Iterated Function System untuk Memperkuat Advanced Encryption Standard pada Cryptosystem
THOHA IKHWANUL HAQ, Nur Rokhman, S.Si., M.Kom., Dr
Universitas Gadjah Mada, 2020 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

Iterated Function System untuk Memperkuat Advanced Encryption Standard pada Kriptosistem

Oleh

Thoha Ikhwanul Haq
15/383254/PA/16914

Munculnya berbagai teknik kriptoanalisis modern dapat membahayakan kerahasiaan dan kemanan data. Teknik kriptoanalisis modern dapat digunakan oleh pihak ketiga untuk memecahkan enkripsi pada kriptosistem. Advanced Encryption Standard (AES) merupakan salah satu teknik enkripsi-dekripsi yang sering digunakan. AES 256-bit single core sudah berhasil dipecahkan dengan relatif cepat pada tahun 2017.

Perkembangan teknik kriptoanalisis perlu diimbangi dengan pengembangan teknik kriptografi yang lebih kuat. AES sudah cukup kuat digunakan selama 20 tahun terakhir sehingga saatnya dikembangkan secara lebih lanjut. Pengembangan AES perlu didasari oleh teknik kriptoanalisis yang sudah ada seperti Kolmogorov-Smirnov Test dan *Avalanche Effect*.

Penelitian ini bertujuan untuk menguji Iterated Function System(IFS) sebagai salah salah satu metode enkripsi-dekripsi pada kriptosistem. IFS merupakan fungsi-fungsi yang dapat diiterasikan secara tidak terbatas untuk mengenkripsi data, sehingga diharapkan Iterated Function System dapat digunakan untuk memperkuat Advanced Encryption Standard pada kriptosistem.

Kata Kunci : Kriptografi, AES, Iterated Function System

UNIVERSITAS
GADJAH MADA
Iterated Function System untuk Memperkuat Advanced Encryption Standard pada Cryptosystem
THOHA IKHWANUL HAQ, Nur Rokhman, S.Si., M.Kom., Dr
Universitas Gadjah Mada, 2020 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

ITERATED FUNCTION SYSTEM TO STRENGTHEN THE ADVANCED ENCRYPTION STANDARD OF A CRYPTOSYSTEM

By

Thoha Ikhwanul Haq

The development of various modern cryptoanalyses techniques can pose a threat to our privacy and data security. These modern cryptoanalyses methods could be used by a third-party to decrypt an encrypted message. The Advanced Encryption Standard, a cryptosystem which has been commonly used for years, has been successfully cracked to a certain degree. The AES 256-bit single has been successfully cracked relatively quickly in 2017 by a Dutch researcher.

The growth and development of various cryptonalysis techniques has proven that cryptography must be improved even further. The AES, which has been coomonly used for 20 years, should be further developed and should be used as a basis for any further development of any cryptography techniques.

This research aims to test the Iterated Function System (IFS) as an encryption-decryption method for a cryptosystem. IFS features a set of functions which can be iterated endlessly to encrypt a message. The IFS can be used in an AES by inserting IFS in between one of the steps in AES thus the IFS is expected to strengthen the AES of a cryptosystem.

Keywords : Cryptography, AES, Iterated Function System