ANALISA DAN PERANCANGAN SISTEM ENKRIPSI DAN DEKRIPSI DOKUMEN BERBASIS ANDROID DENGAN METODE *ADVANCED ENCRYPTION STANDARD* (AES) -128 (STUDI KASUS: PT. KELAB 21 RETAIL)

TUGAS AKHIR

PROGRAM STUDI SISTEM INFORMASI

OLEH :

NAMA : FILDAN HADIKA RAHMAN

NIM : 181070007

FAKULTAS TEKNIK

UNIVERSITAS SATYA NEGARA INDONESIA

JAKARTA

2021

ANALYSIS AND DESIGN OF ENCRYPTION AND DECRYPTION DOCUMENT USED ANDROID SYSTEM BASED WITH ADVANCED ENCRYPTION STANDARD (AES) – 128 METHOD (A CASE STUDY: PT. KELAB 21 RETAIL)

A FINAL ASSIGNMENT

DEPARTMENT OF INFORMATION SYSTEM

BY :

NAME : FILDAN HADIKA RAHMAN

NIM : 181070007

FACULTY OF ENGINEERING

UNIVERSITAS SATYA NEGARA INDONESIA

JAKARTA

2021

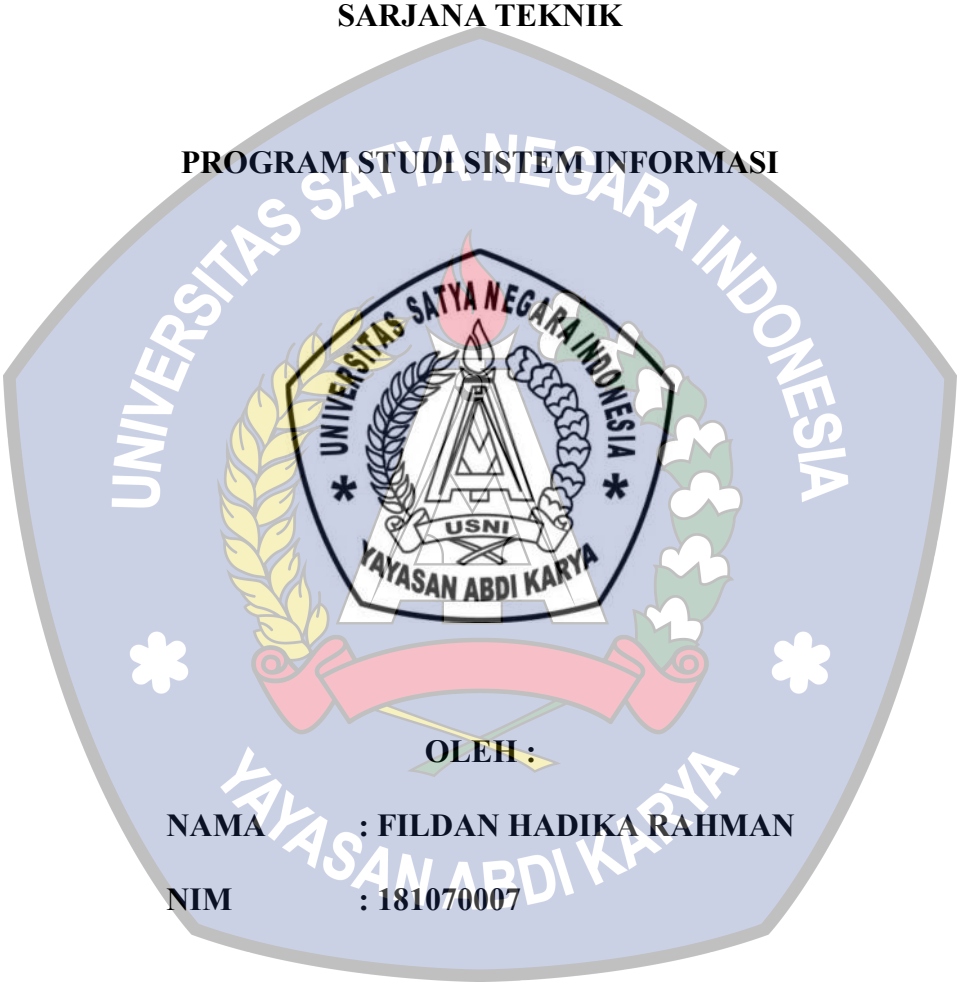
ANALISA DAN PERANCANGAN SISTEM ENKRIPSI DAN DEKRIPSI DOKUMEN BERBASIS ANDROID DENGAN METODE *ADVANCED ENCRYPTION STANDARD* (AES) -128 (STUDI KASUS: PT. KELAB 21 RETAIL)

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar

SARJANA TEKNIK

PROGRAM STUDI SISTEM INFORMASI



OLEH :

NAMA : FILDAN HADIKA RAHMAN

NIM : 181070007

FAKULTAS TEKNIK

UNIVERSITAS SATYA NEGARA INDONESIA

JAKARTA

2021

ANALYSIS AND DESIGN OF ENCRYPTION AND DECRYPTION DOCUMENT USED ANDROID SYSTEM BASED WITH ADVANCED ENCRYPTION STANDARD (AES) – 128 METHOD (A CASE STUDY: PT. KELAB 21 RETAIL)

A SKRIPSI

Presented To The Faculty Of Engineering In Partial Fulfillment

Of The Requirements For The Degree Of

BACHELOR OF ENGINEERING

BY :

NAME : FILDAN HADIKA RAHMAN

NIM : 181070007

FACULTY OF ENGINEERING

UNIVERSITAS SATYA NEGARA INDONESIA

JAKARTA

2021

ABSTRAK

Perkembangan teknologi informasi yang semakin pesat memberi pengaruh yang besar hampir diserluruh aspek kehidupan manusia. Tentunya tingkat keamanan yang tinggi sangat diperlukan agar informasi tersebut tidak dapat diakses oleh orang yang tidak berkepentingan. Kriptografi banyak digunakan untuk menjaga aspek keamanan informasi. Kriptografi adalah ilmu mengenai teknik enkripsi dimana naskah asli (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi naskah acak yang sulit dibaca (*ciphertext*) oleh seseorang yang tidak memiliki kunci dekripsi. salah satu metode kriptografi modern yang dikembangkan adalah algoritma *Advanced Encryption Standard* (AES). *Advanced Encryption Stand*ard (AES) adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. Dalam algoritma kriptografi AES 128, 1blok plainteks berukuran 128 bit terlebih dahulu dikonversi menjadi matriks heksadesimal berukuran 4x4 yang disebut state. Pada proses state enkripsi akan melalui beberapa tahapan yakni Addroaundkey, Subbyte, Shiftrows, dan Mixcolumns sebanyak 10 kali putaran. Namun pada putaran terakhir tidak dilakukan lagi proses Mixcolumns langsung ke proses Addraoundkey, dan untuk proses dekripsi merupakan proses kebalikan dari proses enkripsi yakni InvAddrows, InvShiftrows, InvSubbyte, dan InvMixcolumns menggunakan kunci round yang sama dengan proses enkripsi. Algoritma *Advanced Encryption Standard* (AES) dipilih karena memiliki suatu tingkatan keamanan pertukaran informasi yang cukup bagus. Dan dari hasil implementasi algoritma AES dapat disimpulkan bahwa aplikasi ini dapat mengekripsi semua jenis karakter berupa string, huruf, angka, dan symbol.

Kata Kunci: Enkripsi, Dekripsi, *Advanced Encryption Standard* (AES) – 128

ABSTRACT

The quick development of information technology has had a major influence in almost humans' life aspects. Of course, a high level of security is needed so it cannot be accessed by unauthorized people. The usage of cryptography is to keep the aspects of information's security. Cryptography is a science of encryption techniques where the originao text (plain text) is scrambled by using an encryption key which transforms into scrambled text that is hard to be read (chiper text) by someone who does not have thr description key. One of the modern cryptography methods which is being developed is Advanced Encryption Standard (AES) algorithms. Advanced Encryption Standard (AES) is a cryptographic algorithm which is currently the standard for symmetric key encryption algorithms. In the AES 128 cryptographic algorithm, 1 128-bit plaintext block is first converted into a 4x4 hexadecimal matrix called state. In the state encryption process, it will go through several stages, namely Addroaundkey, Subbyte, Shiftrows, and Mixcolumns for 10 rounds. However, in the last round, the Mixcolumns process was not carried out directly to the Addraoundkey process, and the decryption process was the opposite of the encryption process, namely InvAddrows, InvShiftrows, InvSubbyte, and InvMixcolumns using the same round key as the encryption process. The Advanced Encryption Standard (AES) algorithm was chosen because it has a pretty good level of information exchange security. From the implementation of the AES algorithm, it can be concluded that this application can encrypt all types of characters in the form of strings, letters, numbers, and symbols.

Keyword: Encryption, Decryption, Advanced Encryption Standard (AES) – 128