UNIVERSITAS
GADJAH MADA
MODEL SECURE ELEMEN BERBASIS APLIKASI NEAR FIELD COMMUNICATION HOST CARD EMULATION PADA SMARTPHONE
LN HARNANINGRUM, Dr.techn. Ahmad Ashari, M.Kom.; Dr. Agfianto Eko Putra, M.Si.
Universitas Gadjah Mada, 2022 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN PENGESAHAN iii
PERNYATAAN BEBAS PLAGIASI iv
PRAKATA iv
DAFTAR ISI vi
DAFTAR GAMBAR viii
DAFTAR TABEL x
INTISARI xi
ABSTRACT xii
BAB I PENDAHULUAN 1
1.1. Latar belakang 1
1.2. Rumusan masalah 5
1.3. Batasan Masalah 5
1.4. Tujuan 6
1.5. Manfaat Penelitian 6
1.6. Kontribusi Penelitian 6
BAB II TINJAUAN PUSTAKA 8
2.1. Penelitian tentang Protokol pada Sistem Pembayaran NFC-Enabled Mobile 8
2.2. Penelitian tentang Sistem Keamanan pada NFC-enabled mobile 12
2.3. Penelitian tentang Serangan pada NFC-enabled mobile 22
BAB III LANDASAN TEORI 29
3.1. Mode Operasi NFC 29
3.1.1. Mode Read/Write 30
3.1.2. Mode Peer to peer 31
3.1.3. Mode Card Emulation 33
3.1.4. State Machine dari Card Emulation mode NFC 34
3.1.5. Program flow dan Arsitektur Mode Card Emulation 39
3.2. Host-based Card Emulation (HCE) 40
3.2.1. Card Emulation dengan secure elemen 41
3.2.2. Komponen Ekosistem SE. 42
3.2.3. Komponen Ekosistem HCE. 46
3.2.4. Kartu dan protokol NFC yang didukung. 47
3.2.5. Application Protocol Data Unit (APDU) 49
3.3. Algoritma Kriptografi AES (Advanced Encryption Standard) 50
3.4. Algoritma Kriptografi RSA (Rivest-Shamir-Adleman) 56
3.5. Fermat factorization 58
BAB IV METODOLOGI PENELITIAN 59
4.1. Tahapan Penelitian 59
4.2. Sistem Pembayaran NFC-Enabled Mobile 60
4.3. Model NFC-HCE di Smartphone 62
4.3.1. Model Inisialisasi 67

UNIVERSITAS
GADJAH MADA
MODEL SECURE ELEMEN BERBASIS APLIKASI NEAR FIELD COMMUNICATION HOST CARD EMULATION PADA SMARTPHONE
LN HARNANINGRUM, Dr.techn. Ahmad Ashari, M.Kom.; Dr. Agfianto Eko Putra, M.Si.
Universitas Gadjah Mada, 2022 | Diunduh dari http://etd.repository.ugm.ac.id/

4.3.2. Model Transaksi 69
4.3.3. Model Enkripsi dan Enkapsulasi Data 74
4.4. Pengujian dan analisis hasil uji model 75
4.4.1. Pengujian menggunakan miniatur sistem 75
4.4.2. Prosedur Pengujian 80
4.4.3. Rancangan analisis hasil uji model 81
4.4.4. Analisis keamanan dengan uji keacakan data 81
4.4.5. Analisis kecepatan dengan menghitung waktu eksekusi 83
BAB V MODEL INISIALISASI 85
5.1. Arsitektur Model Inisialisasi 85
5.2. Pengembangan Sistem untuk Model Inisialisasi 90
5.3. Pengujian Waktu Proses 92
5.4. Uji Monobit dan Entropi 95
5.4.1. Uji Frequency (Monobits) 95
5.4.2. Uji Entropi dan Monobit 96
5.5. Analisis ketahanan terhadap serangan faktorisasi. 99
BAB VI MODEL TRANSAKSI 101
6.1. Arsitektur Model Transaksi 101
6.2. Pengembangan Sistem untuk Model Transaksi 104
6.3. Pengujian Waktu Proses 107
6.4. Uji Komunikasi Data 108
6.5. Uji Monobit dan Entropi 114
6.6. Analisis Ketahanan terhadap serangan faktorisasi. 114
6.7. Analisis Keamanan Model Transaksi 115
BAB VII KESIMPULAN 122
7.1. Kesimpulan 122
7.2. Saran 122
Pustaka 124