

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI *RIVEST  
CODE 4 (RC4)* PADA *SMART CARD* APLIKASI KOMISI  
PEMILIHAN UMUM (KPU) UNIVERSITAS BAKRIE**

**TUGAS AKHIR**



**DEDE MOHAMAD SALIM**

**1132001011**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNIK DAN ILMU KOMPUTER**

**UNIVERSITAS BAKRIE**

**JAKARTA**

**2018**

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI *RIVEST  
CODE 4 (RC4)* PADA *SMART CARD* APLIKASI KOMISI  
PEMILIHAN UMUM (KPU) UNIVERSITAS BAKRIE**

**TUGAS AKHIR**

**Diajukan sebagai salah satu syarat untuk memperoleh gelar  
Sarjana Komputer**



**DEDE MOHAMAD SALIM**

**1132001011**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNIK DAN ILMU KOMPUTER**

**UNIVERSITAS BAKRIE**

**JAKARTA**


**2018**

## HALAMAN PERNYATAAN ORISINALITAS

**Tugas Akhir ini adalah hasil karya saya sendiri,  
Dan semua sumber baik yang dikutip maupun dirujuk  
telah saya nyatakan dengan benar.**

**Nama : Dede Mohamad Salim**

**NIM : 1132001011**

**Tanda Tangan : **

**Tanggal : 31 Agustus 2018**


## HALAMAN PENGESAHAN


Tugas Akhir ini diajukan oleh:


Nama : Dede Mohamad Salim  
NIM : 1132001011  
Program Studi : Informatika  
Fakultas : Teknik dan Ilmu Komputer  
Judul Tugas Akhir : Implementasi Algoritma Kriptografi *Rivest Code*  
4 (RC4) Pada *Smart Card* Aplikasi Komisi  
Pemilihan Umum (KPU) Universitas Bakrie

**Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika Fakultas Teknik dan Ilmu Komputer, Universitas Bakrie.**

## DEWAN PENGUJI

Pembimbing : Yusuf Lestanto, S.T., M.Sc.  31/8 18  
(.....)

Penguji 1 : Prof. Dr. Hoga Saragih, S.T., M.Sc.   
(.....)

Penguji 2 : Berkah I. Santoso, S.T., M.T.I.  31/8 18  
(.....)

Ditetapkan di : Jakarta  
Tanggal : 31 Agustus 2018

## UCAPAN TERIMA KASIH

Alhamdulillahrabbi'l'aalamiin, puji dan syukur ke hadirat Allah SWT atas segala rahmat dan karunia-Nya Tugas Akhir yang berjudul “Implementasi Algoritma Kriptografi *Rivest Code 4 (RC4)* Pada *Smart Card* Aplikasi Komisi Pemilihan Umum (KPU) Universitas Bakrie” dapat diselesaikan. Sholawat serta salam penulis haturkan kepada Nabi Besar Muhammad SAW, beserta keluarganya dan para sahabatnya yang telah membimbing umatnya ke masa yang terang benderang penuh dengan cahaya iman.

Penyusunan Tugas Akhir ini tidak lepas dari berbagai hambatan dan kesulitan dari awal hingga akhir penyusunan. Penulis menyampaikan terima kasih yang sebesar-besarnya kepada Bapak Yusuf Lestanto, S.T., M.Sc. selaku dosen pembimbing Tugas Akhir yang telah meluangkan waktu serta mengerahkan tenaga dan pikirannya untuk membantu proses pengerjaan dan penyusunan Tugas Akhir ini. Begitu banyak pihak yang turut membantu dan memberikan dukungan, masukan, nasihat, serta doa selama penyusunan Tugas Akhir ini. Oleh karena itu, dengan segala hormat dan kerendahan hati, penulis mengungkapkan rasa terima kasih kepada:

1. Kedua orangtua yang terhormat dan tercinta, Bapak Sobana dan Ibu Kapsah, yang tidak pernah lelah untuk memberikan dukungan, pembelajaran, motivasi, semangat, dan doa.
2. Bapak Prof. Dr. Hoga Saragih, S.T., M.T. selaku Ketua Program Studi Informatika Universitas Bakrie dan dosen penguji Tugas Akhir, yang senantiasa memberikan motivasi dan masukan terhadap penyusunan Tugas Akhir.
3. Bapak Berkah I. Santoso, S.T., M.T.I. selaku dosen pembahas dan penguji Tugas Akhir yang senantiasa memberikan motivasi, saran serta perbaikan terhadap penyusunan Tugas Akhir.
4. Saudara-saudara tercinta: Abdullah, Roikhatul Jannah, dan Imam Khanafi yang selalu mendukung dan memberikan motivasi kepada penulis.

5. Sahabat Informatika 2013: Amelia Fahmi, Bagus Aryo Pamungkas, Febbie Ramadhini, Fadillah Indra, Fildzah Adra Arifah, Fitriah Febriani, Gusti Maulana Arif, Iman Nurmansyah, Jimmy, Lilyani Barrung, Millah Fatimah, Muhammad Khalish Ramadhansyah, Ridho Gilang Fiesta, Rizky Novriyedi Putra, dan Yusuf Arwadi, yang selalu membantu, memberikan motivasi, semangat, serta kebersamaan dalam suka dan duka selama 4 tahun masa perkuliahan di Universitas Bakrie.
6. Kakak-kakak Informatika Universitas Bakrie Angkatan 2012 yang telah membagikan pengalaman, memberikan motivasi serta semangat selama penyusunan Tugas Akhir.
7. Adik-adik Informatika Universitas Bakrie Angkatan 2014 dan 2015 yang telah memberikan doa, dukungan, dan semangat selama masa perkuliahan dan penyusunan Tugas Akhir.
8. Seluruh pihak Program Studi Informatika Universitas Bakrie yang telah memberikan ilmu dan pembelajaran serta pengalaman yang sangat bermanfaat bagi penulis selama masa perkuliahan.

Semoga Allah SWT senantiasa membalas kebaikan dan memberikan keberkahan kepada kita semua. Penulis berharap Tugas Akhir ini dapat memberi informasi yang berguna dan bermanfaat bagi berbagai kalangan bidang pendidikan, khususnya bidang Informatika.

Jakarta, 31 Agustus 2018

Dede Mohamad Salim

## HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai *civitas* akademik Universitas Bakrie, saya yang bertanda tangan di bawah ini:

Nama : Dede Mohamad Salim  
NIM : 1132001011  
Program Studi : Informatika  
Fakultas : Teknik dan Ilmu Komputer  
Jenis Tugas Akhir : Implementasi Algoritma

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bakrie **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

**Implementasi Algoritma Kriptografi *Rivest Code 4 (RC4)* Pada *Smart Card*  
Aplikasi Komisi Pemilihan Umum (KPU) Universitas Bakrie**

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini, Universitas Bakrie berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta untuk kepentingan akademis.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 31 Agustus 2018

Yang menyatakan,



Dede Mohamad Salim

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI RIVEST CODE 4 (RC4)  
PADA SMART CARD APLIKASI KOMISI PEMILIHAN UMUM (KPU)  
UNIVERSITAS BAKRIE**

**Dede Mohamad Salim**

---

**ABSTRAK**

*E-voting* merupakan kegiatan pemungutan suara dimana proses pelaksanaannya mulai dari pendaftaran pemilih, pelaksanaan pemilih, dan perhitungan suara dilakukan secara digital. Akan tetapi penerapan *e-voting* pada pemilihan ketua BEM dan ketua HMPS di Universitas Bakrie belum sepenuhnya menggunakan media elektronik, seperti pada absensi pemilih dan proses pemberian token untuk melakukan pemilihan masih dilakukan dengan manual. Hal tersebut tentunya tidak sejalan dengan *e-voting* yang sebenarnya bahkan dapat mengurangi nilai dari asas bebas rahasia. Oleh karena itu, dibutuhkan sebuah sistem *e-voting* yang dapat menjamin kerahasiaan data pemilih. Penelitian ini membahas tentang penggunaan algoritma RC4 pada *smart card* untuk mengamankan data pemilih. Aplikasi ini dibangun dengan menggunakan *framework spring boot restfull API* untuk bagian *back end*-nya dan untuk bagian *front end*-nya menggunakan *framework PHP*. Hasil pengujian *Black-box* menunjukkan bahwa 100% fungsionalitas sistem dapat berjalan sesuai dengan kebutuhan. Hasil pengujian validasi terhadap enkripsi RC4 menunjukkan hasil enkripsi aplikasi sama dengan hasil enkripsi yang dihitung secara manual.

**Kata Kunci :** RC4, *E-Voting*, *Smart Card*, *Spring boot restfull API*



**IMPLEMENTATION OF CRYPTOGRAPHY RIVEST CODE  
ALGORITHM 4 (RC4) ON SMART CARD APPLICATION OF KOMISI  
PEMILIHAN UMUM (KPU) IN BAKRIE UNIVERSITY**

**Dede Mohamad Salim**

---

**ABSTRACT**

E-voting is a voting activity where the implementation process starts from voter registration, voter implementation, and vote counting is done digitally. However, the application of e-voting at the election of the chairman of the BEM and the chairman of the HMPS at Bakrie University has not fully used electronic media, such as the voter attendance and the process of giving tokens to make elections still done manually. This is certainly not in line with e-voting which actually can even reduce the value of the secret free principle. Therefore, an e-voting system is needed that can guarantee the confidentiality of voter data. This study discusses the use of RC4 algorithms on smart cards to secure voter data. This application was built using a spring boot restfull API framework for the back end and for the front end part using PHP framework. Black-box test results show that 100% system functionality can run as needed. Validation test results for RC4 encryption show the results of application encryption are the same as the encryption results that are calculated manually.

**Kata Kunci :** RC4, *E-Voting*, *Smart Card*, *Spring boot restfull API*

## DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS.....	iii
HALAMAN PENGESAHAN.....	iv
UCAPAN TERIMA KASIH.....	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI.....	vii
ABSTRAK .....	viii
ABSTRACT .....	ix
DAFTAR ISI.....	x
DAFTAR GAMBAR .....	xii
DAFTAR <i>PSEUDOCODE</i> .....	xiv
DAFTAR <i>LISTING</i> KODE SUMBER .....	xv
DAFTAR TABEL.....	xvi
DAFTAR SINGKATAN .....	xvii
DAFTAR LAMPIRAN.....	xviii
BAB I.....	1
LATAR BELAKANG .....	1
1.1.1    Latar Belakang.....	1
1.2    Rumusan Masalah .....	3
1.3    Batasan Masalah.....	3
1.4    Tujuan Penelitian.....	4
1.5    Manfaat Penelitian.....	4
1.6    Sistematika Penulisan.....	4
BAB II.....	5
TINJAUAN PUSTAKA .....	5
2.1    Penelitian Terkait .....	5
2.2    E-Voting .....	14
2.3    Konsep Dasar Sistem Informasi .....	15
2.3.1    Pengertian Sistem.....	15
2.3.2    Pengertian Informasi .....	16
2.3.3    Pengertian Sistem Informasi .....	16
2.4    Near Field Communication (NFC).....	17
2.4.1    Pengertian NFC.....	17
2.4.2    Perangkat NFC .....	18
2.4.3    Mode Operasi NFC .....	19
2.4.4 <i>Mifare Classic 1K</i> .....	22

2.5	Teori Kriptografi .....	24
2.5.1	Pengertian Kriptografi.....	24
2.5.2	Teknik Enkripsi.....	25
2.6	Algoritma Kriptografi.....	28
2.7	Algoritma RC4 .....	30
2.7.1	Dasar Kerja Algoritma RC4.....	32
2.8	Algoritma Spritz .....	34
2.9	Perbandingan Algoritma RC4 dan Algoritma Spritz.....	35
2.10	<i>Online Evolution Model</i> .....	37
BAB III .....		40
METODE PENELITIAN.....		40
3.1	Kerangka Penelitian .....	40
3.2	Metode Perancangan dan Pengembangan .....	40
3.3	Jenis Penelitian .....	63
3.4	Objek Penelitian .....	63
3.5	Metode Pengumpulan Data .....	64
3.6	Implementasi Algoritma Kriptografi RC4.....	65
BAB IV .....		73
IMPLEMENTASI DAN PENGUJIAN .....		73
4.1	Implementasi Sistem .....	73
4.2	Implementasi Perancangan Antar Muka .....	75
4.3	Implementasi Data.....	83
4.4	Implementasi Algoritma Kriptografi RC4.....	83
4.5	Pengujian Aplikasi KPU Universitas Bakrie.....	87
4.5.1	Pengujian Jarak Baca <i>NFC Reader</i> Terhadap Kartu <i>Mifare Classic</i> 1K .....	87
4.5.2	Pengujian <i>Read Data</i> dan <i>Write Data</i> ke dalam Kartu <i>Mifare Classic</i> 1K .....	88
4.5.3	Pengujian Enkripsi Dan Dekripsi Algoritma RC4.....	89
4.5.4	Pengujian Validasi Enkripsi Algoritma RC4.....	91
4.5.5	<i>Black-Box Testing</i> .....	91
BAB V.....		93
SIMPULAN DAN SARAN .....		93
5.1	Simpulan.....	93
5.2	Saran .....	93
DAFTAR PUSTAKA .....		95

## DAFTAR GAMBAR

Gambar 2.1 <i>Phases of E-Voting System</i> (Al-Ameen & Talab, 2012) .....	16
Gambar 2.2 <i>NFC Standards</i> (Curran et al., 2012) .....	17
Gambar 2.3 <i>Read / Write Mode</i> (Coskun, Ok, & Ozdenizci, 2013) .....	19
Gambar 2.4 <i>Peer to Peer Mode</i> (Coskun et al., 2013) .....	21
Gambar 2.5 <i>Card Emulation Mode</i> (Coskun et al., 2013) .....	21
Gambar 2.6 <i>Memory Organization Mifare Classic 1K</i> (NXP Semiconductors, 2014) .....	23
Gambar 2.7 Contoh Teknik Permutasi(Fiansyah, 2008).....	26
Gambar 2.8 Contoh Enkripsi dengan Teknik Permutasi.....	26
Gambar 2.9 Contoh Enkripsi dengan Teknik Ekspansi .....	27
Gambar 2.10 Enkripsi dengan Teknik <i>Compaction</i> .....	27
Gambar 2.11 Model Algoritma Simetris Sederhana (Stallings, 2005) .....	28
Gambar 2.12 <i>Public Key Cryptography (Encryption)</i> .....	29
Gambar 2.13 <i>Public Key Cryptography (Authentication)</i> .....	29
Gambar 2.14 Rangkaian Proses <i>RC4 Stream Cipher</i> (Arintamy, Cahyani, & Mulyana, 2014) .....	31
Gambar 2.15 <i>Stream Generation</i> (Stallings et al., 2013).....	34
Gambar 2.16 <i>Encipher Time Comparison</i> (Janaki, 2016).....	36
Gambar 2.17 <i>Decipher Time Comparison</i> (Janaki, 2016) .....	36
Gambar 2.18 <i>Execution Time Comparison</i> (Janaki, 2016).....	37
Gambar 2.19 <i>Online Evolution Model</i> Untuk Aplikasi <i>Web</i> Modern(Casteleyn et al., 2009).....	38
Gambar 2.20 <i>Kematangan Aplikasi Web Meningkatkan Sebagai Hasil Kombinasi Pengembangan Inkremental dan Evolusi Berkelanjutan</i> (Casteleyn et al., 2009) .	39
Gambar 3. 1 Kerangka Penelitian .....	40
Gambar 3. 2 <i>Use Case Diagram</i> Aplikasi KPU UB .....	42
Gambar 3. 3 <i>Activity Diagram</i> Login Admin.....	50
Gambar 3. 4 <i>Activity Diagram</i> Registrasi Kandidat .....	51
Gambar 3. 5 <i>Activity Diagram</i> Registrasi Pemilih.....	53
Gambar 3. 6 <i>Activity Diagram</i> View Hasil Perolehan Suara.....	55

Gambar 3. 7 <i>Activity Diagram</i> Absensi Pemilih.....	57
Gambar 3. 8 <i>Activity Diagram</i> Proses Pemilihan .....	59
Gambar 3. 9 <i>Use Case Diagram</i> Aplikasi KPU UB .....	61
Gambar 3. 10 <i>Schema Database</i> Aplikasi KPU UB .....	62
Gambar 3. 11 <i>Flowchart</i> Enkripsi RC4 .....	65
Gambar 3. 12 <i>Flowchart</i> Deskripsi RC4 .....	66
Gambar 4. 1 Halaman Indeks.....	75
Gambar 4. 2 Halaman <i>Login</i> Admin.....	76
Gambar 4. 3 Halaman <i>Home</i> Admin.....	76
Gambar 4. 4 Halaman Registrasi Pemilih .....	77
Gambar 4. 5 Halaman Daftar Nama Pemilih .....	77
Gambar 4. 6 Halaman Registrasi Kandidat Calon Ketua BEM / HMPS .....	78
Gambar 4. 7 Halaman Daftar Nama Kandidat Calon Ketua BEM & HMPS .....	78
Gambar 4. 8 Halaman Cek Daftar Hadir Pemilih .....	79
Gambar 4. 9 Halaman Daftar Hadir Pemilih.....	79
Gambar 4. 10 Halaman Cek Hasil Perolehan Suara Pemilihan Kandidat Calon Ketua BEM / HMPS .....	80
Gambar 4. 11 Halaman Hasil Perolehan Suara.....	80
Gambar 4. 12 Halaman Index Pemilihan .....	81
Gambar 4. 13 Halaman Absensi Pemilih .....	81
Gambar 4. 14 Halaman <i>Vote</i> Pemilih.....	82
Gambar 4. 15 Halaman <i>Voting</i> .....	82
Gambar 4. 16 Halaman Pemilihan Selesai.....	83
Gambar 4. 17 <i>Read</i> Kartu <i>Mifare Sector 0</i> .....	89
Gambar 4. 18 <i>Write Data</i> NIM <i>Into Sector 0 Block 1</i> .....	89
Gambar 4. 19 <i>Write Data</i> Token <i>Into Sector 0 Block 2</i> .....	89

## DAFTAR PSEUDOCODE

<i>Pseudocode 2.1</i> Inisialisasi S dan T (Stallings et al., 2013) .....	32
<i>Pseudocode 2.2</i> Permutasi Awal S (Stallings et al., 2013) .....	32
<i>Pseudocode 2.3 Stream Generation</i> (Stallings et al., 2013) .....	33
<i>Pseudocode 2.4</i> Modul Spritz (Banik & Isobe, 2016). .....	35

## DAFTAR LISTING KODE SUMBER

<i>Listing Kode Sumber 4.1 Fungsi Konversi UID Heksadesimal ke Desimal .....</i>	84
<i>Listing Kode Sumber 4.2 Fungsi Inialisasi Plaintext .....</i>	84
<i>Listing Kode Sumber 4.3 Fungsi Inialisasi State Array S dan K .....</i>	85
<i>Listing Kode Sumber 4.4 Fungsi Key Scheduling.....</i>	85
<i>Listing Kode Sumber 4.5 Fungsi Pseudo Random Generation Algorithm .....</i>	86
<i>Listing Kode Sumber 4.6 Fungsi Proses Enkripsi RC4 .....</i>	86
<i>Listing Kode Sumber 4.7 Fungsi Proses Dekripsi RC4.....</i>	87

## DAFTAR TABEL

Tabel 2. 1 Rangkuman Penelitian Terkait.....	9
Tabel 2. 2 Contoh Tabel Enkripsi dengan Teknik Substitusi .....	25
Tabel 2. 3 Contoh Tabel Enkripsi dengan Teknik <i>Blocking</i> .....	25
Tabel 3. 1 <i>Use Case Scenario Login</i> .....	42
Tabel 3. 2 <i>Use Case Scenario</i> Registrasi Kandidat.....	43
Tabel 3. 3 <i>Use Case Scenario</i> Registrasi Pemilih.....	44
Tabel 3. 4 <i>Use Case Scenario View Result</i> .....	46
Tabel 3. 5 <i>Use Case Scenario</i> Absensi Pemilih.....	47
Tabel 3. 6 <i>Use Case Scenario View</i> Kandidat.....	48
Tabel 3. 7 <i>Use Case Scenario Cast Vote</i> .....	48
Tabel 4.1 Tabel Hasil Uji Jarak Baca <i>NFC Reader</i> Terhadap Kartu <i>Mifare</i> .....	87
Tabel 4.2 Hasil Enkripsi Dan Dekripsi NIM .....	89
Tabel 4.3 Hasil Enkripsi Dan Dekripsi Token.....	90
Tabel 4.4 Hasil Perhitungan Manual dan Perhitungan Sistem.....	91



## DAFTAR SINGKATAN

### *Standard*

BEM	Badan Eksekutif Mahasiswa
E-Vote	<i>Electronic-Vote</i>
E-Voting	<i>Electronic-Voting</i>
GUI	<i>Graphical User Interface</i>
HMPS	Himpunan Mahasiswa Program Studi
IC	<i>Integrated Circuit</i>
IEC	<i>International Electrotechnical Commission</i>
ISO	<i>International Organization of Standardization</i>
KB	<i>Kilo Byte</i>
KPU	Komisi Pemilihan Umum
KPU UB	Komisi Pemilihan Umum Universitas Bakrie
KSA	<i>Key Scheduling Algorithm</i>
KTP Elektronik	Kartu Tanda Penduduk Elektronik
LLCP	<i>Logical Link Control Protocol</i>
MB	<i>Mega Byte</i>
NFC	<i>Near Field Communication</i>
NFCIP-1	<i>Near Field Communication Interface and Protocol-1</i>
RC4	<i>Rivest Code 4</i>
RF	<i>Radio Frequency</i>
UID	<i>Unique Identification</i>
URL	<i>Uniform Resource Locator</i>

## DAFTAR LAMPIRAN

Lampiran 1 : Rancangan Kegiatan Penelitian

Lampiran 2 : Hasil Wawancara

Lampiran 3 : Pengujian *Black-Box* Aplikasi KPU UB

Lampiran 4 : Uji Algoritma RC4 Pada Aplikasi KPU UB

Lampiran 5 : Hasil Uji Validasi Algoritma RC 4