# PENERAPAN ALGORITMA RIVEST-SHAMIR-ADLEMAN (RSA) PADA *E-VOTING* PEMILIHAN GUBERNUR MAHASISWA FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA BERBASIS ANDROID

**SKRIPSI**
**Program Studi Sistem Informasi**
**Jenjang Sarjana**


Oleh

**Wahyu Utama Putra**
**09031381520058**

**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS SRIWIJAYA**
**2021**

**LEMBAR PENGESAHAN**

SKRIPSI

PENERAPAN ALGORITMA RIVEST-SHAMIR-ADLEMAN (RSA) PADA E-VOTING PEMILIHAN GUBERNUR MAHASISWA FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA BERBASIS ANDROID

Sebagai salah satu syarat untuk
Penyelesaian studi di Program Studi
Sistem Informasi S1

Oleh :
Wahyu Utama Putra 09031381520058

Mengetahui,
Ketua Jurusan Sistem Informasi,

Endang Lestari Ruskan, M.T.
NIP 197811172006042001

Palembang, 21 Januari 2022
Pembimbing,

Allsela Meiriza, M.T.
NIP 198305132015109201

## HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis
Tanggal : 30 Desember 2021

Nama : Wahyu Utama Putra
NIM : 09031381520058
Judul : Penerapan Algoritma Rivest-Shamir-Adleman (RSA) Pada *Evoting* Pemilihan Gubernur Mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya Berbasis Android

Tim Penguji :

1. Ketua : Ari Wedhasmara, M.TI.
2. Pembimbing : Allsela Meiriza, M.T.
3. Penguji : Rahmat Izwan Heroza, M.T.
4. Penguji : Dinna Yunika Hardiyanti, M.T.

Mengetahui
Ketua Jurusan Sistem Informasi,

Endang Lestari Ruskan, M.T
NIP 197811172006042001

## SURAT PERNYATAAN BEBAS PLAGIAT

Saya yang bertanda tangan dibawah ini:

| | |
|---|---|
| Nama | : Wahyu Utama Putra |
| NIM | : 09031381520058 |
| Program Studi | : Sistem Informasi Bilingual |
| Judul Skripsi | : Penerapan Algoritma Rivest-Shamir-Adleman (RSA) Pada *E-voting* Pemilihan Gubernur Mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya Berbasis Android |

Hasil Pengecekan Software iThenticate/Turnitin : 3 %

Menyatakan bahwa laporan skripsi saya merupakan hasil karya saya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya dengan ketentuan yang berlaku.

Demikianlah pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, Januari 2022


Wahyu Utama Putra

09031381520058

# KATA PENGANTAR

Alhamdulillahirabbil'alamin, segala puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya serta memberikan kesehatan, kekuatan, dan kesabaran sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul **"PENERAPAN ALGORITMA RIVEST-SHAMIR-ADLEMAN (RSA) PADA *E-VOTING* PEMILIHAN GUBERNUR MAHASISWA FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA BERBASIS ANDROID"**.

Selama pembuatan Tugas Akhir ini, penulis banyak menemukan hambatan dan kesulitan, namun berkat bimbingan dan pengarahan serta bantuan dari berbagai pihak, maka penulis dapat selesaikan. Untuk itu pada kesempatan ini penulis ingin menyampaikan ucapan terimakasih kepada :

1. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
2. Ibu Endang Lestari Ruskan, M.T. selaku Ketua Jurusan Sistem Informasi.
3. Ibu Allsela Meiriza, M.T., selaku Dosen Pembimbing yang selalu sabar dalam membimbing penulis, memberikan masukan serta ide yang membangun sehingga Tugas Akhir ini dapat di selesaikan
4. Bapak Ari Wedhasmara, M.TI., Bapak Rahmat Izwan Heroza, M.T., dan Ibu Dinna Yunika Hardiyanti, M.T., selaku Dosen Penguji yang memberikan kritik dan saran untuk membuat Tugas Akhir ini menjadi lebih baik.
5. Seluruh Dosen Sistem Informasi Fakultas Ilmu Komputer yang telah memberikan ilmu terhadap penulis.
6. Mbak Rifka, yang telah bersedia membantu penulis dan mendengarkan segala cerita penulis di ruangan admin Jurusan SI, nanti penulis akan sering main ke ruangan admin tenang saja.

7. Kedua orang tua, Bapak Jaya Putra dan Ibu Marlina serta kedua adik penulis, Tasya dan Elco yang senantiasa memberikan semangat, dukungan, doa, dan kasih sayang yang tiada henti-hentinya kepada penulis agar selalu ingat untuk menyelesaikan Tugas Akhir ini sampai tuntas tanpa adanya hambatan.
8. Sahabat penulis, M. Abid Sadewa, M. Eldo Julian Pratama, M. Henky Saputra, dan M. Tri Alhadi yang selalu mengingatkan dan memberi dukungan sehingga membuat penulis lupa akan kerumitan mengerjakan Tugas Akhir ini.

Penulis menyadari bahwa Tugas Akhir ini masih jauh dari kesempurnaan, baik teknis penulisan, bahasa maupun cara pemaparannya. Penulis berharap semoga Tugas Akhir ini dapat bermanfaat bagi penulis khususnya, dan bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya pada umumnya serta dapat memberikan masukan sebagai sumbangan pikiran dalam rangka peningkatan mutu dalam pembelajaran.

Palembang, Januari 2022

Penulis,

**Wahyu Utama Putra**

09031381520058

# ABSTRAK

PENERAPAN ALGORITMA RIVEST-SHAMIR-ADLEMAN (RSA) PADA E-VOTING PEMILIHAN GUBERNUR MAHASISWA FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA BERBASIS ANDROID

Oleh

Wahyu Utama Putra
09031381520058

Pelaksanaan pemilihan gubernur mahasiswa fakultas ilmu komputer universitas sriwijaya masih dilakukan secara manual dengan melakukan pencoblosan pada kertas suara di “bilik” suara. Banyak kelemahan pada proses ini dimana memakan waktu dan biaya serta akurasi hasil yang kurang dapat diandalkan karena adanya kemungkinan *human error*. Oleh karena itu, sekaligus melakukan implementasi dari kemajuan teknologi, proses pengambilan suara dilakukan secara elektronik (*e-voting*). Dalam pengembangannya, ilmu kriptografi ditambahkan untuk memastikan keamanan dan kerahasiaan data. Algoritma kriptografi yang diimplementasikan adalah algoritma Rivest Shamir Adleman (RSA).

**Kata Kunci** : *E-voting,* Algoritma RSA, Kriptografi

# ABSTRACT

IMPLEMENTATION OF RIVEST-SHAMIR-ADLEMAN (RSA) ALGORITHM ON ANDROID-BASED E-VOTING GOVERNOR OF STUDENT ELECTION OF COMPUTER SCIENCE FACULTY SRIWIJAYA UNIVERSITY

By

Wahyu Utama Putra
09031381520058

The election of governor for student of computer science faculty of sriwijaya university is still done manually by voting on the voting booth. There are many weaknesses in this process which is time-consuming, costly, and the accuracy of the results is not reliable due to possibility of human error. Therefore as well as implementing technological advances, the voting process is carried out electronically (e-voting). In its development, the science of cryptography is added to ensure data security and confidentiality. The cryptographic algorith implemented is the Rivest-Shamir-Adleman Algorithm.

**Keyword** : *E-voting,* RSA Algorithm, Cryptograph

# DAFTAR ISI

HALAMAN JUDUL ..... i
LEMBAR PENGESAHAN ..... ii
HALAMAN PERSETUJUAN ..... iii
SURAT PERNYATAAN BEBAS PLAGIAT ..... iv
KATA PENGANTAR ..... v
ABSTRAK ..... vii
ABSTRACT ..... viii
DAFTAR ISI ..... ix
DAFTAR TABEL ..... xii
DAFTAR GAMBAR ..... xiii
DAFTAR LAMPIRAN ..... xiv
BAB I ..... 1
PENDAHULUAN ..... 1
1.1 Latar Belakang ..... 1
1.2 Tujuan Penelitian ..... 3
1.3 Manfaat Penelitian ..... 3
1.4 Batasan Masalah ..... 3
BAB II ..... 4
TINJAUAN PUSTAKA ..... 4
2.1 Tinjauan Pustaka ..... 4
2.1.1 Aplikasi ..... 5
2.1.2 *Algoritma RSA* ..... 5
2.1.2.1 Proses Pembentukan Kunci ..... 6
2.1.2.2 Proses Enkripsi Dan Dekripsi ..... 6
2.1.2.3 Contoh Kasus ..... 7
2.1.3 Basis Data *(Database)* ..... 9
2.1.4 Android ..... 10
2.1.5 Kotlin ..... 11
2.1.6 Android Studio ..... 12
2.2 *Rational Unified Process (*RUP) ..... 13
2.3 *Unified Modeling Language* (UML) ..... 19

BAB III ..... 21
METODOLOGI PENELITIAN ..... 21
3.1 Pendahuluan ..... 21
3.2 Objek Penelitian ..... 21
3.3 Teknik Pengumpulan Data ..... 21
3.3.1 Observasi ..... 21
3.3.2 Wawancara ..... 21
3.4 Metode Pengembangan Perangkat Lunak ..... 22
3.5 Manajemen Proyek Pengembangan Perangkat Lunak ..... 23
3.5.1 Melakukan Pengembangan Objek Penelitian Menggunakan RUP (*Rational Unified Process)* ..... 23
3.5.2 Merumuskan Kamus Data ..... 29
BAB IV ..... 30
HASIL DAN PEMBAHASAN ..... 30
4.1. Pernyataan Masalah dan Opportunities ..... 30
4.1.1. Pernyataan Masalah ..... 30
4.1.2. *Opportunities* ..... 31
4.2. Hambatan Proyek ..... 31
4.2.1. *Business Constraints* ..... 31
4.2.2 *Technology Constraints* ..... 32
4.3. Domain Permasalahan ..... 32
4.4 Analisis Kebutuhan ..... 34
4.4.1. *Functional Requirement* ..... 34
4.5.2. *Non Functional Requirement* ..... 35
4.6. Prioritas Kebutuhan Sistem ..... 36
4.6.1. *Mandatory Requirement* ..... 36
4.6.2. *Desirable Requirement* ..... 36
4.7. Perancangan Logika ..... 38
4.7.1. Permodelan Proses ..... 38
4.7.1.1. *Data Flow Diagram* (DFD) level 0 ..... 38
4.7.1.2. *Entity Relationship Diagram* (ERD) ..... 39
4.7.1.3. *Use Case Diagram* ..... 39
4.7.1.4. *Diagram Aktivities Voting dan Result* ..... 40

4.8. Rancangan Interface ..... 41
4.8.1. Halaman Login ..... 41
4.8.2. Halaman Surat Suara ..... 43
4.8.3. Halaman Result ..... 44
4.9. Pembahasan ..... 45
4.9.1. Halaman Utama ..... 45
4.9.2. Halaman Voting ..... 46
4.9.3. Halaman Result ..... 50
4.10 Pengujian Sistem ..... 53
4.11 Hasil Uji coba ..... 53
BAB V ..... 55
KESIMPULAN DAN SARAN ..... 55
5.1. Kesimpulan ..... 55
5.2. Saran ..... 56
DAFTAR PUSTAKA ..... 57

# DAFTAR TABEL

Tabel 2. 1 Simbol-Simbol ERD ..... 18
Tabel 2. 2 Simbol *Unified Modeling Language (UML)* ..... 19
Tabel 3. 1 Aktor ..... 26
Tabel 3. 2 Kebutuhan Fungsional ..... 26
Tabel 3. 3 Definisi Aktor ..... 27
Tabel 3. 4 Definisi Use Case ..... 28
Tabel 3. 5 Kamus Data ..... 29
Tabel 4. 1 Kebutuhan Non Fungsional dengan Framework PIECES ..... 35
Tabel 4. 2 *Desirable Requirement* ..... 37

# DAFTAR GAMBAR

Gambar 2. 1 *Rational Unified Process* (RUP) (SofiePilemalm, 2007)..... 14
Gambar 2. 2 Simbol-Simbol dalam Use Case Diagram..... 20
Gambar 3. 1 Tahapan Pengembangan Sistem Pada Penelitian..... 22
Gambar 3. 2 ERD Sistem..... 25
Gambar 4. 1 *Data Flow Diagram* (DFD) ..... 38
Gambar 4. 2 ERD Sistem..... 39
Gambar 4. 3 ERD Sistem..... 40
Gambar 4. 4 Diagram Aktivitas *Voting* ..... 40
Gambar 4. 5 Diagram Aktivitas *Result* ..... 41
Gambar 4. 6 Halaman Login Mahasiswa..... 42
Gambar 4. 7 Halaman Login Admin..... 42
Gambar 4. 8 Halaman Surat Suara..... 43
Gambar 4. 9 Halaman Result..... 44
Gambar 4. 1 0Halaman Result (2) ..... 45
Gambar 4. 11 Halaman Utama..... 46
Gambar 4. 12 Halaman Voting..... 47
Gambar 4. 13 Verifikasi NIM ditolak..... 48
Gambar 4. 14 Surat Suara pada Aplikasi ..... 48
Gambar 4. 15 Notifikasi Pilihan (Sesuai Pilihan *User*) ..... 49
Gambar 4. 16 Verifikasi Admin..... 50
Gambar 4. 17 Verifikasi Admin diterima ..... 51
Gambar 4. 18 Hasil *e-Calculating* ..... 51
Gambar 4. 19 Tampilan jika Terdeteksi Kecurangan ..... 52

## DAFTAR LAMPIRAN

Lampiran 1 Kartu Konsultasi..... A-1
Lampiran 2 Keterangan Perubahan Judul Skripsi..... B-1
Lampiran 3 Form Perbaikan Ujian Komprehensif..... C-1
Lampiran 4 Hasil Cek Plagiat..... D-1

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Pada era yang semakin maju saat ini, teknologi tentunya akan selalu melekat pada kehidupan orang-orang. Dengan teknologi yang terus bertumbuh, penggunaan *handphone* membawa perubahan dalam kehidupan orang-orang. Dulu, *handphone* hanya digunakan sebagai sarana berkomunikasi, dikenal sebagai telfon dan sms. Sekarang, banyak hal bisa dilakukan melalui benda kecil tersebut. Tidak hanya itu, dengan berkembangnya Android, sistem operasi dengan lisensi terbuka yang tentunya didukung oleh platform lengkap dan tentunya *open source* membuat *handphone* berbasis Android dipilih sebagai penunjang kehidupan bermasyarakat kini.

Kegiatan demokrasi dikawasan fakultas dilakukan dengan pengambilan suara pada pemilihan Gubernur mahasiswa fakultas. Namun, pada umumnya, pelaksanaannya masih dilakukan secara manual dengan melakukan pencoblosan pada kertas suara di “bilik” pada lokasi tertentu yang biasa disebut TPU. Banyak kelemahan pada proses ini, seperti tidak fleksibelnya proses karena harus datang ke lokasi tertentu dimana hal tersebut memakan waktu dan biaya. Ditambah lagi lemahnya akurasi hasil karena adanya kemungkinan *human error.* Tidak sampai disitu, keharusan memproduksi surat suara sekaligus penyimpanan serta pendistribusiannya menggunakan biaya yang tidak sedikit. Oleh sebab itu,

sekaligus melakukan implementasi dari kemajuan teknologi, proses pengambilan suara dilakukan secara elektronik *(e-voting).*

Pengambilan suara dengan menggunakan teknologi komputer merupakan bagian proses dari *e-voting* (pengambilan suara elektronik). Biasanya pemilihan dilakukan melalui jaringan Internet atau Intranet. Untuk itu, penulis membangun software *e-voting* berbasis *Android*. Dimulai dari pengecekan hak pemilih, pengambilan suara, hingga perhitungan suaranya. *Rational Unifed Process* (RUP) akan digunakan sebagai metode yang dipakai dalam pembangunan.

Keamanan tentunya sangat dibutuhkan demi menghasilkan software yang *reliable*. Sehingga, dalam pembangunannya, ilmu kriptografi akan ditambahkan kedalam system agar keamanan informasi dalam system *evoting* terjaga. Kriptografi ditambahkan untuk memastikan bahwa seluruh suara yang ada, integritasnya dapat dipertanggungjawabkan meskipun data pemilik suara tidak diketahui yangmana menjalankan aspek utama demokrasi, kerahasiaan. Algoritma kriptografi yang diimplementasikan adalah algoritma RSA karena lebih mudah dalam perhitungan dan analisisnya.

Berangkat dari paragraf-paragraf diatas, penulis mengangkat judul **Penerapan Algoritma Rivest-Shamir-Adleman (RSA) pada *E-Voting* Pemilihan Gubma Fakultas Ilmu Komputer Universitas Sriwijaya Berbasis Android.**

## 1.2 Tujuan Penelitian

Dapat menerapkan algoritma Rivest-Shamir-Adleman (RSA) pada *e-voting* Pemilihan Gubma Fakultas Ilmu Komputer Universitas Sriwijaya berbasis android dan hasilnya dapat diketahui secara *Real Time*.

## 1.3 Manfaat Penelitian

Adapun manfaat dari penelitian ini, yaitu:

1. *Software e-voting* Pemilihan Gubma Fakultas Ilmu Komputer Universitas Sriwijaya berbasis android yang dihasilkan dapat diterapkan.

2. Bagi admin dapat memudahkan dalam perhitungan, sedangkan bagi mahasiswa memudahkan proses pemilihan, mencegah kecurangan, serta mengurangi biaya.

## 1.4 Batasan Masalah

Berikut merupakan batasan masalah dari penelitian ini:

1. Kunci kriptografi RSA sudah ditentukan yaitu data NIM dan Mahasiswa.

2. Sesuai asas demokrasi, pemilihan secara langsung, umum, bebas dan rahasia, serta jujur & adil.

3. *Software E-voting* hanya untuk pemilihan Gubernur Mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya.

# DAFTAR PUSTAKA


Andika Cahya Putra, Magdalena Simanjuntak, Nurhayati. (2021), Penerapan Algoritma RIVEST SHAMI ADLEMAN (RSA) untuk mengamankan database program Keluarga Harapan (PKH), Jurnal Teknik Informatika Kaputama(JTIK), hal 76-84.

Bruno Gois, Mateus, Matias Martinez. (2019), An empirical studt on quality of Android applications writteb in Kotlin Language, empirical softrware engineering, vol 24(6), Hal 3356-3393.

Indra Gunawan, Sumarno, Heru Satria Tambunan. (2018), Fungsi Algoritma RSA untuk modifikasi dan meningkatkan pengamanan acakan BISS, CESS(*Journal of computer Engineering system and science)* , Vol. 3(2), hal. 155-156.

*Internet Policy Institute, Report of the National Workshop on Int*

Jajang Kharil Azhar, Susy Yulianty. (2019) Implementasi Algoritma RSA (Rivest Sahmir& Adleman) untuk enkripsi dan dekripsi file pdf, Prodi Teknik Informatika, Universitas Siliwangi, Tasikmalaya Indonesia.

Loura Hardjaloka, Varida Megawati Simarmata. (2011). *E-Voting* Kebutuhan vs Kesiapan (menyongsong) E-Demokrasi. Fakultas Hukum Universitas Indonesia Depok, Jawa Barat.

Marcin Moskala, Igor Wojda. (2017) Android Development with Kotlin. Packet publishing Ltd.

Nila Sumanda, Sibarani, Givan Musnawar, Bambang Wisnuadhi. (2018), Analisis Performa aplikasi android pada pemrograman java dan kotlin, prosiding industrial research workshop and National Seminar 9, hal 319-324.

Ricardo Coppola, Luva Ardito, Marco Torchiano. (2019), Characterizing the transtition to kotlin of android apps a study on F-Droid, playstore and github, proceedings off the 3rd ACM SIGSOFT Internasional Workshop on App Market Analytic, Hal 8-14.

Safaat, N., (2011). Android: Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Edisi Revisi. Bandung : Informatika

Siahaan, Daniel. (2020). Analisa Kebutuhan dalam Rekayasa Perangkat Lunak. Yogyakarta : Andi.

Sulastri, Leni, Natalia Zulita. (2015). *Evoting* Pemilihan Walikota Bengkulu di Komisi Pemilihan Umum (KPU) Kota Bengkulu, Vol. 11 No. 2

Sutarman. (2012). Buku Pengantar Teknologi Informasi. Jakarta: Bumi Aksara.

Warouw, Riske P. (2014). Perancangan Aplikasi Voter Berbasis Android Studi Kasus Pemilihan Ketua Himpunan Mahasiswa Jurusan Tekhnik Elektro Universitas Sam Ratulangi Manado. Ejournal Teknik Elektro dan Komputer. Jurnal Teknik Elektro dan Komputer Unsrat. Volume 3, No. 5, http://xaverius.najoan.net/index.php/publication, diakses pada tanggal 10 Agustus 2015

Zainal Arifin, (2016), Studi Kasus Penggunaan Algoritma RSA sebagai Algoritma Kriptografi yang aman, Informatika Mulawarman, Jurnal Ilmiah Komputer, vol. 4(3), hal 7-14.