

**IMPLEMENTASI DIGITAL SIGNATURE DENGAN ALGORITMA RABIN-p DAN
SHA-256 UNTUK FILE PDF PADA APLIKASI ANDROID**

SKRIPSI

SAMFRIANDY GUSBORN SITUMEANG

171401080



PROGRAM STUDI S-1 ILMU KOMPUTER

ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UNIVERSITAS SUMATERA UTARA

MEDAN

2024

**IMPLEMENTASI DIGITAL SIGNATURE DENGAN ALGORITMA RABIN-p DAN
SHA-256 UNTUK FILE PDF PADA APLIKASI ANDROID**

SKRIPSI

SAMFRIANDY GUSBORN SITUMEANG

171401080



**PROGRAM STUDI S-1 ILMU KOMPUTER
ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS SUMATERA UTARA**

MEDAN

2024

PERSETUJUAN

Judul : IMPLEMENTASI DIGITAL SIGNATURE DENGAN
ALGORITMA RABIN-p DAN SHA-256 UNTUK
FILE PDF PADA APLIKASI ANDROID

Kategori : SKRIPSI

Nama : SAMFRIANDY GUSBORN SITUMEANG

Nomor Induk Siswa : 171401080

Program Studi : SARJANA (S-1) ILMU KOMPUTER

Fakultas : FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI
INFORMASI UNIVERSITAS SUMATERA UTARA

Komisi Pembimbing :

Tanggal Sidang : 24 Juni 2024

Dosen Pembimbing II



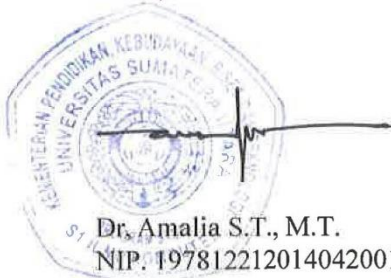
Dr. Maya Silvi Lydia B.Sc., M.Sc.
NIP. 197401272002122001

Dosen Pembimbing I



Dian Rachmawati S.Si., M.Kom.
NIP. 198307232009122004

Diketahui/Disetujui oleh .
Program Studi S1 Ilmu Komputer
Ketua,



Dr. Amalia S.T., M.T.
NIP. 197812212014042001

PERNYATAAN

IMPLEMENTASI *DIGITAL SIGNATURE* DENGAN ALGORITMA RABIN-*p* DAN SHA-256 UNTUK *FILE* PDF PADA APLIKASI ANDROID

SKRIPSI

Saya mengakui bahwa Skripsi ini adalah hasil karya saya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing telah disebutkan sumbernya.

Medan, 24 Juni 2024



Samfriandy Gusborn Situmeang

171401080

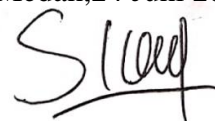
PENGHARGAAN

Dengan penuh rasa syukur, penulis ingin mengungkapkan terima kasih kepada Tuhan yang Maha Esa atas anugerah-Nya yang melimpah. Penulis bersyukur karena telah berhasil menyelesaikan penyusunan skripsi ini dengan baik, sebagai persyaratan untuk menyelesaikan Program Studi S1 Ilmu Komputer, yang berada di bawah naungan Fakultas Ilmu Komputer dan Teknologi Informasi di Universitas Sumatera Utara. Penulis mengakui bahwa pencapaian ini tidak mungkin terwujud tanpa bantuan dan dukungan dari semua pihak yang terlibat, yaitu :

1. Bapak Dr. Muryanto Amin S.Sos., M.Si. selaku Rektor Universitas Sumatera Utara.
2. Ibu Dr. Maya Silvi Lydia B.Sc., M.Sc. selaku Dekan Fasilkom-TI Universitas Sumatera Utara.
3. Ibu Dr. Amalia ST., M.T., Ketua Program Studi S-1 Ilmu Komputer Universitas Sumatera Utara.
4. Ibu Dian Rachmawati S.Si., M.Kom., Dosen Pembimbing I yang memberikan bimbingannya kepada penulis selama proses pengerjaan skripsi.
5. Ibu Dr. Maya Silvi Lydia B.Sc., M.Sc., Dosen Pembimbing II yang bersedia memberikan bimbingannya kepada penulis selama proses pengerjaan skripsi.
6. Bapak Dr. Mohammad Andri Budiman S.T., M.Comp.Sc., M.E.M., Dosen Pembimbing Akademik yang sudah bersedia membimbing penulis selama menempuh perkuliahan.
7. Keluarga penulis Bapak Sahat Situmeang dan Ibu Rumiana Malau yang selalu memberikan doa dan dukungan yang tiada putusnya kepada penulis.
8. Keluarga Besar Mahasiswa Ilmu Komputer Universitas Sumatera Utara 2017 yang telah menjalani perkuliahan bersama dengan penulis.
9. Penulis mengucapkan terima kasih kepada semua pihak yang terlibat secara langsung maupun tidak langsung dalam penyelesaian skripsi ini, meskipun tidak bisa disebutkan satu per satu.

Penulis mengakui bahwa skripsi ini masih jauh dari sempurna. Meskipun begitu, terlintas secercah harapan agar skripsi ini dapat memberi manfaat seusai dibaca serta tidak menutup kemungkinan untuk dijadikan bahan referensi bagi penelitian di masa mendatang.

Medan, 24 Juni 2024



Samfriandy Gusborn Situmeang

ABSTRAK

Dalam era digital yang semakin berkembang, pentingnya keamanan dan keabsahan informasi menjadi semakin terang. Salah satu pendekatan yang efektif adalah melalui penggunaan digital signature. Penelitian ini memiliki tujuan utama untuk mengembangkan aplikasi Android yang memiliki kapabilitas melakukan proses digital signature pada berkas PDF. Proses tersebut melibatkan algoritma Rabin-p untuk menciptakan tanda tangan digital serta algoritma SHA-256 untuk menghasilkan *hash* dari dokumen. Aplikasi ini juga menaruh perhatian khusus pada keamanan dalam menyimpan kunci pribadi pengguna, sehingga tanda tangan digital yang dihasilkan tetap terlindungi dari potensi ancaman dari luar. Metodologi penelitian mencakup tahapan perancangan serta implementasi algoritma Rabin-p dan SHA-256 dalam konteks aplikasi Android, juga terintegrasi dengan penampil PDF yang sudah ada. Pengujian dilakukan untuk menguji efektivitas tanda tangan digital dalam memverifikasi integritas dan otentikasi berkas PDF. Hasil pengujian memverifikasi kemampuan aplikasi ini dalam menghasilkan tanda tangan digital yang sah dan dapat mengidentifikasi perubahan pada berkas PDF.

Kata kunci: *Digital Signature*, Algoritma Rabin-p, SHA-256, File PDF, Aplikasi Android, Keamanan Informasi.

**IMPLEMENTATION OF DIGITAL SIGNATURE WITH RABIN-p
ALGORITHM AND SECURE HASH ALGORITHM - 256 FOR PDF FILES
ON ANDROID APPLICATION**

ABSTRACT

In the rapidly evolving digital era, the importance of information security and authenticity becomes increasingly evident. One effective approach to address these concerns is through the use of digital signatures. The main objective of this research is to develop an Android application with the capability to perform digital signature processes on PDF files. This process involves the use of the Rabin-p algorithm to create digital signatures and the SHA-256 algorithm to generate hashes from documents. The application also places special emphasis on security by securely storing the user's private keys, ensuring that the generated digital signatures remain protected from potential external threats. The research methodology encompasses the stages of designing and implementing the Rabin-p and SHA-256 algorithms within the context of an Android application, integrated with existing PDF viewers. Testing is conducted to evaluate the effectiveness of digital signatures in verifying the integrity and authenticity of PDF files. The test results confirm the application's ability to produce valid digital signatures and identify changes in PDF files.

Keywords: Digital Signature, Rabin-p Algorithm, SHA-256, PDF Files, Android Application, Information Security.

DAFTAR ISI

PERSETUJUAN	ii
PERNYATAAN.....	iii
PENGHARGAAN.....	iv
ABSTRAK	1
ABSTRACT.....	2
DAFTAR ISI.....	3
DAFTAR GAMBAR.....	5
BAB 1	6
1.1. Latar belakang	6
1.2. Rumusan masalah.....	9
1.3. Batasan masalah	9
1.4. Tujuan penelitian	9
1.5. Manfaat penelitian	10
1.6. Metodologi penelitian	10
1.7. Sistematika penelitian	11
BAB 2.....	12
2.1. Keamanan data	12
2.2. Kriptografi	12
2.2.1. Terminologi kriptografi.....	13
2.2.2. Jenis kriptografi	14
2.2.3. Pembangkitan kunci.....	15
2.2.4. Enkripsi	16
2.2.5. Dekripsi	17
2.3. Rabin-p.....	19
2.4. <i>Digital signature</i>	19
2.5. SHA-256	22
2.6. File teks	23
BAB 3	24
3.1. Analisis sistem.....	24

3.1.1.	Analisis masalah	24
3.1.2.	Analisis kebutuhan	25
3.1.3.	Analisis proses.....	26
3.2.	Pemodelan sistem.....	27
3.2.1.	Diagram umum sistem.....	27
3.2.2.	<i>Use case diagram</i>	28
3.2.3.	<i>Activity diagram</i>	29
3.2.3 1.	<i>Diagram Activity</i> Enkripsi Rabin-p.....	29
3.2.3 2.	<i>Diagram Activity</i> Penyisipan	30
3.2.3 3.	<i>Diagram Activity</i> Ekstraksi	31
3.2.3 4.	<i>Diagram Activity</i> Dekripsi Rabin-p.....	32
3.2.4.	Sequence diagram	33
3.3.	Flowchart.....	34
3.3.1.	<i>Flowchart</i> sistem	34
3.3.2.	<i>Flowchart</i> enkripsi rabin-p	35
3.3.3.	<i>Flowchart</i> ekstraksi	36
3.3.4.	<i>Flowchart</i> dekripsi rabin-p	37
3.4.	Perancangan antarmuka	38
3.4.1.	Desain Rancangan dari Halaman About.....	38
3.4.2.	Desain Rancangan dari Halaman utama.....	39
3.4.3.	Desain Rancangan dari Halaman Pembangkit kunci	40
3.4.4.	Desain Rancangan dari Halaman Tanda tangan	41
3.4.5.	Desain Rancangan dari Halaman Verifikasi.....	42
BAB 4	43
	Implementasi sistem.....	43
4.1.	Halaman <i>about</i>	43
4.2.	Halaman utama.....	44
4.3.	Halaman Pembangkit kunci	45
4.4.	Halaman Tanda tangan	46
4.5.	Halaman Verifikasi.....	47
4.6.	Pengujian.....	48
4.6.1.	Pengujian Sistem <i>Digital Signature</i>	48

BAB 5	53
5.1. Kesimpulan.....	53
5.2. Saran	53
DAFTAR PUSTAKA.....	54
LAMPIRAN.....	55

DAFTAR GAMBAR

Gambar 2.1 Skema dari Proses Enkripsi dan Dekripsi	13
Gambar 2.2 Skema dari Kriptografi Simetris	14
Gambar 2.3 Skema dari kriptografi Asimetris.....	15
Gambar 2.4 Diagram Digital Signature.....	20
Gambar 2.5 Arsitektur sederhana SHA-256.....	22
Gambar 3.1 Diagram ishikawa	24
Gambar 3.2 Diagram umum sistem	27
Gambar 3.3 Use case diagram pada sistem	28
Gambar 3.4 Diagram enkripsi rabin-p	29
Gambar 3.5 Diagram Penyisipan	30
Gambar 3.6 Diagram Ekstraksi	31
Gambar 3.7 Diagram Dekripsi Rabin-p.....	32
Gambar 3.8 Diagram Sequence pada Sistem	33
Gambar 3.9 Desain Skema Flowchart dari Enkripsi dan Dekripsi	34
Gambar 3.10 Desain Skema Flowchart dari Enkripsi Rabin-P	35
Gambar 3.11 Desain Skema Flowchart dari Ekstraksi	36
Gambar 3.12 Desain Skema Flowchart dari Dekripsi Rabin-p.....	37
Gambar 3.13 Desain Rancangan dari Halaman About	38
Gambar 3.14 Desain Rancangan dari Halaman utama	39
Gambar 3.15 Desain Rancangan dari Halaman Pembangkit kunci	40
Gambar 3.16 Desain Rancangan dari Halaman tanda tangan.....	41
Gambar 3.17 Desain Rancangan dari Halaman Verifikasi	42
Gambar 4.1 Halaman about	43
Gambar 4.2 Halaman utama	44
Gambar 4.3 Halaman pembangkit kunci.....	45
Gambar 4.4 Halaman tanda tangan.....	46
Gambar 4.5 Halaman verifikasi	47

BAB 1

PENDAHULUAN

1.1. Latar belakang

Dengan berjalannya perkembangan teknologi sekarang masyarakat kini terbiasa untuk mengirimkan berkas secara daring. Kebiasaan baru ini memungkinkan kalangan dsecara luas dari keperluan akademik hingga bisnis bahkan pemerintahan melakukan pengiriman berkas berupa *file* dokumen seperti PDF. Keamanan dari suatu data teks harus menjadi perhatian dalam menjaga kerahasiaan data itu sendiri, terutama bila data teks tersebut hanya boleh diketahui pihak yang tertentu saja, terdapat banyak cara pendekatan yang dilakukan untuk mewujudkan kerahasiaan data tersebut dimulai dari pengamanan atau perlindungan secara fisik hingga kedalam bentuk algoritma berbasis matematika yang membuat data menjadi tidak terbaca. Sehingga data yang ada didalamnya tidak dapat mudah diketahui oleh pihak-pihak yang tidak berhak dan hanya penerima data teks yang dimaksud mampu menguraikan data teks tersebut. (Murdani, 2017).

Keamanan data sangat penting dalam *digital signature* karena *digital signature* bertujuan untuk memastikan keaslian dan integritas dokumen, transaksi, atau pesan digital. Dengan *digital signature*, dapat menghindari adanya pemalsuan, perubahan, atau penyalahgunaan data oleh pihak yang tidak berwenang. *Digital signature* juga bisa memberikan bukti identitas, asal, dan status data yang ditandatangani secara digital. *Digital signature* menggunakan teknik kriptografi asimetris yang melibatkan dua kunci, yaitu kunci pribadi dan kunci publik. Kunci pribadi digunakan untuk mengenkripsi data yang terkait dengan tanda tangan, sedangkan kunci publik digunakan untuk dekripsi data. Hanya penerima yang memiliki kunci publik yang sesuai dengan kunci pribadi pengirim yang bisa membuka data tersebut. Jika data tidak bisa dibuka, berarti ada masalah dengan data atau tanda tangannya.

Algoritma Rabin-p adalah sebuah algoritma yang menerapkan kunci asimetris yaitu kunci yang menggunakan dua jenis kunci yang terdiri dari kunci *public* (public key)

dan kunci rahasia (*secret key*). Kunci *public* digunakan untuk mengenkripsi pesan sedangkan kunci rahasia digunakan untuk mendekripsi pesan. Kelebihan algoritma Rabin-p yaitu memiliki tingkat keamanan yang sangat baik namun kelemahan algoritma Rabin-p yaitu menghasilkan ciphertext yang beberapa kali lebih panjang dari plaintext. Fungsi yang tepat untuk aplikasi keamanan seperti autentikasi dan integritas pesan adalah fungsi *hash*. Fungsi *hash* adalah algoritma yang mengambil masukan *string* dengan panjang yang bervariasi dan mengubahnya menjadi *string* keluaran dengan panjang tetap (biasanya jauh lebih pendek dari panjang string asli). *Output* atau enkripsi yang dihasilkan oleh fungsi hash ini disebut sebagai *message digest*.

Untuk memastikan bahwa pesan dapat diotentikasi oleh penerima, *message digest* hasilnya disertakan bersama pesan. *Message digest* ini dapat dianggap sebagai tanda tangan digital, tetapi berbeda dengan tanda tangan digital karena fungsi *hash* yang digunakan hanya bergantung pada pesan itu sendiri dan tidak bergantung pada pengirim, penerima, atau kunci. Ada berbagai jenis algoritma fungsi hash satu arah yang tersedia, seperti *Secure Hash Algorithm* (SHA), sebagai contoh. SHA dikembangkan oleh *National Institute of Standards and Technology* (NIST). SHA sebenarnya merupakan perkembangan dari fungsi *hash* sebelumnya, yaitu MD5.

Salah satu algoritma dari keluarga generasi kedua SHA, yaitu SHA-256, telah dihasilkan dari SHA-1 generasi pertama. SHA-256 mengoperasikan 32bit untuk setiap kata, menghasilkan message digest dengan panjang 256bit.

Algoritma asimetris adalah jenis algoritma kriptografi yang menggunakan dua kunci yang berbeda untuk enkripsi dan dekripsi data. Kunci yang digunakan untuk enkripsi disebut kunci publik, yang dapat disebarluaskan tanpa mengurangi keamanan. Kunci yang digunakan untuk dekripsi disebut kunci pribadi, yang harus dirahasiakan oleh pemiliknya. Algoritma asimetris juga dikenal sebagai kriptografi kunci publik atau kriptografi kunci pasangan. Algoritma asimetris bekerja berdasarkan prinsip

matematika yang menghasilkan fungsi satu arah, yaitu fungsi yang mudah dihitung ke satu arah, tetapi sulit dihitung ke arah yang berlawanan.

Implementasi kedua algoritma ini pada aplikasi *Android* akan memungkinkan pengguna untuk dengan mudah dan aman menandatangani berkas PDF. Selain itu, aplikasi ini juga akan menekankan keamanan dalam pengelolaan kunci pribadi pengguna, yang merupakan elemen penting dalam proses tanda tangan digital. Kunci pribadi akan dienkripsi dan diamankan dengan cermat untuk melindunginya dari potensi ancaman keamanan.

Metodologi penelitian ini mencakup tahap perancangan dan implementasi algoritma Rabin-p dan SHA-256 dalam konteks aplikasi *Android*. Aplikasi ini juga akan terintegrasi dengan penampil PDF yang sudah ada. Pengujian akan dilakukan untuk memverifikasi efektivitas tanda tangan digital dalam memastikan integritas dan otentikasi berkas PDF. Hasil pengujian akan memvalidasi kemampuan aplikasi ini dalam menghasilkan tanda tangan digital yang sah dan mampu mendeteksi perubahan pada berkas PDF dengan akurasi tinggi. Penelitian ini diharapkan dapat memberikan kontribusi penting dalam pengembangan teknologi tanda tangan digital yang aman dan efisien untuk berkas PDF di *platform Android*. Keberhasilan aplikasi ini akan memberikan solusi praktis dalam menjaga integritas dan keaslian berkas elektronik, serta meningkatkan keamanan informasi dalam lingkungan digital yang terus berkembang.

Berdasarkan penelitian Implementasi Digital Signature pada Bukti Transfer menggunakan Kriptografi Kunci Publik RSA, Fungsi Hash SHA-256, dan Steganografi (Riyadi, 2022). Penelitian ini membahas tentang cara melakukan verifikasi pembayaran dengan mengunggah citra digital bukti transfer yang telah ditandatangani secara digital menggunakan algoritma RSA dan fungsi hash SHA-256. Tanda tangan digital ini kemudian disisipkan ke dalam citra menggunakan metode steganografi LSB. Dengan

demikian, citra bukti transfer dapat menjamin autentikasi, integritas, dan non-repudiation dari transaksi pembayaran.

1.2. Rumusan masalah

Berdasarkan latar belakang yang telah diuraikan, maka permasalahan yang dirumuskan pada penelitian ini yaitu pesan digital memiliki sisi keamanan yang masih rendah dan mudah dipalsukan oleh orang lain. Oleh karena itu, dibutuhkan sebuah aplikasi Digital Signature pada android dengan menerapkan algoritma SHA-256 untuk menjamin keaslian pesan dan algoritma Rabin-p untuk menjaga keamanan data sehingga data yang dikirim terjamin keamanan dan keaslian datanya.

1.3. Batasan masalah

Dalam melakukan penelitian ini, peneliti membatasi ruang masalah yang akan diteliti. Batasan-batasan masalah yang digunakan adalah :

1. Jenis *file* yang digunakan adalah *file* yang berekstensi (.pdf) dan hanya mengenkripsi berupa string (tidak mengenkripsi gambar dan tabel).
2. Menggunakan Algoritma *SHA-256* dan *Rabin-p*.
3. Verifikasi dan autentikasi berupa *Digital Signature*.
4. Bahasa pemrograman yang digunakan adalah Java.
5. Penelitian ini menggunakan *platform mobile application* android.
6. *Integrated Development Environment* (IDE) yang digunakan pada penelitian ini adalah Android Studio.
7. Database yang digunakan pada penelitian ini adalah *SQLite*.

1.4. Tujuan penelitian

Tujuan dari penelitian ini adalah:

1. Untuk mengimplementasikan Algoritma SHA-256 dan Algoritma Rabin-p dengan teknik Signcryption.
2. Memberikan solusi kepada masyarakat khusus nya pengguna untuk mengatasi resiko keamanan data pada dokumen ber format pdf.

1.5. Manfaat penelitian

Penulis mengharapkan hasil penelitian ini dapat membantu dalam keamanan dan keaslian data *file* yang dapat digunakan oleh berbagai pihak yang membutuhkan. Selain itu, dapat menjadi referensi bacaan dan bahan penelitian selanjutnya yang mempunyai topik yang relevan.

1.6. Metodologi penelitian

1. Studi pustaka

Pada titik ini, penelitian dimulai dengan mencari referensi berupa artikel ilmiah, buku, makalah, jurnal, skripsi, serta materi tersusun lainnya yang terkait dengan penelitian ini.

2. Analisis dan perancangan sistem

Pada titik ini, penulis akan melakukan analisis pada berbagai hal yang diperlukan dan dapat dimanfaatkan untuk menyelesaikan penelitian, dan dirancang dalam berbagai konsep analisis, seperti algoritma program, flowchart sistem, use-case diagram, activity diagram, ishikawa diagram dan sequence diagram.

3. Implementasi sistem

Pembuatan aplikasi berdasarkan diagram alir yang telah ditentukan akan digunakan untuk mengimplementasikan sistem. Dengan program Android Studio yang ditulis dalam bahasa pemrograman Java dengan menggunakan database dari SQLite dalam penelitian ini.

4. Pengujian sistem

Di tahap ini, akan dilakukan pengujian (testing) sistem dengan menggunakan *file* dokumen pada sistem yang telah dirancang.

5. Dokumentasi sistem

Pada titik terakhir ini, penelitian akan diselesaikan dengan menyusun laporan hasil analisa dan perancangan sistem, serta hasil pengujian kedalam bentuk skripsi.

1.7. Sistematika penelitian

Berikut adalah sistematika penulisan dari skripsi ini:

BAB 1 PENDAHULUAN

Pada Bab 1, akan dibahas mengenai aspek pendahuluan dalam skripsi, termasuk konteks latar belakang, perumusan masalah, pembatasan masalah yang telah ditetapkan, tujuan penelitian, metode penelitian yang digunakan, dan struktur penulisan yang akan dipergunakan dalam studi ini.

BAB 2 LANDASAN TEORI

Pada Bab 2, terdapat penjelasan mengenai bidang keamanan data, algoritma SHA-256, algoritma Rabin-p, digital signature, dan bidang ilmu signcryption.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Pada bab 3, akan dibahas mengenai perancangan konsep dan kebutuhan sistem yang relevan dengan penelitian ini, dengan merujuk pada batasan masalah yang telah ditetapkan sebelumnya.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Pada bab 4, akan dibahas mengenai sistem yang dibuat, lalu dilakukan pengujian terhadap sistem dokumen pdf dan dilihat kinerjanya apakah sudah sesuai dengan tujuan penelitian.

BAB 5 KESIMPULAN DAN SARAN

Pada bab 5, akan dibahas mengenai hasil dari penelitian lalu diambil beberapa kesimpulan, memberikan beberapa saran dan masukan dari penulis untuk penelitian dimasa mendatang.

BAB 2

LANDASAN TEORI

2.1. Keamanan data

Keamanan data adalah proses pengelolaan informasi digital di dalam suatu sistem, bertujuan untuk melindungi data dari risiko kehilangan, peretasan, atau akses yang tidak sah, melibatkan aspek-aspek yang mencakup perangkat keras, perangkat lunak, media penyimpanan, perangkat pengguna, administrasi akses dan pengendalian, serta kebijakan dan prosedur organisasi.

Keamanan data menggunakan alat dan teknologi yang meningkatkan visibilitas data perusahaan dan cara penggunaannya. Alat-alat ini dapat melindungi data melalui proses seperti penyamaran data, enkripsi, dan informasi sensitif. Proses ini juga membantu organisasi memudahkan prosedur audit mereka dan mematuhi peraturan perlindungan data yang semakin ketat (Kumar, et al., 2018).

2.2. Kriptografi

Kriptografi memiliki akar kata dalam bahasa Yunani, yaitu Kripto berasal dari kata *kryptós*, yang artinya tersembunyi, sementara Grafi berasal dari kata *gráphein*, yang artinya menulis. Oleh karena itu, Kriptografi dapat diartikan sebagai ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. (Sentot, 2010). Contoh penerapan kriptografi dalam kehidupan sehari-hari adalah penggunaan kartu kredit online, kunci mobil pintar, penggunaan VPN (Virtual Private Network), transaksi di berbagai aplikasi / situs belanja online, dsb.

2.2.1. Terminologi kriptografi

1. Pengirim dan Penerima Pesan

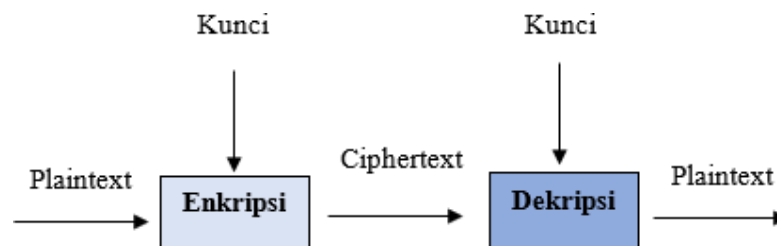
Pihak yang mengirim pesan pertama kali umumnya dikenal sebagai pengirim (sender), sedangkan pihak kedua yang menerima pesan disebut penerima (receiver). Kesuksesan dalam proses pengiriman dan penerimaan pesan dicapai ketika pesan tersebut berhasil sampai kepada penerima yang benar tanpa ada pihak ketiga yang dapat mengakses atau memahami isi pesan tersebut.

2. Pesan, plaintext dan ciphertext

Pesan merujuk pada informasi atau data yang hendak diungkapkan atau disampaikan dari satu entitas kepada yang lain. Plaintext adalah istilah yang digunakan untuk menggambarkan pesan asal atau informasi yang belum mengalami proses enkripsi. Ciphertext merujuk pada pesan yang telah diubah melalui proses enkripsi sehingga tidak dapat dipahami tanpa didekripsi terlebih dahulu.

3. Enkripsi dan Dekripsi

Enkripsi merupakan proses mengubah data atau pesan asal (plaintext) menjadi bentuk lain yang sulit dimengerti atau tidak dapat dibaca (ciphertext). Dekripsi merupakan proses mengembalikan ciphertext ke bentuk plaintext dengan menggunakan kunci dekripsi yang sesuai. Proses enkripsi dan dekripsi dieksekusi menggunakan sebuah algoritma. Skema dari proses Enkripsi serta Dekripsi dapat dilihat pada Gambar 2.1 sebagai berikut:



Gambar 2.1 Skema dari Proses Enkripsi dan Dekripsi

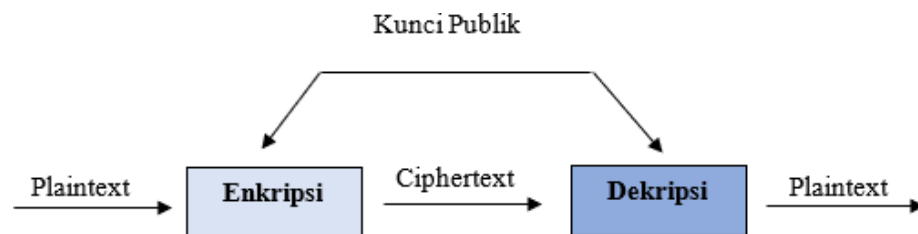
2.2.2. Jenis kriptografi

1. Kriptografi simetris

Kriptografi simetris adalah teknik kriptografi yang menggunakan kunci yang identik dalam mengenkripsi dan mendekripsi suatu data. Dalam kebanyakan kasus, kunci ini sering disebut sebagai kunci Publik yang dapat digunakan oleh pengirim dan penerima pesan.

Contoh algoritma yang menggunakan metode ini adalah DES (*Data Encryption Standard*), AES (*Advanced Encryption Standard*), 3DES (*Triple DES*), RC4 (*Rivest Cipher 4*), *Twofish*, *Chacha20*.

Skema dari Kriptografi Simetris dilihat pada Gambar 2.2 dibawah ini :



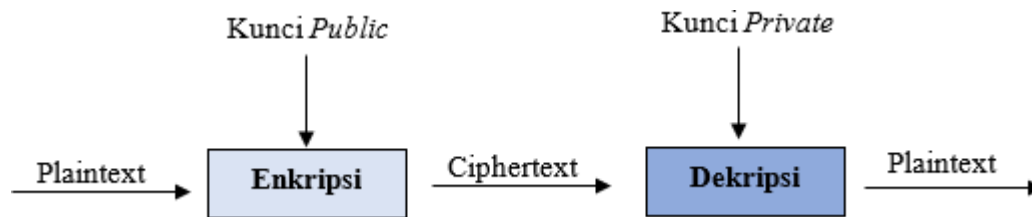
Gambar 2.2 Skema dari Kriptografi Simetris

2. Kriptografi asimetris

Kriptografi Asimetris merupakan teknik kriptografi yang memanfaatkan pasangan kunci yang berbeda untuk melaksanakan tahap enkripsi dan dekripsi. Pada tahap enkripsi kunci pertama yang dipakai adalah kunci Publik, di mana kunci ini dapat diakses oleh siapa pun yang ingin mengamankan pesan yang akan mereka kirim. Pada tahap dekripsi kunci kedua yang dipakai adalah kunci Privat, di mana kunci ini sangat rahasia dan hanya dapat diakses oleh penerima pesan yang telah menerima pesan yang telah dienkripsi sebelumnya dengan kunci Publik untuk mengembalikan *Chipertext* menjadi *Plaintext*.

Contoh algoritma yang menggunakan metode ini adalah Rabin, RSA (*Rivest-Shamir-Adleman*), El-Gamal, *Elliptic Curve Cryptography*, *Diffie-Hellman*, PQC (*Post-Quantum Cryptography*), *McEliece*, dan Rabin-p.

Skema dari Kriptografi Asimetris dapat dilihat pada Gambar 2.3 di bawah ini :



Gambar 2.3 Skema dari kriptografi Asimetris

2.2.3. Pembangkitan kunci

Algoritma Rabin-p terlebih dahulu membentuk kunci *public* dan kunci *private*, dengan menggunakan parameter pengamananan k . Langkah-langkah pembentukkan kunci *public* N dan kunci *private* p dalam skema algoritma Rabin-p adalah sebagai berikut :

1. Secara acak, tentukan nilai k sebagai parameter pengamananan.
2. Secara acak, tentukan nilai bilangan prima p dan q , di mana $p \neq q$, $2^k < p$, $q < 2^{k+1}$, yang memenuhi $p \equiv q \equiv 3 \pmod{4}$.
3. Tentukan nilai $N = p^2q$.
4. Simpan N sebagai kunci *public*, dan p sebagai kunci *private*.

Contoh:

Misalkan $k = 5$, $p = 107$, $q = 47$.

- *Memeriksa kelayakan bilangan prima p dan q .*

$$2^k < p$$

$$2^5 < 107$$

$$32 < 107 \quad (\checkmark)$$

$$107 \equiv 3 \pmod{4} \quad (\checkmark)$$

$$q < 2^{k+1}$$

$$47 < 2^{5+1}$$

$$47 < 64 \quad (\checkmark)$$

$$47 \equiv 3 \pmod{4} \quad (\checkmark)$$

- *Menentukan nilai N .*

$$N = p^2q$$

$$N = (107^2) \times 47$$

$$N = 538103 \quad (\checkmark)$$

- **Jadi didapatkan bahwa kunci public $N = 538103$, dan kunci private $p = 107$.**

2.2.4. Enkripsi

Setelah menentukan nilai kunci, maka pesan siap untuk melewati proses enkripsi, dengan menggunakan kunci *public* N dan *plaintext* m , yang akan menghasilkan *ciphertext* c . Dalam algoritma Rabin-p, proses enkripsi adalah sebagai berikut :

1. Tentukan nilai *plaintext* m yang akan dienkrripsikan. Nilai m harus memenuhi kondisi bahwa $0 < m < 2^{2k-1}$, dan memenuhi kaidah *Euclidean* dalam menentukan *Greatest Common Divisor* (GCD), yaitu di mana $\text{GCD}(m, N) = 1$.
2. Tentukan nilai $c = m^2 \pmod{N}$.
3. Simpan nilai c sebagai *ciphertext*.

Contoh :

Misalkan $k = 5$, $N = 538103$, $m = 74$

- *Memeriksa kelayakan plaintext m .*

$0 < m < 2^{2k-1}$	GCD (m, N)
$0 < 74 < 2^{(2(5))-1}$	GCD (76, 538103)
$0 < 74 < 2^9$	$74 \bmod 538103 = 74$
$0 < 74 < 512$ (✓)	$538103 \bmod 74 = 49$
	$74 \bmod 49 = 25$
	$49 \bmod 25 = 24$
	$25 \bmod 24 = 1$ (✓)

- *Menentukan nilai c .*

$$c = m^2 \pmod{N}$$

$$c = 74^2 \pmod{538103}$$

$$c = 5476 \pmod{538103}$$

$$\mathbf{c = 5476 (✓)}$$

2.2.5. Dekripsi

Dengan menggunakan kunci *private* p , algoritma Rabin-p akan mendekripsikan *ciphertext* c dan mengembalikannya ke bentuk *plaintext* m . Proses dekripsi pada algoritma Rabin-p adalah sebagai berikut :

1. Tentukan $w \equiv c \pmod{p}$.
2. Tentukan $m_p \equiv w^{(p+1)/4} \pmod{p}$.
3. Tentukan $i = (c - (m_p)^2) / p$.
4. Tentukan $j \equiv (i/2m_p) \pmod{p}$.
5. Tentukan $m_l = m_p + jp$.
6. Jika $m_l < 2^{2k+1}$, maka nilai $m = m_l$.
7. Jika tidak, maka nilai $m = p^2 - m_l$.

Contoh :

Misalkan $k = 5, p = 107, c = 5476$

- Menentukan nilai w .

$$w \equiv c \pmod{p}$$

$$w \equiv 5476 \pmod{107}$$

$$\mathbf{w \equiv 19 \pmod{107}}$$

- Menentukan nilai m_p .

$$m_p \equiv w^{(p+1)/4} \pmod{p}$$

$$m_p \equiv 19^{(107+1)/4} \pmod{107}$$

$$m_p \equiv 19^{108/4} \pmod{107}$$

$$m_p \equiv 19^{27} \pmod{107}$$

$$\mathbf{m_p \equiv 33}$$

- Menentukan nilai i .

$$i = (c - (m_p)^2) / p$$

$$i = (5476 - 33^2) / 107$$

$$i = 4387 / 107$$

$$\mathbf{i = 41}$$

- Menentukan nilai j .

$$j \equiv (i/2m_p) \pmod{p}$$

$$j \equiv (41/2(33)) \pmod{107}$$

$$j \equiv (41/66) \pmod{107}$$

$$\mathbf{j \equiv 106}$$

- Menentukan nilai m_1 .

$$m_1 = m_p + jp$$

$$m_1 = 33 + (106)(107)$$

$$m_1 = 33 + 11342$$

$$\mathbf{m_1 = 11375}$$

- Mengecek kondisi m_1 .

$$m_1 < 2^{2k+1}$$

$$11375 < 2^{2(5)+1}$$

$$11375 < 2^{10}$$

$$\mathbf{11375 < 1024}$$

Dari kondisi tersebut, maka didapatkanlah nilai $\mathbf{m \neq m_1}$

- Maka menggunakan kondisi berikut $m = p^2 - m_1$

$$m = 107^2 - 11375$$

$$m = 11449 - 11375$$

$$\mathbf{m = 74 (\checkmark)}$$

2.3. Rabin-p

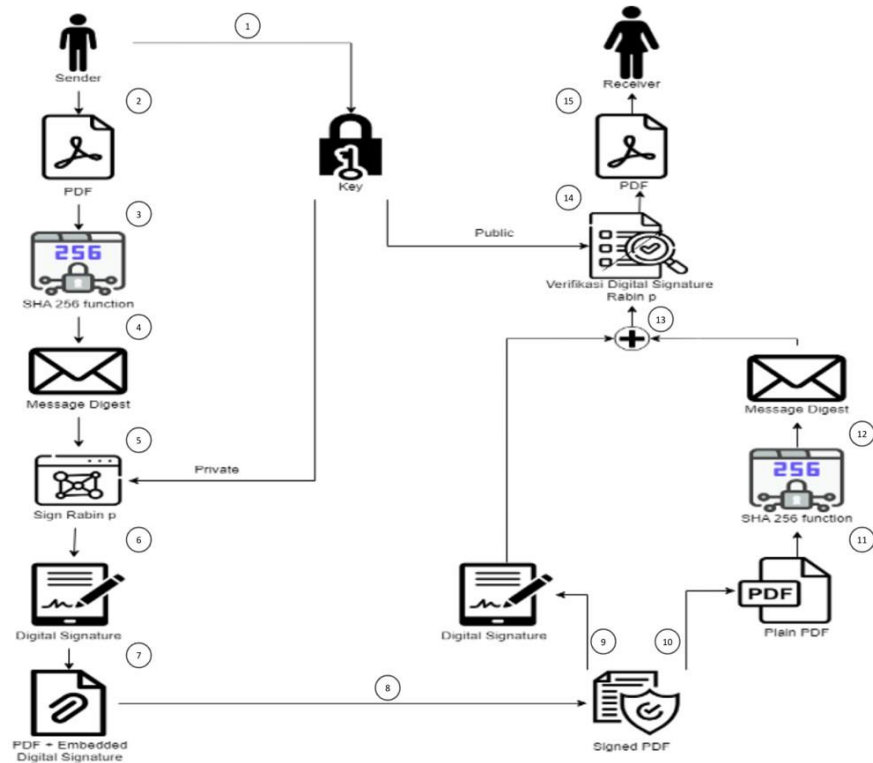
Algoritma Rabin-p merupakan sebuah algoritma kunci asimetris yang memiliki tingkat keamanan serupa dengan algoritma RSA, yakni dalam hal kesulitan untuk melakukan faktorisasi (Mubaroka, 2018). Ketika menggunakan algoritma Rabin-p untuk melakukan enkripsi, *ciphertext* yang dihasilkan memiliki panjang beberapa kali lebih besar dibandingkan dengan *plaintext*. Dibandingkan dengan variasi algoritma Rabin lainnya, Rabin-p dapat meningkatkan efisiensi dan performa dalam skema pengenkripsian data, karena hanya menggunakan satu bilangan prima sebagai kunci, dan juga selama proses dekripsi hanya melibatkan satu eksponen modular, yang secara positif akan mempengaruhi proses enkripsi dan dekripsi secara keseluruhan. (Asbullah, M. & Ariffin, M. 2016).

2.4. Digital signature

Digital signature adalah teknik matematika yang digunakan untuk memvalidasi keaslian dan integritas suatu pesan, *software*, atau dokumen digital. *Digital signature* dianggap setara dengan tanda tangan tertulis atau stempel, namun tingkat keamanannya lebih canggih. *Digital signature* dibuat dengan tujuan untuk menghindari adanya proses *tampering* dalam komunikasi digital. *Tampering* bisa berupa penipuan, penggelapan dokumen, kerusakan, penyuapan, dan lain sebagainya. *Digital signature* bisa memberi bukti identitas, asal, dan status dokumen elektronik, transaksi, maupun pesan.

Digital signature bekerja berdasarkan *public key* kriptografi yang dikenal juga dengan nama kriptografi asimetris. *Public key* adalah nilai numerik besar untuk enkripsi data. *Digital signature* menggunakan dua *public key* kriptografi yang saling memastikan tingkat autentikasi satu sama lain. Seseorang yang membuat *digital signature* akan menggunakan kunci pribadi untuk mengenkripsi data yang terkait dengan tanda tangan. Sementara satu-satunya cara untuk dekripsi data adalah menggunakan *public key*. Jika penerima tidak bisa membuka dokumen

dengan *public key* dari pemilik tanda tangan, maka ini menjadi pertanda bahwa terdapat masalah dengan dokumen atau tanda tangannya. Begitulah cara digital signature bisa diketahui keasliannya.



Gambar 2.4 Diagram Digital Signature

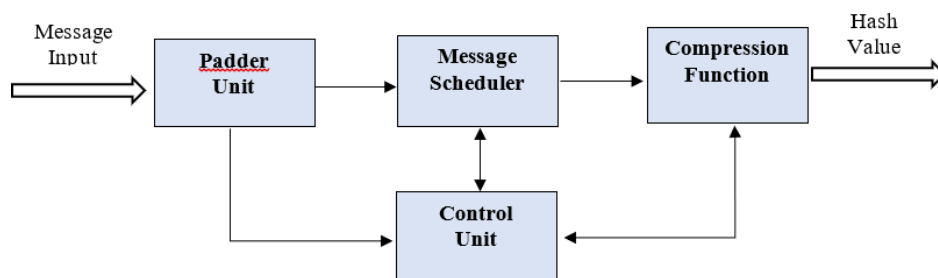
Berikut penjalan alur proses diagram digital signature gambar 2.4.

1. Sender men-generate kunci private dan kunci publik menggunakan algoritma rabin-p.
2. Sender memilih file pdf yang akan ditandatangani dengan digital signature.
3. Bytes file pdf di-hashing menggunakan algoritma sha-256, agar ukuran message menjadi lebih kecil.
4. Hasil dari hashing sha-256 berupa message digest dengan ukuran 256 bytes (32 kb)

5. Melakukan enkripsi pada message digest menggunakan algoritma rabin-p dengan private key yang sudah di-generate sebelumnya.
6. Hasil dari enkripsi rabin-p berupa digital signature berupa array bytes.
7. Melakukan embed digital signature (hasil enkripsi rabin-p) ke dalam file pdf original.
8. Hasil dari embed digital signature berupa file signed pdf dengan embedded digital signature.
9. Melakukan ekstraksi embedded digital signature (array bytes) dari file signed pdf.
10. Menghapus embedded digital signature dari file signed pdf menjadi file plain pdf
11. Bytes file plain pdf di-hashing menggunakan algoritma sha-256.
12. Hasil dari hashing sha-256 berupa message digest dengan ukuran 256 bytes (32 kb)
13. Menggabungkan message digest dengan digital signature yang akan digunakan dalam proses verifikasi digital signature.
14. Melakukan verifikasi digital signature menggunakan algoritma rabin-p dengan public key yang sudah di-generate sebelumnya.
15. Receiver menerima file pdf dengan status verifikasi tanda tangan yang sah.

2.5. SHA-256

Secure Hash Algorithm (SHA) adalah sebuah kriptografi fungsi hash yang dirancang oleh *National Security Agency* (NSA) dan dipublikasikan oleh *National Institute of Standard and Technology* (NIST) sebagai sebuah *Federal Information Processing Standard* (FIPS) oleh Amerika Serikat. Ada empat algoritma untuk keamanan fungsi hash yaitu SHA-0, SHA-1, SHA-2, dan SHA-3. NIST memperbaharui SHA-2, dengan panjang *output* (256 atau 512-bit di atas 160-bit pada SHA-1) dan perbedaan-perbedaan pada SHA ini merupakan besar pesan yang ada pada proses komputasi. SHA (Algoritma keamanan fungsi hash) merupakan algoritma enkripsi fungsi hash yang dapat digunakan untuk menghasilkan penggambaran konsolidasi dari sebuah data teks yang disebut sebuah proses pesan. SHA-256 dan SHA-512 adalah fungsi hash dengan kapasitas terbaru dengan panjang 32-bit dan 64-bit kata secara terpisah. Kedua fungsi hash ini dalam proses matematisnya menggunakan penjumlahan karakter yang berbeda dan ditambah dengan konstanta substansi. Meski demikian, struktur keduanya pada dasarnya tidak jauh berbeda, perbedaannya hanya terletak pada jumlah putaran saja. Arsitektur sederhana dari algoritma SHA-256 ditunjukkan oleh gambar berikut:



Gambar 2. 5 Arsitektur Sederhana SHA-256

2.6. File teks

File teks adalah sebuah *file* komputer yang berisikan data maupun informasi dalam bentuk karakter teks atau *letters*. Di dalamnya, *file* teks berisikan karakter berupa huruf, angka, simbol, tanda baca, dan lain-lain. Masukan dan keluaran dari *file* teks ditampilkan dalam kode tertentu yang dikenali oleh sistem komputer, yang dikenal sebagai *character set*. Contoh *character set* yang sudah dikenal luas secara internasional adalah *American Standard Code for Information Exchange* atau **ASCII**.

Beberapa contoh ekstensi *file* teks yang sering dipergunakan oleh masyarakat luas :

2.2.1. .txt

.txt merupakan ekstensi *file* teks yang sederhana, di mana *file* ini mengandung editor untuk teks yang menggunakan skema character set ASCII. *File* ini biasanya mengandung karakter-karakter umum (angka, simbol, spasi, dsb).

2.2.2. .doc dan docx

Ekstensi-ekstensi *file* teks ini lumrah dikenal oleh masyarakat luas ketika menggunakan perangkat lunak pengolah kata yang populer. .doc merupakan versi lama sedangkan .docx merupakan versi yang lebih baru. Perbedaan umumnya adalah bahwa .docx lebih mudah diubahkan ke ekstensi *file* lain.

2.2.3. .pdf

.pdf merupakan ekstensi *file* yang dipergunakan pada berbagai transaksi dokumen digital. *File* ini dapat memuat berbagai keperluan dokumen pada umumnya, seperti teks, juga gambar dan grafik.

BAB 3

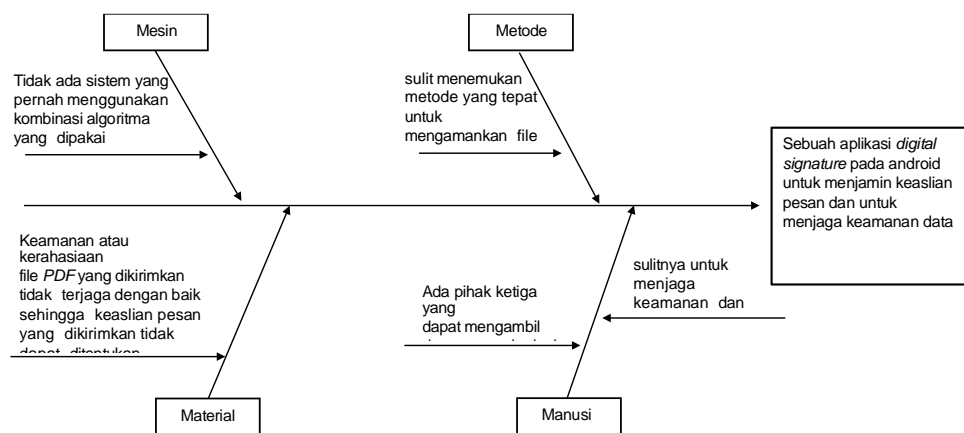
ANALISIS DAN DESAIN RANCANGAN SISTEM

3.1. Analisis sistem

Sebelum membangun suatu sistem atau program, perlu dilakukan berbagai penyusunan dari analisis terhadap program yang akan dibuat. Hal ini dilakukan untuk dapat mempelajari permasalahan atau kasus (case) yang akan diselesaikan oleh sistem tersebut dengan atribut-atribut berbeda dari program yang dibuat secara terintegrasi satu sama lain untuk mencapai tujuan dari program yang dibangun. Analisis yang akan dilakukan melalui langkah-langkah berikut :

3.1.1. Analisis masalah

Analisis masalah merupakan suatu proses identifikasi yang bertujuan untuk menggambarkan permasalahan yang timbul untuk selanjutnya dapat diselesaikan oleh sistem yang akan dibuat nantinya. Pada penelitian ini akan dibahas bagaimana cara menjaga kerahasiaan pesan atau *file* pdf yang akan dikirim oleh pengirim dalam keadaan asli atau tidak diubah ketika sampai diterima oleh penerima. Diagram tersebut dapat menampilkan serta mengidentifikasikan permasalahan-permasalahan yang ada serta menjelaskan sebab, akibat, maupun dampak dari permasalahan-permasalahan tersebut. Diagram ishikawa ditampilkan pada gambar 3.1.



Gambar 3.1 Diagram Ishikawa untuk Analisis Masalah

3.1.2. Analisis kebutuhan

Analisis kebutuhan merupakan proses penentuan daftar kebutuhan yang ada pada sistem yang dibuat. Ada dua jenis kebutuhan dalam sistem, yaitu kebutuhan fungsional dan kebutuhan *non* fungsional.

a. Kebutuhan fungsional

Pada analisis ini mencakup seluruh proses yang harus terjadi pada sistem, seperti:

1. Sistem dapat menerima inputan berupa pesan teks ter enkripsi oleh pengirim.
2. Sistem memproses inputan pesan teks menjadi pesan yang terdekripsi menggunakan algoritma rabin-p dan SHA-256.
3. *Output* yang dikeluarkan sistem sesuai dengan perhitungan algoritma rabin-p dan SHA-256

b. Kebutuhan non-fungsional

Kebutuhan non-fungsional yaitu membatasi layanan yang diberikan ke sistem. Kebutuhan non-fungsional yang diperlukan untuk proses penelitian ini:

- a. Sistem memiliki halaman yang sederhana dan efisien agar mudah dipahami dan digunakan.
- b. Sistem dirancang untuk digunakan di perangkat android dengan spesifikasi ringan (*android kitkat* 4.4.2) agar bisa menjangkau pengguna dengan mudah.
- c. Sistem dirancang dengan *user interfacce* dan *user experience* yang baik.

3.1.3. Analisis proses

Sistem yang akan dibangun di sini adalah sistem *Digital signature* pada *file* ber format PDF, di mana pengguna akan melakukan inputan pesan teks ter enkripsi dan sistem akan menyisipkan pesan *digital signature* ter enkripsi pada gambar pembungkus. Di dalam sistem akan digunakan algoritma Rabin-p dan SHA-256 dalam proses enkripsi dan dekripsi.

Proses yang akan dikerjakan sistem berupa:

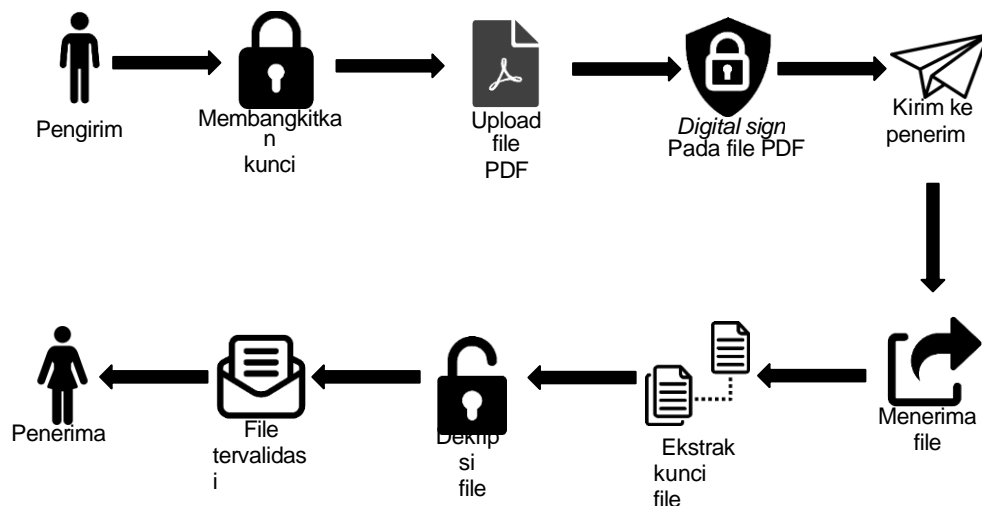
1. Menerima *file* format pdf yang di hashing dengan Sha-256 dan menampilkan kunci.
2. Melakukan enkripsi pada *file* yang sudah di hash dengan rabin-p dan menampilkan enkripsi.
3. Menampilkan cipherteks *file* yang di *sign* dengan algoritma rabin-p.
4. Membuat *User Interface* kemudian dirancang agar mempermudah pengguna dalam menggunakan program yang telah dirancang.

3.2. Pemodelan sistem

Dalam penelitian, memodelkan sistem berguna untuk memberikan informasi tentang koneksi, serta interaksi yang terjadi antara suatu bagian dengan bagian lainnya pada sistem yang dibangun tersebut.

3.2.1. Diagram umum sistem

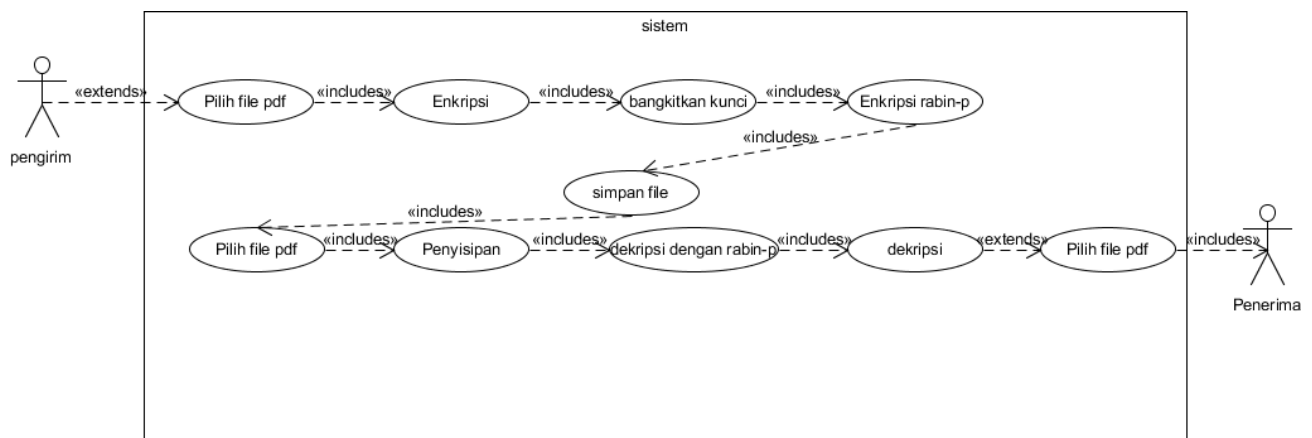
General Architecture System menjelaskan tahapan dari aplikasi yang dalam mengembangkan sistem, Pertama, user mengunggah file pdf ke aplikasi. Kemudian, aplikasi mengenkripsi file pdf dengan algoritma kriptografi. Selanjutnya, aplikasi menambahkan tanda tangan digital dengan fungsi *hash*. Setelah itu, aplikasi mengirim file pdf ke penerima. Lalu, penerima mendownload file pdf. Selanjutnya, penerima mendekripsi file pdf dengan kunci kriptografi. Kemudian, penerima memvalidasi file pdf dengan fungsi *hash*. Terakhir, penerima membuka file pdf yang valid. Proses ini bertujuan untuk menjamin autentikasi. Adapun *General Architecture System* dari penelitian ini ditunjukkan pada gambar 3.2 berikut:



Gambar 3.2 Diagram umum sistem

3.2.2. Use case diagram

Diagram Use-Case ialah sebuah diagram yang disusun untuk menampilkan tugas maupun pekerjaan komponen-komponen dalam satu sistem saat user menggunakan sistem tersebut. Diagram Use-Case memiliki dua bagian, yaitu actor sebagai user ataupun bagian dari sistem yang melakukan suatu proses atau aksi terhadap sebuah sistem, dan use-case sebagai bentuk respon sistem tersebut atas aksi actor tersebut. Gambar 3.3 menunjukkan Diagram Use-Case dari sistem.



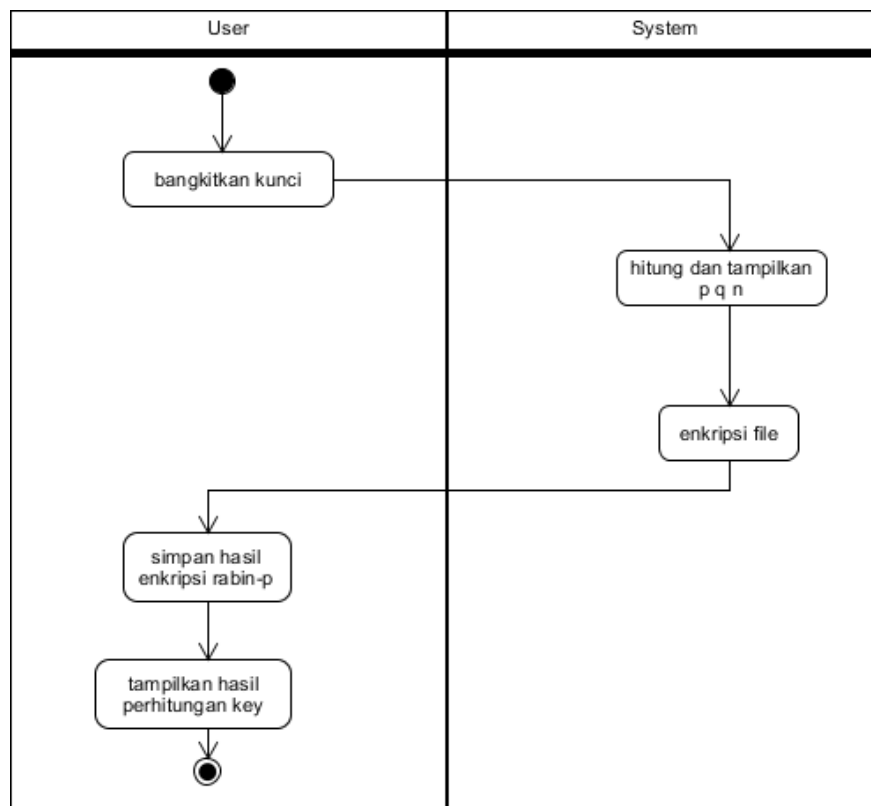
Gambar 3.3 Use case diagram pada sistem

3.2.3. Activity diagram

Diagram of Activity ialah diagram yang disusun untuk menjelaskan aliran dan kinerja dari suatu sistem. *Diagram of Activity* yang akan dipergunakan pada penelitian meliputi diagram untuk menjelaskan proses enkripsi, penyisipan, ekstraksi serta dekripsi yang akan menampilkan hasil.

3.2.3 1. Diagram Activity Enkripsi Rabin-p

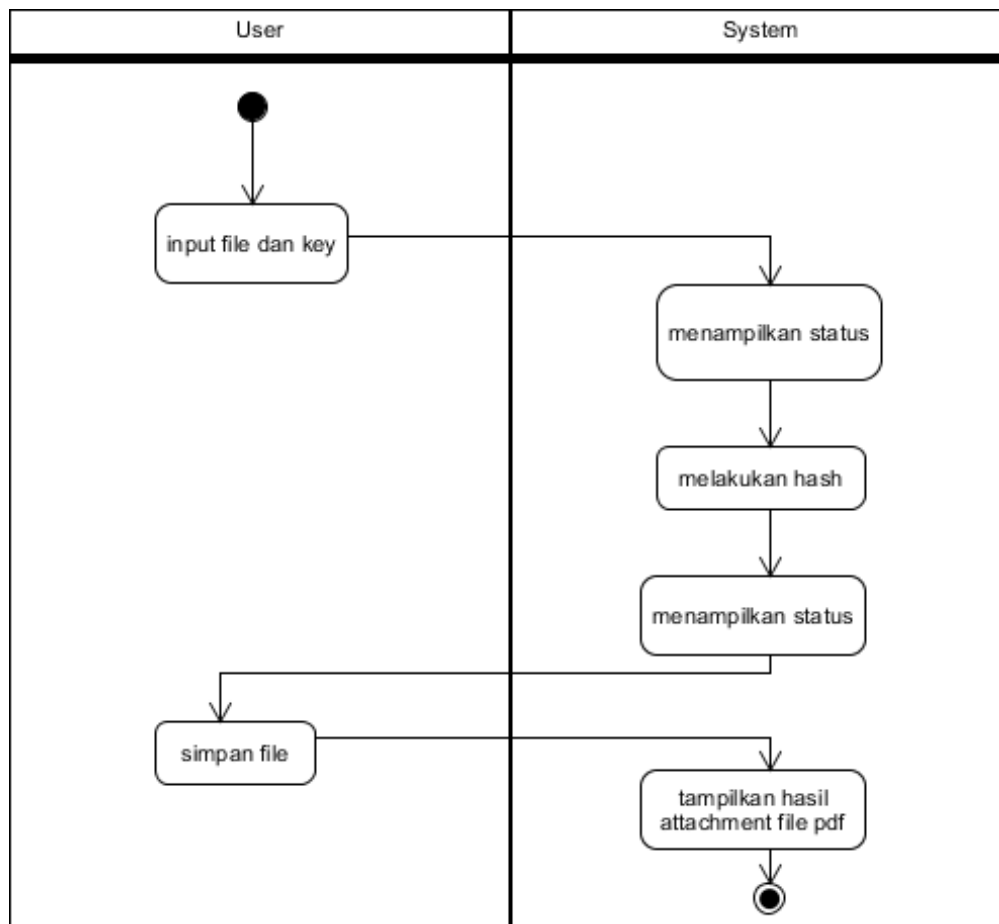
Diagram *activity* enkripsi rabin-P dimulai dari User memulai proses dengan membangkitkan kunci publik dan privat. Sistem menghitung dan menampilkan kunci p , q , dan n yang digunakan untuk enkripsi dan dekripsi file. Sistem juga melakukan enkripsi file dengan algoritma Rabin-p. User menyimpan hasil enkripsi dan melihat hasil perhitungan yang dilakukan oleh sistem.



Gambar 3.4 Diagram enkripsi rabin-p

3.2.3 2. Diagram Activity Penyisipan

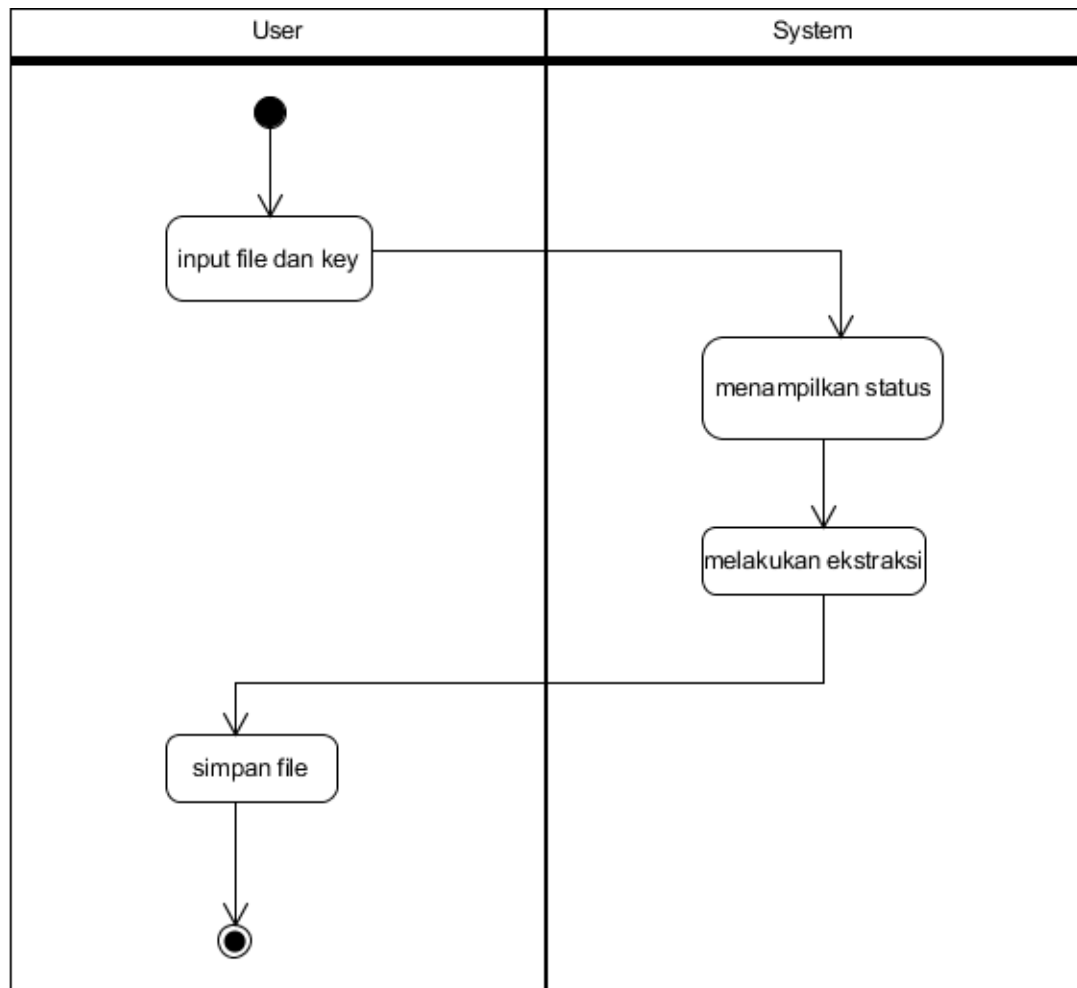
User memulai proses dengan menginput file pdf dan kunci yang digunakan untuk tanda tangan digital. Sistem menampilkan status proses input. Sistem melakukan hash pada file pdf untuk menghasilkan nilai unik yang merepresentasikan file tersebut. Sistem menampilkan status proses hash. User menyimpan file pdf yang telah dihash. Sistem menampilkan hasil attachment file pdf yang berisi tanda tangan digital.



Gambar 3.5 Diagram Penyisipan

3.2.3 3. Diagram Activity Ekstraksi

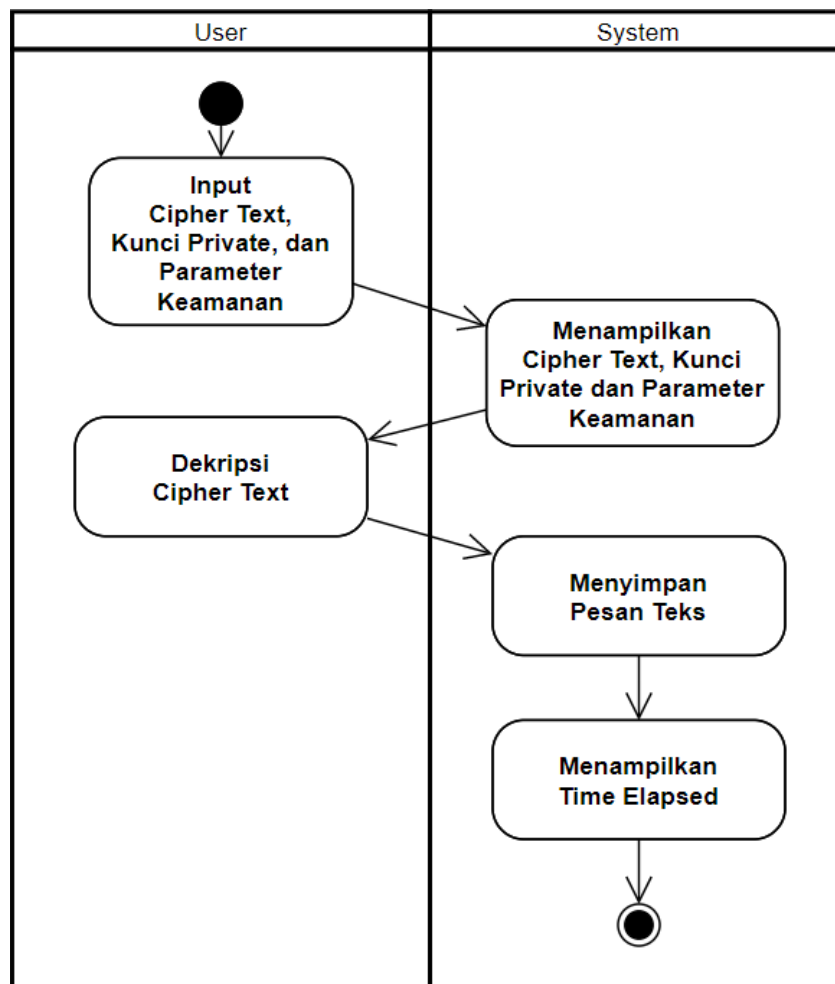
User memulai proses dengan menginput file pdf dan kunci yang digunakan untuk tanda tangan digital. Sistem menampilkan status proses input. Sistem melakukan ekstraksi pada file pdf untuk mendapatkan nilai tanda tangan digital yang terdapat di dalam file tersebut. User menyimpan file pdf yang telah diekstraksi.



Gambar 3.6 Diagram Ekstraksi

3.2.3 4. Diagram Activity Dekripsi Rabin-p

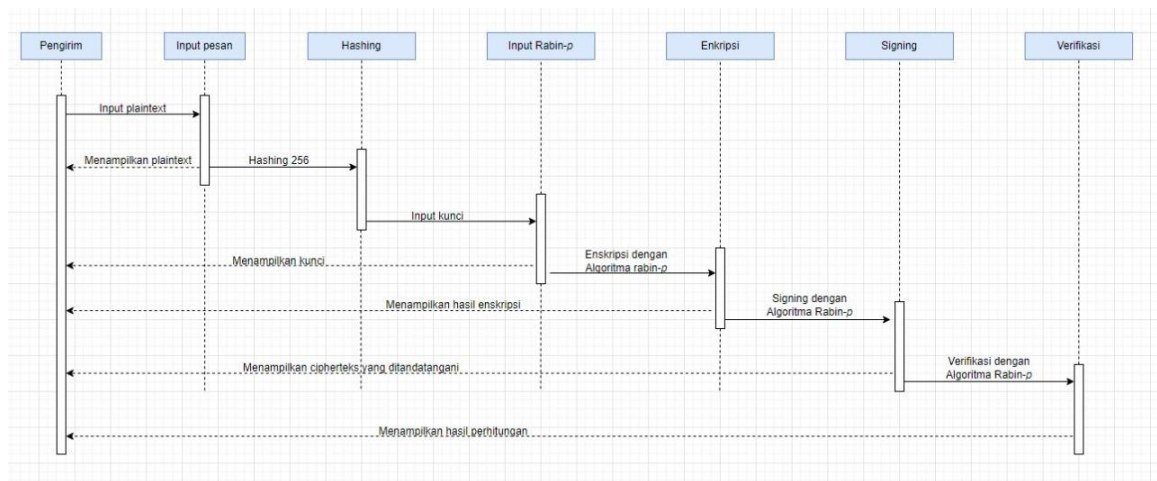
User memulai proses dengan menginput *cipher text*, kunci *privat*, dan parameter keamanan yang dibutuhkan untuk dekripsi. Sistem menampilkan *cipher text*, kunci *privat*, dan parameter keamanan yang diinput oleh *user*. User melakukan dekripsi *cipher text* dengan menggunakan algoritma Rabin-p dan kunci privat yang sesuai. Sistem menyimpan pesan teks yang telah didekripsi dan menampilkan waktu yang dibutuhkan untuk proses dekripsi.



Gambar 3.7 Diagram Dekripsi Rabin-p

3.2.4. Sequence diagram

Diagram of Sequence adalah sebuah diagram yang disusun untuk menunjukkan interaksi-interaksi yang terjadi pada sistem dalam bentuk send and receive responses antar komponen pada sistem sesuai dengan urutan waktu yang semestinya. Diagram Sequence di bawah ini akan menjelaskan interaksi yang terjadi pada sistem dari penelitian ini.



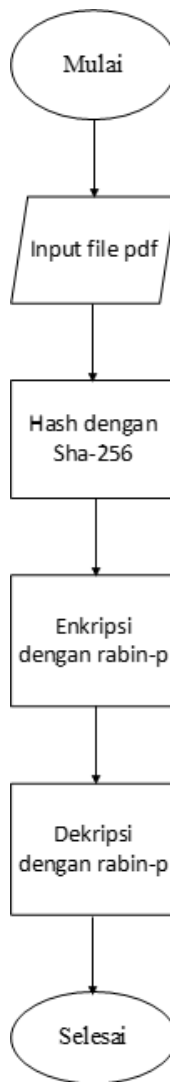
Gambar 3.8 *Diagram Sequence* pada Sistem

3.3. Flowchart

Flowchart merupakan sebuah skema yang menunjukkan langkah demi langkah dari pengerjaan sistem secara berurut dalam sebuah sistem yang ada secara logis. Dalam penelitian ini flowchart system akan menggambarkan cara kerja sistem yang akan dibuat.

3.3.1. Flowchart sistem

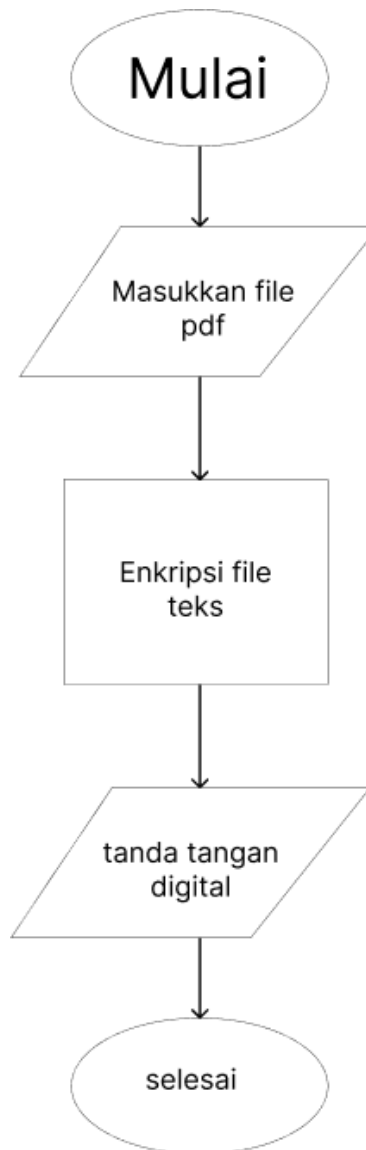
Flowchart sistem yang dibuat dibagi atas 2 tahapan, yaitu flowchart enkripsi dan penyisipan, serta flowchart ekstraksi dan dekripsi.



Gambar 3.9 Desain Skema *Flowchart* dari Enkripsi dan Dekripsi

3.3.2. *Flowchart* enkripsi rabin-p

Tahapan proses dari enkripsi dengan Algoritma Rabin-p pada sistem diawali dengan menerima input sebelum nya, lalu dienkripsi menggunakan kunci Public N dan kunci Private p yang telah sebelumnya dibangkitkan secara acak.



Gambar 3.10 Desain Skema *Flowchart* dari Enkripsi Rabin-P

3.3.3. *Flowchart* ekstraksi

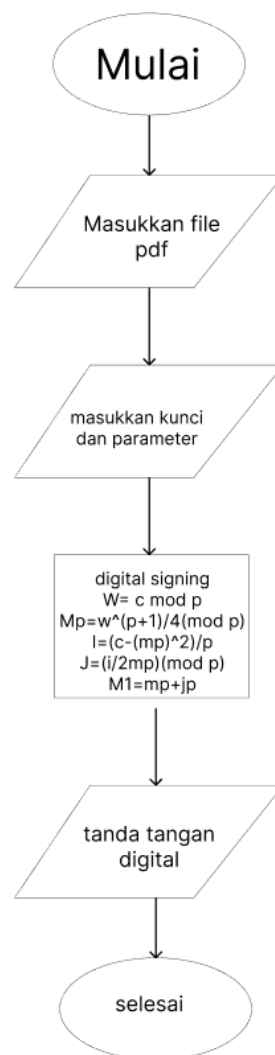
Proses ekstraksi dengan algoritma pada sistem diawali dengan menerima input *file* lalu mengambil byte akhir dan sistem akan menghasilkan *digital signing* yang sebelumnya telah disisipkan.



Gambar 3.11 Desain Skema *Flowchart* dari Ekstraksi

3.3.4. Flowchart dekripsi rabin-p

Proses dekripsi dengan Algoritma Rabin-p pada sistem diawali dengan menerima *file* pdf, kunci private p, dan parameter keamanan k, lalu *file* akan didekripsikan menggunakan kunci dan parameter tersebut dan akan menghasilkan sebuah *output* sama seperti semula. dengan menggunakan kunci Public N dan kunci Private p yang telah dibangkitkan sebelumnya.



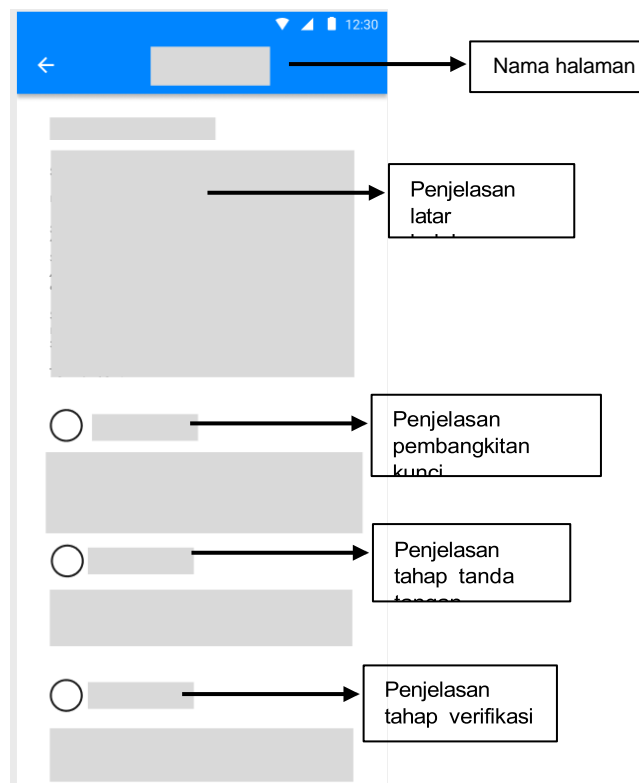
Gambar 3.12 Desain Skema Flowchart dari Dekripsi Rabin-p

3.4. Perancangan antarmuka

Antarmuka pengguna (dikenal dengan istilah user interface) ialah bentuk desain dan tampilan sebuah sistem secara fungsional maupun atribut pendukung sistem tersebut untuk memudahkan interaksi antara sistem tersebut dengan pengguna. User interface berguna agar pengguna dapat dengan mudah menjalankan sistem. Dan diperlukan adanya perancangan user interface, yang terdiri dari beberapa bagian berikut:

3.4.1. Desain Rancangan dari Halaman About

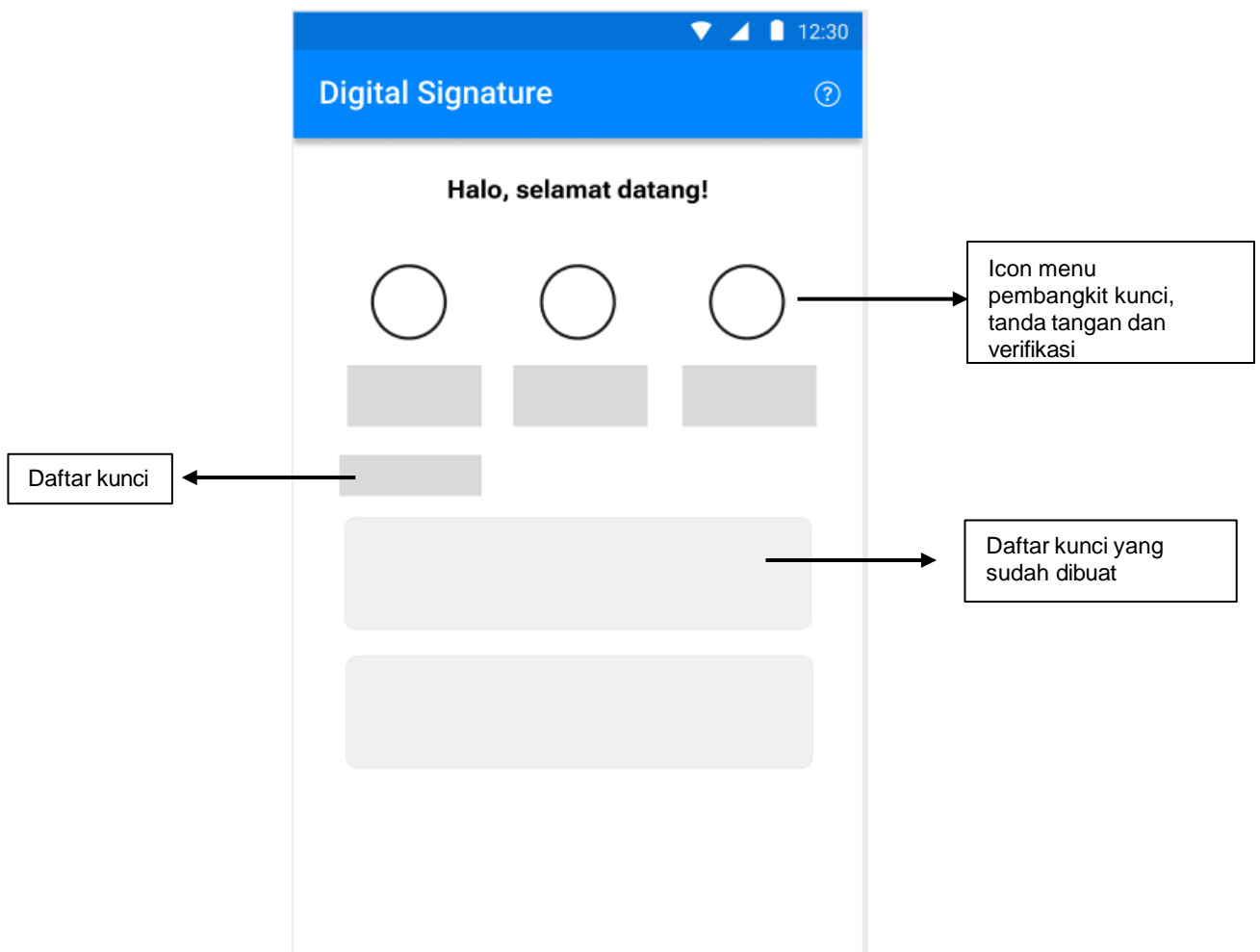
Halaman About adalah halaman awal yang tampil ketika sistem dimulai (sebagai MainForm dari sistem), yang mengandung informasi singkat tentang sistem dan pembuat sistem. Gambar 3.17. menampilkan desain rancangan dari Halaman About.



Gambar 3.13 Desain Rancangan dari Halaman *About*

3.4.2. Desain Rancangan dari Halaman utama

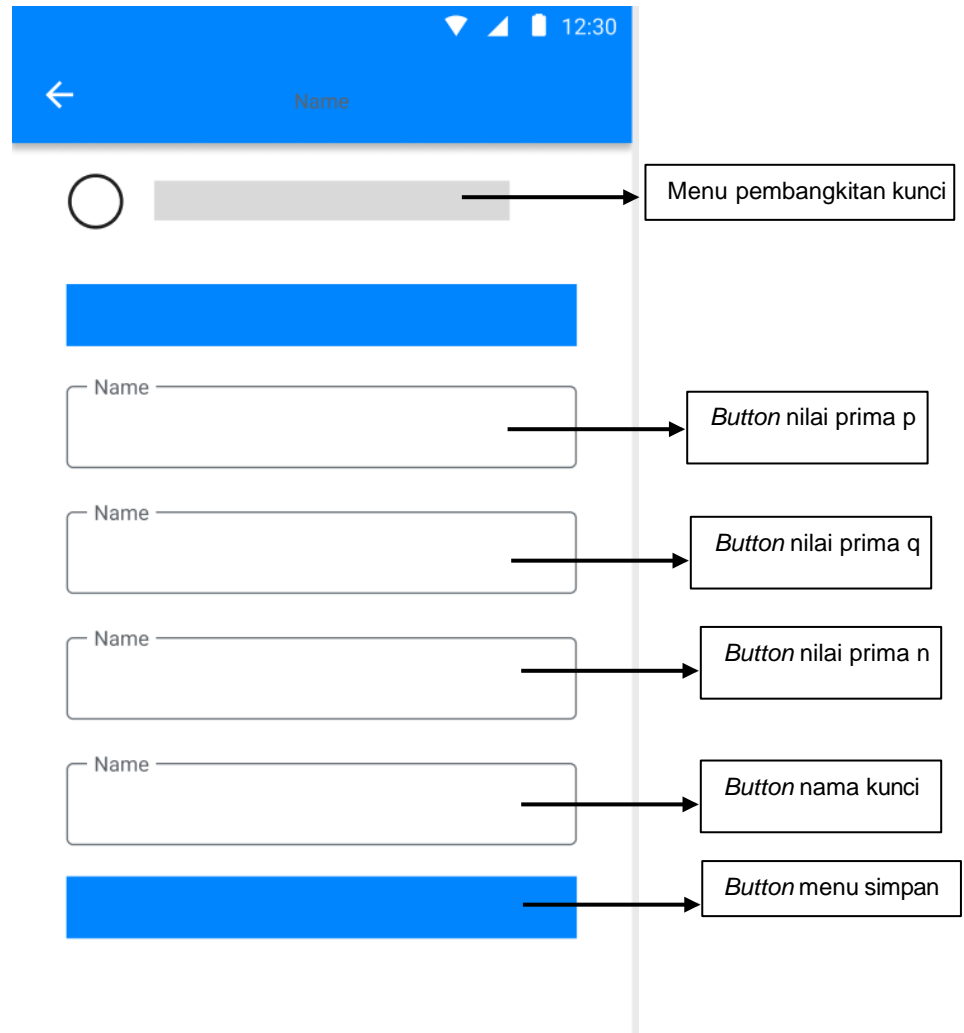
Halaman ini akan tampil setelah aplikasi dibuka, yang memiliki kegunaan untuk melakukan pembangkitan kunci tanda tangan dan proses verifikasi. Gambar 3.14 akan menampilkan desain rancangan dari Halaman utama.



Gambar 3.14 Desain Rancangan dari Halaman utama

3.4.3. Desain Rancangan dari Halaman Pembangkit kunci

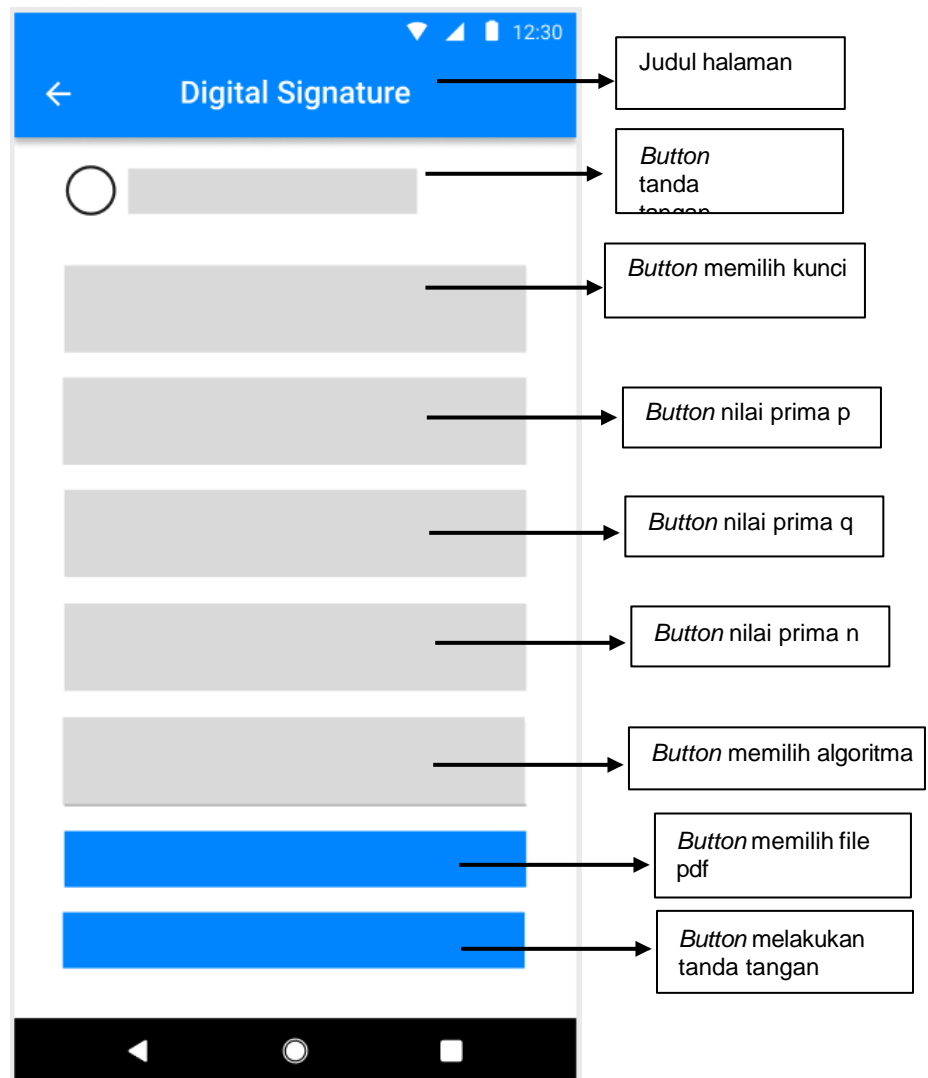
Halaman ini terdapat di dalam pada halaman utama, yang memiliki kegunaan untuk melakukan pembangkitan *key*. Gambar 3.15 akan menampilkan desain rancangan dari Halaman Pemangkitan kunci.



Gambar 3.15 Desain Rancangan dari Halaman Pembangkit kunci

3.4.4. Desain Rancangan dari Halaman Tanda tangan

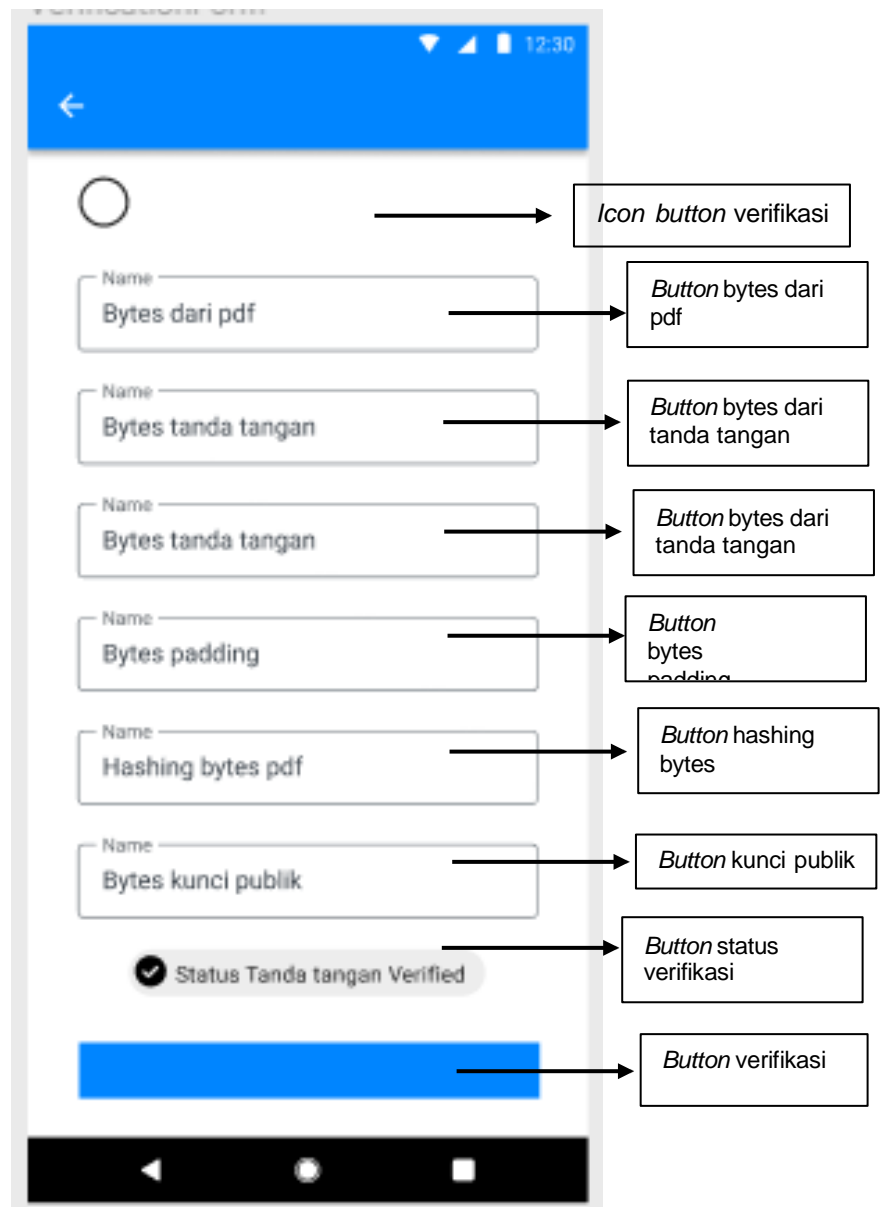
Halaman ini terdapat di dalam menu halaman utama, yang memiliki kegunaan untuk melakukan penanda tangan digital yang telah dienkripsi ke sebuah media pdf. Gambar 3.16 menunjukkan Desain Rancangan dari Halaman Tanda tangan.



Gambar 3.16 Desain Rancangan dari Halaman tanda tangan

3.4.5. Desain Rancangan dari Halaman Verifikasi

Halaman ini terdapat di dalam menu halaman utama, yang memiliki kegunaan untuk melakukan verifikasi kepadapenerima yang menerima *file* pdf. Gambar 3.17 menunjukkan Desain Rancangan dari Halaman Verifikasi.



Gambar 3.17 Desain Rancangan dari Halaman Verifikasi

BAB 4

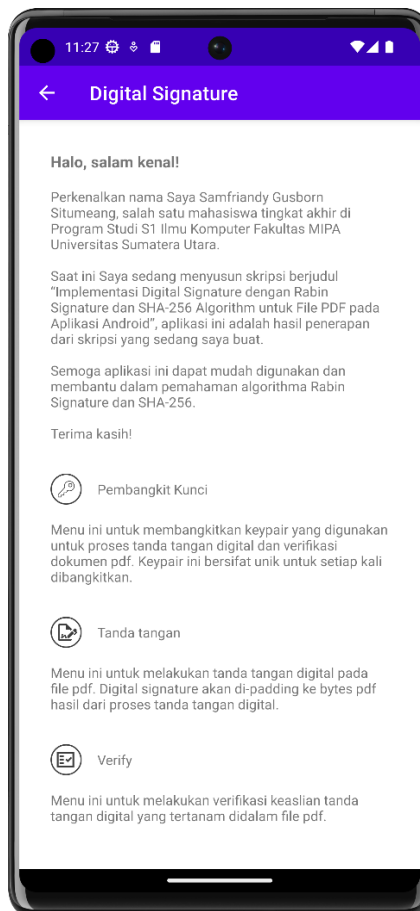
IMPLEMENTASI DAN PENGUJIAN SISTEM

Implementasi sistem

Pada bab ini merupakan proses penerapan dari rancangan yang sudah dibuat pada bab 3. Tujuan dari implementasi merupakan untuk melihat apakah sistem telah berjalan dan sesuai dengan harapan.

4.1. Halaman *about*

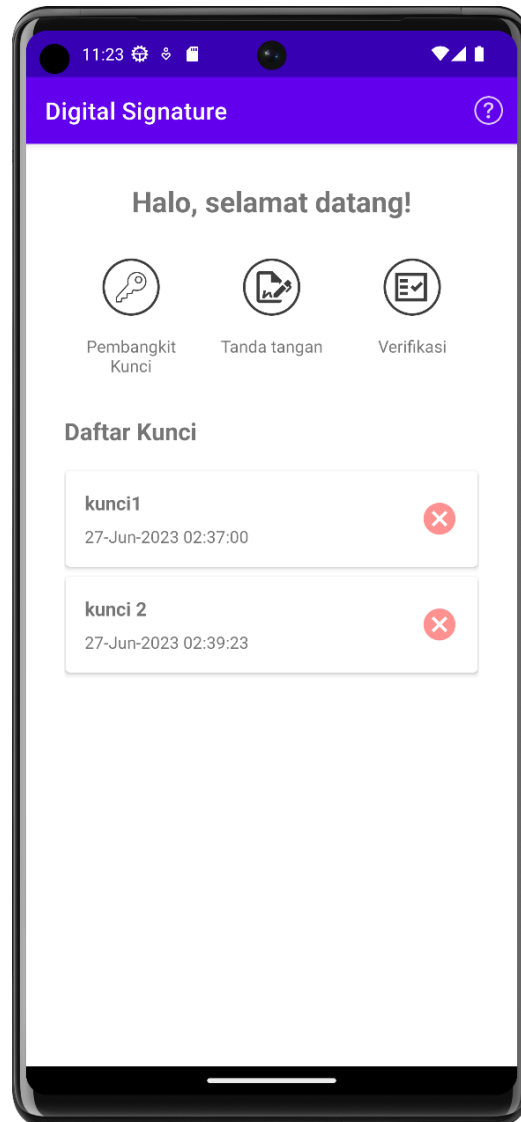
Halaman yang menjelaskan tentang penulis, tujuan dan manfaat penelitian dan tahapan pada penggunaan aplikasi



Gambar 4.1 Halaman *about*

4.2. Halaman utama

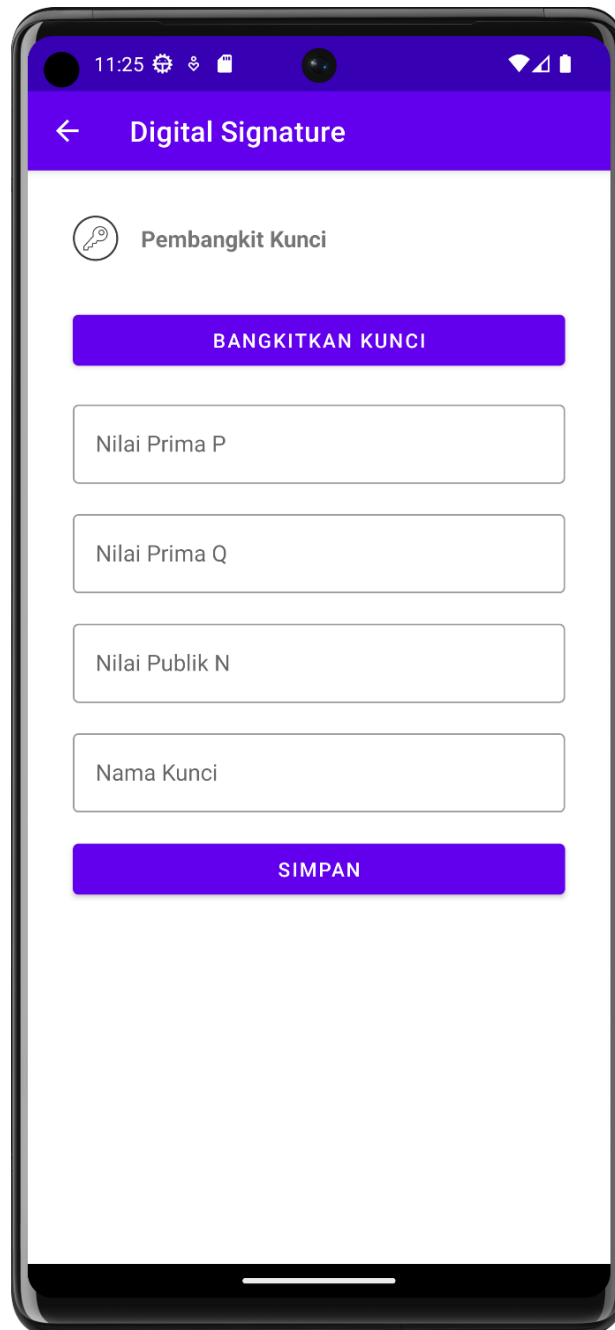
Halaman ini merupakan halaman awal saat pengguna berhasil melakukan login akun, pada halaman ini terdapat sebuah gambar animasi dan 3 button yaitu pembangkitan kunci, tanda tangan dan verifikasi.



Gambar 4.2 Halaman utama

4.3. Halaman Pembangkit kunci

Halaman yang menampilkan menu untuk membangkitkan *key* yang terdiri dari nilai *prime* P, *prime* Q dan *public* N dan sebuah *action button* kepada pengguna untuk membangkitkan kunci.

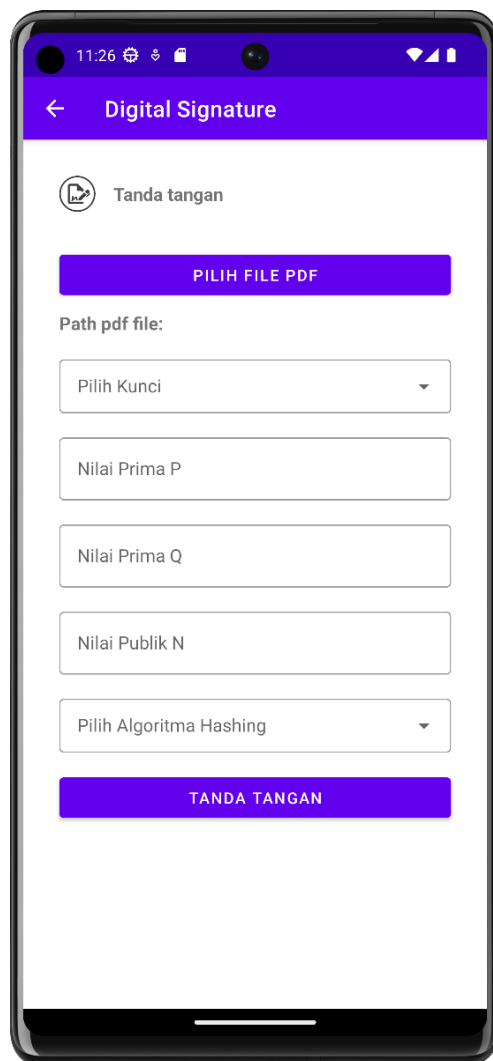


The screenshot shows a mobile application interface for digital signatures. The top status bar displays the time 11:25 and various system icons. The app's header is purple with a white back arrow and the text 'Digital Signature'. The main content area is white and features a section titled 'Pembangkit Kunci' (Key Generator) with a key icon. Below this title are four input fields for generating a key: 'Nilai Prima P', 'Nilai Prima Q', 'Nilai Publik N', and 'Nama Kunci'. There are two prominent purple buttons: 'BANGKITKAN KUNCI' (Generate Key) located above the input fields and 'SIMPAN' (Save) located below them.

Gambar 4.3 Halaman pembangkit kunci

4.4. Halaman Tanda tangan

Halaman *activity* utama dimana pengguna akan memasukkan *file* pdf dan *key* yang akan di *hashing* menggunakan Sha-256.

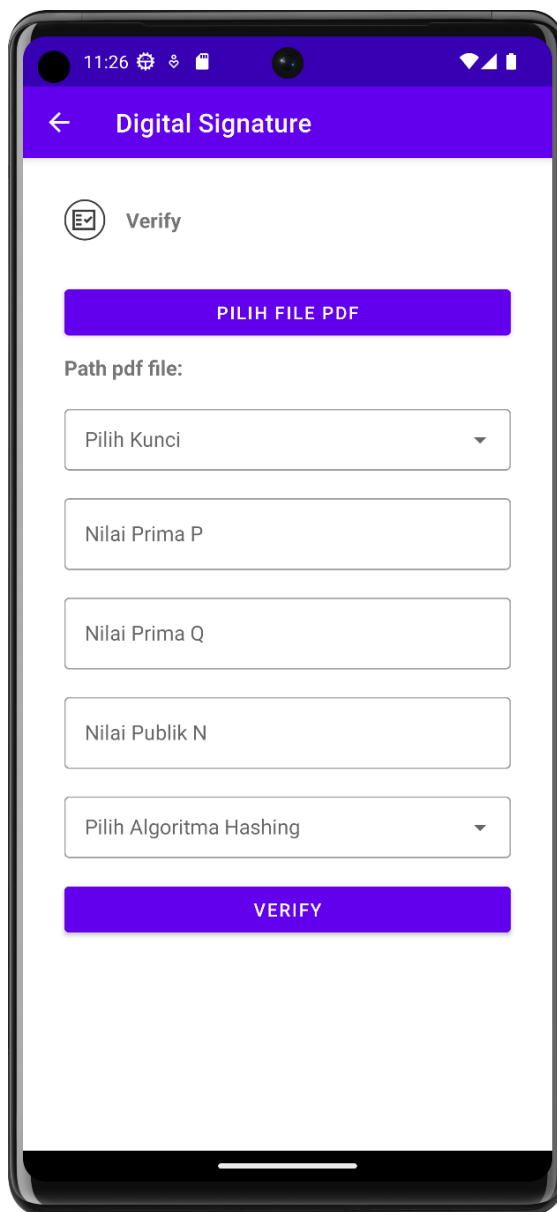


The screenshot shows a mobile application interface titled "Digital Signature". At the top, there is a status bar with the time 11:26 and various icons. Below the title bar, there is a back arrow and the text "Digital Signature". The main content area is titled "Tanda tangan" with a document icon. It features a purple button labeled "PILIH FILE PDF". Below this, the text "Path pdf file:" is followed by a series of input fields: a dropdown menu labeled "Pilih Kunci", and four text input fields labeled "Nilai Prima P", "Nilai Prima Q", "Nilai Publik N", and "Pilih Algoritma Hashing" (which is a dropdown menu). At the bottom, there is a purple button labeled "TANDA TANGAN".

Gambar 4.4 Halaman tanda tangan

4.5. Halaman Verifikasi

Halaman yang ditujukan kepada penerima *file* dimana penerima akan melakukan verifikasi terhadap *file* yang di hash berdasarkan *key* yang sudah diabngkitkan.



The screenshot shows a mobile application interface for digital signature verification. At the top, there is a status bar with the time 11:26 and various icons. Below the status bar is a purple header with a back arrow and the text "Digital Signature". The main content area has a white background. It starts with a "Verify" button featuring a checkmark icon. Below this is a purple button labeled "PILIH FILE PDF". Underneath is the text "Path pdf file:". This is followed by a series of input fields: a dropdown menu labeled "Pilih Kunci", three text input fields labeled "Nilai Prima P", "Nilai Prima Q", and "Nilai Publik N", and another dropdown menu labeled "Pilih Algoritma Hashing". At the bottom of the form is a purple button labeled "VERIFY".

Gambar 4.5 Halaman verifikasi

4.6. Pengujian

Pengujian aplikasi ini merupakan tahap berikutnya setelah implementasi. Pengujian ini dilakukan untuk memastikan dan membuktikan bahwa sistem yang dibangun dapat berfungsi dengan baik, serta hasil yang diperoleh setelah proses enkripsi dapat dikembalikan ke bentuk aslinya saat diverifikasi. Pengujian ini dilakukan sebanyak 20 kali dengan *key* yang dibangkitkan sebanyak 20 kali.

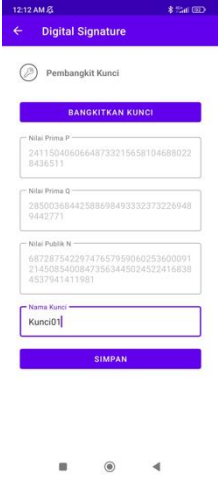
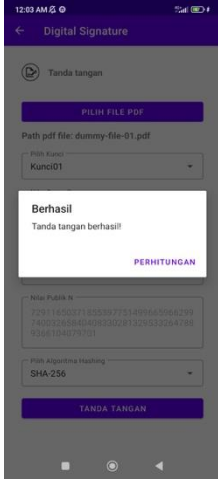
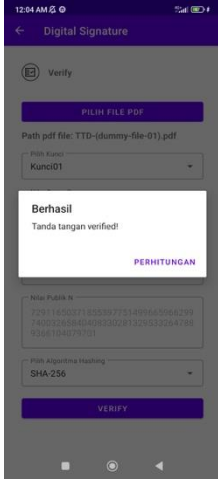
4.6.1. Pengujian Sistem *Digital Signature*

Sub bab ini menampilkan data pengujian dari sistem yang dibangun adapun contoh data dari pengujian yang dibangun adalah sebagai berikut:

Pengujian ini menunjukkan tahapan dan nilai pada sistem, seperti berikut:

Nilai	Fungsi
Hex Bytes Pesan	Menyimpan bytes pesan dalam bentuk hexadecimal
Hex Bytes Padding	Menyimpan bytes padding dalam bentuk hexadecimal
Hex Bytes Hash Bytes Pesan Padding	Menyimpan bytes hash pesan padding dalam bentuk hexadecimal

Pengujian 3 sampai pengujian 20 tertera pada lampiran.

Pengujian 1		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p>Nilai P: 219899354750532893775086362139943214939</p> <p>Nilai Q: 331568277926830556469272009590825919759</p> <p>Nilai N: 72911650371855397751499665966299740032658404083302813295332647889366104079701</p> <p>Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Perhitungan Putaran ke-: 1</p> <p>Hex Bytes Padding: d3bab081b25573f07a0f346435170d4d</p> <p>Hex Bytes Hash Bytes Pesan Padding: 525b8e49819ed946657f57170f491bd58bf2a9870ea928cb6eeca34a61fd4648146340f9c9cad861b5c66e537280f16d9607be9c0dbfedd2531f894ed59e8d4c</p> <p>Nilai Hash Pesan Padding: 6745469874522611294552539776834085517766993386895021945949332141557515499433</p> <p>Nilai Hash Pesan Padding Mod P: 21991281466667748068134018638118300449</p> <p>Nilai Perhitungan Akhir P: 1485976992771557869317715772693516774294499567551295168126163260775533706740543787752650438044231908152202571636515</p> <p>Nilai Hash Pesan Padding Mod Q: 86042546779263352902769135525644987902</p> <p>Nilai Perhitungan Akhir Q: 459507067861460529497369341498176824015028590093518621725818552464735071051681834429704853873048198441943416470234</p> <p>Nilai Perhitungan Tanda tangan: 49339682769958834198454435148004146626009343614329221480908742954783073110008</p>		

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
66166180497332786456947126189465654514891410696407791349383315747808588580268

Perhitungan Putaran ke-: 2 (**Valid**)

Hex Bytes Padding: 1be756e2ccaa09bf99b4e1136d6ca800

Hex Bytes Hash Bytes Pesan Padding:

10d8cc898e2a9b409843a20a502dc49f38a31c968abb0360e80d4dd75e4064f79c3fc26dcf66e50c7dd904590ad283fe03859af8ff9613df2b7b63022c8f3847

Nilai Hash Pesan Padding:

61537491741652065592447196087773286248482649261675480592526507871389198822023

Nilai Hash Pesan Padding Mod P: 216730732967380729426119750009710919901

Nilai Perhitungan Akhir P:

14644752890102677544653106922318024213371382843410230643711362266588330617234885118827915253234176047090914356795735

Nilai Hash Pesan Padding Mod Q: 10241068077338767253728315300698153243

Nilai Perhitungan Akhir Q:

54692048761179530181739413797446132110749420489749614940766090449237125235692340626547281393260683571979816644481

Nilai Perhitungan Tanda tangan:

6593630825005592602857220336333016705237348604951930329304210783649833991114

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

61537491741652065592447196087773286248482649261675480592526507871389198822023

Perhitungan verifikasi tanda tangan

Nilai N:

72911650371855397751499665966299740032658404083302813295332647889366104079701

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...

Hex Bytes Padding: 1be756e2ccaa09bf99b4e1136d6ca800

Nilai Hash Pesan Padding Mod N:

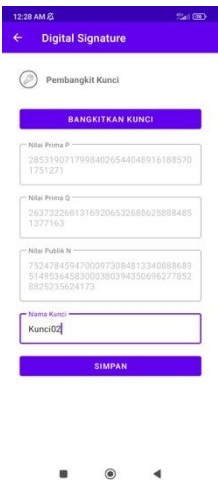
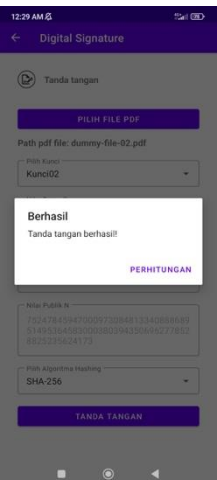
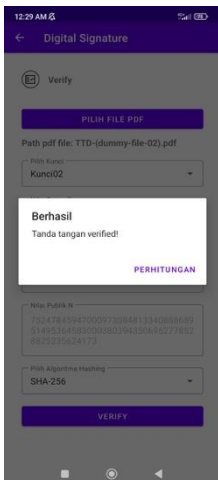
61537491741652065592447196087773286248482649261675480592526507871389198822023

Nilai Tanda Tangan:

6593630825005592602857220336333016705237348604951930329304210783649833991114

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

61537491741652065592447196087773286248482649261675480592526507871389198822023

Pengujian 2		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p>Nilai P: 285319071799840265440489161885701751271</p> <p>Nilai Q: 263732268131692065326886258884851377163</p> <p>Nilai N: 75247845947000973084813340888689514953645830003803943506962778528825235624173</p> <p>Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Perhitungan Putaran ke-: 1</p> <p>Hex Bytes Padding: a05fd56f6a56e639e520ca18b7d2b652</p> <p>Hex Bytes Hash Bytes Pesan Padding: f4b1d7c0853ad2003438f997538d3148cecb0cda4b135d756aedbdc9608f8b6d3746931dd127c64faa5623a9d561c778788c4c03fec85dab640d97965004ce3e</p> <p>Nilai Hash Pesan Padding: 35970576955479776610152658692373997525688977820919334531796720791330247401894</p> <p>Nilai Hash Pesan Padding Mod P: 84259178726040117269192534197804143380</p> <p>Nilai Perhitungan Akhir P: 2035724135786834132203878451915166618942028972247692286887269812595947740870482048645609908369073608306887086269120</p> <p>Nilai Hash Pesan Padding Mod Q: 186234777509004260905554161979286432826</p> <p>Nilai Perhitungan Akhir Q: 9514284162650973236940063122047492624856802531121804603311310854765308493465228632370112894187013546098639874492300</p> <p>Nilai Perhitungan Tanda tangan: 62054414414534964829728216765825309728986639917176371899651222658397716734374</p>		

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
39277268991521196474660682196315517427956852182884608975166057737494988222279

Perhitungan Putaran ke-: 2 (**Valid**)

Hex Bytes Padding: ecae5761ab825a45602090122ba7feaa

Hex Bytes Hash Bytes Pesan Padding:
3f79d7f4a55e44595f1458a36e4752fc79ab27265f835b8bd6e93cf76684c7f992433b1fb5c69b2b8
bcd2003e4785a8875482eebef98e7442583dce91d980951

Nilai Hash Pesan Padding:
52206119386994102064473912455459346911987490057450657651684809712049785898968

Nilai Hash Pesan Padding Mod P: 31892599594965328463049144864230880873

Nilai Perhitungan Akhir P:
77053367633159166165626557232643385297118508419694184907160594743624724853710
5935328735215669633693037094215344752

Nilai Hash Pesan Padding Mod Q: 20058096173271778634012479415763942181

Nilai Perhitungan Akhir Q:
10247196002103470300362972334245279427460595909995237000075458332840215794711
00584094475427215682426766466951002550

Nilai Perhitungan Tanda tangan:
7396132600678490445256373038734515496529122259615849189889018567586796057735

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
52206119386994102064473912455459346911987490057450657651684809712049785898968

Perhitungan verifikasi tanda tangan

Nilai N:
75247845947000973084813340888689514953645830003803943506962778528825235624173

Hex Bytes Pesan:
255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: ecae5761ab825a45602090122ba7feaa

Nilai Hash Pesan Padding Mod N:
52206119386994102064473912455459346911987490057450657651684809712049785898968

Nilai Tanda Tangan:
7396132600678490445256373038734515496529122259615849189889018567586796057735

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
52206119386994102064473912455459346911987490057450657651684809712049785898968

BAB 5

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Kesimpulan yang didapatkan dari hasil penelitian yaitu:

1. Algoritma Rabin-p dan Sha-256 dapat digunakan ke dalam sistem Digital signature pada *file* pdf.
2. Hasil pengujian sistem pada aplikasi sebanyak 20 kali kepada beberapa *user* dengan format *file* pdf menemukan keberhasilan dalam melakukan pembangkitan *key*, *hashing* dan *verification* dengan status berhasil sebesar 100% jika *key* sesuai.
3. Hasil verifikasi dari sistem dapat digunakan sebagai alat untuk melakukan verifikasi *digital signature* pada *file* berformat pdf pada perangkat *mobile*. Dan menghasilkan sistem yang sesuai dengan penerapan kriptografi sebagai dasar dalam pengamanan data.
4. Hasil pengujian sistem lainnya pada aplikasi yaitu berupa *gradle* pada android studio yang mengalami *update* akan berdampak pada kodingan yang dibuat.

5.2. Saran

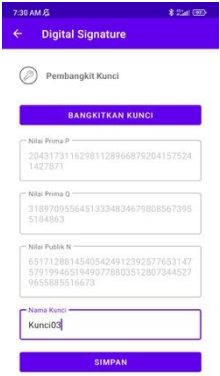
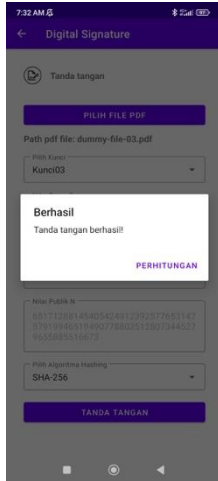
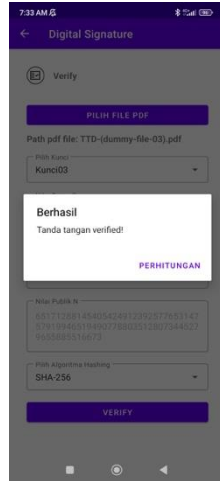
Saran dari penulis yang diberikan agar mengembangkan penelitian selanjutnya yaitu:

1. Sistem yang akan dibuat selanjutnya dapat dikembangkan dengan menambahkan jenis format *file* yang dapat di *hash*.
2. Kedepan nya algorititma rabin-p dan Sha-256 dapat dikembangkan untuk studi kasus lainnya.

DAFTAR PUSTAKA

- Ariffin, M. A. (2019). Rabin-p Cryptosystem: Practical and Efficient Method for Rabin based Encryption Scheme. 13.
- Dr. Sunil Karforma, S. B. (2019). Object oriented modeling of RSA digital signature for security in e-learning. *International Journal of Advanced Technology in Engineering and Science*, 8.
- Hakim, K. M. (2021). Rancang bangun aplikasi enkripsi-dekripsi sms pada android dengan metode rc6. *Journal of Computing and Applied Informatics*, 12.
- Irvida, M. A. (2023). Securing text using Rabin-p public key cryptosystem and Spritz algorithm in a hybrid cryptosystem: a tutorial. *Journal of Physics: Conference Series*, 5.
- Muhammad Fadlan, H. (2019). Rekayasa aplikasi kriptografi dengan penerapan kombinasi algoritma knapsack merkle hellman dan affine cipher. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIK)*, 7.
- Muhammad Farras Muttaqin, Y. S. (2020). Implementation of AES-128 and Token-Base64 to Prevent. *International Journal of Advanced Trends in Computer Science and Engineering*, 6.
- Raffaele Martino, A. C. (2020). Designing a SHA-256 processor for blockchain-based IoT applications. *Internet of Things 11*, 9.
- Stallings, W. (2020). *Cryptography and Network Security: Principles and Practise*.
- Taufan Maynard Prananda Sancaka, V. L. (2022). Penerapan metode playfair cipher dalam aplikasi enkripsi-dekripsi file teks. *Jurnal ilmiah elektronika dan komputer*, 11.
- Triasanti, D. (2019). Pengamanan data menggunakan kriptografi ec signcryption dan steganografi least significant bit (lsb). *Jurnal Teknologi dan Rekayasa*, 9.

LAMPIRAN

Pengujian 3		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p>Nilai P: 204317311629811289668792041575241427871</p> <p>Nilai Q: 318970955645133348346798085673955184863</p> <p>Nilai N:</p> <p>65171288145405424912392577653147579199465194907788035128073445279655885516673</p> <p>Hex Bytes Pesan:</p> <p>255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Perhitungan Putaran ke-: 1</p> <p>Hex Bytes Padding: cf64c0fbb0c56e55e289cd070dbfc252</p> <p>Hex Bytes Hash Bytes Pesan Padding:</p> <p>2054b7ecb87e0e0e9746481afda4ec9ed622cc7871447035c10eb4cbefb18552e25a81456c154cd1e8b0711af9da0a2e7bb36ea4d383addf681d21d98c102c55</p> <p>Nilai Hash Pesan Padding:</p> <p>28543813053141919799466377612132651192826269174406184458842448440644207076262</p> <p>Nilai Hash Pesan Padding Mod P: 113860317666250990632886732467648319028</p> <p>Nilai Perhitungan Akhir P:</p> <p>4018458054500558988290929159836113800631965325339000154861655736747218058576547407110333329200195974919909437487896</p> <p>Nilai Hash Pesan Padding Mod Q: 213445277532832952585260491383726766647</p> <p>Nilai Perhitungan Akhir Q:</p> <p>6377406006762790236300358375630977140561440643902456509096429243460382883099926834273532104478106512432556205512124</p>		

Nilai Perhitungan Tanda tangan:

23657698681022157586580059624203975383988272075423834233624529738378913016227

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

13260688315253929896126815095844940001741516945652748701520810205711123330310

Perhitungan Putaran ke-: 2

Hex Bytes Padding: 1752f05f87851b13408ece53720ad322

Hex Bytes Hash Bytes Pesan Padding:

a32a7dec0c542173253a2b9bda56fc8b3398f6bb5429a3abeb7345d4d12449db59ecfa9e1b63d676
4f75d5615c123091f138c83ce225c3bb627dfe3e55a7cec2

Nilai Hash Pesan Padding:

19811370155348553957332946642319541301244263897680205945995000209457081376276

Nilai Hash Pesan Padding Mod P: 46467690028001778152709462741225034644

Nilai Perhitungan Akhir P:

16399784147309356904537037484317874173829265384560775191324713577985427337047
55989355874264942663994242502215275608

Nilai Hash Pesan Padding Mod Q: 15254033249543735962628545504514892721

Nilai Perhitungan Akhir Q:

45576629474988217047442395914872137508230557237548925592543264600397815777113
8973020710556910619806966501769916132

Nilai Perhitungan Tanda tangan:

53287156763874733634672392529639140209747696571764631772766761899292926100773

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

45359917990056870955059631010828037898220931010107829182078445070198804140397

Perhitungan Putaran ke-: 3

Hex Bytes Padding: d2ffbe7728f6db44c17f522f9d08b382

Hex Bytes Hash Bytes Pesan Padding:

44c0d03122f7e76e42edf15a1f5e59215fad098c8918ef305436bf69eb60e90d46577b47239f70fd2
8f4f3b712278e9db4861ba91c7b6d8dc5e3750c8c06f7e0

Nilai Hash Pesan Padding:

26665715612817173930129083162921182345901719347749174060015231171294497654110

Nilai Hash Pesan Padding Mod P: 34891336550326311816792052371265048710

Nilai Perhitungan Akhir P:

12314156087631184704397590503626120623705723848269492728352414303407334398112
39337131366194161500244244972274151220

Nilai Hash Pesan Padding Mod Q: 211989963109496014611398932812099571260

Nilai Perhitungan Akhir Q:

63339235223883591548665344230141219686974998793885648301777495818635341653333
57676605331864872273055206057786103920

Nilai Perhitungan Tanda tangan:

62070251474290960928149571866902929371746211141223314540249952289449176046385

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

54745620133742725887415517674248365453638348415731683999818875885717886746909

Perhitungan Putaran ke-: 4

Hex Bytes Padding: e3ce082e348be8bfec93db2ac70ee004

Hex Bytes Hash Bytes Pesan Padding:

21c2e978d30845adedfe27164803d681fe2eb408a55e759b28265845bb5e0e67cb2e52306398e350
04c008a066b9b183ed643c955aef59526df41bbfd0d76e23

Nilai Hash Pesan Padding:

41156707215179078180224383127379799786307727118251402435200053246521052365510

Nilai Hash Pesan Padding Mod P: 85983828933647552459096750608061141267

Nilai Perhitungan Akhir P:

30346165988049892927333608901876995244597593503305284715429091463563943422184
23736029218577472721940554022592332794

Nilai Hash Pesan Padding Mod Q: 204050819515310222520985041662911078567

Nilai Perhitungan Akhir Q:

60967145167296393158206002012007631677030228389591953080018332745195031317377
08841885303009249515504636595841424764

Nilai Perhitungan Tanda tangan:

24363040170980606414484446972936127796374487117072539157548769593605474808847

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

6940253360031168306766523016321329728763761284905803350087079918246627367159

Perhitungan Putaran ke-: 5 (**Valid**)

Hex Bytes Padding: b35839993b3b252a8ecbd0120c1df043

Hex Bytes Hash Bytes Pesan Padding:

5a0bd5c5be5263d9c8b82ff9960b44ced99f7b3183a5b9f2c34a316382fde068e473eff713ac40a5cc
7c6b1a751bfb61226e68d1f7bf811bfa9244076f9c03de

Nilai Hash Pesan Padding:

53340932037962499142891363909844762550073682727947682524435183543874092723724

Nilai Hash Pesan Padding Mod P: 161189675501845976541024729837628427959

Nilai Perhitungan Akhir P:

56888472041802264773838556105890737669859915597052375104105370094384920530807
56180823026618701643664073576894437938

Nilai Hash Pesan Padding Mod Q: 194322845623588738893608087897472758418

Nilai Perhitungan Akhir Q:

58060581018967879374093557319996653460682013940725707315104357988382208415262
77576886324478320933962529323923230856

Nilai Perhitungan Tanda tangan:

48653516153722807163099878686820199233660948042603346604134803253665413035782

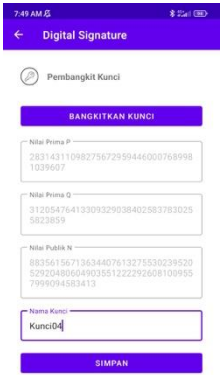
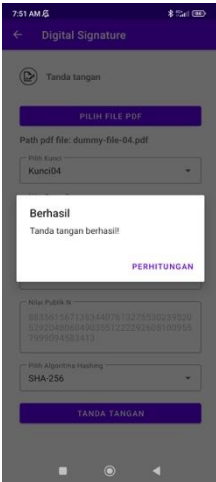
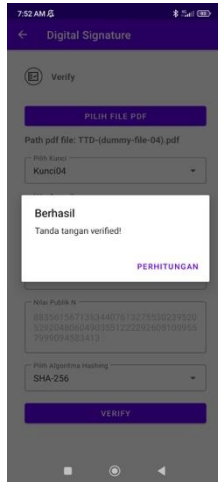
Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

53340932037962499142891363909844762550073682727947682524435183543874092723724

Perhitungan verifikasi tanda tangan

Nilai N:
 65171288145405424912392577653147579199465194907788035128073445279655885516673
 Hex Bytes Pesan:
 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
 a2f5061676573203220...
 Hex Bytes Padding: b35839993b3b252a8ecbd0120c1df043
 Nilai Hash Pesan Padding Mod N:
 53340932037962499142891363909844762550073682727947682524435183543874092723724
 Nilai Tanda Tangan:
 48653516153722807163099878686820199233660948042603346604134803253665413035782
 Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
 53340932037962499142891363909844762550073682727947682524435183543874092723724

Pengujian 4

Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		

Perhitungan tanda tangan

Nilai P: 283143110982756729594460007689981039607
 Nilai Q: 312054764133093290384025837830255823859
 Nilai N:
 88356156713634407613275530239520529204806049035512222926081009557999094583413
 Hex Bytes Pesan:
 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
 a2f5061676573203220...
 Perhitungan Putaran ke-: 1
 Hex Bytes Padding: 59f8c85a55b32a47f343c7704851d269
 Hex Bytes Hash Bytes Pesan Padding:
 809f5f5fe99ecf88d05904bf6f90922a0fa56c081ad19c31f3a1dba201db9a5f19dd698cf0254d3286

96e54d68b3535559e1399c635937ac121fbc3648e10beb

Nilai Hash Pesan Padding:

76552736496413658696346235124258167808331589254678207209346035781350333091450

Nilai Hash Pesan Padding Mod P: 178841363878105812556578069776781085892

Nilai Perhitungan Akhir P:

15032180531860917467636392613658628466385962023808171624817397611705667227299
946491815054580020986807377673181338932

Nilai Hash Pesan Padding Mod Q: 283906011079955011227433534900505495945

Nilai Perhitungan Akhir Q:

12216486024017328754790922652933619457785850039269757768520702147776692650667
92091079223619341011063874278814524385

Nilai Perhitungan Tanda tangan:

8421874480773946645322480849343736932259214442164221949736450170325872898809

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

79687444170665101482792451575475884623504029987068891831399028210332127685223

Perhitungan Putaran ke-: 2

Hex Bytes Padding: 033cec724c1e696a7e1db3ecfed0754b

Hex Bytes Hash Bytes Pesan Padding:

d223e412ae4804dab56680aa76792f0c18ab4e4365e48504fd077a4acefbde8dedebe6f7d71c9116a
fe6fb7062b68e41c6e2c437bbe1422d1fdbaf7f0eb43c48a

Nilai Hash Pesan Padding:

34848492096277501811930770318011163079446401175781091679811313840503068787869

Nilai Hash Pesan Padding Mod P: 51439688241239047954480632167067423710

Nilai Perhitungan Akhir P:

43236679892017518409994552595842408068793592800041366271180680537002892248012
61729400679300108300116590235942623910

Nilai Hash Pesan Padding Mod Q: 310158357708297227121274750637339590019

Nilai Perhitungan Akhir Q:

13346125458078063698512959592501777949667501581089409027892373313422559330207
19764846438668868326320998739276693067

Nilai Perhitungan Tanda tangan:

8594583767197430160850814037704457753432812941939715102226005153713155551446

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

60844730122792850723609129629624938277911568835468091869595687034638593983234

Perhitungan Putaran ke-: 3

Hex Bytes Padding: 4e02792f0399f2173f8840aeacb34f51

Hex Bytes Hash Bytes Pesan Padding:

616b62aeb9a2b68cabf72235e4fc2e63696e8c4c14cee6dccb6be52f522a588b3294b2b435ddd321e
fca6166b8d21085a1b415717eb6f8414091eb4ff6fd5fcc

Nilai Hash Pesan Padding:

42298846898221231834020731949283964454113764161821576551442839745005694189126

Nilai Hash Pesan Padding Mod P: 158588489715354533054430718565838209546

Nilai Perhitungan Akhir P:

13329862599914025006286645642487961848318627134265906774487965628144955386429
096838673460336962783061016394941628066

Nilai Hash Pesan Padding Mod Q: 17653447542634331504131237697434291788

Nilai Perhitungan Akhir Q:

75962849240123789625526281777915800008651953875356610599638730589050856216980
737197394789899967274545455833003884

Nilai Perhitungan Tanda tangan:

23482029133137435051495865223267938919642007728359308379275638826233763321082

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

5566770096021606853615979624606091047379253664585327077457117515300703326884

Perhitungan Putaran ke-: 4

Hex Bytes Padding: 5204d0869f89e479eb70423294a5cea6

Hex Bytes Hash Bytes Pesan Padding:

a43a6eb5ae38f71338581bafb99037ad78c04919492fd232c1ea9488e3fd00751acbfa0b76bc1de0
f82f7d32ab6cd76e57e6e282c9084633e3c4bd3e19401df

Nilai Hash Pesan Padding:

41731890386699516326221870180993651912290491866961875350812749912654342545134

Nilai Hash Pesan Padding Mod P: 210946393840045884725944141164311320310

Nilai Perhitungan Akhir P:

17730709529311540827806354715572101423874032426245645879415911452698249515730
698759423307590585207985351330252412510

Nilai Hash Pesan Padding Mod Q: 100003046912230664240919063795586146185

Nilai Perhitungan Akhir Q:

43031347603920862547760664397779010419367766319158567348900271244963559712720
5831596353523183681290973869329844705

Nilai Perhitungan Tanda tangan:

58982963941438097590992502988572941476240986515044126375163368809902080398550

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

27088220510302249646344477963524452270218725268240062881468182283042279024705

Perhitungan Putaran ke-: 5

Hex Bytes Padding: 432a26f6af635c7c7cfdb6ba665df66

Hex Bytes Hash Bytes Pesan Padding:

5697244520ad8258d64405ef99af37ff55b7891a9164918909ce4871c2fee03dcf7c15ec7a2e32ea7
d828a2ac5b743425a4c75972e3cf518956e02961af65ef4

Nilai Hash Pesan Padding:

54143892689957403776084462764208457417935530338859696938792518841263256908351

Nilai Hash Pesan Padding Mod P: 137617841241203064932961787470680752603

Nilai Perhitungan Akhir P:

11567213473907050264234522331102822026735352435380787982683445523443808617056
562840686730279316006789946524496616463

Nilai Hash Pesan Padding Mod Q: 255861701429205326429265514573275596089

Nilai Perhitungan Akhir Q:

11009738355666226829538794638350050902216276004009202074209591442556175185656
57783512893419797659680074463159746577

Nilai Perhitungan Tanda tangan:

47218231469720649849479247330078413739708817215144198183328085775713277923455

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

53620080270579682546538137029446607554799303606360229495388942284637896120556

Perhitungan Putaran ke-: 6

Hex Bytes Padding: cafc6bde019f35cbfa771a31cdc4b84a

Hex Bytes Hash Bytes Pesan Padding:

5a20ed29e4e954f08592e251c09fe7c1519843ed5caad49b6727152ed74a12cc23f6afa7f4b2db70b
d37c1e572984b480b0ddacc0607da2d3d5f60522bbf5f4f

Nilai Hash Pesan Padding:

48846405745770345559988740885459052640773201877958441504570777709060960062622

Nilai Hash Pesan Padding Mod P: 151706004048725337782598433674836375266

Nilai Perhitungan Akhir P:

12751367978729910522110487626761361395026051650814512594909586086616155901244
551148958341746278640318125617372540186

Nilai Hash Pesan Padding Mod Q: 311437377173407970738749309592515120872

Nilai Perhitungan Akhir Q:

13401161712367061808173329347340696500306880186043083366774604000413451783226
73640603581132895356554301137424355496

Nilai Perhitungan Tanda tangan:

14653057094810473615052568899314633684980474694718910166671281014072580785664

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

39509750967864062053286789354061476564032847157553781421510231848938134520791

Perhitungan Putaran ke-: 7 (Valid)

Hex Bytes Padding: f121a645c8a2e729f5387928287fb90d

Hex Bytes Hash Bytes Pesan Padding:

4299e65bf12c9ab81052d44adc1d97470e482c049eb684775d1817039d5d29d6533a179576f17de
2945dbbe89321ebc5ecb6f22ebdc80f58b0bb2328a40c071d

Nilai Hash Pesan Padding:

24966223579360025252777184624845884602930310227118734927485179107702272097599

Nilai Hash Pesan Padding Mod P: 255413541902362624663368893292904542326

Nilai Perhitungan Akhir P:

21468313531623482600922470133040093885972288361810440810628394004707865399799
718739304132768429547046409293939284446

Nilai Hash Pesan Padding Mod Q: 45382182584802898979080359836232515090

Nilai Perhitungan Akhir Q:

19527969738214219174095542274082851942116167532869050944400306978553064961571
6332927620174611459196372216399346370

Nilai Perhitungan Tanda tangan:

35936075193265064147764201789900617649448244601866533712496648226691127973670

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

24966223579360025252777184624845884602930310227118734927485179107702272097599

Perhitungan verifikasi tanda tangan

Nilai N:

88356156713634407613275530239520529204806049035512222926081009557999094583413

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: f121a645c8a2e729f5387928287fb90d

Nilai Hash Pesan Padding Mod N:

24966223579360025252777184624845884602930310227118734927485179107702272097599

Nilai Tanda Tangan:

35936075193265064147764201789900617649448244601866533712496648226691127973670

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

24966223579360025252777184624845884602930310227118734927485179107702272097599

Pengujian 5

Bangkitkan kunci

Tanda tangan

Verifikasi tanda tangan

Perhitungan tanda tangan

Nilai P: 222276474522757172678493202102427675743

Nilai Q: 319926075858402573794726305562540918299

Nilai N:

71112040249705898257480232555172359068885578295629944410301181784699427121157

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...

Perhitungan Putaran ke-: 1

Hex Bytes Padding: 5197a8555177aead22e93d7a52f0f387

Hex Bytes Hash Bytes Pesan Padding:

d8864e1f19eb42853ab4f005d24181549bd20f14003195a0fdb59c9d2d1222d296d2a7789b4d6cd418247cc0040c4a7a420aa2d0e036cc8d73431a8b0a7a61

Nilai Hash Pesan Padding:

66425236898308632898040872962701554749969237075753753947626687348996668391948

Nilai Hash Pesan Padding Mod P: 162629632831169437142340072326070715478

Nilai Perhitungan Akhir P:

10807071224671266133747460636954251211175757158246023728454533811365885184803908605030475170991606882516142409838974

Nilai Hash Pesan Padding Mod Q: 71955505272664367933977888599801126099

Nilai Perhitungan Akhir Q:

335312513880537527624137070250851044096050723751837112240423769695241652514499385580498977960342583818589565343275

Nilai Perhitungan Tanda tangan:

63133717236222465209279541457633374246510810554893116643147685754755577256545

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

62277317294753884594038322437668363015424702503486836630396189402841710702627

Perhitungan Putaran ke-: 2

Hex Bytes Padding: f5199c86c03686044b626b099df682fe

Hex Bytes Hash Bytes Pesan Padding:

228158f12e3958af7862a848c4bd30e97c19bd78e60653c1f3a78add892bd853e3460a1a85aec395e666ff2f06020f77a4d1ce6e189d99ee11ceb7510cb64a4b

Nilai Hash Pesan Padding:

47328474055679961240882396389644686485932017066742076387602971161289532536916

Nilai Hash Pesan Padding Mod P: 191847571556665872721324910569727956275

Nilai Perhitungan Akhir P:

12748662921999395724522706599319065127589960485317313671256463449067701138021738974591397252638936176989200631729575

Nilai Hash Pesan Padding Mod Q: 93274996161979523739130563010383967844

Nilai Perhitungan Akhir Q:

434661299740085141646073180194953807269030424479922391122771817728743242447649873232336151889195461165554015840900

Nilai Perhitungan Tanda tangan:

41538764781603908566865040962685771690406509343538788123663864464575867251103

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
23783566194025937016597836165527672582953561228887868022698210623409894584241

Perhitungan Putaran ke-: 3

Hex Bytes Padding: b84e2ea449ba2e0eb61f85dc63a0f4a2

Hex Bytes Hash Bytes Pesan Padding:
1970097e8286642e38565ed0a76c8e710800db2208d0d6b42b9e933284156f50bb6d07ea9290a1c
ab49cd2185edcfd3a5be2f5b4bc1dfee467a536bed584630

Nilai Hash Pesan Padding:
34640788372358991501080154291545428958323034609795758822677417485492754113311

Nilai Hash Pesan Padding Mod P: 215688857425955916376743324322157663793

Nilai Perhitungan Akhir P:
14332965056805570470321592479361599676150187045894826605639724407973443235812
113714050519652412659855724375140781869

Nilai Hash Pesan Padding Mod Q: 86819403890744307064981637354640832707

Nilai Perhitungan Akhir Q:
40457825237834298890106807436819926316873701845546055140192334860475016318853
7057557439612808931990379414210162075

Nilai Perhitungan Tanda tangan:
26515169074068595460667470863295336550215470893689020704622176120259396550593

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
24213142080976089804668940361351065831361583832737740197267999343610361290672

Perhitungan Putaran ke-: 4 (**Valid**)

Hex Bytes Padding: 93e6da52c8c6aa142d8df9d0d1d87ba0

Hex Bytes Hash Bytes Pesan Padding:
65c5be395b5ee475d270b3c37055d7624304d736bd62b7c777a9dc73219a0770aa0e8b09214e55e
e2fab1bafc10c41d81ec3a50595b0e8714f551b6b7d589b91

Nilai Hash Pesan Padding:
21517927102598078986185960983064850659358830928914750602154819333811285187051

Nilai Hash Pesan Padding Mod P: 169160950855188315382851363064303679088

Nilai Perhitungan Akhir P:
11241090645657273988787451678100493917360055547969233179109006877016290065645
792262236966331281370873491222934397104

Nilai Hash Pesan Padding Mod Q: 302317055229691381698325918094450170959

Nilai Perhitungan Akhir Q:
14087968862688186156212295066452428090573541309165969391499226185627828057045
15379192171398713421624972685515376775

Nilai Perhitungan Tanda tangan:
9237226881378391782783954953572842808330289361805013294607902957852514848030

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
21517927102598078986185960983064850659358830928914750602154819333811285187051

Perhitungan verifikasi tanda tangan
<p>Nilai N: 71112040249705898257480232555172359068885578295629944410301181784699427121157</p> <p>Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Hex Bytes Padding: 93e6da52c8c6aa142d8df9d0d1d87ba0</p> <p>Nilai Hash Pesan Padding Mod N: 21517927102598078986185960983064850659358830928914750602154819333811285187051</p> <p>Nilai Tanda Tangan: 9237226881378391782783954953572842808330289361805013294607902957852514848030</p> <p>Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N: 21517927102598078986185960983064850659358830928914750602154819333811285187051</p>

Pengujian 6		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p>Nilai P: 229760631764716083945500688368103734747</p> <p>Nilai Q: 292179836864177810978350114433326771007</p> <p>Nilai N: 67131423906825175801193745140362035649653265900717892779999366747534738080229</p> <p>Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Perhitungan Putaran ke-: 1</p>		

Hex Bytes Padding: 024b4925c20a5ba47261426a8924ff00

Hex Bytes Hash Bytes Pesan Padding:

69753985a7aaf4156e420db6a8cb6e6243d087c9630cbd0f2bf41f33c322bcd274fe501b44aaab7a7f98f7f91da783a6b5ae6193b734fe8b1bbc1a6fce6889aa

Nilai Hash Pesan Padding:

18231260184826421596578925128815773416596744520754299700317454935693283639038

Nilai Hash Pesan Padding Mod P: 181099555660529400459758096220394173763

Nilai Perhitungan Akhir P:

1254225307552803562597806383525621413872041651696594306070418385984672525998117548379369477892275863011196623636836

Nilai Hash Pesan Padding Mod Q: 177708018521793544792072639771987122797

Nilai Perhitungan Akhir Q:

10699055486749886386377633204565760843691614185985855132644617916809383668034001078620472651618446577704709954679826

Nilai Perhitungan Tanda tangan:

33407265961138669670377806406142397433097156286258926450179892517515137125074

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

48900163721998754204614820011546262233056521379963593079681911811841454441191

Perhitungan Putaran ke-: 2

Hex Bytes Padding: a17b348baace4f4f6e86fc64b88069a1

Hex Bytes Hash Bytes Pesan Padding:

8965032cbb995fc6641afa6670e865d92e884466312290d62f542a961cf0e8a61733dff7255c6b8bca0c414c19dd6b55290ed669f36aa70ed648a040d51e929c

Nilai Hash Pesan Padding:

14969844403082382931213000317663585509766320380276360017930535602479533985453

Nilai Hash Pesan Padding Mod P: 155066935509007197625294467136101494677

Nilai Perhitungan Akhir P:

1073933473611741755184704159316849500623960472287170187972623757812695380312109961373569059517573638750934725382844

Nilai Hash Pesan Padding Mod Q: 75953898390349907692655511139590065235

Nilai Perhitungan Akhir Q:

4572866098406570109891574388929039650473505330760920323582277931001676770757066625077620993957300251443837242571630

Nilai Perhitungan Tanda tangan:

33719093772116141402451226415410525496483233053049419303534709030224496892165

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

52660734741102820444026459521567160777361972448381855648814073034739168379929

Perhitungan Putaran ke-: 3 (**Valid**)

Hex Bytes Padding: e2f376625471e6940d72c07e7d1b4822

Hex Bytes Hash Bytes Pesan Padding:

1271139d3d7386b6e4531330479d9ac1c4a919d86e1407309a4664b9f61552ccf7acfe97081e34fd

6563137d919f79a6b63e639f7251d4b1571ebee7ddd25ece

Nilai Hash Pesan Padding:

29039134442391776432843132820594675047861738990276194697709170206944918396277

Nilai Hash Pesan Padding Mod P: 170954816343505160492408082819017537374

Nilai Perhitungan Akhir P:

11839667763072136978698912708215310457052614442349079396510720850413550865478
28323804722724531667235026947205009128

Nilai Hash Pesan Padding Mod Q: 280830249611624340084547965222347531706

Nilai Perhitungan Akhir Q:

16907613105731144724191025846145670595637917922998744286039276356736745916710
064647299524040435141869127352763563748

Nilai Perhitungan Tanda tangan:

5620360002018103334530825732651930787464899918144111905244654311381781054858

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

29039134442391776432843132820594675047861738990276194697709170206944918396277

Perhitungan verifikasi tanda tangan

Nilai N:

67131423906825175801193745140362035649653265900717892779999366747534738080229

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: e2f376625471e6940d72c07e7d1b4822

Nilai Hash Pesan Padding Mod N:

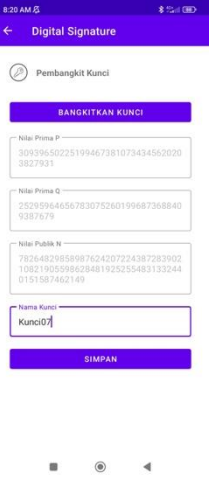
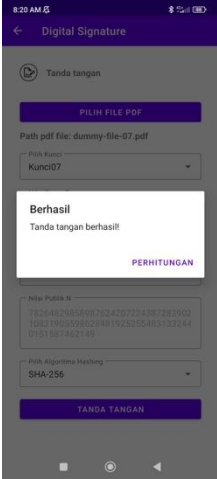
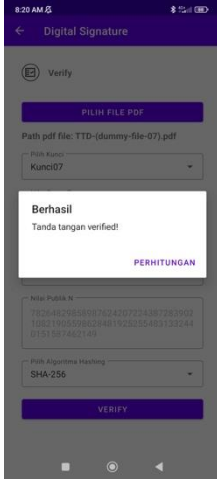
29039134442391776432843132820594675047861738990276194697709170206944918396277

Nilai Tanda Tangan:

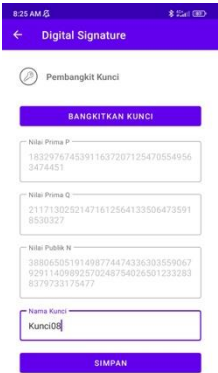
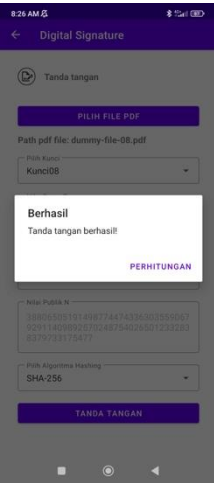
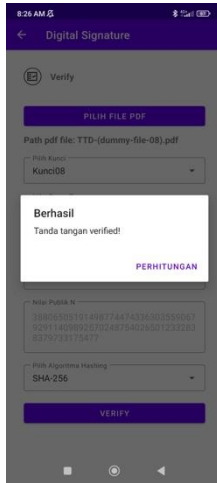
5620360002018103334530825732651930787464899918144111905244654311381781054858

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

29039134442391776432843132820594675047861738990276194697709170206944918396277

Pengujian 7		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p>Nilai P: 309396502251994673810734345620203827931</p> <p>Nilai Q: 252959646567830752601996873688409387679</p> <p>Nilai N: 78264829858987624207224387283902108219055986284819252554831332440151587462149</p> <p>Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Perhitungan Putaran ke-: 1 (Valid)</p> <p>Hex Bytes Padding: 8cae7f3e81932a0b1faa347c306b9c38</p> <p>Hex Bytes Hash Bytes Pesan Padding: 2d523d9893466b3d7445c4a6d554c4c8cde5268e1ba65e73990936b25956218a70817febce68f43f446e144d8eb4cf75100314cec622bffac724949cef2fb208</p> <p>Nilai Hash Pesan Padding: 58481172017052761246906494380444619145002881296249502994862151445695313033435</p> <p>Nilai Hash Pesan Padding Mod P: 196538359765257844737694893459035077988</p> <p>Nilai Perhitungan Akhir P: 8271829755261065380797685640919864718908910880730851098281698454723927675531248877230514379643759357157590886083500</p> <p>Nilai Hash Pesan Padding Mod Q: 79986382367673291195333757778466803960</p> <p>Nilai Perhitungan Akhir Q: 2893684973433999381659986217840472174206537103818108470101033706201869027812712521767738080127825617699275135169000</p> <p>Nilai Perhitungan Tanda tangan: 4376644832045377613673824185976509863472192047226721795186970417222976121464</p>		

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N: 58481172017052761246906494380444619145002881296249502994862151445695313033435
Perhitungan verifikasi tanda tangan
Nilai N: 78264829858987624207224387283902108219055986284819252554831332440151587462149 Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670 a2f5061676573203220... Hex Bytes Padding: 8cae7f3e81932a0b1faa347c306b9c38 Nilai Hash Pesan Padding Mod N: 58481172017052761246906494380444619145002881296249502994862151445695313033435 Nilai Tanda Tangan: 4376644832045377613673824185976509863472192047226721795186970417222976121464 Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N: 58481172017052761246906494380444619145002881296249502994862151445695313033435

Pengujian 8		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
Nilai P: 183297674539116372071254705549563474451 Nilai Q: 211713025214716125641335064735918530327 Nilai N: 38806505191498774474336303559067929114098925702487540265012332838379733175477 Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670 a2f5061676573203220...		

Perhitungan Putaran ke-: 1

Hex Bytes Padding: 5b275d54ee569204f064c9d76505ef12

Hex Bytes Hash Bytes Pesan Padding:

892c8a2eb13ace45f1cfcdd8ff119eaa6f5a439b0dc1bc0e7aef420e80918a635f933848dcc892c0f0761c6f83431ab7472aef4ab33543c1cf9726d3eb10d8c9

Nilai Hash Pesan Padding:

30962933963636641950551187860641922883709396876115365715893646400237206389267

Nilai Hash Pesan Padding Mod P: 47994383917209928829988335595257038594

Nilai Perhitungan Akhir P:

39062943711212917658060740537291978666678575448861990046869085500837091511900357646560658495763411524737779015674

Nilai Hash Pesan Padding Mod Q: 4388112170181004236522864571807239099

Nilai Perhitungan Akhir Q:

134572165084583326258430627932558389245962606615435076146988022812472099440906510990992590603416777661250531259043

Nilai Perhitungan Tanda tangan:

33138606033133798892470834922115328966963633185024842298845744930124953984359

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

31014826528422414232611163771325905365930201111042506895372559554423021500491

Perhitungan Putaran ke-: 2 (**Valid**)

Hex Bytes Padding: 7d5a504cfb17bcaaec16c97313f0abc6

Hex Bytes Hash Bytes Pesan Padding:

3db47482d8c427cab20141eae684774c9bc080ad9215fabdbb418288a6fdef44c28f933b7480a18406bad30338ed34788d3378bfa6b7bd97dcfa669f6cd5abd

Nilai Hash Pesan Padding:

29418793207520982698755954600748665587075126020192528397238089635703182342830

Nilai Hash Pesan Padding Mod P: 153690586077356065769223404662158533111

Nilai Perhitungan Akhir P:

1250897755712267325002818822991616382737401638979349128645028494212478225827378433368488986693932774715490634079131

Nilai Hash Pesan Padding Mod Q: 10788267777250486123446992699313933084

Nilai Perhitungan Akhir Q:

3308485508247208617626060577475715510792315077903945571992395516089833646075485423931996229564428118298600424272188

Nilai Perhitungan Tanda tangan:

36889802388792606479142374393947301419285824332843986605299998878359098073281

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

29418793207520982698755954600748665587075126020192528397238089635703182342830

Perhitungan verifikasi tanda tangan

Nilai N:

38806505191498774474336303559067929114098925702487540265012332838379733175477

Hex Bytes Pesan:
255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: 7d5a504cfb17bcaaec16c97313f0abc6

Nilai Hash Pesan Padding Mod N:
29418793207520982698755954600748665587075126020192528397238089635703182342830

Nilai Tanda Tangan:
36889802388792606479142374393947301419285824332843986605299998878359098073281

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
29418793207520982698755954600748665587075126020192528397238089635703182342830

Pengujian 9

Bangkitkan kunci

Tanda tangan

Verifikasi tanda tangan

Perhitungan tanda tangan

Nilai P: 319496036255178460338399822231867184091

Nilai Q: 225722581085963480566538562509387209031

Nilai N:

72117469950253447986897874863304931770638942414165874973181787393991574725821

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Perhitungan Putaran ke-: 1

Hex Bytes Padding: d1f037e7bea266c8afdb9b6b1bab2dee

Hex Bytes Hash Bytes Pesan Padding:

ac7d8be8414f97a2eba887a43d7f866ea08d7e4a4d949252060086ecac18c6621fea9893fec94d323

a1b242b1fde00e666b754774c1eb311d81ea089459909c4

Nilai Hash Pesan Padding:

28761306483791123508948772450633111504500889361191768382906465120053747118252

Nilai Hash Pesan Padding Mod P: 32584040733104287934906671712286924310

Nilai Perhitungan Akhir P:

13050557171958487865353794448255137464454673089968149884020837681905572421225
15948686928615105726773045130577023080

Nilai Hash Pesan Padding Mod Q: 67755845449674729275598588313799642901

Nilai Perhitungan Akhir Q:

21726236131289384230377072304174533677333840162670706812848613544920403568549
29561545431452977967100319220396065354

Nilai Perhitungan Tanda tangan:

19328521396670577912987120919694414649124120980662962753639439219264852296378

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

43356163466462324477949102412671820266138053052974106590275322273937827607569

Perhitungan Putaran ke-: 2

Hex Bytes Padding: fb68ad14dd08911f3aec218875625c22

Hex Bytes Hash Bytes Pesan Padding:

9ff11066b63f74bfa2e181f22146086edf1bd1eb2c24613e2a6f7dc430ddc573f5c4265ac7d771c8bb
0cb84a8e62c46c1ee4933d5bd9ffe4389dc5f91ef5c025

Nilai Hash Pesan Padding:

38841667498141787467019768782445850570413950239906949763647709993746323415941

Nilai Hash Pesan Padding Mod P: 103723369919692190382738770028043240203

Nilai Perhitungan Akhir P:

41543275135605930509583137726371156974639707525838659066749240501812721237569
07641607389559494911404747145956554804

Nilai Hash Pesan Padding Mod Q: 125182896116300380171129173641150063198

Nilai Perhitungan Akhir Q:

40140494780505574542824885192089525881690724348582474694717933063597668225717
02253217794621799780940620766399015292

Nilai Perhitungan Tanda tangan:

44638388760400061872215198023956086349625606905769679027778344049619110253629

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

40080490752728477828416787817230850614611252426544200372287746818185810576554

Perhitungan Putaran ke-: 3

Hex Bytes Padding: 4f907a8716d61be13f467787677bdc18

Hex Bytes Hash Bytes Pesan Padding:

54eccdc58758d0bb00af30565766d5a29d0e7c6d614905ca6a95f640893f067c7daea3780be6f0d33
7f6ed4c2ee7e28989da00e384c4d948ed6720875e201b7d

Nilai Hash Pesan Padding:

52573846880738967029602149188710461706024713264451421148258248324586255951095

Nilai Hash Pesan Padding Mod P: 96603251940538830685425801093060964279

Nilai Perhitungan Akhir P:

38691526099347657840072582885980945016363076718388700745897191357584873496117
20656192954978530249800898052671923972

Nilai Hash Pesan Padding Mod Q: 170873342132784890927005077929783033408

Nilai Perhitungan Akhir Q:

54791354975813467194189717916778333784081910849984257417665587264976043285832
54616908264897242479511073965773333632

Nilai Perhitungan Tanda tangan:

11435827441891476705567515295919232361131754335692016451282754207108041286725

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

22003412347447877063043312388938863146270242293203621731982205101175342580048

Perhitungan Putaran ke-: 4 (**Valid**)

Hex Bytes Padding: 66aff72fdb40b59d841900051896558

Hex Bytes Hash Bytes Pesan Padding:

2ee3089ec696892578d422eedac507f4b2f1b6eb96aa50e2b5a38571cabd54ae8204aef79b62f7913
c03d97f8d60139c5e540cab24cbfc195d1f90d13d524cf6

Nilai Hash Pesan Padding:

27173484327323531947182458053787768624697788603325733653087262215423312199096

Nilai Hash Pesan Padding Mod P: 108198964782816742260926483804067739763

Nilai Perhitungan Akhir P:

43335840002503764449828777614175051276918712597925119766968850375523411077938
81549737059598313345947522311615444884

Nilai Hash Pesan Padding Mod Q: 173042345174566476264681658018907861371

Nilai Perhitungan Akhir Q:

55486856182277386882923656041518852783890246194259067114940565254914949777237
05575825641582894759612908380182251734

Nilai Perhitungan Tanda tangan:

30679769473166242274306930958240580117488236384342754127190030746606961090204

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

27173484327323531947182458053787768624697788603325733653087262215423312199096

Perhitungan verifikasi tanda tangan

Nilai N:

72117469950253447986897874863304931770638942414165874973181787393991574725821

Hex Bytes Pesan:

255044462d312e340a25f6e4fcd0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

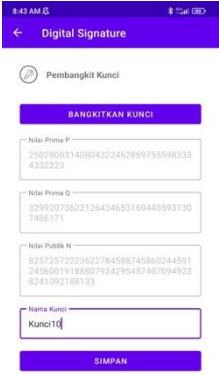
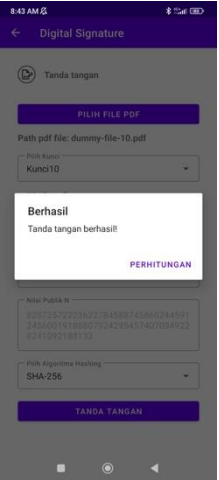
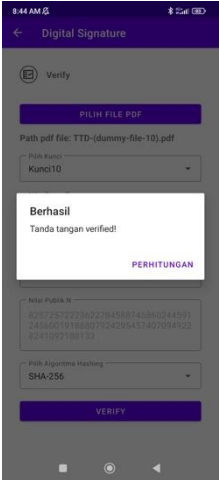
Hex Bytes Padding: 66aff72fdb40b59d841900051896558

Nilai Hash Pesan Padding Mod N:

27173484327323531947182458053787768624697788603325733653087262215423312199096

Nilai Tanda Tangan:
 30679769473166242274306930958240580117488236384342754127190030746606961090204
 Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
 27173484327323531947182458053787768624697788603325733653087262215423312199096

Pengujian 10

Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		

Perhitungan tanda tangan

Nilai P: 250280031408043224628697555983334332223
 Nilai Q: 329920736221264346531694405931307486171
 Nilai N:
 82572572223622784588745860244591245600191888079242954574070949228241092188133
 Hex Bytes Pesan:
 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
 a2f5061676573203220...

 Perhitungan Putaran ke-: 1
 Hex Bytes Padding: 7d4f813c585d9319a951aa8b553e0f79
 Hex Bytes Hash Bytes Pesan Padding:
 02541cbae61422a558e4e825358b5a8c3745884aec3d4808adc6df1427dd3cc0b38c217223d7b47a
 f838857e5d078c1d84d0d5f849013ef87498c69f55995ab1
 Nilai Hash Pesan Padding:
 12122988778665181731541097319729072025036175201577551197478693465990533089637
 Nilai Hash Pesan Padding Mod P: 170827478962230078417389959993349575771
 Nilai Perhitungan Akhir P:
 11470324709785492294418818960244557182737755956774149380604156812052944438585
 297003177740442782495503912811195086659

Nilai Hash Pesan Padding Mod Q: 17124531218819315894420790258996900052

Nilai Perhitungan Akhir Q:

26417855089299197236700524356301757408820205574343348714860700920386490051205
5400327861891743684942532011603969860

Nilai Perhitungan Tanda tangan:

47168729812525803439287312611185945160273470534298746864941594313165185453247

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

77533883165192946374083416448368313548317283731456289496168270148505031791509

Perhitungan Putaran ke-: 2

Hex Bytes Padding: 8cdfff9b6c730eb72d4e3e0ae87e1094

Hex Bytes Hash Bytes Pesan Padding:

2a032682c0970cc6c9f8df0538badf0dba4c550692270ab75e56573266a7fb0eaa10ab3fc9c4804ae
c491dd044c8e9480d578ee6628267c486c873b9600aceb2

Nilai Hash Pesan Padding:

28593995706552136724387875540367960891548091265252193524732895382873834311146

Nilai Hash Pesan Padding Mod P: 58380028439386230225406020140465109356

Nilai Perhitungan Akhir P:

39199658441036201814710981740965030656555060850902656891175142150462500139756
95651389945806951779573990206425466124

Nilai Hash Pesan Padding Mod Q: 174224198544914200832786377726291096690

Nilai Perhitungan Akhir Q:

26877405117815380785226392695952609468362819837441205284633073183567656231990
91573880550687043270161692474769245450

Nilai Perhitungan Tanda tangan:

21262360008622727705395118510490127288248180460573893412115230326464219674829

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

28593995706552136724387875540367960891548091265252193524732895382873834311146

Perhitungan verifikasi tanda tangan

Nilai N:

82572572223622784588745860244591245600191888079242954574070949228241092188133

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: 8cdfff9b6c730eb72d4e3e0ae87e1094

Nilai Hash Pesan Padding Mod N:


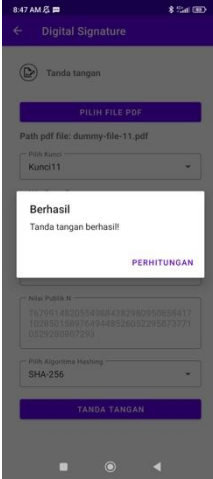
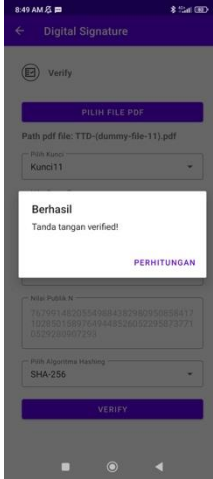
28593995706552136724387875540367960891548091265252193524732895382873834311146

Nilai Tanda Tangan:

21262360008622727705395118510490127288248180460573893412115230326464219674829

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

28593995706552136724387875540367960891548091265252193524732895382873834311146

Pengujian 11		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p>Nilai P: 295200871080543037774323194024329104799</p> <p>Nilai Q: 260158948462573785460245709821471066307</p> <p>Nilai N: 76799148205549884382980950858417102850158976494485260522958737710529280907293</p> <p>Hex Bytes Pesan: 255044462d312e340a25f6e4fcd0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Perhitungan Putaran ke-: 1</p> <p>Hex Bytes Padding: ffa1d975756f60cf99645725649555f0</p> <p>Hex Bytes Hash Bytes Pesan Padding: 5bd9631869de5889cc6c3ab0c82593a9a75f172211bfe0b3dd63d6b336edc1feeb0c9950eecd3a51fd343988059594f9ceb61dfa3d0aa535ff4e37a9386ed02</p> <p>Nilai Hash Pesan Padding: 58449420563420287140682525457896644676804886655539102774920599689068357883998</p> <p>Nilai Hash Pesan Padding Mod P: 173100412174041192575092299298173258677</p> <p>Nilai Perhitungan Akhir P: 10032241186089224157423434710948023109922607176370386676598584655984482499229229270601899864434540395836505109457844</p> <p>Nilai Hash Pesan Padding Mod Q: 201641898395451522217976019382964693588</p> <p>Nilai Perhitungan Akhir Q: 3799528921501299990135104814647854108867182731359609809005412763530013288285553321003241041985175277025101078096136</p> <p>Nilai Perhitungan Tanda tangan: 15956210611971213894231366964435542495964634176359782076008118456411850292878</p>		

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
18349727642129597242298425400520458173354089838946157748038138021460923023295

Perhitungan Putaran ke-: 2

Hex Bytes Padding: 18415c7a42a431e293631a50280f41cb

Hex Bytes Hash Bytes Pesan Padding:
f268b961bac503b7f9d2d9afa795b98aac6bf9500d94841850d6d5e5718e4b66f9b54bb9bce53c02
d4c61b4b4f255262ed10f5dadd9e6e453f3f32c247558c0e

Nilai Hash Pesan Padding:
56209618541446103940802750930561792946264565869642800062500973546690572598763

Nilai Hash Pesan Padding Mod P: 115670923440625409422075115441792863882

Nilai Perhitungan Akhir P:
67038465570334416596195516596017472232939286453373369276208888663477045887130
87217994387424621458307200322810544104

Nilai Hash Pesan Padding Mod Q: 170610152996813438501516270904682113644

Nilai Perhitungan Akhir Q:
32147991849484431907561532313043625465283431281629849634273783629445171272209
82198361206642900678628040136958683768

Nilai Perhitungan Tanda tangan:
56388914726995637537563877512123016712844897167011153476246746144237082534285

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
20589529664103780442178199927855309903894410624842460460457764163838708308530

Perhitungan Putaran ke-: 3

Hex Bytes Padding: 097e5b101ecabba2f20569950bb77035

Hex Bytes Hash Bytes Pesan Padding:
28e6c566bd0a3818c049fe02b17d8b213beb0ebebcc617873c9bdf8c66b846b075273ff20737f985
41026897fdc9e072e1e333bdc408b9a146e67cfd6e80dcb3

Nilai Hash Pesan Padding:
50369838050312314489811687207375250764337582417938251581864730076028358366324

Nilai Hash Pesan Padding Mod P: 149068444349155895531375671791774817336

Nilai Perhitungan Akhir P:
86394397804335257345471343435728206717532815442142533075424158947695117298650
86153258836604641577247362980250688992

Nilai Hash Pesan Padding Mod Q: 1770287673305795786520960109020941693

Nilai Perhitungan Akhir Q:
33357448365772485574493833875300274149360794768624830685328499094529416093957
701612210763405914389148936543028946

Nilai Perhitungan Tanda tangan:
61926548650898559829543486324512404484883281735027765141875412967154317585068

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
451173000369124543062495063432849022739341160773932068529416000589482581205

Perhitungan Putaran ke-: 4

Hex Bytes Padding: fc6990d284ef7ab27ab51c1c2b84b5e6

Hex Bytes Hash Bytes Pesan Padding:

3be9e7b9bde52f92db503b3683012e883947ba6c92d5a53f65cd9339857747c28fb31f4f08147f7ec
25ec920c4988d9de95b15f060f699d4a14a4122f507fd49

Nilai Hash Pesan Padding:

64403937093628699224957462504785436305725250287907280236804300068574899507133

Nilai Hash Pesan Padding Mod P: 73672580384521547827036296799105961397

Nilai Perhitungan Akhir P:

42697824108930956218457435503885789759569481576040630438099754502935655148790
39235192032246194227021688920887669684

Nilai Hash Pesan Padding Mod Q: 205102348397809202168912163190150654585

Nilai Perhitungan Akhir Q:

38647340200943602043227822170826410345557771771248240499757763907755225365969
35593326345710202874523874474683387370

Nilai Perhitungan Tanda tangan:

67783661480029783512305933230250989055724299715218863544553305122201490490826

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

9016826144658090632231934460828543708782386305020884309614545048285024303335

Perhitungan Putaran ke-: 5

Hex Bytes Padding: 669d8f2bcfe844fced1d0933306967bd

Hex Bytes Hash Bytes Pesan Padding:

5ee28af07e05593e66605eef2fb54261064213026ce14bd7ea14a32500a942b33e6d1f64f9586e510
a5c59b97be853108d02a9c202cf7939efd94f12f791d905

Nilai Hash Pesan Padding:

9393097844486415414165025362902867955191718481063485092289346444143981095718

Nilai Hash Pesan Padding Mod P: 291450627675887301734509897394202158114

Nilai Perhitungan Akhir P:

16891369315410979058558361334459035132449085511700117534990364056810773661267
449847079396932027225304595290829678408

Nilai Hash Pesan Padding Mod Q: 225028052635810371501471470880689926233

Nilai Perhitungan Akhir Q:

42401931391366268333193896281364656958762023859429592955400273537078460014752
27681105634426137595126678299505414826

Nilai Perhitungan Tanda tangan:

31563019837515489766491634567830023629035481363201139924245958163987791582076

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

23401250194611616510747859861392498312701835161909195918258880774421610961159

Perhitungan Putaran ke-: 6

Hex Bytes Padding: 4a9c74b72e5dd41602a151bb1cb40e52

Hex Bytes Hash Bytes Pesan Padding:

cb6a0255df0e69d604222e67938c7b0777575f7b24b7fd992d5c6bd8b45d60eda7e1d88ac365c3af99e3432de57872eaf008d5556e04953636dc777532e60cf4

Nilai Hash Pesan Padding:

72536796914698943536921746299542651308606793784096305867709891553786798410514

Nilai Hash Pesan Padding Mod P: 62976990532760210266553141432475464122

Nilai Perhitungan Akhir P:

3649906723292339787763401668333016367833585243569210962445260476831965544952695378790523416070775417569848015433384

Nilai Hash Pesan Padding Mod Q: 84470260991705719117456133296649395154

Nilai Perhitungan Akhir Q:

1591669202673945039164654302079512882773519972612227852403307179824720880930533038667511693072157996677129735395988

Nilai Perhitungan Tanda tangan:

49789876548003625187716203921203694005502757038497020047329947851133481945218

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

53788341916672383309574514456964260911308679111858835619045388553145884826331

Perhitungan Putaran ke-: 7

Hex Bytes Padding: ed012ada9b202e9b8cbc7de280888625

Hex Bytes Hash Bytes Pesan Padding:

ce701478060e125d2a5d78983b60e0e975b99a36d41b90f458478fa8d3da0dfc4b2506d9016dbefbcb0068b380197c360a38d026913a9ded22ebbd3bfe8ad09

Nilai Hash Pesan Padding:

22795698836988157109317207692871207083588188515982704870941954522576423749847

Nilai Hash Pesan Padding Mod P: 267993323388951791332472092923515597784

Nilai Perhitungan Akhir P:

15531873221632684493151271951674866162177532755888743159612117184493075572571509336684134065072281665385892272535648

Nilai Hash Pesan Padding Mod Q: 198504806396276152886648939431456656795

Nilai Perhitungan Akhir Q:

3740416842736294581465608380676953997722591853861007417492690980830767041602277464678201155163025881177281521784990

Nilai Perhitungan Tanda tangan:

8844714054570017694931091804729365995742907494166257250329721239358069183122

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

54003449368561727273663743165545895766570787978502555652016783187952857157446

Perhitungan Putaran ke-: 8

Hex Bytes Padding: e6f5ade49838a1e37e98ce3c75d91947

Hex Bytes Hash Bytes Pesan Padding:

417a2c635532cea7e6fafd3f403f266105552e79637505ecc2e2581fea4442c4f18a80b52945b30e7

4175a467acc6248a3dfb5e30e9360190a4826c4393e0cfd

Nilai Hash Pesan Padding:

63276883795225901434397535771200995226109915483183067882119835523052135625520

Nilai Hash Pesan Padding Mod P: 274626930056060905602417534859929008184

Nilai Perhitungan Akhir P:

15916331821021670884281695322043022333796164633731681174756932347263271769815
650876410009423544225727313652757204448

Nilai Hash Pesan Padding Mod Q: 240819640204866832805718407574691321787

Nilai Perhitungan Akhir Q:

45377532898915052541352964807000703817603270240578849468296108336620072165257
73869652597241937264535888903351579614

Nilai Perhitungan Tanda tangan:

68099919267269678557438868122137245536239353613429942850022807743285238923133

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

8452064506720602156138804829527248437016156414568791248955637407284455466182

Perhitungan Putaran ke-: 9

Hex Bytes Padding: bde0ed76a05b1b117465e7c6210cfde0

Hex Bytes Hash Bytes Pesan Padding:

38afb56a9551ae7e77db8cfa27581c0b365a07ae1decea625e7f301c62be96f61dbc10e0f45c54e59b
f0e52ca317fc09f3e3e19e1e59b023b989e7dffaac2e4

Nilai Hash Pesan Padding:

40025570429336994506256820302804884177770734174132472815274230733519916879786

Nilai Hash Pesan Padding Mod P: 4635606757642706449834007763192533761

Nilai Perhitungan Akhir P:

26866212767753788434003970127411723668729776193972284241646838634853281888169
7770712643327731783694446815576949092

Nilai Hash Pesan Padding Mod Q: 89011067270549132541105272238253183038

Nilai Perhitungan Akhir Q:

16772314043824636872402092446933801858293677971701933177110001249199020083571
56406806214016362396677503164001569036

Nilai Perhitungan Tanda tangan:

13331861178262472915319037417718992896537919910715523717576545443518818302704

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

13387354149995709465268933132602991745824759531952087606781488185979914450385

Perhitungan Putaran ke-: 10 (**Valid**)

Hex Bytes Padding: c01145ea5e3ee8e75242db7e21e4febc

Hex Bytes Hash Bytes Pesan Padding:

30407e78ff0b1e2c81aca732400335d03540ea64d1b4b142ea53576accb14293aff387ab8e8d28c8e
df1dac5a4dfc0c0b2f8a243633e1208a5c0114265e421df

Nilai Hash Pesan Padding:

680233181313029860998325518657405933420983298759147260845446194385153361475

Nilai Hash Pesan Padding Mod P: 291387823747361217626183671025511927515

Nilai Perhitungan Akhir P:

16887729438703036292879794288074855925128497940165673082875151351574346797582
928372485627329509409011353939741885580

Nilai Hash Pesan Padding Mod Q: 64485513303403903047133394408994036713

Nilai Perhitungan Akhir Q:

12150975306413144177967684057315804468833896302992761450492458201616611420146
14379056796415563598416400660934957386

Nilai Perhitungan Tanda tangan:

48233729749899359574248589179706558421588358169794515211203800584172691526999

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

680233181313029860998325518657405933420983298759147260845446194385153361475

Perhitungan verifikasi tanda tangan

Nilai N:

76799148205549884382980950858417102850158976494485260522958737710529280907293

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: c01145ea5e3ee8e75242db7e21e4febc

Nilai Hash Pesan Padding Mod N:

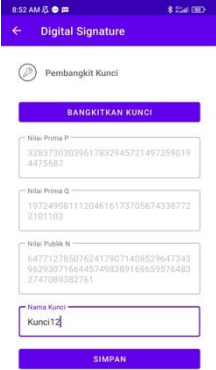
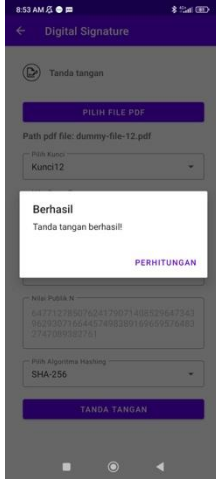
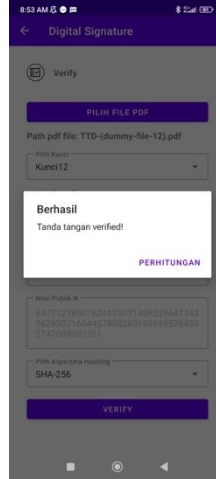
680233181313029860998325518657405933420983298759147260845446194385153361475

Nilai Tanda Tangan:

48233729749899359574248589179706558421588358169794515211203800584172691526999

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

680233181313029860998325518657405933420983298759147260845446194385153361475

Pengujian 12		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p>Nilai P: 328373030396178329457214973590194475687</p> <p>Nilai Q: 197249081112046161737056743387722101103</p> <p>Nilai N:</p> <p>64771278507624179071408529647343962930716644574983891696595764832747089382761</p> <p>Hex Bytes Pesan:</p> <p>255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Perhitungan Putaran ke-: 1</p> <p>Hex Bytes Padding: 59f4ee86604715a3b61eefc21dafd692</p> <p>Hex Bytes Hash Bytes Pesan Padding:</p> <p>bdc2760ea4769b12bc2f18b5eeae28ea18885781afca79f35d7d58ec5d9838319483db4967b4a068ec7fef031f32f2288d4c0170869dd4020a8aa9f645f54ea4</p> <p>Nilai Hash Pesan Padding:</p> <p>22369630109795366442586658406764843756268313809173013226487929276160321892990</p> <p>Nilai Hash Pesan Padding Mod P: 256338560280110500925904848203111671943</p> <p>Nilai Perhitungan Akhir P:</p> <p>7159190474735966487430364620559449244413488066133193565786308521821113059818482268340631925934794405782093851669722</p> <p>Nilai Hash Pesan Padding Mod Q: 164806804774925070982254752139125643185</p> <p>Nilai Perhitungan Akhir Q:</p> <p>6071915534633557075250529934473996869092111444182555391501845802702132802553467786396160449252963366305434496528980</p> <p>Nilai Perhitungan Tanda tangan:</p> <p>56050820726234173546968435133725210291449281179720989262176177385672899828688</p>		

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
59908555328270578759580583713953539821145132951640260419773769597228086930631

Perhitungan Putaran ke-: 2

Hex Bytes Padding: 41553808d6514df877110cba1f3783b1

Hex Bytes Hash Bytes Pesan Padding:

56ccf171a534c71dce6b2b340e4335f1d13189f8145ca5f90370c5beb1feddbd316ac3ccddcbd2c85
06796e2a360d1326e64bd385fbfe61712a7ebaad9ff5c05

Nilai Hash Pesan Padding:

9188875184704321530464416959327474358746787698645684566970465689753468829861

Nilai Hash Pesan Padding Mod P: 69233438275927683861559534298655743197

Nilai Perhitungan Akhir P:

19335966126072535963733720853272453151023703130314453608693677016522036745001
82803074595915633623742686063655451838

Nilai Hash Pesan Padding Mod Q: 50016100008068847762949940083645661880

Nilai Perhitungan Akhir Q:

18427244860157922423115509779096454299731546271216974280071806856564256340461
69196262728381104942708854760291603040

Nilai Perhitungan Tanda tangan:

12845819167763186196462691088061190372503830847915129023424636790833486169682

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

9188875184704321530464416959327474358746787698645684566970465689753468829861

Perhitungan verifikasi tanda tangan

Nilai N:

64771278507624179071408529647343962930716644574983891696595764832747089382761

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: 41553808d6514df877110cba1f3783b1

Nilai Hash Pesan Padding Mod N:


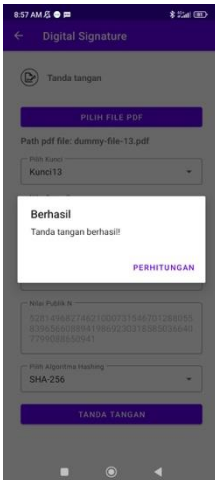
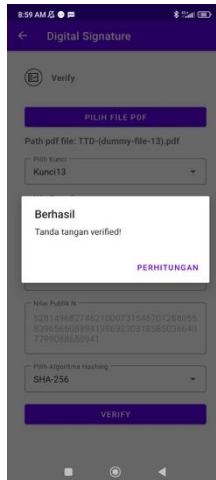
9188875184704321530464416959327474358746787698645684566970465689753468829861

Nilai Tanda Tangan:

12845819167763186196462691088061190372503830847915129023424636790833486169682

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

9188875184704321530464416959327474358746787698645684566970465689753468829861

Pengujian 13		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p>Nilai P: 246729530453647393443053907867624173071</p> <p>Nilai Q: 214060182328046249585461655444675769971</p> <p>Nilai N:</p> <p>52814968274621000731546701288055839656608894198692303185850366407799088650941</p> <p>Hex Bytes Pesan:</p> <p>255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Perhitungan Putaran ke-: 1</p> <p>Hex Bytes Padding: 121cf23200b9bb8c60eb3c9d4274f817</p> <p>Hex Bytes Hash Bytes Pesan Padding:</p> <p>b6cfabb687310a183cf7792122599698c94530ea0c72abb7b9905a8db90418848204160cdd83152445b35000ed22a9631ac494e12f335b660bc7c0b8902e8eda</p> <p>Nilai Hash Pesan Padding:</p> <p>52717291988112058228544404158689274283933577905022884371623483470920542924292</p> <p>Nilai Hash Pesan Padding Mod P: 218392630310383935694844772946180359371</p> <p>Nilai Perhitungan Akhir P:</p> <p>791530038944755573058538094077204129295464989397716436539439486747940083064596146766779012244646527256272829250148</p> <p>Nilai Hash Pesan Padding Mod Q: 126805857707088560841401004413402990819</p> <p>Nilai Perhitungan Akhir Q:</p> <p>6237659290889671480553164395124197513679628296538184027748859686963265652821126895641248284194290850926716774439926</p> <p>Nilai Perhitungan Tanda tangan:</p> <p>37502058091602211376020156269596821771598202692472334193485278881230989970365</p>		

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
 21955471445151661624090358020431552557926084644526946462733871790863488923846

Perhitungan Putaran ke-: 2
 Hex Bytes Padding: c705840a4fcd1a115e1f19d895aedb05
 Hex Bytes Hash Bytes Pesan Padding:
 188038932c4b207db075e173050fa26376d4c76cc488a05b5318e453463b2f0259d78f03ed1ace9a
 93ce6d179de6840c457117f96d9e0620138a87104d471bd2
 Nilai Hash Pesan Padding:
 22336951709261729706366621946542286675594489876752123490562851242264351292781
 Nilai Hash Pesan Padding Mod P: 140849376745404291470398305088172441239
 Nilai Perhitungan Akhir P:
 51048660617433640893044342337063657854416330009507406760483298953013494820222
 0323294956726373404557027380762908532
 Nilai Hash Pesan Padding Mod Q: 97018004520181972529533590184790461387
 Nilai Perhitungan Akhir Q:
 47723761995031239484524372831307639012259604859969882595213734112607344487532
 28488234461382113141915335254584700998
 Nilai Perhitungan Tanda tangan:
 2718421117912861568722707562426803579219292254435846761303768772188037470695
 Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
 30478016565359271025180079341513552981014404321940179695287515165534737358160

Perhitungan Putaran ke-: 3
 Hex Bytes Padding: 769564eaf45c5862af28a0f3448e11bf
 Hex Bytes Hash Bytes Pesan Padding:
 84b032ef35234ab14e2188d11e86ad7b91cb3d3295c55140b703462790a06a2a8a658ff292f1bdbc
 31b37f8c46f95cbcf79043258a8943f9466c9a450e62b71f
 Nilai Hash Pesan Padding:
 37053273441767081401443712897477710287440587478622991558304973638930355647978
 Nilai Hash Pesan Padding Mod P: 195762343073862679190543703174260090292
 Nilai Perhitungan Akhir P:
 70951009114616456322426055492444529808195881429627156697945351993549085743928
 7290249149152735938552776375805971696
 Nilai Hash Pesan Padding Mod Q: 103893372884781868179590038451296293613
 Nilai Perhitungan Akhir Q:
 51105798608576268812975592765593682353527205737726689236300965324536725992758
 63721477070069256538990747875176569002
 Nilai Perhitungan Tanda tangan:
 27304626203717221344087066870306751176330485951143546756410103305927468275194
 Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
 36654312591553406983425051723091401066423814606855305678118439732955718726612

Perhitungan Putaran ke-: 4

Hex Bytes Padding: df66b6d7e1e0a9070267c5b9bbd9d8bd

Hex Bytes Hash Bytes Pesan Padding:

908fc58dc4435e5be7fb72182db8b8e104aa50843254789da69a57adf23bfb7313356ef245d4e06f456e41a6254f51cc3c0b5d03a9ac69f75600fbd188bffbfb

Nilai Hash Pesan Padding:

18731206803668310837705524352979381078890280759106417377449263279196411345987

Nilai Hash Pesan Padding Mod P: 3312151881520082028839203090868378130

Nilai Perhitungan Akhir P:

12004378096662739286217950782199102638419789171659543249751198030782563907743850682182597408979753910319524540440

Nilai Hash Pesan Padding Mod Q: 116805313365556358292910678783847466245

Nilai Perhitungan Akhir Q:

5745726272542796026857344970043603564721277531631163033363405007394492418697180144020830323536673704122574078000730

Nilai Perhitungan Tanda tangan:

14212010096549039822264991956578356788550423388183550943283902348094057869513

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

11156279803733339420129743096509708101398327533351623135442740944580794627400

Perhitungan Putaran ke-: 5

Hex Bytes Padding: e5abc2628c5b8b666507c69f9fb08be9

Hex Bytes Hash Bytes Pesan Padding:

97792fc26ac8af128d6f9fe81771e2f40d4d9c7c915f3fe2d05920bd826b3a1e6822228732ba37cbcd0cae27913889763f68fc715ea500d38524d2c6676874ef

Nilai Hash Pesan Padding:

39226147572181672138638159543035008010053325712385798403161133684661475118535

Nilai Hash Pesan Padding Mod P: 161589460789420744717450008541710240864

Nilai Perhitungan Akhir P:

585655807203448675397943830677223243135593511726715798148818726203205643851884391252540040644236448752360686588032

Nilai Hash Pesan Padding Mod Q: 204016895525550633301500741935842444687

Nilai Perhitungan Akhir Q:

10035718435129354067402694290792372707057032513342401878780117908394782162830320172400143344015132951573617069789198

Nilai Perhitungan Tanda tangan:

283425154725804899471586054704176952378279116191770645080841217366924354973

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

13588820702439328592908541745020831646555568486306504782689232723137613532406

Perhitungan Putaran ke-: 6

Hex Bytes Padding: a41d202263a928374d8390bebd801819

Hex Bytes Hash Bytes Pesan Padding:

338f045aaebe54283e7521be6425d7f7ff67e32130fe5fa01e05b9b0f0ed2e724c34a8b23f0f2bc33183ac5620a3b137f76b4bd1af0527301c70aa24f5ae844d

Nilai Hash Pesan Padding:

3379274771729175114650293857318358489146745470848174086667544729014060597258

Nilai Hash Pesan Padding Mod P: 44784301795312207124490987559010147447

Nilai Perhitungan Akhir P:

162313719532465848998718375619111459929441458386569262064645470874297513840202249939073030747181826184752971278836

Nilai Hash Pesan Padding Mod Q: 156890918232983328529870431759386558742

Nilai Perhitungan Akhir Q:

7717562196793325344542708735169482120776470104597105750949357235457765051426438575025024913496975881894018164214668

Nilai Perhitungan Tanda tangan:

21278193428014825251803534052711307040743082457267688410217406324515355613098

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

3379274771729175114650293857318358489146745470848174086667544729014060597258

Perhitungan verifikasi tanda tangan

Nilai N:

52814968274621000731546701288055839656608894198692303185850366407799088650941

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...

Hex Bytes Padding: a41d202263a928374d8390bebd801819

Nilai Hash Pesan Padding Mod N:


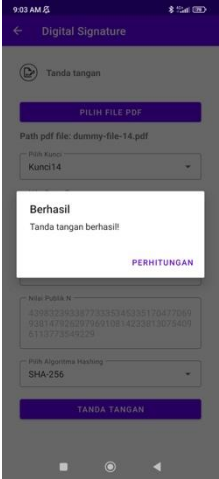
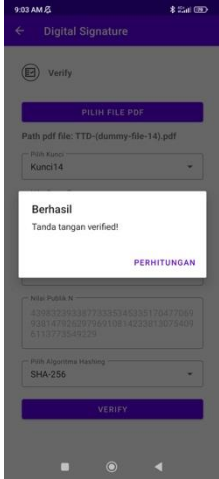
3379274771729175114650293857318358489146745470848174086667544729014060597258

Nilai Tanda Tangan:

21278193428014825251803534052711307040743082457267688410217406324515355613098

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

3379274771729175114650293857318358489146745470848174086667544729014060597258

Pengujian 14		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p> Nilai P: 242438499664385996569520093294156779451 Nilai Q: 181420192748513509763478611843031402679 Nilai N: 43983239338773335345335170477069938147926297969108142338130754096113773549229 Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670 a2f5061676573203220... </p> <p> Perhitungan Putaran ke-: 1 Hex Bytes Padding: 1c437acb802d895d7a48c5ed852f2b97 Hex Bytes Hash Bytes Pesan Padding: f17392138d32f4947ff978d1aa3643ceea0e12c3b42deba0f8e87cefd7d73f3020ffde1a88d92f4ffbf 5b248bade94f864578d68180d92b5f41cea2d026fd01c Nilai Hash Pesan Padding: 18499210276020698290678758504314847393120683884808401788561193289113568175262 Nilai Hash Pesan Padding Mod P: 28185760436591630334283126241931977695 Nilai Perhitungan Akhir P: 77218395215219458546889961705430912666397238111304907813158659406742682601112 761304894343517510276599888160825790 Nilai Hash Pesan Padding Mod Q: 122578433417654381328473625887713369528 Nilai Perhitungan Akhir Q: 50555777155448851552923935575784726652080945567074700243765575444683789124223 59272197145238339232973939410737592224 Nilai Perhitungan Tanda tangan: 11973274365031480558425123046626860247393901016883135414884715550354130729672 </p>		

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
19450029840861567264342795442585935371162311139764577978378953564051183757912

Perhitungan Putaran ke-: 2

Hex Bytes Padding: 25579845542f9f09d0ffd50dca413916

Hex Bytes Hash Bytes Pesan Padding:
6b5063a99add62275699daa3a928ef2952dd1703b7a7bf92bc74844c1d8ef771ba15d90fd0c2ad43
55798f9e9c5bc0a23187b22d5484405a1b6083af157e61ef

Nilai Hash Pesan Padding:
22215149983581872418224137520131237066611319965638022108667765178564873124020

Nilai Hash Pesan Padding Mod P: 75456468317536681756617623312006864723

Nilai Perhitungan Akhir P:
20672237689652411778859206845881619869264843200034790846215288095284093746205
5148019315064347079873664470573732006

Nilai Hash Pesan Padding Mod Q: 65710905706585037837177798035347714454

Nilai Perhitungan Akhir Q:
27101552964588339080481146940412262329906935074421529325979729888643394266333
05077867362915955797736627500017938632

Nilai Perhitungan Tanda tangan:
36470516496509453079152372861419092971144023662220711258258759036175751266558

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
15336298329227755780584172268812649518884019013502432453061004206098150973003

Perhitungan Putaran ke-: 3

Hex Bytes Padding: ca761c971501dd892a504ed4100629eb

Hex Bytes Hash Bytes Pesan Padding:
bdd01f4a12007959f025783a21526ea999ffcc57e713094c96070626d26295d34eb725152b39ae1b
3047ec93dbab96ecf858d2a5359e0439132def9b174c7a0a

Nilai Hash Pesan Padding:
13271404804145535890275969405186725615184201076397971624114209519501073564236

Nilai Hash Pesan Padding Mod P: 67378658029135811706235485835810099241

Nilai Perhitungan Akhir P:
18459221125041561621169808816190168105206070235952624203066903082897651084437
4515528570762659646685724203744786002

Nilai Hash Pesan Padding Mod Q: 143748540041075836272278825743396437528

Nilai Perhitungan Akhir Q:
59287094426930971917563409874559366228573518099684377214440521933938094847962
09215168899333132402390095639568136224

Nilai Perhitungan Tanda tangan:
18416800892473001709843824020323013635665956644390048142076677627266841685320

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
30711834534627799455059201071883212532742096892710170714016544576612699984993

Perhitungan Putaran ke-: 4

Hex Bytes Padding: fb3e40b222611ee18e2477b096942f62

Hex Bytes Hash Bytes Pesan Padding:

4b0227a3bc7b747f744450638308d79c513a01403f17c4c552c9817dcb930353e294d78914f6923
2da7cceedcd389bca29cc008b7cc63420ae4a461d5febebbc4

Nilai Hash Pesan Padding:

10782383340342314043250953191550520745491010473240651008613079665315960273069

Nilai Hash Pesan Padding Mod P: 7599401454547113611303281643500536720

Nilai Perhitungan Akhir P:

20819505162419282987647389624507273022503939790743942363216856077232106306358
710871572203143655182117201160791840

Nilai Hash Pesan Padding Mod Q: 57862363684575473560713988234457206596

Nilai Perhitungan Akhir Q:

23864530509684425792855336643674599600977732343712332436693866740034103868656
62526691219686171950293954988944654768

Nilai Perhitungan Tanda tangan:

1306689672370507032476414056530565411057944792615753474037586622820840259481

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

26009631571984862797151959656253753474456185530462757142645406326396975333511

Perhitungan Putaran ke-: 5 (**Valid**)

Hex Bytes Padding: 995c3c58fa65cd3443b33e938867b7cc

Hex Bytes Hash Bytes Pesan Padding:

4e5a45deec5c919d75707cd722ebc1bde0630b22249a2e90d863c0ceda3042e59ec941a2033925c4
13b49ced4f7ccc0a2528caa272b79949b1f70ca04d9bb1c2

Nilai Hash Pesan Padding:

31345287763941765740249841479521005795364351991848033476276068968727185425166

Nilai Hash Pesan Padding Mod P: 181981458015176815100609819505579264943

Nilai Perhitungan Akhir P:

49856083104341710554621369816978213858349985174412701889639116350560028049089
8311655793521957342673112420068970846

Nilai Hash Pesan Padding Mod Q: 131366603931270353213092553230844262175

Nilai Perhitungan Akhir Q:

54180336367889122480271944437683411204900580774652178987481601317909753547754
29227916624066833473341330537803634900

Nilai Perhitungan Tanda tangan:

22284889311342317711105908655031383742302932217333147030425585977638777414749

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

31345287763941765740249841479521005795364351991848033476276068968727185425166

Perhitungan verifikasi tanda tangan

Nilai N:

43983239338773335345335170477069938147926297969108142338130754096113773549229

Hex Bytes Pesan:
255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...

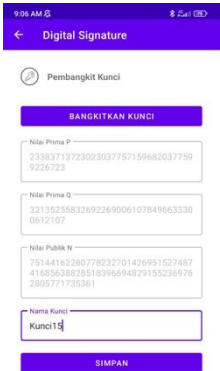
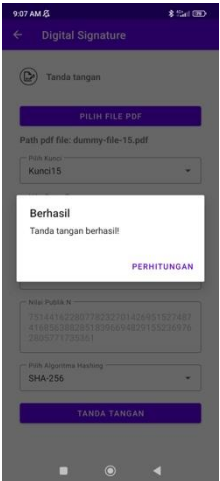
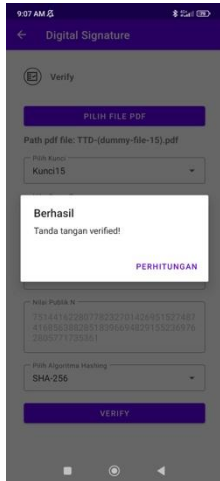
Hex Bytes Padding: 995c3c58fa65cd3443b33e938867b7cc

Nilai Hash Pesan Padding Mod N:
31345287763941765740249841479521005795364351991848033476276068968727185425166

Nilai Tanda Tangan:
22284889311342317711105908655031383742302932217333147030425585977638777414749

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
31345287763941765740249841479521005795364351991848033476276068968727185425166

Pengujian 15

Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		

Perhitungan tanda tangan

Nilai P: 233837137230230377571596820377599226723

Nilai Q: 321352558326922690061078496633300612107

Nilai N:
75144162280778232701426951527487416856388285183966948291552369762805771735361

Hex Bytes Pesan:
255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...

Perhitungan Putaran ke-: 1

Hex Bytes Padding: 28202a31c8bb2abb05ddbd5d4b617dfb

Hex Bytes Hash Bytes Pesan Padding:
9db8d0104504eb712e7efcf74039e0efdccf93c82eaa1396b4226e1ac77e441bd8fba54623650cbc70078fda5aefa7e518254542214ee27204d157d7a89e6f9

Nilai Hash Pesan Padding:
22847943087231856121886834035136365975672882803599210023552020315352075919444

Nilai Hash Pesan Padding Mod P: 1866167313493614863942539323866671705

Nilai Perhitungan Akhir P:
20205581679286407580220573516435582703289101020522681656542690352104767367451
652001994205026347012462770762454340

Nilai Hash Pesan Padding Mod Q: 311679078979722613361744181078428823102

Nilai Perhitungan Akhir Q:
20046215667671553753439874305242395017617681604286000995817499949390069074110
782778599045551693297897665414565689028

Nilai Perhitungan Tanda tangan:
3880495148168683347183475761732774691372684425613068975949796594352887630479

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
59650566771686372657558091125786485565412297824690336569152648766164676506662

Perhitungan Putaran ke-: 2 (**Valid**)

Hex Bytes Padding: bd4f243b39b31d4911014f663b97a25d

Hex Bytes Hash Bytes Pesan Padding:
05f1421a9e5b356f1534dd3b19c4b3dfabcaead95a66cba96bd6d561cd19ff5cca92191979489d62c
cdca313fa4fa41652697ea0b85178603185d9d8003e6f66

Nilai Hash Pesan Padding:
28785142310176048226429339279442061746037888342849192372966107240394946006685

Nilai Hash Pesan Padding Mod P: 182517011138550681475224845213190172172

Nilai Perhitungan Akhir P:
19761692050619184446373253046245128272601564256393496348196569076122981744607
42173753624173638846874738682516974256

Nilai Hash Pesan Padding Mod Q: 176821062558991157389561429072140614710

Nilai Perhitungan Akhir Q:
11372573245042817147144558005413667304629227257124138955625608117359150813083
822874009674835470608518625227585193940

Nilai Perhitungan Tanda tangan:
36980153434914179029247564978084558572499222842440965641969105094929747992147

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
28785142310176048226429339279442061746037888342849192372966107240394946006685

Perhitungan verifikasi tanda tangan

Nilai N:
75144162280778232701426951527487416856388285183966948291552369762805771735361

Hex Bytes Pesan:
255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: bd4f243b39b31d4911014f663b97a25d

Nilai Hash Pesan Padding Mod N:

28785142310176048226429339279442061746037888342849192372966107240394946006685

Nilai Tanda Tangan:

36980153434914179029247564978084558572499222842440965641969105094929747992147

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

28785142310176048226429339279442061746037888342849192372966107240394946006685

Pengujian 16

Bangkitkan kunci

Tanda tangan

Verifikasi tanda tangan

Perhitungan tanda tangan

Nilai P: 192062250206247680065941706428848201263

Nilai Q: 303936179578314814254254898761234621731

Nilai N:

58374666568901326360137147006034860593601417134552597781268447528459561446253

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...

Perhitungan Putaran ke-: 1

Hex Bytes Padding: da57c665a1ffe2284aba73acb7498f90

Hex Bytes Hash Bytes Pesan Padding:

39adfd52107223f830f4cb6fdfe4dfe7c5e910d7cdbe5c98a039f64a6f63dde4881d58ebcd3589ca9b7563ef4aa17c9fead68b24f14de923cd7b2a5cc69bb39d

Nilai Hash Pesan Padding:

9797552454413423498840147124688539360909390201372230678949288520649806217300

Nilai Hash Pesan Padding Mod P: 157775923815182310686665606955043385946

Nilai Perhitungan Akhir P:

48370733448318610747392327888799918417618969767336284342167778764453437296580

64902705621549984213239521642163528112

Nilai Hash Pesan Padding Mod Q: 207344827378377257824769407968188066294

Nilai Perhitungan Akhir Q:

57469349475762442062193527624211903966368113477546238188303733148481342659617
98611796688168743287773176555443329508

Nilai Perhitungan Tanda tangan:

17680177200529361595277841151495569378818922959677364846585044608026428286606

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

36655873471877348828711966328546601179815419810698906350663883877915372840615

Perhitungan Putaran ke-: 2 (**Valid**)

Hex Bytes Padding: d6bbf9597e8f48a54d4b37e66c049480

Hex Bytes Hash Bytes Pesan Padding:

607de3f24e505711062ef4d26475e4e4158c9964c473d9e3b50c7a384577d6d27886ca07e8541847
aa4740fb926d5841d43255b3c24db0b9334cd61b0af62866

Nilai Hash Pesan Padding:

37916492905448849870889296357548727935667017397877099365254475491100216269111

Nilai Hash Pesan Padding Mod P: 108349273689559656930701616232292621736

Nilai Perhitungan Akhir P:

33217576612613003382510584564427149861656882479925259945117742114910933854765
18339706657379331593967296085558604992

Nilai Hash Pesan Padding Mod Q: 75344094386464669164387637707539648496

Nilai Perhitungan Akhir Q:

20882971357317382464678587367028297307134079710280201779970700386023621350929
90985348157992432950258876037527002272

Nilai Perhitungan Tanda tangan:

54695143323617189956236097817515092995364583937841709613993422269722731894400

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

37916492905448849870889296357548727935667017397877099365254475491100216269111

Perhitungan verifikasi tanda tangan

Nilai N:

58374666568901326360137147006034860593601417134552597781268447528459561446253

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: d6bbf9597e8f48a54d4b37e66c049480

Nilai Hash Pesan Padding Mod N:

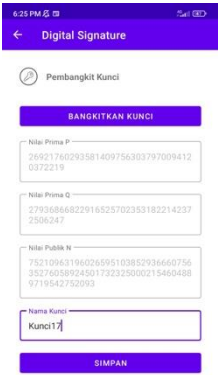
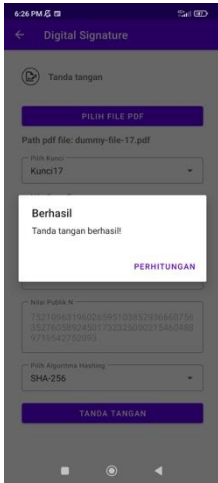
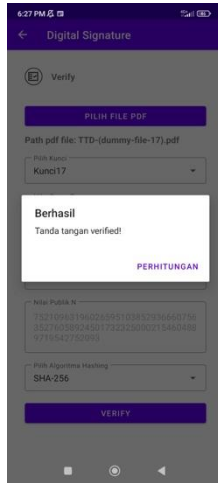
37916492905448849870889296357548727935667017397877099365254475491100216269111

Nilai Tanda Tangan:

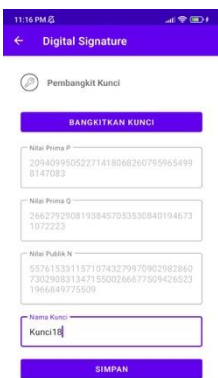
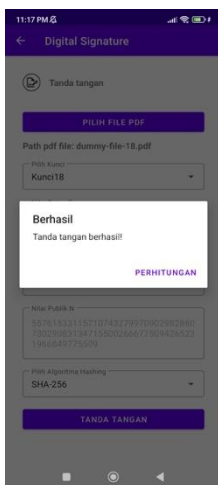
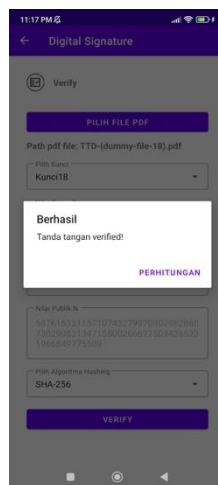
54695143323617189956236097817515092995364583937841709613993422269722731894400

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

37916492905448849870889296357548727935667017397877099365254475491100216269111

Pengujian 17		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p>Nilai P: 269217602935814097563037970094120372219</p> <p>Nilai Q: 279368668229165257023531822142372506247</p> <p>Nilai N: 75210963196026595103852936660756352760589245017323250002154604889719542752093</p> <p>Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Perhitungan Putaran ke-: 1 (Valid)</p> <p>Hex Bytes Padding: b2236ccedbec8806178c44c67388e271</p> <p>Hex Bytes Hash Bytes Pesan Padding: 32ffa98a2a6b290bea87f00d9d630c608ecbdf77cc9de3995896dae0e7b51a13db99bc2a2482c3d68b8ee1001787df5ade2acd964dca588b0a7c80359ba85b</p> <p>Nilai Hash Pesan Padding: 11921854233752886750396810547874155376056603461600725994984866774654316389327</p> <p>Nilai Hash Pesan Padding Mod P: 84970552683585505536480988202334768281</p> <p>Nilai Perhitungan Akhir P: 3723699347126418763435804620978432447498022480871819787295935670506273774109916061790347082505838468581344943657669</p> <p>Nilai Hash Pesan Padding Mod Q: 93135104961131991825016574984049740708</p> <p>Nilai Perhitungan Akhir Q: 2923283084460911405973410374309463852730582148716271411668557634025605405732676368374744461017549347490493151698660</p> <p>Nilai Perhitungan Tanda tangan:</p>		

56561274255635169476985445873979375735823797998196160654359237178979206023095
Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N: 11921854233752886750396810547874155376056603461600725994984866774654316389327
Perhitungan verifikasi tanda tangan
Nilai N: 75210963196026595103852936660756352760589245017323250002154604889719542752093 Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220... Hex Bytes Padding: b2236ccdbec8806178c44c67388e271 Nilai Hash Pesan Padding Mod N: 11921854233752886750396810547874155376056603461600725994984866774654316389327 Nilai Tanda Tangan: 56561274255635169476985445873979375735823797998196160654359237178979206023095 Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N: 11921854233752886750396810547874155376056603461600725994984866774654316389327

Pengujian 18		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
Nilai P: 209409950522714180682607959654998147083 Nilai Q: 266279290819384570535308401946731072223 Nilai N: 55761533115710743279970902982860730290831347155002666775094265231966849775509		

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...

Perhitungan Putaran ke-: 1

Hex Bytes Padding: 06b7bad29ac494c145c5e48e91512560

Hex Bytes Hash Bytes Pesan Padding:

6ab2b2debf2e0da4b269195773a2303d61d549976f8694745f9284f531ca45acc673daa4f2a3c0bfc038946ce633e712cf6a3dee0227fbde2061958aeab22f5a

Nilai Hash Pesan Padding:

34319602487626131682464255538486758606840817495693674668523819305104746302374

Nilai Hash Pesan Padding Mod P: 64930945976006228579406761270255023614

Nilai Perhitungan Akhir P:

2468302874744597751484359099683634033170190377743010845208426650147634944160931574511700015320135132108607295296996

Nilai Hash Pesan Padding Mod Q: 160642238864686562346546779081592099371

Nilai Perhitungan Akhir Q:

2850959182407514073722439194699256887588654552125981198228625633540503637600941387488874878446209087944997561843416

Nilai Perhitungan Tanda tangan:

37612595969902529552145366737518145498698071362358737934802493215108313512921

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

51420111070870303743163160406819689625097427402744695337666904884325811762096

Perhitungan Putaran ke-: 2

Hex Bytes Padding: 75d5bd394d350c263cfd9db43f94020b

Hex Bytes Hash Bytes Pesan Padding:

5d87304d0532b685057298bfbfdc1b98e19a06b38de1bb56da7d38a571279fb0c4e24615f3628219515ab580c6277a595c88221e08887853d8c52787a5f2fd15

Nilai Hash Pesan Padding:

28150063760109722332719321570696007688177351702031005190860231238294977799377

Nilai Hash Pesan Padding Mod P: 116084149771944661319097099850410444401

Nilai Perhitungan Akhir P:

4412854861228334481044122305094241900305675455811360538131932707954187555871380810794766564728953031856373626919214

Nilai Hash Pesan Padding Mod Q: 21704914562757497026181884216375446421

Nilai Perhitungan Akhir Q:

385202708287620183077851410492159156932281368927120623916090899217381665485344549280518752328461491697048165650216

Nilai Perhitungan Tanda tangan:

30020638409361556448574036571376185839641397695353271477427805561599330209560

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

43531920926203942658177461369103953524502440738843717855391226108073179519812

Perhitungan Putaran ke-: 3

Hex Bytes Padding: f3850bc9bdbc0207ea4f97b44a14f6ea

Hex Bytes Hash Bytes Pesan Padding:

8901449f0455cfd937b59eca081ac09719d12d0bf30dbca2d946e11cd050886373942f1f9e6430ae430b1218f3b22b49b6271abc4a7541343f3328300f398475

Nilai Hash Pesan Padding:

6641375700057399606143154707016647892502617075422520760469774541114643215838

Nilai Hash Pesan Padding Mod P: 207235377029015387858016524128155331181

Nilai Perhitungan Akhir P:

7877902734676310683868288841469732480516890129976667181528042029410864027092338359623578125125730635220081229862134

Nilai Hash Pesan Padding Mod Q: 113328533289722270937650484288660781799

Nilai Perhitungan Akhir Q:

2011270665140948979061723447205782059577406905079470868862450953618938577165968614503186300889323711275864404574904

Nilai Perhitungan Tanda tangan:

3776587782277497000589219119625192138422213328268863152990846872794041599928

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

49120157415653343673827748275844082398328730079580146014624490690852206559671

Perhitungan Putaran ke-: 4

Hex Bytes Padding: 8b367c3d02a179041d8a856c1afae5c7

Hex Bytes Hash Bytes Pesan Padding:

dffca3c02fee2d7fad7d319bc4e48bfc4695ee9ffef9f62b64c8685fe7020368b632382dbed93c132f8a5be252ee1b5244308c7f8bcaebea2e72517e47533700

Nilai Hash Pesan Padding:

12343628455729976645995069749569631245259139229603529128016930663642141878822

Nilai Hash Pesan Padding Mod P: 196041225578003237975569264666788315999

Nilai Perhitungan Akhir P:

7452365176405252217108917926251539829352025865115296000229628738643419450086157788306283316378229261235229034766386

Nilai Hash Pesan Padding Mod Q: 230141737676397492306899025564694286413

Nilai Perhitungan Akhir Q:

4084384685626916000215202930303104918670382989514516902079992933098834361986075837500800353636111287996280954147048

Nilai Perhitungan Tanda tangan:

43796796266333187576543972145062447414393522805661876894693036709425129147056

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

52413871133823623648273752999632207060598264926330392543110995591099602216192

Perhitungan Putaran ke-: 5

Hex Bytes Padding: f06495c2aabc3ed2fd9bcd3b184b8ea2

Hex Bytes Hash Bytes Pesan Padding:

525f3c1cca5513147d391d17e3d2a778990eb1ecfa73150ba90d478eaaedf0633793a1b2846fe88e260b5e7f86a32f9a42ddf895ebda0253f4f56a76ca295bf1

Nilai Hash Pesan Padding:

38472768411953254502546740058277546828136215512155062209785251749987960780610

Nilai Hash Pesan Padding Mod P: 207804582493154013089867732539785525333

Nilai Perhitungan Akhir P:

7899540668058228103190921781231161141298654662087773587734613163983721598904876225906180737204995089491642922135462

Nilai Hash Pesan Padding Mod Q: 120415715682212505198736051826911657868

Nilai Perhitungan Akhir Q:

2137048716181972804978784755315152742934829952521723575104041367868846365778611717190287152480882064291678691205728

Nilai Perhitungan Tanda tangan:

52468127219610384240710753354793290729770053973301208042283335482894463975915

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

47070487031835752913774945073032113291988838616118233398248048306029872657056

Perhitungan Putaran ke-: 6

Hex Bytes Padding: effdf182fc1550ed5ee67d4469f85c21

Hex Bytes Hash Bytes Pesan Padding:

02504555d492538771246a03a5a1c1941996de3241e3ebe3b802e4beb67dfbd528370c79f1c4e83a61b80ca2bb6cc76651f683784a4604417c6f34454827440c

Nilai Hash Pesan Padding:

36997086536518587946013021310883142362641553423261492238677336243668043903116

Nilai Hash Pesan Padding Mod P: 82103548662291882989487484948986859862

Nilai Perhitungan Akhir P:

3121106925883309232727449115070492567701770018046691131004540608554150896330855659109977248671497529345340902489268

Nilai Hash Pesan Padding Mod Q: 238939576728925005814610219573022216711

Nilai Perhitungan Akhir Q:

4240522200949235692980565288275155700246183418791119435427375819810548732541638134424582146468176037378771251760056

Nilai Perhitungan Tanda tangan:

11389429007104678219168069880841246045397544511989099935691940190861406725464

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

49436240484210892826095015426681383186738766610433613780303979902400692109292

Perhitungan Putaran ke-: 7

Hex Bytes Padding: 3781544abda3df81189611ce2a3511f5

Hex Bytes Hash Bytes Pesan Padding:

f2700f3213c29201e4868dffafa23a54b7a3624287526548064a483299b1da0f2edf8f8fb1988b64aa

a22d6005feb7a40b96a984231b846c68f78a32a1199583

Nilai Hash Pesan Padding:

29399710794689490616792821534445116310925179482019297539268298992271655026953

Nilai Hash Pesan Padding Mod P: 91090786490630144380282300381379090378

Nilai Perhitungan Akhir P:

34627502614955462455094122901655288915420812179259879714373705694171369163619
31350511827763750984166101211722638092

Nilai Hash Pesan Padding Mod Q: 245311955244176985974948975324987139423

Nilai Perhitungan Akhir Q:

43536144435015627551148574297278131716832819957254397608502962333049134321032
83525370524028960415328912372816614008

Nilai Perhitungan Tanda tangan:

21245082667997587621429484062598149833815831471833958126624069118253263947602

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

39735045802392756000850301093500439849638508219705268920622388901258078961561

Perhitungan Putaran ke-: 8 (**Valid**)

Hex Bytes Padding: 13907435b3a5edaa732047ef692eaa98

Hex Bytes Hash Bytes Pesan Padding:

be694cc98f2ecbd2484d69d92498fda8984aabd08d05748c005a5cbec3c97acc24747de8a04bf6d9d
548337eaf4c96cc2a5317adc68fd44e9fdb6800d3e8b61f

Nilai Hash Pesan Padding:

36041348876505995529558395057898336611923014605985553801358937108622961997311

Nilai Hash Pesan Padding Mod P: 80822310272989309509127310956684946197

Nilai Perhitungan Akhir P:

30724015766540325605944607907103982799894956186933770987068758565162473120321
75777457583622443478673387541720593958

Nilai Hash Pesan Padding Mod Q: 231082949689115215453309633346661885001

Nilai Perhitungan Akhir Q:

41010886176015575960519650009068338603327575459491416438013949608987573777191
56506885742336668737420035556240477896

Nilai Perhitungan Tanda tangan:

11251174822232721109179807745705024696498546150560272357539044878007014538908

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

36041348876505995529558395057898336611923014605985553801358937108622961997311

Perhitungan verifikasi tanda tangan

Nilai N:

55761533115710743279970902982860730290831347155002666775094265231966849775509

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: 13907435b3a5edaa732047ef692eaa98

Nilai Hash Pesan Padding Mod N:
36041348876505995529558395057898336611923014605985553801358937108622961997311

Nilai Tanda Tangan:
11251174822232721109179807745705024696498546150560272357539044878007014538908

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:
36041348876505995529558395057898336611923014605985553801358937108622961997311

Pengujian 19

Bangkitkan kunci

Tanda tangan

Verifikasi tanda tangan

Perhitungan tanda tangan

Nilai P: 283821376760357508868802997503452069223

Nilai Q: 335603508105984298370236149998002392547

Nilai N:

95251449716246264788932336348449889341436020166723931805655375203291863280981

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...

Perhitungan Putaran ke-: 1

Hex Bytes Padding: 9e5f2c7231ff57745058d56383b35f81

Hex Bytes Hash Bytes Pesan Padding:

3022ef56f3f69a838164979ec5a8c5b8f23ad742396554f02b638d7e451dc0324567f30e1c346e81b8361140a59f230ea93db6511dc29cdd421b6418bfe444b9

Nilai Hash Pesan Padding:

42221572449839929849222960579786293610014494542782871899241702419176358024171

Nilai Hash Pesan Padding Mod P: 134761988048660288615988307918725768913

Nilai Perhitungan Akhir P:

11768050887503117136351948272994100773689791300846103615976394162897149205386

092998015392734368459746088190894306820

Nilai Hash Pesan Padding Mod Q: 243548598609737124732310558269617253664

Nilai Perhitungan Akhir Q:

19305475022257526648906414135927680640825294431360557507416811991596477645237
49295849245915596440748784899242753088

Nilai Perhitungan Tanda tangan:

92529219908655990606507663807595640513517190797473633927077916075026937482525

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

26219450565492786447789741367395756147924992256469026820942940226794970956528

Perhitungan Putaran ke-: 2 (**Valid**)

Hex Bytes Padding: 93968ef8a27b96b0d4c0e52f99017056

Hex Bytes Hash Bytes Pesan Padding:

29b1fd13b41174bd4719debd0f0fc7d1b878bf98325b591fb17b41473e3f4883426c2299378506bc
154c2355884cea6846e0065387143ff7a2d480d61460b4bd

Nilai Hash Pesan Padding:

87780289171785721216581614112206713122774305631495559704815878434888991365749

Nilai Hash Pesan Padding Mod P: 273699527801212597584431459275097530415

Nilai Perhitungan Akhir P:

23900730596874450548699058708857052383455002055853871225560067902031241077278
688375572484962539416352433379109103100

Nilai Hash Pesan Padding Mod Q: 119563958700626001596230950439855079338

Nilai Perhitungan Akhir Q:

94775294599657855255180724156411541167226035805261888256445784556146282185169
9018944927951093171945606552985508596

Nilai Perhitungan Tanda tangan:

83567760977702585995721006439460273794356513847950934080230214794510354097685

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

87780289171785721216581614112206713122774305631495559704815878434888991365749

Perhitungan verifikasi tanda tangan

Nilai N:

95251449716246264788932336348449889341436020166723931805655375203291863280981

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: 93968ef8a27b96b0d4c0e52f99017056

Nilai Hash Pesan Padding Mod N:

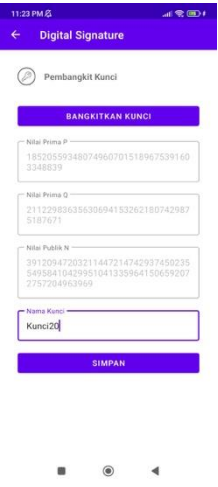
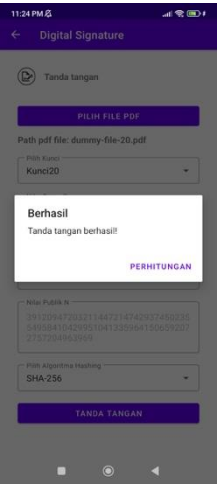
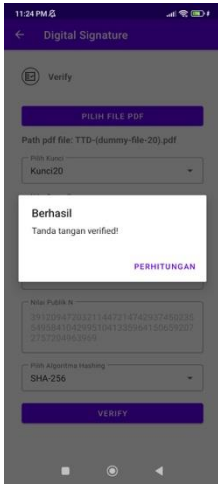
87780289171785721216581614112206713122774305631495559704815878434888991365749

Nilai Tanda Tangan:

83567760977702585995721006439460273794356513847950934080230214794510354097685

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

87780289171785721216581614112206713122774305631495559704815878434888991365749

Pengujian 20		
Bangkitkan kunci	Tanda tangan	Verifikasi tanda tangan
		
Perhitungan tanda tangan		
<p>Nilai P: 185205593480749607015189675391603348839</p> <p>Nilai Q: 211229836356306941532621807429875187671</p> <p>Nilai N: 39120947203211447214742937450235549584104299510413359641506592072757204963969</p> <p>Hex Bytes Pesan: 255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670a2f5061676573203220...</p> <p>Perhitungan Putaran ke-: 1</p> <p>Hex Bytes Padding: c631df5a0170e95b3754807e28433b55</p> <p>Hex Bytes Hash Bytes Pesan Padding: 0005469be3ab560162349eb700e9cb9810a655b815d690f330989e8f98ac8bbba50463ad141a8db34029094d76761a10c5f5390ce7f1d8cbd55cc264c42fb65c</p> <p>Nilai Hash Pesan Padding: 22143840141629506956644597921730299685621526262899825055375305792656715478954</p> <p>Nilai Hash Pesan Padding Mod P: 107553826748490760995420092570484923832</p> <p>Nilai Perhitungan Akhir P: 3652858863045881055459737678835249460366166495486883871035534566489682887372052027284048594100707846028879718648992</p> <p>Nilai Hash Pesan Padding Mod Q: 155133055192106745337637026446001120614</p> <p>Nilai Perhitungan Akhir Q: 800156215494336069771175217559157538853187082599349607058311778806144925889925922318065094231050821120769889179396</p> <p>Nilai Perhitungan Tanda tangan:</p>		

31755667900342550016502830263400115190799453685977306818255321880677520617545

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

16977107061581940258098339528505249898482773247513534586131286280100489485015

Perhitungan Putaran ke-: 2

Hex Bytes Padding: 33ac82cc2d797de58ce4a9cac23250e4

Hex Bytes Hash Bytes Pesan Padding:

fdb73473e526d71b0a181c5eef300bc9b543fc1b7adad0acc1ed6ff6de5f635dddbab6c6678ce263ecdadc12b79b09fd9ef36b0838cb163a7a0a8c18f000400

Nilai Hash Pesan Padding:

6236592900113885736386339292669040526238166523252391819866554322725798734750

Nilai Hash Pesan Padding Mod P: 83738209106821224148113069264902702497

Nilai Perhitungan Akhir P:

2844007215352135356920619807927565164706444911928197911152340649963558487196684504633811194996350919186811634734732

Nilai Hash Pesan Padding Mod Q: 172705277871904299782212711817627554361

Nilai Perhitungan Akhir Q:

89079146521515739176842577137317075756668975056801757458436465794282430123901342132102784310142776732597171965254

Nilai Perhitungan Tanda tangan:

24389439017370581640236927516308046614052765665137853610614515140383652723070

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

32884354303097561478356598157566509057866132987160967821640037750031406229219

Perhitungan Putaran ke-: 3

Hex Bytes Padding: b7f55a8d8704d1c0ad169dab668a09c9

Hex Bytes Hash Bytes Pesan Padding:

ca142d5616d72426270270e6c8c0eef2432278adbd6c2952ff89d10ff4925ef72a051598fd68ca1e2c32a076ca52e693a11d852978ec09db082dfcafd33c56d

Nilai Hash Pesan Padding:

37792192591575673690410249497543627066575385859969293577503190311476174217280

Nilai Hash Pesan Padding Mod P: 47032933124732667152965446017488745388

Nilai Perhitungan Akhir P:

1597383113308283670421154462643395571017501682747055632516747229781678513577925798486221191620882894106338223501328

Nilai Hash Pesan Padding Mod Q: 157365350834161730969952031393238613791

Nilai Perhitungan Akhir Q:

811670107427936681672746123162321630018020122783171759256043960231146788004080449295236092913245281312787141843274

Nilai Perhitungan Tanda tangan:

27275428938616278097409365135169503881861731231439001069931810594090189334601

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

1328754611635773524332687952691922517528913650444066064003401761281030746689

Perhitungan Putaran ke-: 4 (**Valid**)

Hex Bytes Padding: 92e0c70f27e0cac75cb52b3986d8981d

Hex Bytes Hash Bytes Pesan Padding:

1cd875529369784615b750ea37b863f30c21ac1ed02b6c326473722692d24be70796788c3a15cea
13158f35634b233fd6debc94112fe711c1048cd4c14febd85

Nilai Hash Pesan Padding:

14627128770941122175793138091410749791843240867687359904792737907706697684658

Nilai Hash Pesan Padding Mod P: 183315935035492915486735238654342907240

Nilai Perhitungan Akhir P:

62259731547984156316236054524606070289080514024558418154091428049216802556123
09776541624628857898379789105663113440

Nilai Hash Pesan Padding Mod Q: 66394923131493792653331473175065688976

Nilai Perhitungan Akhir Q:

34245641817048750741322842339620288897235358234223195947497041749057368128594
3027982636364523808623423225493152864

Nilai Perhitungan Tanda tangan:

1682364741669834670154844810472317657427854247162249949860891330381842069263

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

14627128770941122175793138091410749791843240867687359904792737907706697684658

Perhitungan verifikasi tanda tangan

Nilai N:

39120947203211447214742937450235549584104299510413359641506592072757204963969

Hex Bytes Pesan:

255044462d312e340a25f6e4fcdf0a312030206f626a0a3c3c0a2f54797065202f436174616c6f670
a2f5061676573203220...

Hex Bytes Padding: 92e0c70f27e0cac75cb52b3986d8981d

Nilai Hash Pesan Padding Mod N:

14627128770941122175793138091410749791843240867687359904792737907706697684658

Nilai Tanda Tangan:

1682364741669834670154844810472317657427854247162249949860891330381842069263

Nilai Perhitungan Tanda Tangan Pangkat 2 Mod N:

14627128770941122175793138091410749791843240867687359904792737907706697684658