IMPLEMENTASI QR CODE MENGGUNAKAN ALGROTIRMA RSA

Disusun dan Diajukan Untuk Memenuhi Persyaratan Ujian Akhir
Memperoleh Gelar Sarjana Komputer Pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH :

NAMA	: ARIFFIN
N.P.M	: 1514370078
PROGRAM STUDI	: SISTEM KOMPUTER

PROGRAM STUDI SISTEM KOMPUTER
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

LEMBAR PENGESAHAN

IMPLEMENTASI QR CODE MENGGUNAKAN ALGORITMA RSA

Disusun Oleh :

Nama	: ARIFFIN
NPM	: 1514370078
Program Studi	: SISTEM KOMPUTER

Skripsi telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 29 Agustus 2019

Dosen Pembimbing I	Dosen Pembimbing II
Andysah Putera Utama S, S.Kom.,M.Kom.,Ph.D	Hendry P, S.Kom.,M.Kom

Mengetahui,

Dekan Fakultas Sains dan Teknologi	Ketua Program Sistem Komputer
Sri Shinta Indiva, ST.,M.sc.	Dr. Muhammad Iqbal, S.Kom.,M.Kom

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	: ARIFFIN
NPM	: 1514370079
Prodi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Judul Skripsi	: IMPLEMENTASI QR CODE MENGGUNAKAN ALGORITMA RSA

Dengan ini menyatakan bahwa :

1. Tugas Akhir/Skripsi saya bukan hasil Plagiat
2. Saya tidak akan menuntut perbaikan nilai Indeks Prestasi Kumulatif (IPK) setelah ujian Sidang Meja Hijau
3. Skripsi saya dapat dipublikasikan oleh pihak lembaga, dan saya tidak akan menuntut akibat publikasi tersebut

Demikian pernyataan ini saya perbuat dengan sebenar-benarnya, terima kasih

Medan, 29 Agustus 2019

Yang membuat pernyataan

ARIFFIN

1514370078

SURAT PERNYATAAN

Saya Yang Bertanda Tangan Dibawah Ini :

Nama	:	ARIFFIN
N. P. M	:	1514370078
Tempat/Tgl. Lahir	:	Medan / 10 Maret 1998
Alamat	:	Jl. Luku I
No. HP	:	081262176964
Nama Orang Tua	:	SYAHDAN/MISTIAWATI
Fakultas	:	SAINS & TEKNOLOGI
Program Studi	:	Sistem Komputer
Judul	:	IMPLEMENTASI QR CODE MENGGUNAKAN ALGORITMA RSA

Bersama dengan surat ini menyatakan dengan sebenar - benarnya bahwa data yang tertera diatas adalah sudah benar sesuai dengan ijazah pada pendidikan terakhir yang saya jalani. Maka dengan ini saya tidak akan melakukan penuntutan kepada UNPAB. Apabila ada kesalahan data pada ijazah saya.

Demikianlah surat pernyataan ini saya buat dengan sebenar - benarnya, tanpa ada paksaan dari pihak manapun dan dibuat dalam keadaan sadar. Jika terjadi kesalahan, Maka saya bersedia bertanggung jawab atas kelalaian saya.

Medan, 27 Agustus 2019

Hormat Pernyataan

ARIFFIN

1514370078

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

rsitas : Universitas Pembangunan Panca Budi
tas : SAINS & TEKNOLOGI
n Pembimbing I : Andylala Adeta Utama Siahaan, S.Kom., M.Kom
n Pembimbing II : Hendry, S.Kom., M.Kom
Mahasiswa : ARIFFIN
an/Program Studi : Sistem Komputer
r Pokok Mahasiswa : 1514370078
ng Pendidikan : Strata Satu (S1)
Tugas Akhir/Skripsi : Implementasi QR Code Menggunakan Algoritma RSA.

ANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
7/2	Revisi Proposal / Judul		
28/2	Acc Seminar Judul		
3/3	Revisi Judul		
5/3	Revisi Bab I, II		
10/3	Revisi Bab III, IV		
12/3	Revisi Bab IV, Kesimpulan		
14	Acc Seminar Proposal		
15/6	Acc Sidang		
20/7	Acc Jilid		

Medan, 22 Februari 2019
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

t yang tidak perlu

FM-BPAA-2012-038

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

ersitas : Universitas Pembangunan Panca Budi
ltas : SAINS & TEKNOLOGI
en Pembimbing I : Andysah Putera Utama Siahaan, S.Kom, M.Kom
en Pembimbing II : Hendry, S.Kom, M.Kom
e Mahasiswa : ARIFFIN
san/Program Studi : Sistem Komputer
or Pokok Mahasiswa : 1514370078
ang Pendidikan : Strata Satu (S1)
l Tugas Akhir/Skripsi : Implementasi QR Code Menggunakan Algoritma RSA.

ANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
-3. 2019	Acc Judul	[paraf]	
-3. 2019	Acc Seminar Proposal	[paraf]	
7. 2019	Acc Bab 1, lanjut Bab 2	[paraf]	
7. 2019	[illegible]	[paraf]	
3. 2019	perbaiki Bab 2, [illegible]	[paraf]	
3. 2019	[illegible]	[paraf]	
-3. 2019	Acc Bab 2, lanjut Bab 3	[paraf]	
0. 7. 2019	perbaiki Bab 3.	[paraf]	
3. 4. 2019	Acc Bab 3, lanjut Bab 4.	[paraf]	
-4. 2019	[illegible] Bab 4 & lanjut Bab 5	[paraf]	
8. 4. 2019	Acc Seminar Hasil	[paraf]	
6. 6. 2019	Acc Sidang	[paraf]	
1. 7. 2019	Acc Jilid	[paraf]	

Medan, 22 Februari 2019
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

ret yang tidak perlu

Plagiarism Detector v. 1092 - Originality Report:

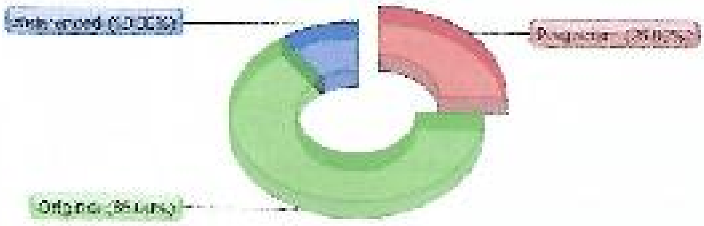
Analyzed document: 23/04/2019 09:26:49

"ARIFFIN_1514370078_SISTEM KOMPUTER.doc"

Licensed to: **Universitas Pembangunan Panca Budi_License4**

UNIVERSITAS PEMBANGUNAN PANCA BUDI

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 73 wrds: 7821 [illegible]

% 25 wrds: 2013 https://en.wikipedia.org/wiki/Latin_Extended-A

% 17 wrds: 1029 [illegible]

[Show other Sources:]

Processed resources details:

154 - Ok / 26 - Failed

[Show other Sources:]

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:
Wiki Detected!	[not detected]	[not detected]	[not detected]

Excluded Urls:

Included Urls:

Detailed document analysis:

IMPLEMENTASI QR CODE MENGGUNAKAN ALGORITMA RSA

SKRIPSI

Telah Diperiksa oleh LPMU
dengan Plagiarisme......25 %
Medan 27 Juni 2019
Ka. LPMU
UNPAB
[illegible signature]
Dr. ... Yoenoro, SE., MM

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 26 Juni 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah di terima
berkas persyaratan
dapat di proses
Medan, 27 JUN 2019
Ka. BPAA
TEGUH WAHYONO, SE., MM.

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: ARIFFIN
Tempat/Tgl. Lahir	: Medan / 10 Maret 1998
Nama Orang Tua	: SWARMAN
N. P. M.	: 1514370078
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 081262176964
Alamat	: Jl. [illegible]

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul IMPLEMENTASI QR CODE MENGGUNAKAN ALGORITMA RSA,
Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkipnya sebanyak 1 lembar.
7. Terlampir pelunasan kwitansi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 exemplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 exemplar untuk penguji (bentuk dan warna penjilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
9. Soft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
10. Terlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
11. Setelah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
12. Bersedia melunaskan biaya-biaya uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1.	[102] Ujian Meja Hijau	: Rp.	100.000
2.	[170] Administrasi Wisuda	: Rp.	1,500,000
3.	[202] Bebas Pustaka	: Rp.	100,000
4.	[221] Bebas LAB	: Rp.	5,000
Total Biaya		: Rp.	1,605,000
			1.705.000
S-Uk. Tertutup		Rp.	2.650.000
			4.355.000

Ukuran Toga : **XL**

Diketahui/Disetujui oleh :

Hamdani, S.T., M.Sc.
Dekan Fakultas SAINS & TEKNOLOGI

Hormat saya

ARIFFIN
1514370078

Catatan :

- 1.Surat permohonan ini sah dan berlaku bila ;
  - a. Telah dicap Bukti Pelunasan dari UPT Perpustakaan UNPAB Medan.
  - b. Melampirkan Bukti Pembayaran Uang Kuliah aktif semester berjalan
- 2.Dibuat Rangkap 3 (tiga), untuk - Fakultas - untuk BPAA (asli) - Mhs.ybs.

TANDA BEBAS PUSTAKA
No. 2491/Perp/BP/2019
Dinyatakan tidak ada sangkut
paut dengan UPT. Perpustakaan
Medan, 27 JUN 2019
Ka. UPT. Perpustakaan
UNIVERSITAS PEMBANGUNAN PANCA BUDI
UNPAB INDONESIA
UPT. PERPUSTAKAAN
[illegible signature]

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km 4,5 Medan Fax. 061-8458077 PO BOX : 1099 MEDAN

PROGRAM STUDI TEKNIK ELEKTRO	(TERAKREDITASI)
PROGRAM STUDI TEKNIK ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

Saya yang bertanda tangan di bawah ini :

Nama Lengkap	: ARIFFIN
Tempat/Tgl. Lahir	: Medan / 10 Maret 1998
Nomor Pokok Mahasiswa	: 1514370078
Program Studi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Jumlah Kredit yang telah dicapai	: 141 SKS, IPK 3.70
Nomor Hp	: 081262176964
Dengan ini mengajukan judul sesuai bidang ilmu sebagai berikut	:

No.	Judul
1.	IMPLEMENTASI QR CODE MENGGUNAKAN ALGORITMA RSA

Catatan : Diisi Oleh Dosen Jika Ada Perubahan Judul

*Coret Yang Tidak Perlu

Medan, 05 April 2019

Pemohon,

(Ariffin)

Dekan,

(Ir. Iskandar Alamsyah, M.T., Ph.D.)

Tanggal : 16 April 2019

Disetujui oleh:

Dekan,

(Dr. Sahnidi Indra, S.T., M.Sc.)

Tanggal : .....

Disetujui oleh:

Dosen Pembimbing I :

(Andysah Putera Utama Siahaan, S.Kom., M.Kom)

Tanggal : 16 April 2019

Disetujui oleh:

Ka. Prodi Sistem Komputer

(MUHAMMAD IQBAL, S.Kom, M.Kom.)

Tanggal : .....

Disetujui oleh:

Dosen Pembimbing II:

(HENDRY, S.KOM., M.KOM.)

ABSTRAK

ARIFFIN
Implementasi *QR Code* Menggunakan Algoritma RSA
2019

QR Code (*Quick Response Code)* merupakan bentuk evolusi kode batang dari satu dimensi menjadi dua dimensi. *QR Code* dikembangkan oleh *Denso Wave* yang dipublikasikan pada tahun 1994, *QR Code* memiliki kemampuan untuk menyampaikan informasi dan merespon dengan cepat. *QR Code* merupakan suatu teknologi yang paling rentan terhadap pencurian informasi/pesan karena merupakan media pertukaran informasi berbasis *scan* dan kamera. Dalam pertukaran pesan dapat dimanipulasi isinya oleh pihak ketiga sehingga pesan dengan isi yang berbeda akan diterima oleh peerima. Oleh karena itu dibutuhkan mekanisme untuk mengamankan pesan yang disimpan di dalam *QR Code* sehingga pesan tersebut tidak dapat dibaca maupun dimanipulasi oleh pihak yang tidak berwenang.

Dalam penelitian ini digunakan algoritma RSA untuk mengamankan pesan dan informasi yang ada di dalam *QR Code*. RSA merupakan algoritma kriptografi asimetris yang menggunakan sepasang kunci, yaitu *public key* dan *private key*. Keamanan algoritma kriptografi RSA terletak pada sulitnya memfaktorkan bilangan prima. Dalam penelitian ini pengujian dilakukan dengan memasukkan teks ke dalam *QR Code*. Teks tersebut dienkripsi menggunakan algoritma kriptografi RSA, sehingga teks yang disimpan ke dalama *QR Code* berupa *ciphertext* yang tidak bisa dibaca oleh pihak yang tidak berwenang.

Kata Kunci: Algoritma RSA, keamanan pesan, *QR Code*.

KATA PENGANTAR

Puji syukur Tuhan yang Maha Esa karena dengan berkat dan kasih anugerah-Nya penulis masih diberikan kesehatan sehingga akhirnya penulis dapat menyelesaikan Skirpsi dengan judul : **"IMPLEMENTASI QR CODE MENGGUNAKAN ALGORITMA RSA".**

Dalam penyusunan Skirpsi ini penulis menyadari banyak mengalami kesulitan namun berkat bantuan dan dorongan dari berbagai pihak, akhirnya Skirpsi ini dapat juga diselesaikan. Penulis dengan segala kerendahan hati menyampaikan terima kasih kepada:

1. Ayahanda dan Ibunda beserta keluarga yang telah berjasa dalam memberikan dukungan moril dan materil.
2. Bapak H.M. Isa Indrawan, SE, MM, selaku Rektor Universitas Pembangunanan Panca Budi Medan.
3. Rektor I, Bapak Ir. Bhakti Alamsyah, M.T, Ph.D
4. Ibu Sri Shindi Indira, ST., M.Sc, selaku Dekan Fakultas Sains Dan Teknologi Universitas Pembangunan Panca Budi Medan
5. Bapak Dr. Muhammad Iqbal, S.Kom., M.Kom, selaku Ketua Program Studi Sistem Komputer Fakultas Sains Dan Teknologi Universitas Pembangunan Panca Budi Medan.
6. Dosen Pembimbing 1, Bapak Andysah Putera Utama S, S.Kom.,M.Kom.,Ph.D
7. Dosen Pembimbing 2, Bapak Hendry S.Kom.,M.Kom
8. Seluruh Dosen dan Staf Pegawai Fakultas Sains Dan Teknologi yang telah banyak membantu dalam kelancaran seluruh aktivitas perkuliahan.
9. Staf Perpustakaan Universitas Pembanguan Panca Budi yang telah berjasa memberikan pinjaman buku-buku yang ada.
10. Teman-teman yang telah memberikan berbagai saran, inspirasi, dorongan, doa, motivasi dan moril maupan materil yang diperlukan sehingga penulis dapat menyelesaikan Skirpsi ini.

Penulis juga menyadari bahwa penyusunan Skripsi ini belum sempurna baik dalam penulisan maupun isi disebabkan keterbatasan kemampuan penulis. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun dari pembaca untuk penyempurnaan isi Skirpsi ini.

Medan, Agustus 2019
Penulis,

ARIFFIN
NPM : 1514370078

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kode QR atau biasa dikenal dengan istilah *Qr Code* adalah singkatan dari *Quick Response Code* atau respons cepat, yang sesuai dengan tujuannya untuk menyampaikan informasi dengan cepat dan mendapatkan respons yang cepat pula. *Qr Code* merupakan bentuk evolusi kode batang dari satu dimensi menjadi dua dimensi, yang memiliki kemampuan menyimpan banyak data. *Qr Code* dikembangkan oleh *Denso Wave* sebuah devisi *Denso Corporation* sebuah perusahaan di Jepang yang dipublikasikan tahun 1994. Pada awalnya penggunaan *Qr Code* sebagai pelacakan kendaraan bagian di manufaktur, namun kini digunakan sebagai keperluan komersil, yang biasa berisi teks berupa iklan, promosi dan link ke url alamat tertentu. *Qr Code* kini sudah sangat lazim, seseorang dapat mudah menyimpan informasi dan data penting pada *Qr Code.*

Hidayat, Yogi dan Paulus (2017), Penggunaan *QR-Code* dapat memberikan keuntungan, seperti pembacaan *QR-Code* cukup hanya dengan menggunakan kamera, kapasitas *Qr Code* yang cukup besar, serta mudah menggunakannya, sehingga pengelolaan data akan lebih cepat. Sedangkan metode kriptografi RSA akan berguna untuk merahasiakan suatu input data ataupun informasi pada *Qr Code* selanjutnya akan diubah menggunakan suatu kunci enkripsi dan dekripsi sehingga kode tersebut tidak dapat diartikan atau diciptakan oleh orang lain.

Oleh karena itu untuk lebih meningkatkan keamanan data yang tersimpan pada *Qr Code*, pentingnya diimplementasikan algoritma RSA (Rivest Shamir Adleman) sebagai keamanan datanya. RSA merupakan algoritma kriptografi asimetris, dimana kunci untuk melakukan enkripsi berbeda dengan kunci untuk dekripsi. Algoritma RSA terletak pada sulitnya memfaktorkan bilangan prima, sehingga dengan pengimplementasian algoritma RSA pada *Qr Code*, dapat terjaga kerahasiakan data yang tersimpan pada *Qr Code.*

Berdasarkan pada uraian latar belakang permasalahan tersebut, maka penulis mengambil judul untuk skripsi **"Implementasi *Qr Code* Menggunakan Algoritma RSA"**

1.2 Rumusan Masalah

Adapun masalah yang akan dibahas dalam skripsi ini yaitu:

1. Bagaimana cara mengimplementasikan algoritma RSA pada *Qr Code?*
2. Bagaimana bentuk komponen media aplikasi *Qr Code* menggunakan algoritma RSA?

1.3 Batasan Masalah

Karena keterbatasan dan waktu maka penulis akan membatasi pokok permasalahan yang akan dibahas yaitu:

a. Media aplikasi *Qr Code* menggunakan algoritma RSA dibuat dengan menggunakan *Visual Basic versi 1.1.*

b. Keamanan data dan informasi berupa teks.

c. Keamanan ini menggunakan algoritma RSA.

d. Aplikasi ini hanya mengubah pesan dan akan diubah menjadi *QR Code.*

e. *Ciphertext* yang disimpan pada *QR Code* hanya berupa *hexadecimal*

f. *QR Code* memiliki Batasan 100 karakter

1.4 Tujuan Penulisan

Tujuan penelitian ini adalah menerapkan algoritma RSA dalam mengamankan data, pesan, dan informasi yang terkandung dalam *Qr Code*.

1.5 Manfaat Penelitian

Manfaat dari hasil penelitian ini adalah agar dapat meminimalisir pemalsuan serta terjaminnya keaslian data dan informasi yang terkandung dalam *Qr Code*.

BAB II

LANDASAN TEORI

2.1 *Qr Code*

Quick Response Code disebut juga dengan *Qr Code* merupakan pengembangan dari *barcode* (kode batang) yang berupa gambar dua dimensi. *Qr Code* ditemukan oleh *Denso Corporation* salah satu perusahaan Jepang yang bergerak dibidang otomotif dan dipublikasikan pada tahun 1994. Penggunaan Kode QR sebuah hal yang umum di Jepang, hal ini dikarenakan kemampuannya dalam menyimpan data jauh lebih besar daripada kode batang, sehingga mampu mengkodekan informasi dalam bahasa Jepang berupa huruf kanji.

Qr Code memiliki kapasitas tinggi dalam data pengkodean, mampu menyimpan berbagai jenis data seperti data numerik, alphanumerik, kanji, kana, hiragana, simbol dan biner. Kode QR mampu menyimpan data jenis numerik sampai dengan 7.089 karakter, alphanumerik sampai dengan 4.296 karakter, kode biner sampai dengan 2.844 byte, dan huruf kanji sampai dengan 1.817 karakter. Tampilan *Qr Code* lebih kecil daripada kode batang. Hal ini dikarenakan kode QR mampu menampung data secara horizontal dan vertical. QR Code dapat menyimpan informasi lebih banyak dibandingkan dengan barcode hanya menyimpan informasi secara horizontal(Widiyanti,2017). Oleh karena itu secara otomatis ukuran dari tampilannya gambar kode QR bisa hanya 1/10 dari ukuran sebuah kode batang. Tidak hanya itu kode QR juga tahan terhadap kerusakan, dikarenakan kode QR mampu memperbaiki kesalahan sampai dengan 30%.

Dengan demikian, meskipun sebagian simbol *Qr Code* kotor atau rusak, data tetap dapat disimpan dan dibaca. Tiga tanda berbentuk persegi di tiga sudut memiliki fungsi agar simbol dapat dibaca dengan hasil yang sama dari sudut manapun sepanjang 360 derajat.

2.2 Kriptografi

2.2.1 Teori Kriptografi

Kriptografi berasal dari Bahasa Yunani, yaitu *Crypto* yang berarti *secret* (rahasia) dan *Graphia* yang berarti *writing* (tulisan)(Atika,2014). Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian pesan yang bertujuan untuk menjaga keamanan dan kerahasian suatu pesan dari pihak ketiga ketika pesan dikirim dari suatu tempat ke tempat lain.

Kriptografi memiliki catatan sejarah yang sangat menarik dan panjang, dan pada dasarnya kriptografi sudah dikenal sejak lama. Menurut catatan sejarah, kriptografi sudah digunakan 4000 tahun yang lalu oleh raja yang bernama Julius Caesar pada Zaman Romawi Kuno. Raja tersebut ingin mengirimkan pesan rahasia kepada seorang jendral di medan perang. Pesan tersebut dikirmkan melalui seorang kurir, karena pesan tersebut mengandung rahasia, Julius Caesar kemudian memikirkan bagaimana mengatasi agar pesan rahasia tersebut agar tidak sampai terbuka dijalan. Ia kemudian mengacak pesan tersebut hingga menjadi suatu pesan yang tidak dapat dipahami oleh siapapaun terkecuali oleh jendralnya saja (Ariyus, 2006).

Kriptografi merupakan ilmu yang mempelajari Teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentikasi entitas dan keaslian data(Zulkarnain 2019). Pada dasarnya kriptografi terdiri dari beberapa komponen, antara lain yaitu :

1. Enkripsi : merupakan suatu hal yang mendasar dan sangat penting dalam kriptografi, enkripsi merupakan cara pengamanan data berupa *plaintext* (pesan asli) yang akan diubah menjadi *cipher* atau kode yang tidak dapat dimengerti oleh orang lain, sehingga pesan tersebut terjaga kerahasiaannya.
2. Dekripsi : merupakan kebalikan dari enkripsi. Pesan diterima dari seseorang yang berbentuk enkripsi akan dikembalikan ke bentuk asalnya, sehingga pesan tersebut dapat dibaca.
3. Kunci : merupakan kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi pada dua bagian yaitu kunci rahasia (*private key)* dan kunci umu (*public key*).
4. *Ciphertext* : merupakan suatu pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
5. *Plaintext* : sering disebut dengan cleartext. Teks asli merupakan suatu bagian pesan yang diketik atau ditulis yang memiliki makna. Teks asli inilah yang akan melalui diproses menggunakan algoritma kriptografi untuk menjadi *ciphertext*.

Adapun prinsip-prinsip yang mendasari kriptografi adalah:

1. *Authentication* : merupakan sesuatu hal yang berhubungan dengan identifikasi, agar penerima informasi dapat memastikan keaslian pesan, bahwa pesan tersebut bersumber dari orang yang dimintai informasi.
2. *Integrity* (keutuhan data) : merupakan layanan yang dapat memastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak.
3. *Confidentiality* (kerahasiaan) : merupakan suatu usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.
4. *Non-repudiation* (anti penyangkalan) : merupakan suatu hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa pesan tersebut berasal darinya.

2.3 Algoritma Kriptografi

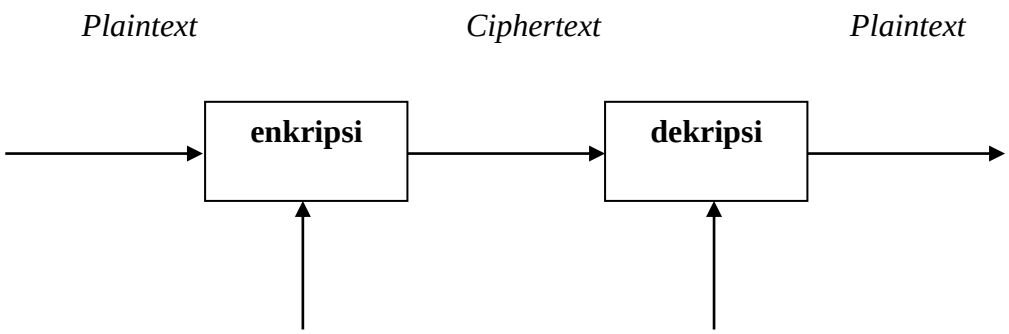
Berdasarkan kunci yang dipakainya Algoritma kriptografi dibagi menjadi beberapa bagian yaitu:

1. Algoritma Simetris : menggunakan satu kunci untuk enkripsi dan dekripsinya.
2. Algoritma Asimetris : menggunakan dua kunci yang berbeda untuk enkripsi dan dekripsinya.

2.3.1 Algoritma Simetris

Algoritma Simetris (*symmetric algorithm*) atau sering disebut dengan single-key algorithm merupakan algoritma hanya menggunakan

satu kunci yang sama untuk melakukan kegiatan enkripsi dan dekripsi. Berikut diagram proses enkripsi dan dekripsi pada algoritma simetris.



Gambar 2.1 Diagram proses enkripsi dan dekripsi algoritma simetris

Bila ingin mengirim pesan dengan menggunakan algoritma ini pengirim dan penerima harus memilih satu kunci yang sama untuk digunakan sebagai enkripsi dan dekripsi. Dan kunci ini haruslah rahasia dari pihak yang tidak berkepentingan. Jika kunci tersebut diketahui oleh orang lain maka, orang tersebut dapat melakukan enkripsi dan dekripsi terhadap pesan.

Kelemahan algoritma kriptografi simetris adalah :

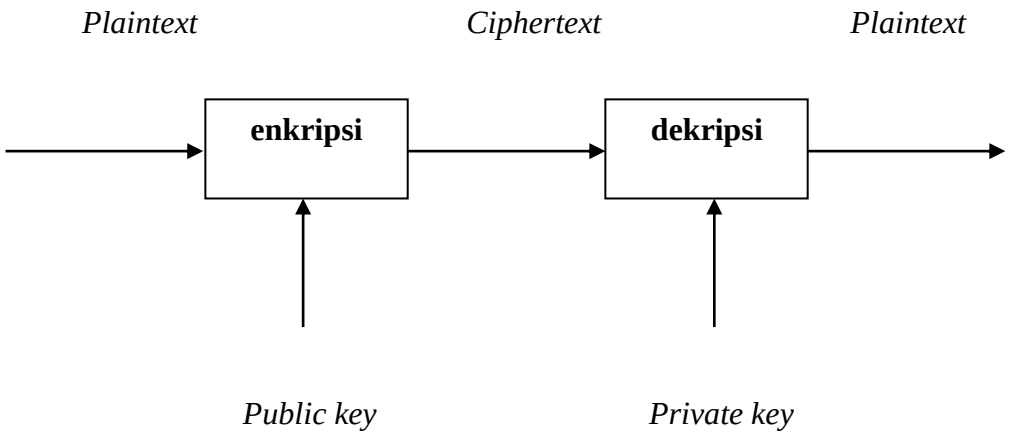
a. Untuk tiap pengiriman pesan dengan dengan pengguna yang berbeda membutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.

Algoritma yang memakai kunci simetris diantaranya adalah :

1. *Data Encryption Standard (DES)*
2. RC2, RSC4, RC5, RC6
3. *Advanced Encryption Standard* (AES), dan lain sebagainya.

2.3.2 Algoritma Asimetris

Algoritma asimetris (*asymmetric algorithm*) atau biasa disebut dengan algoritma kunci publik merupakan suatu algoritma dimana kunci enkripsi berbeda dengan kunci dekripsi. Pada algoritma ini kunci terbagi menjadi dua bagian yakni kunci umum (*public key*) dank kunci rahasia (*private key*). Kunci publik merupakan kunci yang boleh semua orang tahu (dipublikasikan) dan kunci rahasia merupakan kunci yang hanya boleh diketahui satu orang saja. Berikut diagram proses enkripsi dan dekripsi pada algoritma asimetris.



Gambar 2.2 Diagram proses enkripsi dan dekripsi algrotima asimetris

Pada umumnya kunci public digunakan sebagai kunci enkripsi dank unci rahasia diguanakan sebagai kunci dekripsi.

Kelebihan pada algoritma asimetris adalah :

a. Keamanan pada distribusi kunci dapat lebih baik.

b. Manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit.

Kelemahan pada algoritma asimetris adalah :

a. Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris.

Tingkat keamanan sama, kunci yang diguanakan lebih panjang dibandingkan dengan algoritma simetris.

2.4 Algoritma RSA

Dari sekian banyak algoritma kriptografi kunci-publik yang pernah dibuat, RSA merupakan algoritma yang paling popular. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Algoritma ini dirasa aman karena terletak pada sulitnya memfaktorkan bilangan yang besar menjadi factor-faktor prima (Wibowo, 2009). Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin (Syaputra, 2012). Cara yang dapat digunakan dalam pemfaktoran adalah dengan menggunakan pohon faktor, jika semakin besar bilangan yang akan difaktorkan maka semakin lama pula waktu yang dibutuhkan (Albert, 2015).

RSA memliki dasar proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmatika modulo. Kunci enkripsi dan dekripsi merupakan bilangan bulat. Kunci enkripsi merupakan kunci publik yang tidak dirahasiakan dan dapat

diketahui oleh umum dan kunci privat digunakan sebagai kunci dekripsi, kunci privat ini merupakan kunci yang bersifat rahasia.

Pembangkitan kunci pada algoritma RSA dapat dijelaskan sebagai berikut:

1. Pilih dua bilangan prima secara acak, dimana p dan q tidak sama ($p \neq q$)
2. Hitung N dengan persamaan :

   $$N = p.q$$

3. Hitung $\Phi(n)$ dengan persamaan :

   $$\Phi(n) = (p-1)(q-1)$$

4. Pilih bilangan bulat (*integer*) antara satu dan Φ ($1 < e < \Phi$) yang juga merupakan *coprime* dari Φ
5. Hitung d dengan persamaan :

   $$de \equiv 1 \pmod{\Phi}$$

Hasil dari algoritma ini:

Kunci Publik : pasangan (N,e)

Kunci privat : pasangan (N,d)

Algoritma enkripsi yang digunakan pada algoritma RSA sebagai berikut :

1. Susun *plaintext* menjadi blok-blok P1,P2, …, Pn
2. Hitung *ciphertext* Ci dengan rumus :

   $$C_i = P_i^e \bmod N$$

Algoritma dekripsi yang digunakan pada algoritma RSA sebagai berikut:

1. Gunakan kunci privat untuk pangkat nilai dari *ciphertext*
2. Carilah nilai P dengan rumus:

   $$P_i = C_i^d \bmod N$$

2.5 ASCII *System*

ASCII (*American Standart Code for Information Interchange)* merupakan suatu standar internasional dalam kode huruf dan symbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal. Dalam Bahasa pemrograman komputer 0 dan 1 tidak ada cara lain untuk mewakili huruf dan karakter yang bukan nomer. Semuanya harus menggunakan 0 dan 1. Salah satu cara untuk berbahasa dengan komputer dengan cara menggunakan tabel ASCII. Tabel ASCII merupakan tabel yang bersi semua huruf dalam alfabet romawi ditambah beberapa karakter tambahan. Dalam tabel ASCII setiap karakter akan selalu diwakili oleh sejumlah kode yang sama. Misal untuk huruf "b" (b kecil) selalu diwakili oleh urutan nomer 98, dan kalo dipresentasi menggunakan 0 dan 1 dalam bilangan biner, 98 adalah bilangan biner 110 0010. Contoh lainnya 124 adalah untuk karakter "|". ASCII selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks.

Tabel 2.1 Tabel ASCII I *(American Standard Code for Information Interchange)*

DEC	HEX	Symbol	Description
0	0	NUL	*Null char*
1	1	SOH	*Start of Heading*
2	2	STX	*Start of Text*
3	3	ETX	*End of Text*
4	4	EOT	*End of Transmission*
5	5	ENQ	*Enquiry*
6	6	ACK	*Acknowledgment*
7	7	BEL	*Bell*
8	8	BS	*Back Space*
9	9	HT	*Horizontal Tab*
10	A	LF	*Line Feed*
11	B	VT	*Vertical Tab*

12	C	FF	*Form Feed*
13	D	CR	*Carriage Return*
14	E	SO	*Shift Out / X-On*
15	F	SI	*Shift In / X-Off*
16	10	DLE	*Data Line Escape*
17	11	DC1	*Device Control 1 (oft. XON)*
18	12	DC2	*Device Control 2*
19	13	DC3	*Device Control 3 (oft. XOFF)*
20	14	DC4	*Device Control 4*
21	15	NAK	*Negative Acknowledgement*
22	16	SYN	*Synchronous Idle*
23	17	ETB	*End of Transmit Block*
24	18	CAN	*Cancel*
25	19	EM	*End of Medium*
26	1A	SUB	*Substitute*
27	1B	ESC	*Escape*
28	1C	FS	*File Separator*
29	1D	GS	*Group Separator*
30	1E	RS	*Record Separator*
31	1F	US	*Unit Separator*
32	20		*Space*
33	21	!	*Exclamation mark*
34	22	"	*Double quotes (or speech marks)*
35	23	#	*Number*
36	24	$	*Dollar*
37	25	%	*Per cent sign*
38	26	&	*Ampersand*
39	27	'	*Single quote*
40	28	(	*Open parenthesis (or open bracket)*
41	29	)	*Close parenthesis (or close bracket)*
42	2A	*	*Asterisk*
43	2B	+	*Plus*
44	2C	,	*Comma*
45	2D	-	*Hyphen*
46	2E	.	*Period, dot or full stop*
47	2F	/	*Slash or divide*
48	30	0	*Zero*
49	31	1	*One*

50	32	2	*Two*
51	33	3	*Three*
52	34	4	*Four*
53	35	5	*Five*
54	36	6	*Six*
55	37	7	*Seven*
56	38	8	*Eight*
57	39	9	*Nine*
58	3A	:	*Colon*
59	3B	;	*Semicolon*
60	3C	<	*Less than (or open angled bracket)*
61	3D	=	*Equals*
62	3E	>	*Greater than (or close angled bracket)*
63	3F	?	*Question mark*
64	40	@	*At symbol*
65	41	A	*Uppercase A*
66	42	B	*Uppercase B*
67	43	C	*Uppercase C*
68	44	D	*Uppercase D*
69	45	E	*Uppercase E*
70	46	F	*Uppercase F*
71	47	G	*Uppercase G*
72	48	H	*Uppercase H*
73	49	I	*Uppercase I*
74	4A	J	*Uppercase J*
75	4B	K	*Uppercase K*
76	4C	L	*Uppercase L*
77	4D	M	*Uppercase M*
78	4E	N	*Uppercase N*
79	4F	O	*Uppercase O*
80	50	P	*Uppercase P*
81	51	Q	*Uppercase Q*
82	52	R	*Uppercase R*
83	53	S	*Uppercase S*
84	54	T	*Uppercase T*
85	55	U	*Uppercase U*
86	56	V	*Uppercase V*
87	57	W	*Uppercase W*
88	58	X	*Uppercase X*

89	59	Y	*Uppercase Y*
90	5A	Z	*Uppercase Z*
91	5B	[	*Opening bracket*
92	5C	\	*Backslash*
93	5D	]	*Closing bracket*
94	5E	^	*Caret – circumflex*
95	5F	_	*Underscore*
96	60	`	*Grave accent*
97	61	a	*Lowercase a*
98	62	b	*Lowercase b*
99	63	c	*Lowercase c*
100	64	d	*Lowercase d*
101	65	e	*Lowercase e*
102	66	f	*Lowercase f*
103	67	g	*Lowercase g*
104	68	h	*Lowercase h*
105	69	i	*Lowercase i*
106	6A	j	*Lowercase j*
107	6B	k	*Lowercase k*
108	6C	l	*Lowercase l*
109	6D	m	*Lowercase m*
110	6E	n	*Lowercase n*
111	6F	o	*Lowercase o*
112	70	p	*Lowercase p*
113	71	q	*Lowercase q*
114	72	r	*Lowercase r*
115	73	s	*Lowercase s*
116	74	t	*Lowercase t*
117	75	u	*Lowercase u*
118	76	v	*Lowercase v*
119	77	w	*Lowercase w*
120	78	x	*Lowercase x*
121	79	y	*Lowercase y*
122	7A	z	*Lowercase z*
123	7B	{	*Opening brace*
124	7C	|	*Vertical bar*
125	7D	}	*Closing brace*
126	7E	~	*Equivalency sign – tilde*
127	7F	•	*Delete*

128	80	€	*Euro sign*
129	81	•	
130	82	‚	*Single low-9 quotation mark*
131	83	*ƒ*	*Latin small letter f with hook*
132	84	„	*Double low-9 quotation mark*
133	85	…	*Horizontal ellipsis*
134	86	†	*Dagger*
135	87	‡	*Double dagger*
136	88	ˆ	*Modifier letter circumflex accent*
137	89	‰	*Per mille sign*
138	8A	Š	*Latin capital letter S with caron*
139	8B	‹	*Single left-pointing angle quotation*
140	8C	Œ	*Latin capital ligature OE*
141	8D	•	
142	8E	Ž	*Latin capital letter Z with caron*
143	8F	•	
144	90	•	
145	91	‘	*Left single quotation mark*
146	92	’	*Right single quotation mark*
147	93	“	*Left double quotation mark*
148	94	”	*Right double quotation mark*
149	95	•	*Bullet*
150	96	–	*En dash*
151	97	—	*Em dash*
152	98	˜	*Small tilde*
153	99	™	*Trade mark sign*
154	9A	š	*Latin small letter S with caron*
155	9B	›	*Single right-pointing angle quotation mark*
156	9C	œ	*Latin small ligature oe*
157	9D	•	
158	9E	ž	*Latin small letter z with caron*
159	9F	Ÿ	*Latin capital letter Y with diaeresis*
160	A0		*Non-breaking space*
161	A1	¡	*Inverted exclamation mark*
162	A2	¢	*Cent sign*
163	A3	£	*Pound sign*
164	A4	¤	*Currency sign*
165	A5	¥	*Yen sign*
166	A6	¦	*Pipe, Broken vertical bar*

167	A7	§	*Section sign*
168	A8	¨	*Spacing diaeresis – umlaut*
169	A9	©	*Copyright sign*
170	AA	ª	*Feminine ordinal indicator*
171	AB	«	*Left double angle quotes*
172	AC	¬	*Not sign*
173	AD		*Soft hyphen*
174	AE	®	*Registered trade mark sign*
175	AF	¯	*Spacing macron – overline*
176	B0	°	*Degree sign*
177	B1	±	*Plus-or-minus sign*
178	B2	²	*Superscript two – squared*
179	B3	³	*Superscript three – cubed*
180	B4	´	*Acute accent - spacing acute*
181	B5	µ	*Micro sign*
182	B6	¶	*Pilcrow sign - paragraph sign*
183	B7	·	*Middle dot - Georgian comma*
184	B8	¸	*Spacing cedilla*
185	B9	¹	*Superscript one*
186	BA	º	*Masculine ordinal indicator*
187	BB	»	*Right double angle quotes*
188	BC	¼	*Fraction one quarter*
189	BD	½	*Fraction one half*
190	BE	¾	*Fraction three quarters*
191	BF	¿	*Inverted question mark*
192	C0	À	*Latin capital letter A with grave*
193	C1	Á	*Latin capital letter A with acute*
194	C2	Â	*Latin capital letter A with circumflex*
195	C3	Ã	*Latin capital letter A with tilde*
196	C4	Ä	*Latin capital letter A with diaeresis*
197	C5	Å	*Latin capital letter A with ring above*
198	C6	Æ	*Latin capital letter AE*
199	C7	Ç	*Latin capital letter C with cedilla*
200	C8	È	*Latin capital letter E with grave*
201	C9	É	*Latin capital letter E with acute*
202	CA	Ê	*Latin capital letter E with circumflex*
203	CB	Ë	*Latin capital letter E with diaeresis*
204	CC	Ì	*Latin capital letter I with grave*
205	CD	Í	*Latin capital letter I with acute*

206	CE	Î	*Latin capital letter I with circumflex*
207	CF	Ï	*Latin capital letter I with diaeresis*
208	D0	Đ	*Latin capital letter ETH*
209	D1	Ñ	*Latin capital letter N with tilde*
210	D2	Ò	*Latin capital letter O with grave*
211	D3	Ó	*Latin capital letter O with acute*
212	D4	Ô	*Latin capital letter O with circumflex*
213	D5	Õ	*Latin capital letter O with tilde*
214	D6	Ö	*Latin capital letter O with diaeresis*
215	D7	×	*Multiplication sign*
216	D8	Ø	*Latin capital letter O with slash*
217	D9	Ù	*Latin capital letter U with grave*
218	DA	Ú	*Latin capital letter U with acute*
219	DB	Û	*Latin capital letter U with circumflex*
220	DC	Ü	*Latin capital letter U with diaeresis*
221	DD	Ý	*Latin capital letter Y with acute*
222	DE	Þ	*Latin capital letter THORN*
223	DF	ß	*Latin small letter sharp s - ess-zed*
224	E0	à	*Latin small letter a with grave*
225	E1	á	*Latin small letter a with acute*
226	E2	â	*Latin small letter a with circumflex*
227	E3	ã	*Latin small letter a with tilde*
228	E4	ä	*Latin small letter a with diaeresis*
229	E5	å	*Latin small letter a with ring above*
230	E6	æ	*Latin small letter ae*
231	E7	ç	*Latin small letter c with cedilla*
232	E8	è	*Latin small letter e with grave*
233	E9	é	*Latin small letter e with acute*
234	EA	ê	*Latin small letter e with circumflex*
235	EB	ë	*Latin small letter e with diaeresis*
236	EC	ì	*Latin small letter i with grave*
237	ED	í	*Latin small letter i with acute*
238	EE	î	*Latin small letter i with circumflex*
239	EF	ï	*Latin small letter i with diaeresis*
240	F0	ð	*Latin small letter eth*
241	F1	ñ	*Latin small letter n with tilde*
242	F2	ò	*Latin small letter o with grave*
243	F3	ó	*Latin small letter o with acute*
244	F4	ô	*Latin small letter o with circumflex*

245	F5	õ	*Latin small letter o with tilde*
246	F6	ö	*Latin small letter o with diaeresis*
247	F7	÷	*Division sign*
248	F8	ø	*Latin small letter o with slash*
249	F9	ù	*Latin small letter u with grave*
250	FA	ú	*Latin small letter u with acute*
251	FB	û	*Latin small letter u with circumflex*
252	FC	ü	*Latin small letter u with diaeresis*
253	FD	ý	*Latin small letter y with acute*
254	FE	þ	*Latin small letter thorn*
255	FF	ÿ	*Latin small letter y with diaeresis*

2.6 Bilangan Relatif Prima

Bilangan relatif prima adalah bilangan bulat lebih dari 1 yang habis dibagi oleh 1. Dua bilangan a dan b dikatakan relatif prima jika FPB (faktor persekutuan terbesar) dari dua bilangan (a,b) = 1, dengan kata lain a dan b tidak mempunyai faktor prima bersama.

Misalkan . Misalnya (20,3) adalah relatif prima sebab PBB (20,3) = 1 tetapi 20 dan 5 tidak termasuk relatif prima karena PBB (20,5) ≠ 1 atau $5^1$1. Jika a dan b merupakan bilangan relatif prima, maka terdapat bilangan bulat *m* dan *n* hingga menjadi *m*a + *n*b = 1.

2.7 Aritmatika Modulo

Aritmatika modulo (*modular arithmethic*) merupakan sisa dari hasil pembagian dua bilangan. Aritmatika modulo memainkan peranan yang penting pada algoritma kriptografi dalam komputasi *integer*. Operator yang digunakan pada *modular arithmethic* adalah mod. Misalkan a dan m adalah bilangan bulat (m > 0). Dalam pengoperasian a *mod* m dibaca “a modulo m” memberikan sisa

pembagian jika a dibagi dengan m. “a *mod* m = r” sedemikian sehingga a = mq + r, dengan $0 \leq r < m$, bilangan m disebut modulus atau modulo dan hasil aritmatika modulo m terletak di dalam himpunan {0, 1, 2, …, m-1}.

Kongruen modulo dapat dinyatakan apabila sebuah bilangan bulat positif a dan b merupakan kongruen modulo dari bilangan bulat positif m, jika (a-b) dibagi m tidak memiliki sisa, atau a dan b memiliki sisa bagi yang sama ketika dibagi m. Dan notasi $a \equiv b \pmod{m}$ dibaca a kongruen b modulo m. Negasinya adalah $a \not\equiv b \pmod{m}$ dibaca a tidak kongruen b modulo m.

2.8 ***Great Common Divisor*** (GCD)

Greate Common Divisor atau biasa dikenal dengan GCD yang memiliki istilah Indonesia FPB (Faktor Persekutuan Terbesar) adalah bilangan terbesar yang dapat membagi dua bilangan atau beberapa bilangan. Dalam arti lain adalah dua buah bilangan bulat tidak nol *a* dan *b* memiliki elemen terbesar *d* bernilai sama dan habis membagi *a* maupun *b*. Sebagai contoh *Gcd* dari (12,20) adalah sebagai berikut :

Faktor dari 12 adalah : 1, 2, 3, 4, 6, 12

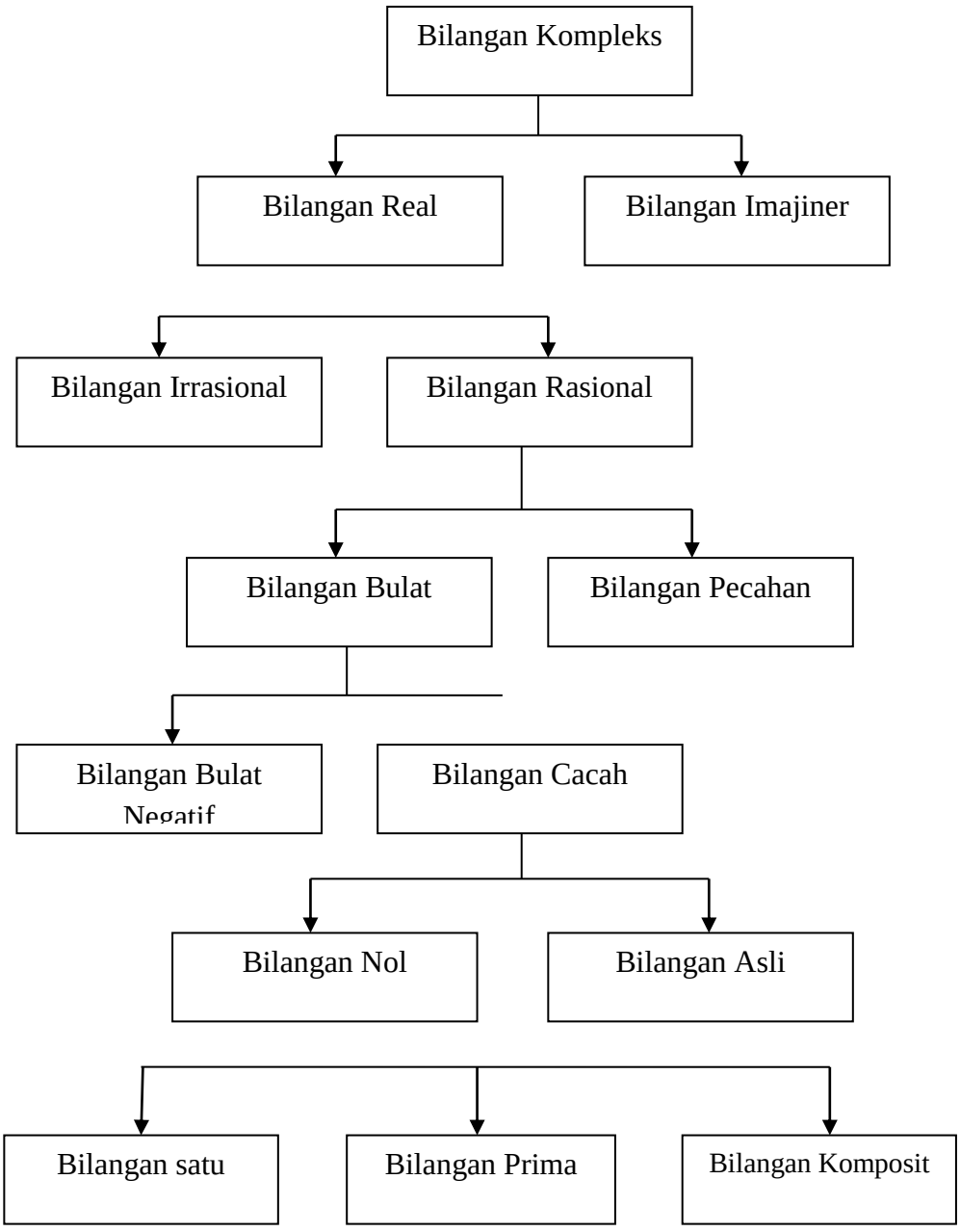
Faktor dari 20 adalah : 1, 2, 4, 5, 10, 20

Karena 4 merupakan bilangan faktor sekutu dari 12 dan 20 dan merupakan faktor yang terbesar, maka GCD (12,20) = 4. Faktor bersama yang terbesar inilah yang disebut dengan *Greatest Common Divisior* (GCD).

2.9 Bilangan Bulat

Bilangan bulat adalah himpunan bilangan yang terdiri dari bilangan cacah, bilangan asli, bilangan prima, bilangan komposit, bilangan nol, bilangan satu,

bilangan negativ, bilangan ganjil, dan bilangan genap. Bilangan merupakan suatu konsep dari matematika yang sering digunakan untuk pencacahan dan pengukuran. Bilangan bulat berasal dari *Zahlen* yang berarti dalam Bahasa Jerman adalah bilangan. Himpunan semua bilangan bulat dalam matematika dilambangkan dengan Z.



Gambar 2.3 Struktur Bilangan Kompleks

BAB III

METODE PENELITIAN

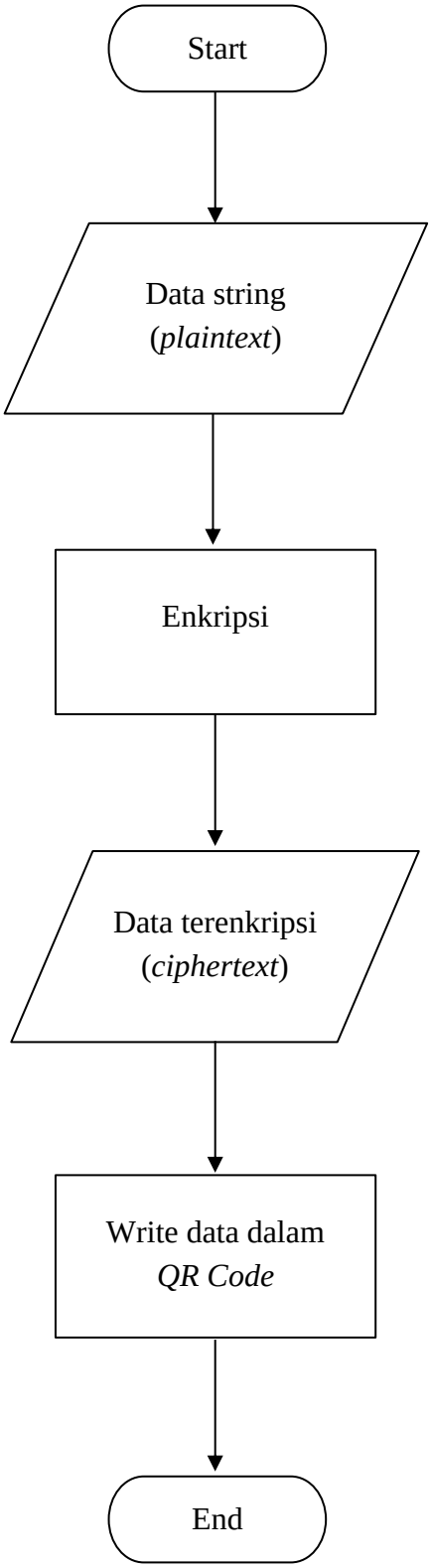
Dalam pembuatan sebuah aplikasi terlebih dahulu dibutuhkan suatu perencanaan, dengan tujuan agar aplikasi yang dibuat dapat berfungsi dengan baik dan sesuai dengan yang diharapkan. Pada bab ini akan membahas tentang desain dan perancangan aplikasi *QR Code* dengan mengimplementasikan algoritma RSA sebagai keamanan pesan dan informasi didalamnya. Desain dan perancangan sistem ini meliputi perancangan sistem, perancangan perhitungan, dan perancangan *interface*.

3.1 Perancangan Sistem

Pada sub bab ini akan membahas mengenai perancangan sistem yang dikerjakan pada skripsi ini. Tujuan pembuatan sistem ini adalah menerapkan algoritma RSA untuk mengamankan pesan dan informasi pada *QR Code* sehingga pesan dan informasi tersebut menjadi tidak terbaca. Proses utama yang dilakukan pada aplikasi ini adalah melakukan enkripsi pada pesan dan akan diubah menjadi *QR Code*. Berikut ini merupakan *flowchart* sistem untuk enkripsi pesan, *flowchart* algoritma kriptografi RSA, dan , *flowchart* pembangkit kunci.

3.1.1 *Flowchart* Sistem Untuk Enkripsi Pesan

Flowchart sistem menggambarkan urutan proses secara detail dan hubungan antara satu proses dengan proses lainnya. Adapun *flowchart* sistem untuk enkripsi pesan dapat dilihat pada Gambar 3.1 dibawah ini :



Gambar 3.1 *Flowchart* Sistem Enkripsi Pesan

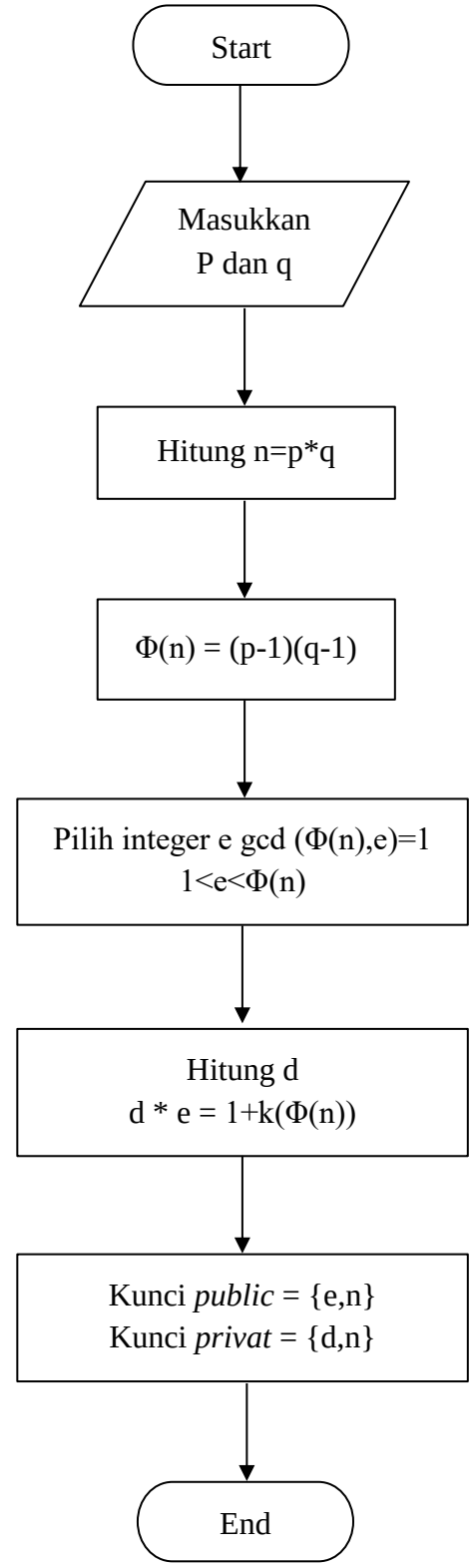
Berdasarkan pada Gambar 3.1 diatas, pada sistem ini, pesan yang yang akan di*input* dalam penelitian ini adalah data *string* yang masih berupa *plaintext*, sebelum dimasukkan kedalam *QR Code*, *plaintext* tersebut akan melalui proses enkripsi terlebih dahulu menggunakan algoritma kriptografi RSA. *Plaintext* yang telah terenkripsi menjadi *ciphertext* dan akan disimpan ke dalam *QR Code*.

3.1.2 *Flowchart* Algoritma Kriptografi RSA

Algoritma yang digunakan pada penelitian ini untuk melakukan enkripsi dan dekripsi pesan adalah algoritma kriptografi RSA. Algoritma RSA merupakan algoritma asimetris yang memiliki dua kunci yang berbeda yaitu kunci *public* dan kunci *privat.*

RSA memiliki dasar proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmatika modulo. Kunci enkripsi dan dekripsi merupakan bilangan bulat yang dibangkitkan dari beberapa bilangan prima. Semakin besar bilangan pada kunci *public* maka akan semakin sulit kunci *privat*nya untuk ditebak dan semakin sulit juga dalam pemfaktorannya maka dapat dinyatakan bahwa semakin kuat algoritma RSA-nya. Kunci *public* atau kunci enkripsi tidak dirahasiakan dan dapat diketahui oleh orang banyak (umum), namun kunci untuk dekripsi hanya diketahui oleh pribadi dan bersifat rahasia sehingga kunci ini dikatakan sebagai kunci *privat*.

Adapun *flowchart* dalam proses pembangkitan kunci algoritma RSA dapat dilihat dibawah ini :



Gambar 3.2 *Flowchart* Pembangkitan Kunci Algoritma RSA

Pada *flowchart* diatas dapat dilihat bahwa pembangkitan kunci algoritma RSA melewati beberapa proses yang dapat dijelaskan sebagai berikut :

1. Pilih dua bilangan prima p dan q
2. Hitung n dengan persamaan :

   $n = p*q$
3. Hitung Φ(n) dengan persamaan :

   $\Phi(n) = (p-1)(q-1)$
4. Pilih nilai e yang merupakan bilangan bulat (*integer*) gcd (Φ(n),e)=1 dan juga merupakan *coprime* dari Φ(n)
5. Hitung d dengan persamaan :

   $de \equiv 1 \bmod \Phi(n)$

Pada algoritma ini akan menghasilkan :

Kunci *public* : pasangan (n,e)

Kunci *privat* : pasangan (n,d)

Contoh :

1. Pilih bilangan prima p = 13 dan q = 19
2. Hitung nilai n :

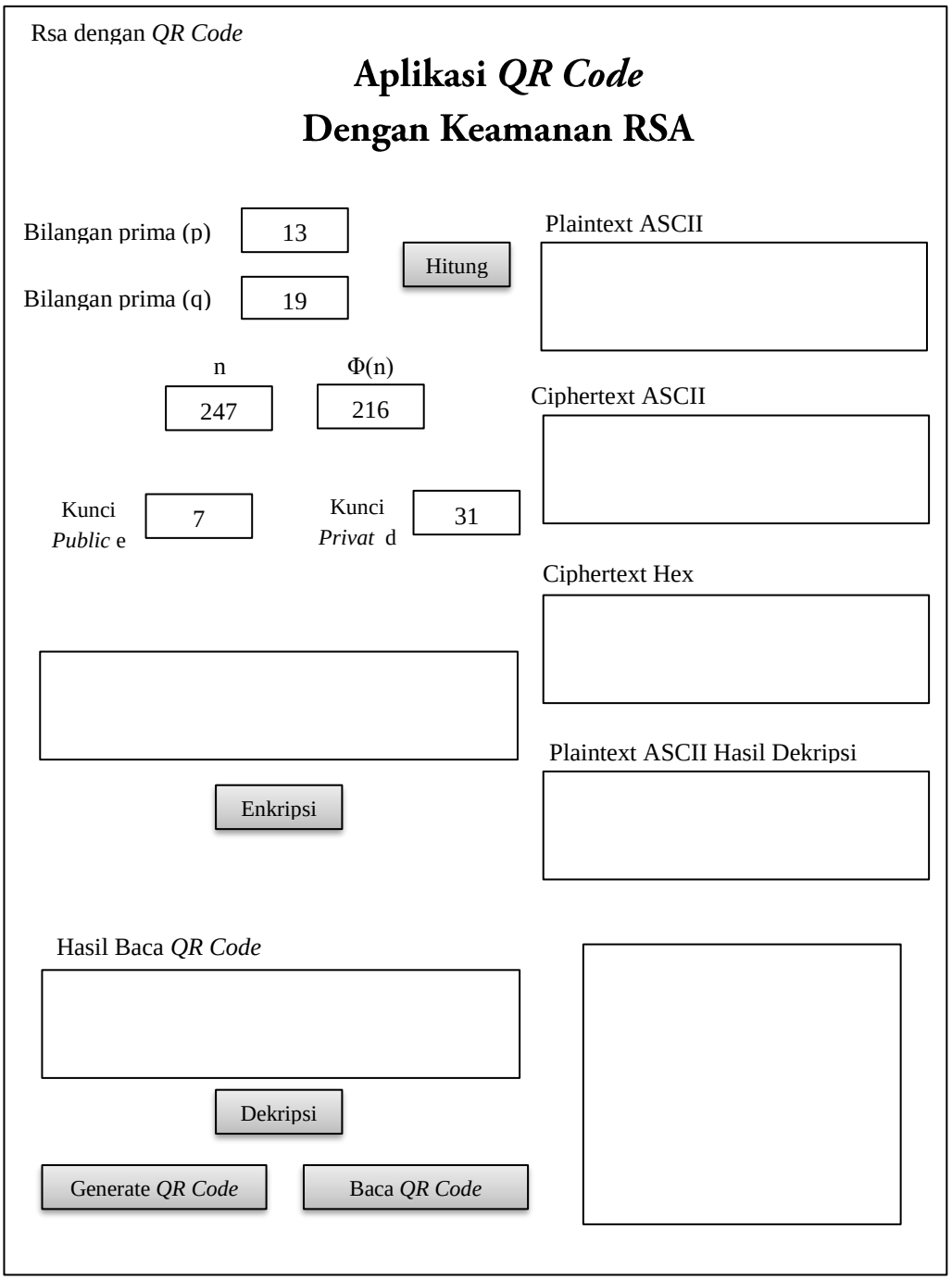
   $n = p*q$

   $n = 13*19 = 247$
3. Hitung nilai Φ(n) :

   $\Phi(n) = (p-1)(q-1)$

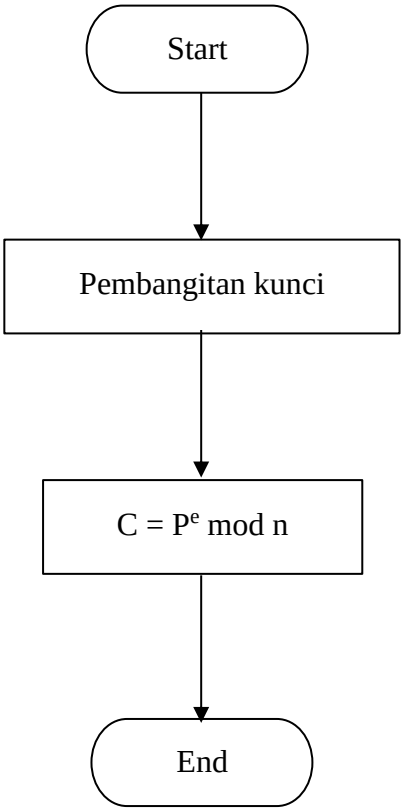
   $\Phi(n) = (13-1)(19-1) = 216$

Dengan suatu proses pemilihan e gcd (Φ(n),e)=1 dan d * e = 1+k(Φ(n)) maka akan diperoleh nilai e=7 dan d=31. Agar lebih jelas dapat dilihat pada gambar dibawah ini.



Gambar 3.3 Tampilan Proses Pembangkitan Kunci

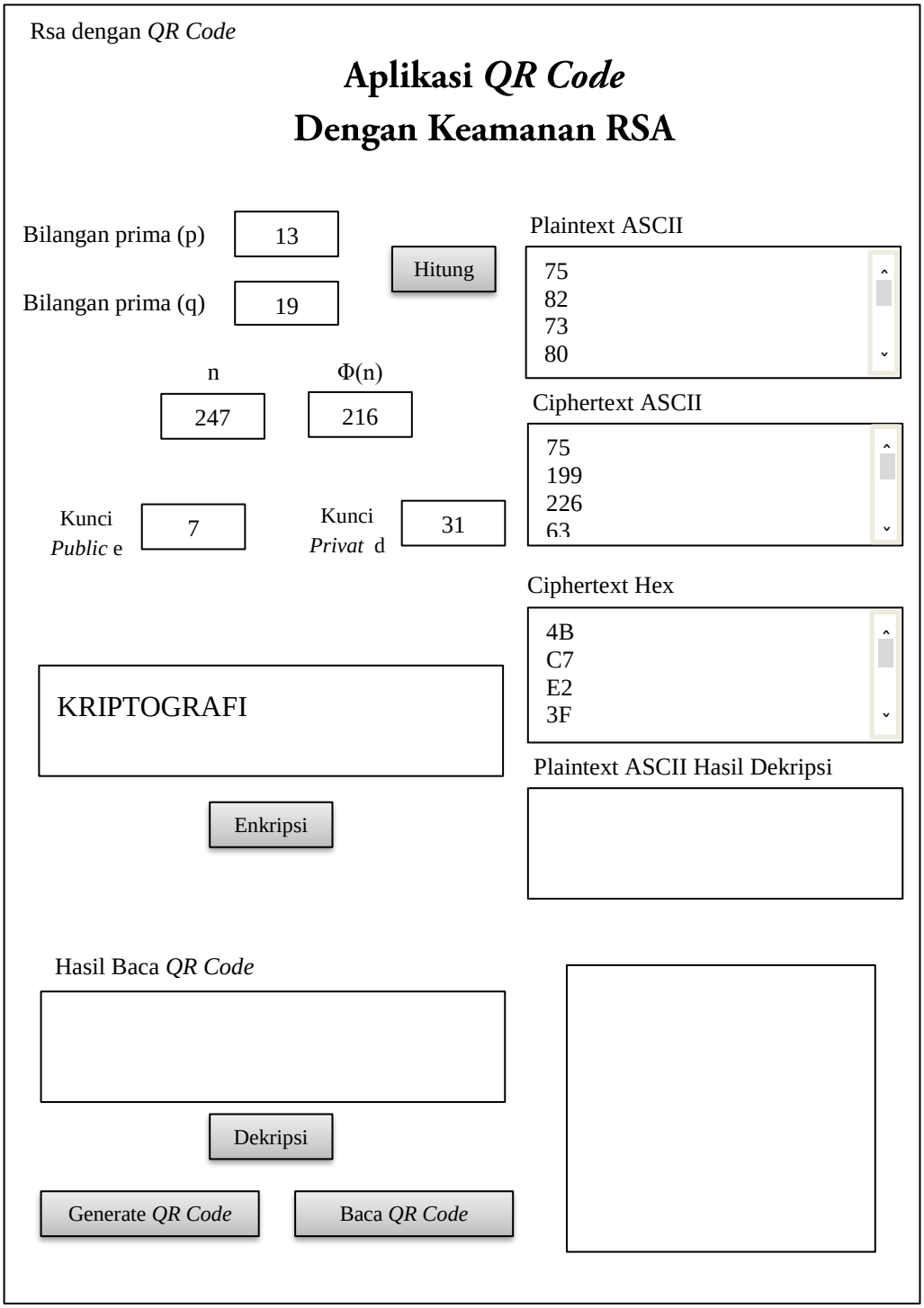
Setelah melalui proses pembangkitan kunci maka langkah selanjutnya adalah proses enkripsi pesan, adapun *Flowchart* proses enkripsi algoritma kriptografi RSA dapat dilihat pada gambar dibawah ini :



Gambar 3.4 *Flowchart* Enkripsi Algoritma RSA

Proses enkripsi dilakukan dengan menggunakan bilangan hasil dari proses pembangkitan kunci. Dengan rumus $C = P^e \bmod n$, dimana C merupakan sisa hasil pembagian dari dua bilangan, P bilangan ASCII dari pesan asli dan dipangkatkan dengan kunci e dibagi dengan n.

Untuk lebih jelasnya proses enkripsi dapat dilihat pada gambar tampilan proses enkripsi dibawah ini.



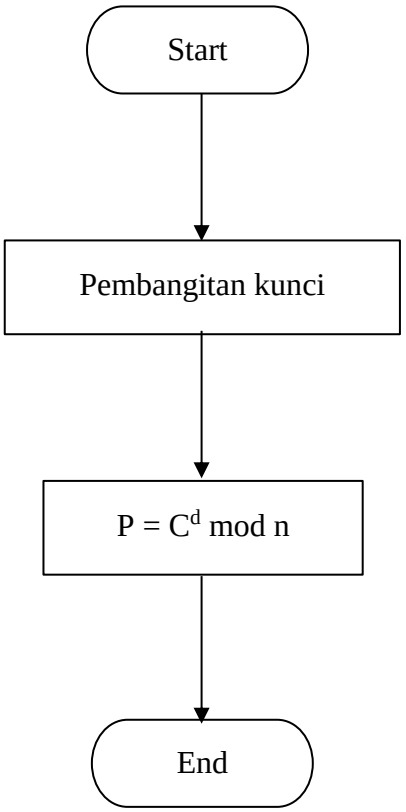
Gambar 3.5 Gambar Tampilan Proses Enkripsi

Algoritma dekripsi yang digunakan dalam algoritma RSA dapat dihitung dengan cara sebagai berikut :

1. Menggunakan kunci *privat* untuk mendekripsikan ciphertext menjadi *plaintext*.
2. Carilah M dengan rumus

$$P = C^d \bmod n$$

Flowchart proses dekripsi kriptografi RSA dapat dilihat pada gambar dibawah ini :

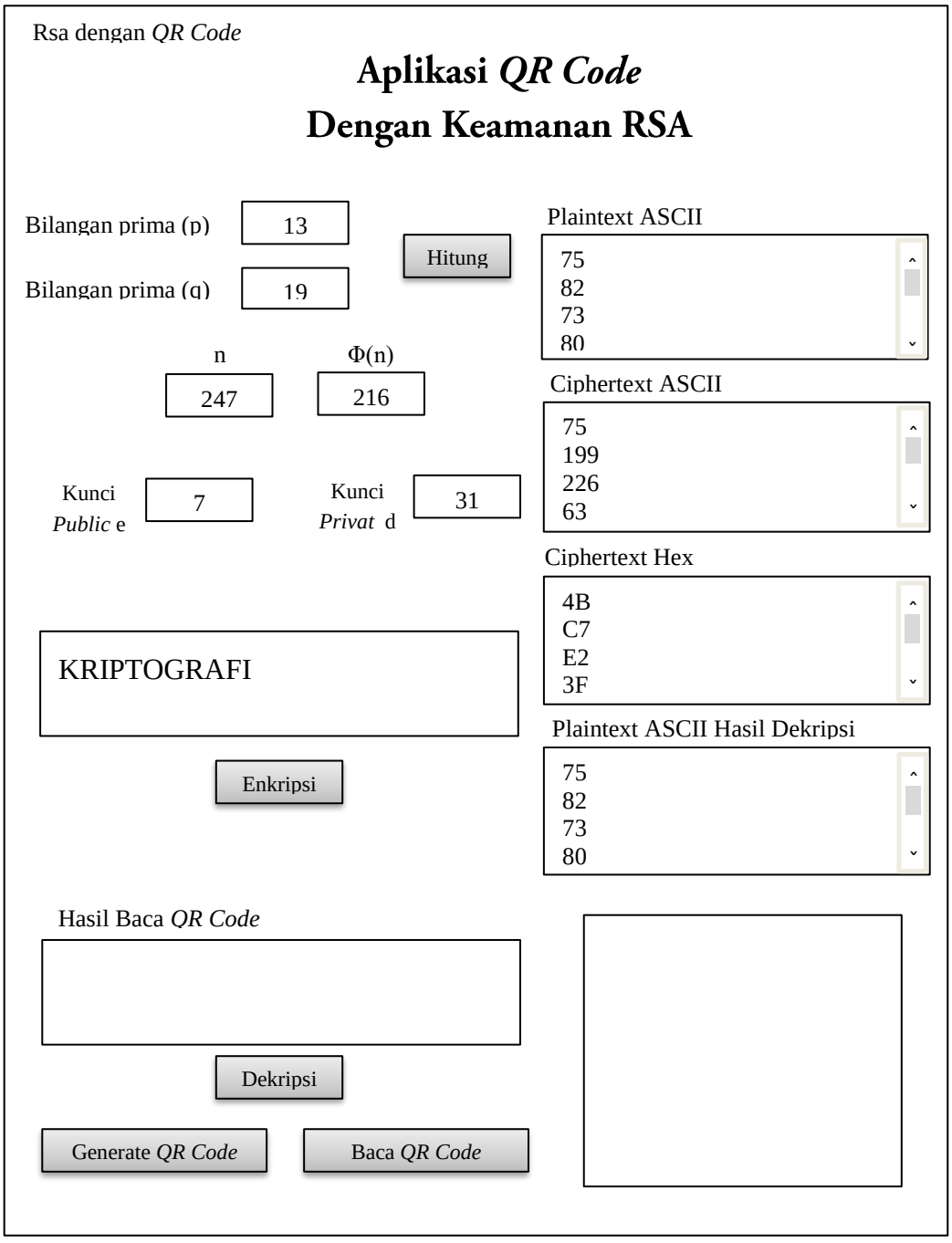


Gambar 3.6 *Flowchart* Dekripsi Algoritma RSA

Untuk mengembalikan pesan rahasia *ciphertext* menjadi *plaintext* diperlukan suatu proses dekripsi. Proses dekripsi ini memerlukan *private key* sebagai bilangan pemfaktorannya, dengan cara $P = C^d \bmod n$, P

merupakan hasil bagi dari dua bilangan *ciphertext* difaktorkan dengan d kunci private dan dibagi dengan n.

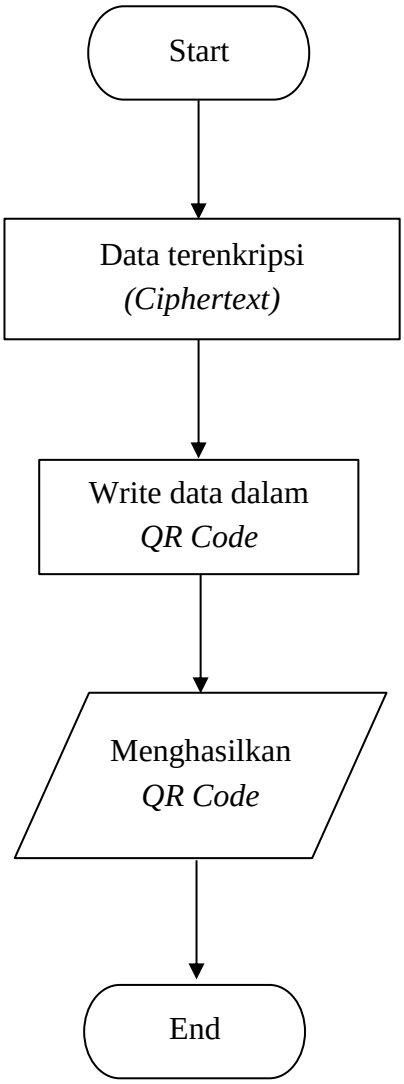
Untuk lebih jelasnya proses dekripsi dapat dilihat pada gambar tampilan proses dekripsi dibawah ini.



Gambar 3.7 Tampilan Proses Dekripsi

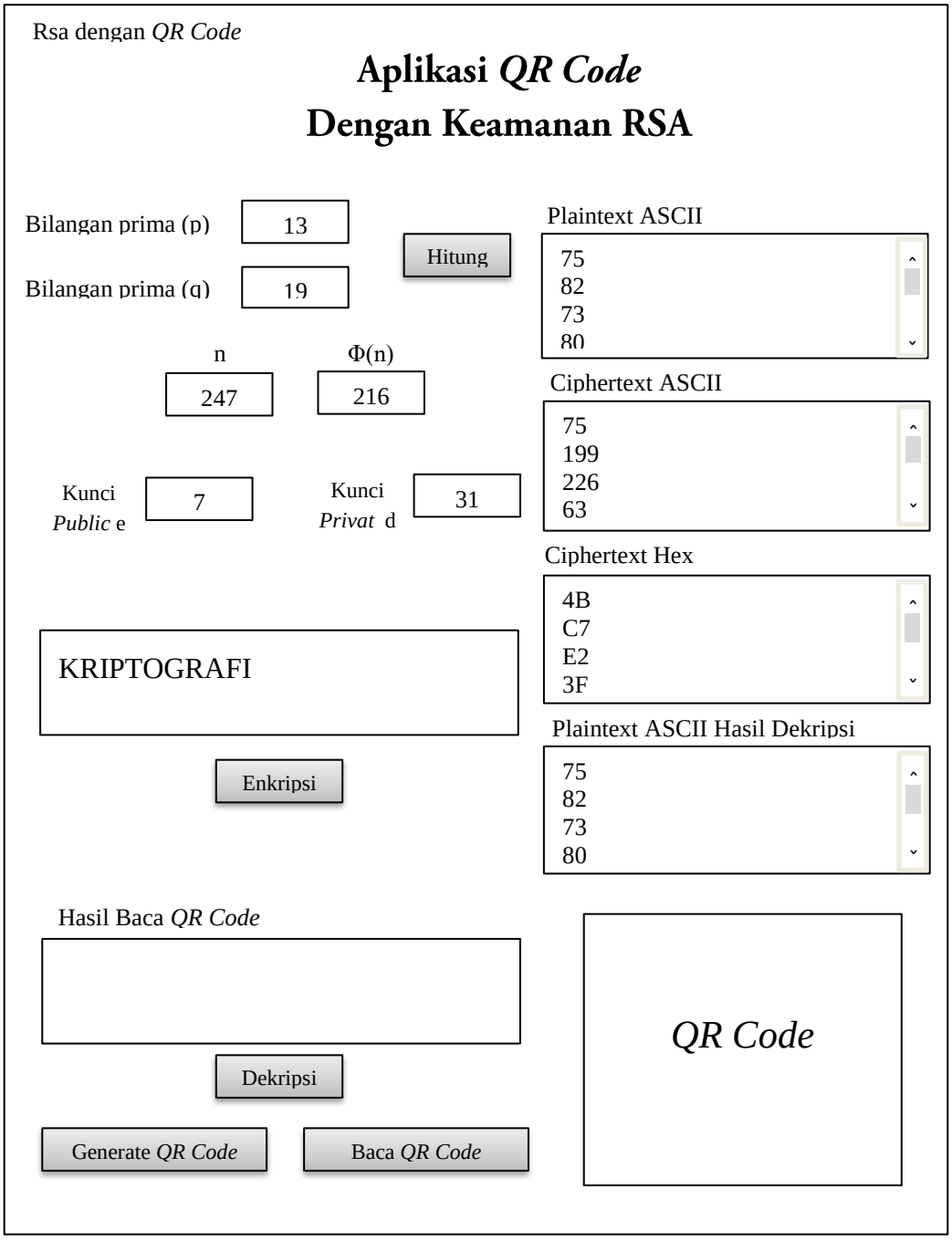
3.1.3 *Flowchart QR Code*

Pada flowchart ini merupakan suatu proses menghasilkan *QR Code* setelah proses *plaintext* menjadi *ciphertext*. *Ciphertext* akan dimasukkan ke *QR Code*, sehingga pesan yang berada pada *QR Code* bukanlah pesan asli melainkan pesan rahasia yang telah diproses dengan algoritma kriptografi RSA. Berikut ini *flowchart QR Code.*



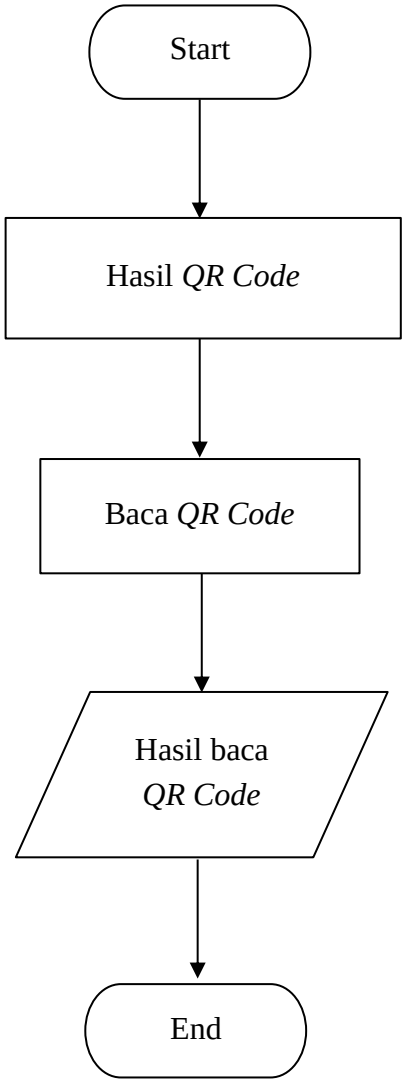
Gambar 3.8 *Flowchart QR Code*

Adapun tampilan proses menghasilkan *QR Code* dapat dilihat pada gambar dibawah ini.



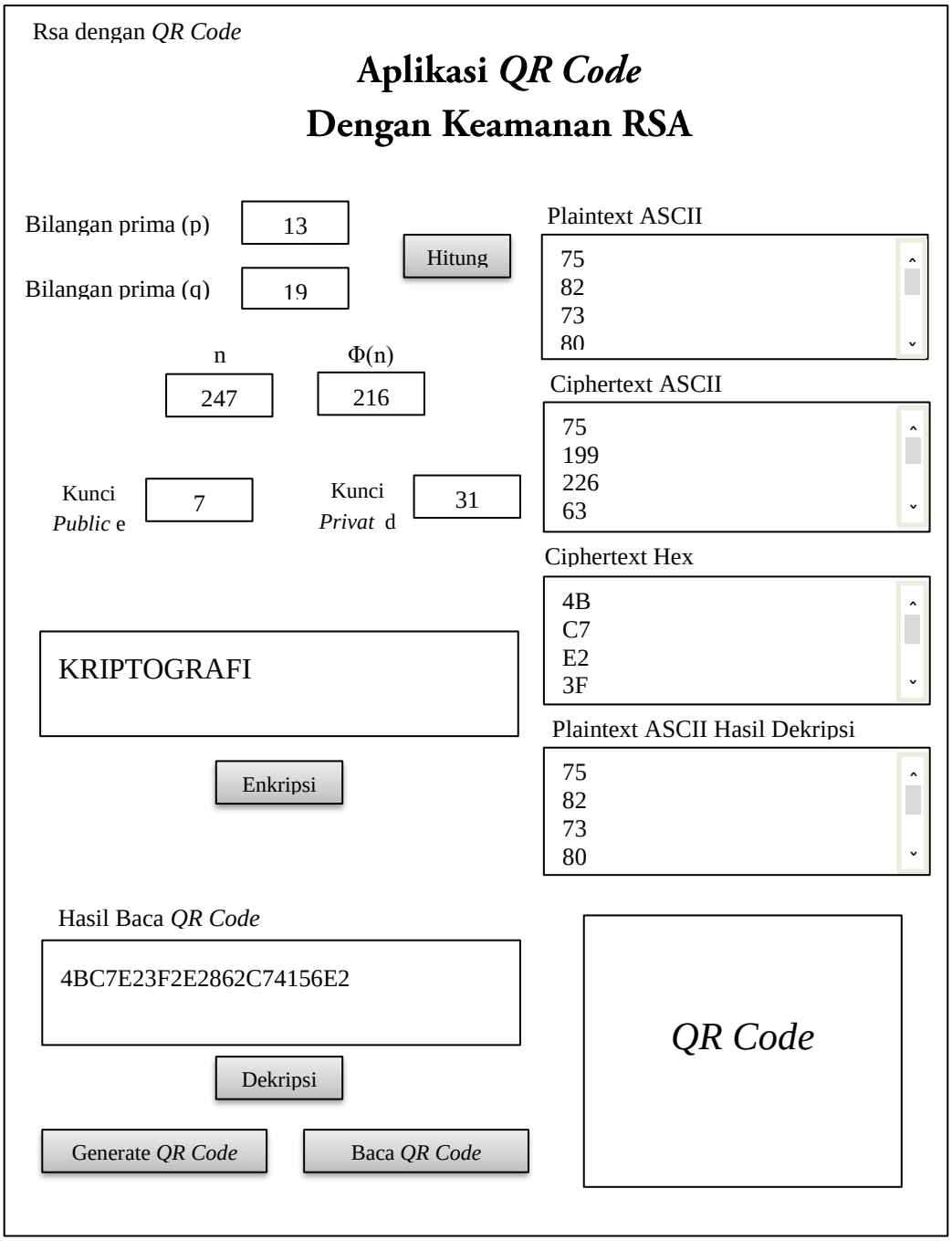
Gambar 3.9 Tampilan Menghasilkan *QR Code*

Pada bagian *QR Code* ini terdapat proses membaca *QR Code*. Sebagaimana flowchart pada proses hasil baca *QR Code* adalah sebagai berikut :



Gambar 3.10 *flowchart* hasil baca *QR Code*

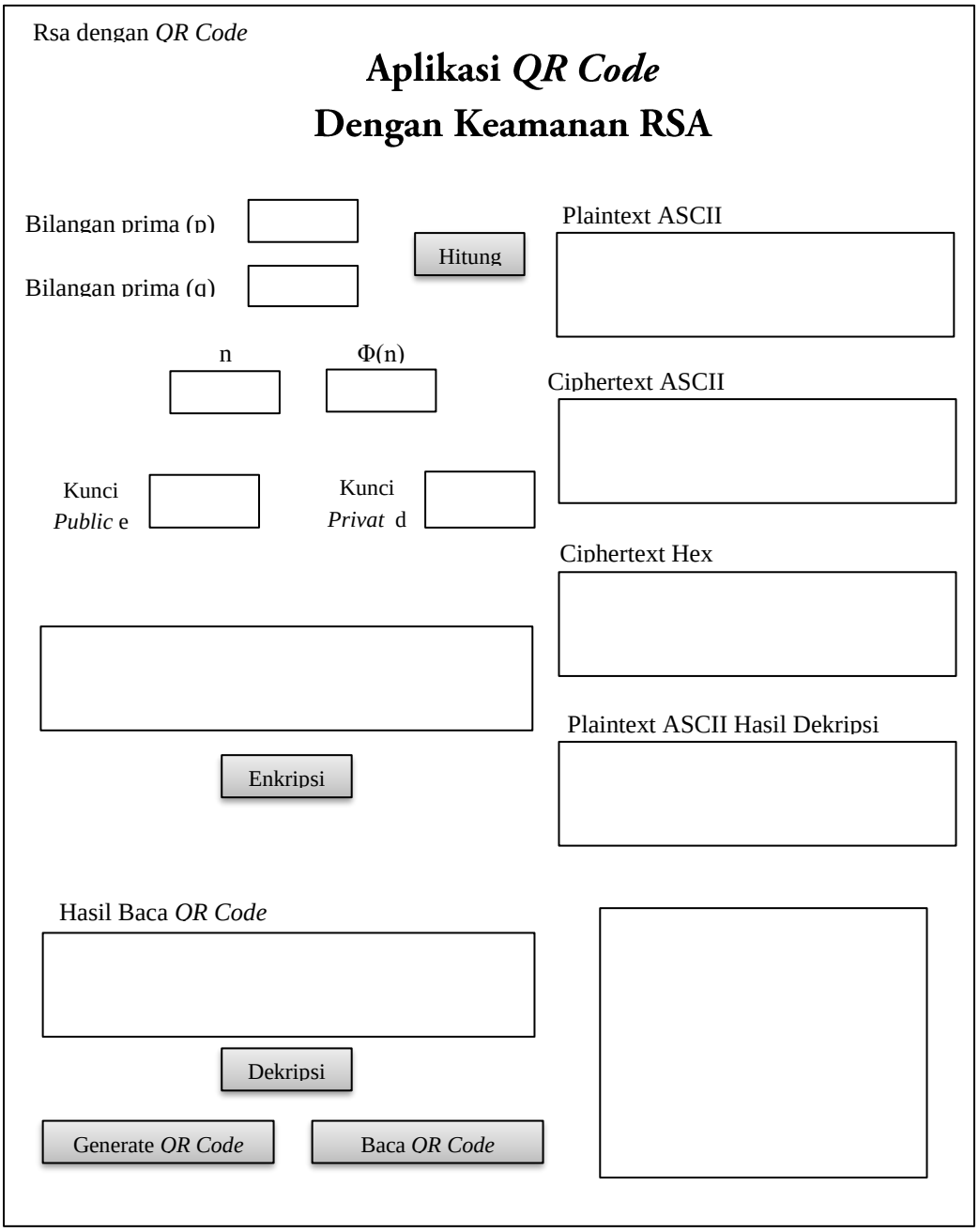
Proses hasil baca *QR Code* dapat dilihat pada rancangan aplikasi berikut ini :



Gambar 3.11 Tampilan Hasil Baca *QR Code*

3.2 Perancangan *Interface* Halaman Utama

Rancangan *interface* halaman utama merupakan rancangan tampilan pertama ketika aplikasi dijalankan. Adapun rancangan *interface* halaman utama dapat dilihat pada gambar berikut.



Gambar 3.12 *Interface* Halaman Utama

Pada *interface* halaman utama pengguna dihadapkan langsung pada pembangkitan kunci kriptografi RSA. Proses awal pada rancangan aplikasi tersebut ialah dengan memasukkan bilangan prima sebagai nilai p, dan q, pada saat *klik* hitung maka nilai p dan q akan diproses dan menampilkan hasil nilai n dan Φ(n), inputkan nilai e dan d sebagai kunci *public* dan kunci *privat*. *Plaintext* sebagai pesan asli diproses melalui tombol enkripsi, diubah bilangan ASCII dan pesan rahasia *ciphertext.* Melalui tombol *generate QR Code* akan menghasilkan *QR Code* dengan *ciphertext* yang terkandung didalamnya.

BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini dibahas tentang hasil serta pembahasan dari perancangan yang dibuat. Serta melakukan pengujian terhadap aplikasi untuk mengetahui apakah aplikasi tersebut telah berjalan sesuai yang diharapkan.

4.1 Kebutuhan Spesifikasi Minimum Hardware Dan Software

Perangkat keras (*hardware*) yang digunakan dalam pembuatan aplikasi ini adalah sebagai berikut :

1. *Prosesor intel core* i3,2.0 GHz
2. RAM 4096 MB
3. *HardDisk* dengan kapasitas 500GB
4. Monitor 14”
5. *Keyboard*

Adapun perangkat lunak (*software*) yang digunakan dalam pembuatan aplikasi ini adalah sebagai berikut :

1. Sistem operasi *Windows 10 Home Single Languange* 64-bit
2. *Visual basic* 1.1
3. *Net Framework* 4.0

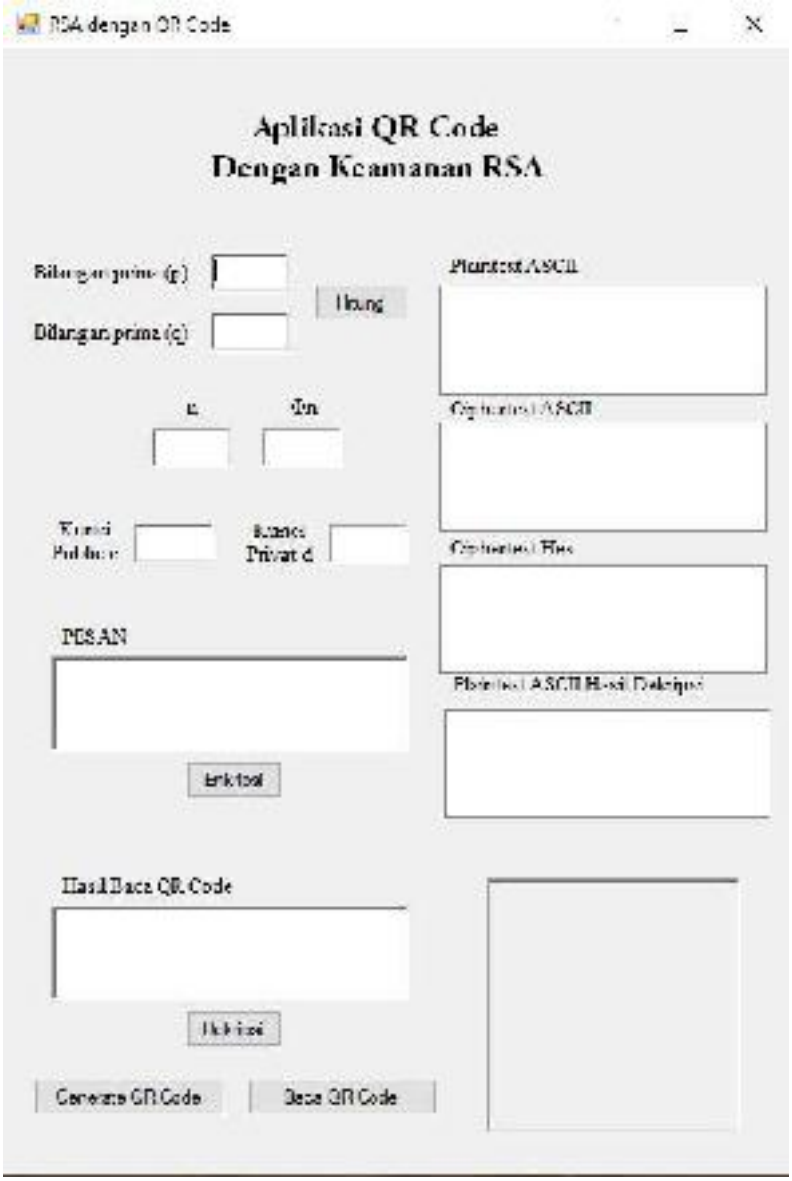
4.2 Pengujian Aplikasi Dan Pembahasan

Di dalam sub bab ini akan dijelaskan tentang implementasi dan pengujian aplikasi yang meliputi implementasi *interface*, dan implementasi *procedural* dari

algoritma kriptografi RSA yang diimplementasikan beserta kegunaan dari program yang dibuat. selain itu akan dibahas hasil implementasi algoritma RSA yang dibuat.

4.2.1 Implementasi *Interface*

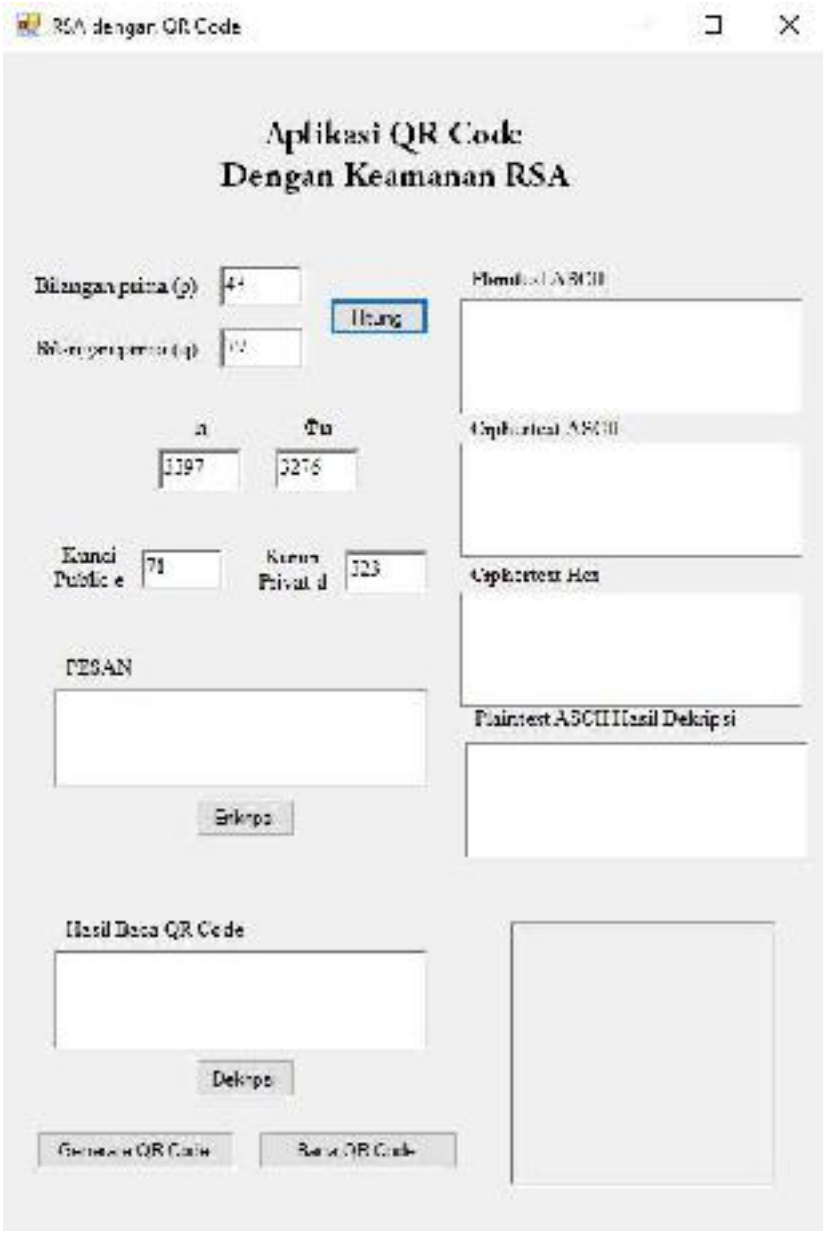
Implementasi *Interface* menampilkan implementasi hasil dari perancangan *interface.* Adapun *interface* program yang dibuat dapat dilihat pada gambar berikut ini :



Gambar 4.1 *Interface* Program

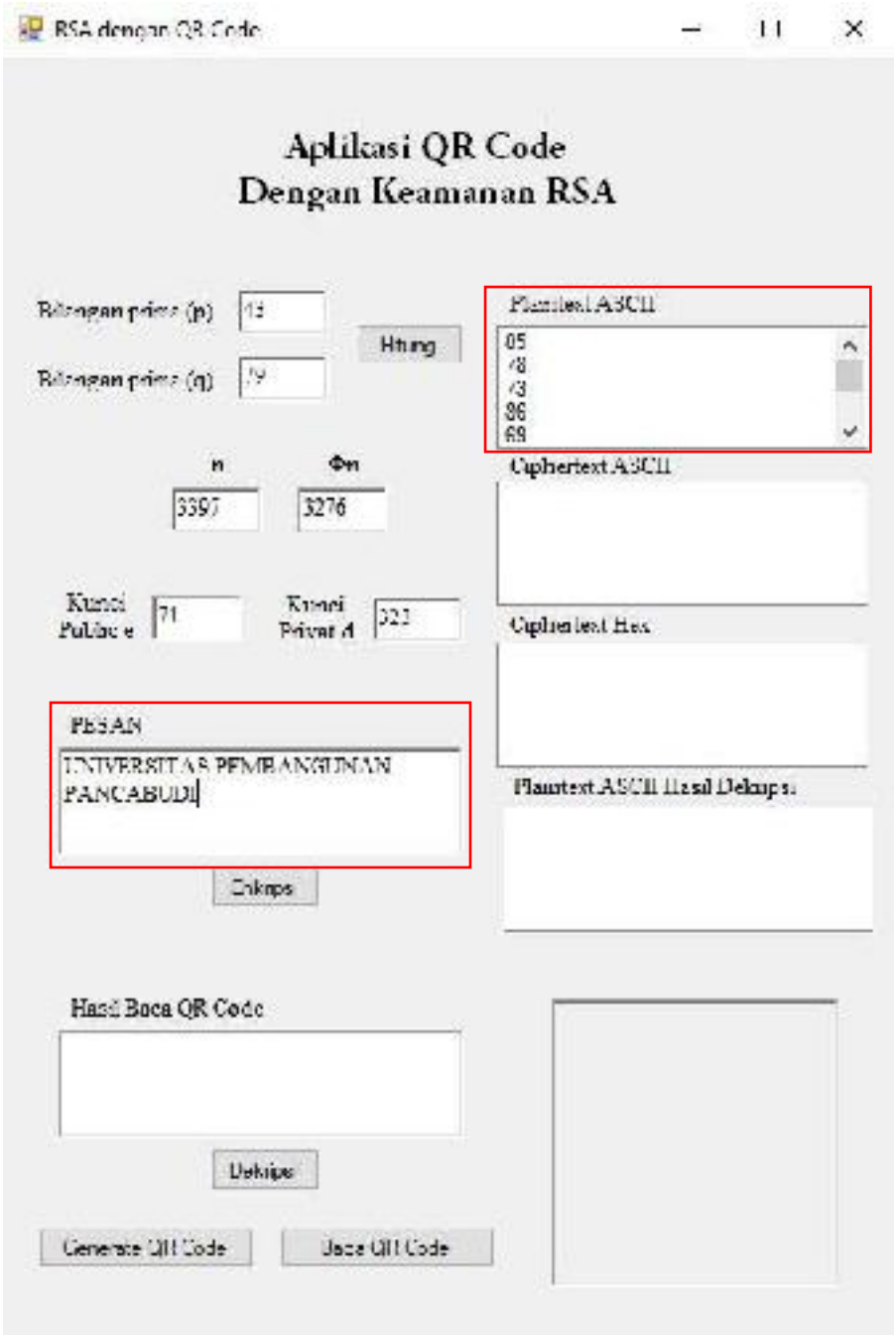
4.2.2 Pengujian Proses Enkripsi dan Dekripsi

Pada sub bab ini dibahas tentang pengujian sistem yang telah berjalan. Pengujian dilakukan untuk mengetahui apakah sistem berjalan sesuai yang diharapkan. Sebelum dilakukannya proses enkripsi dan dekripsi, algoritma kriptografi RSA terlebih dahulu melakukan proses pembangkitan kunci. Pengujian pembangkitan kunci RSA dapat dilihat pada gambar berikut ini :



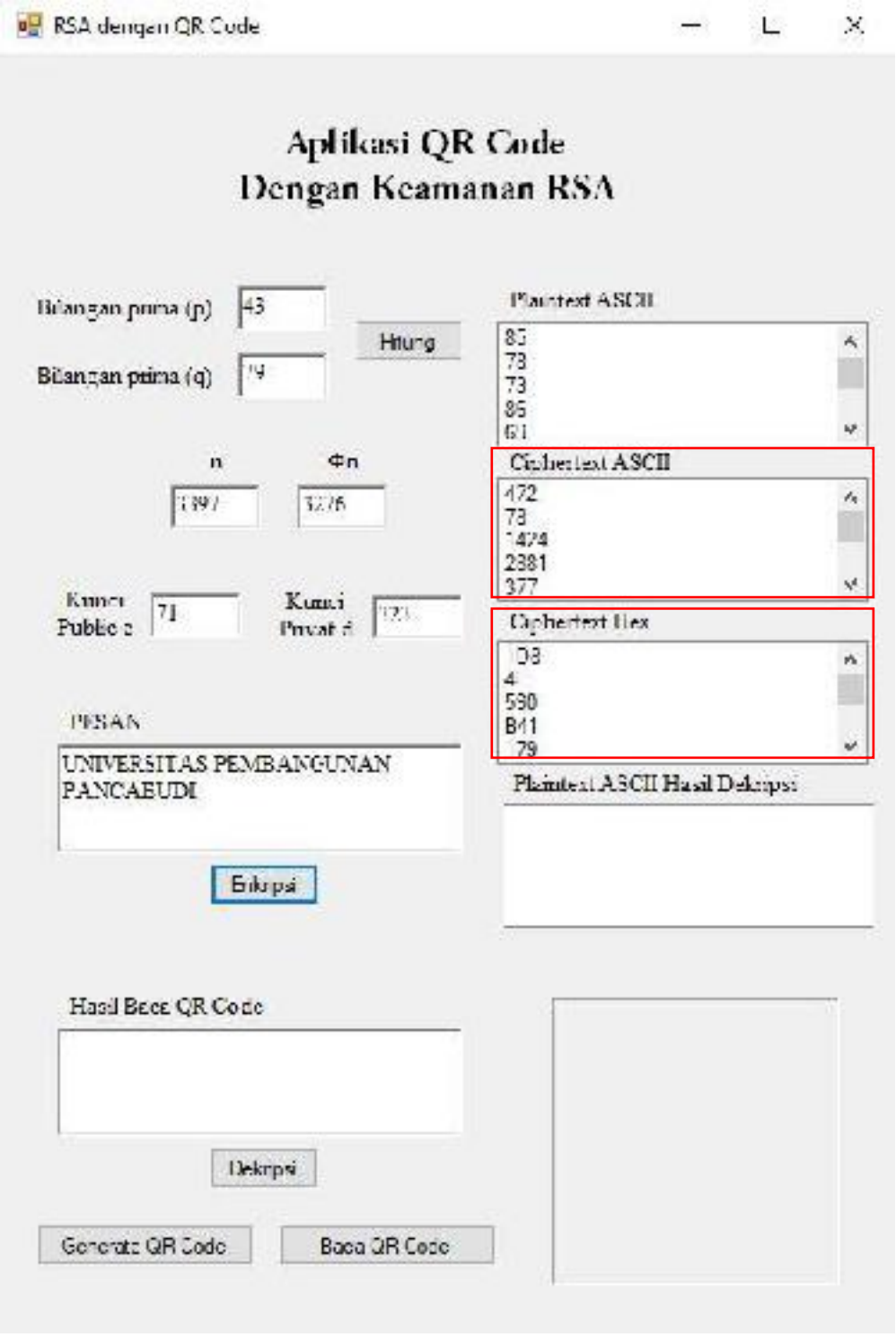
Gambar 4.2 Proses Pembangkitan Kunci RSA

Setelah proses pembangkitan kunci, dapat diteruskan dengan proses enkripsi. Pengujian proses enkripsi dilakukan pada *plaintext* “UNIVERSITAS PEMBANGUNAN PANCABUDI”. *Plaintext* tersebut terlebih daulu diubah menjadi bilangan *decimal.*



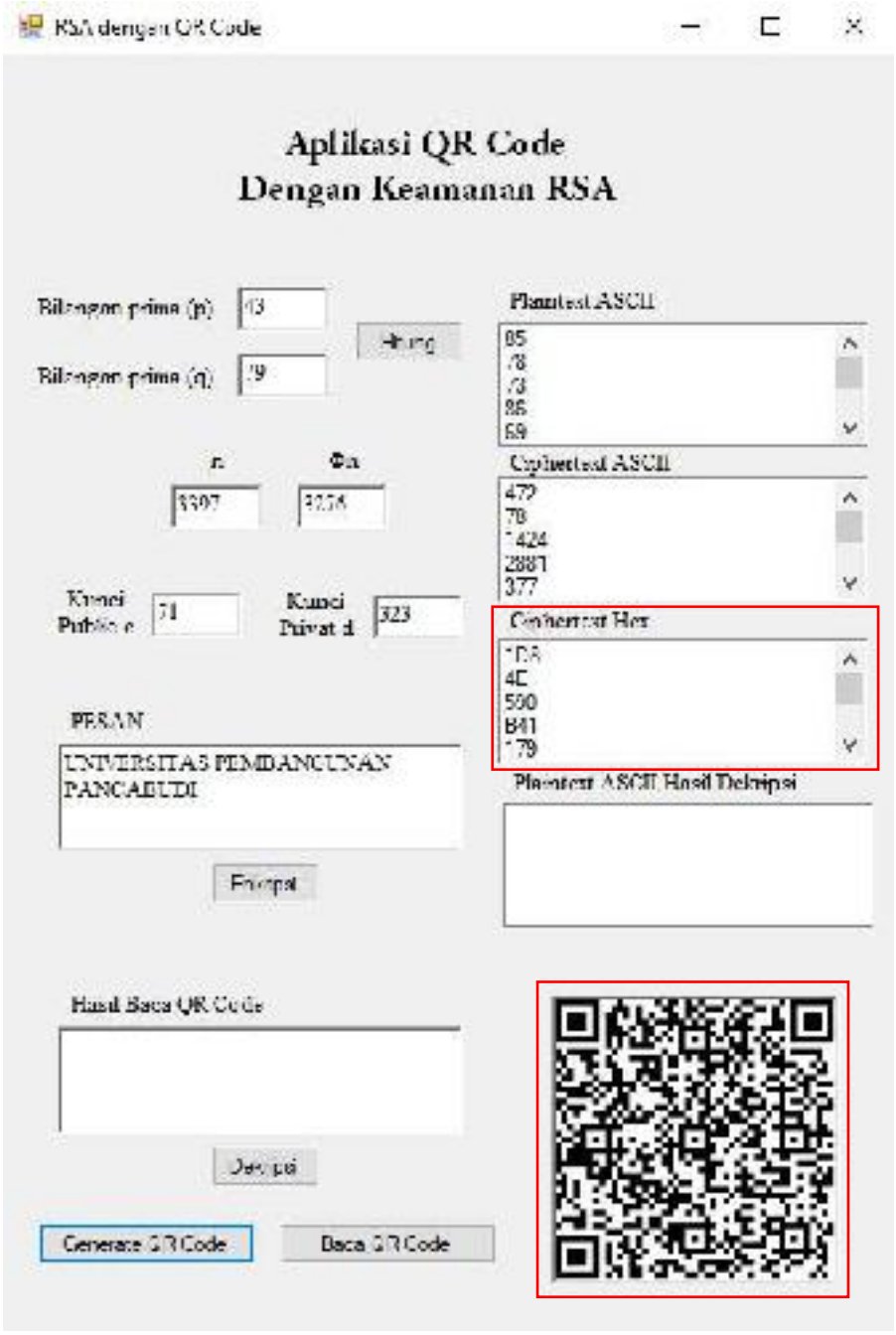
Gambar 4.3 Proses mengubah *plaintext* menjadi *decimal*

Pada program yang dibuat proses enkripsi dilakukan dengan menghasilkan bilangan ciphertext ASCII dan diubah menjadi bilangan hexadecimal.



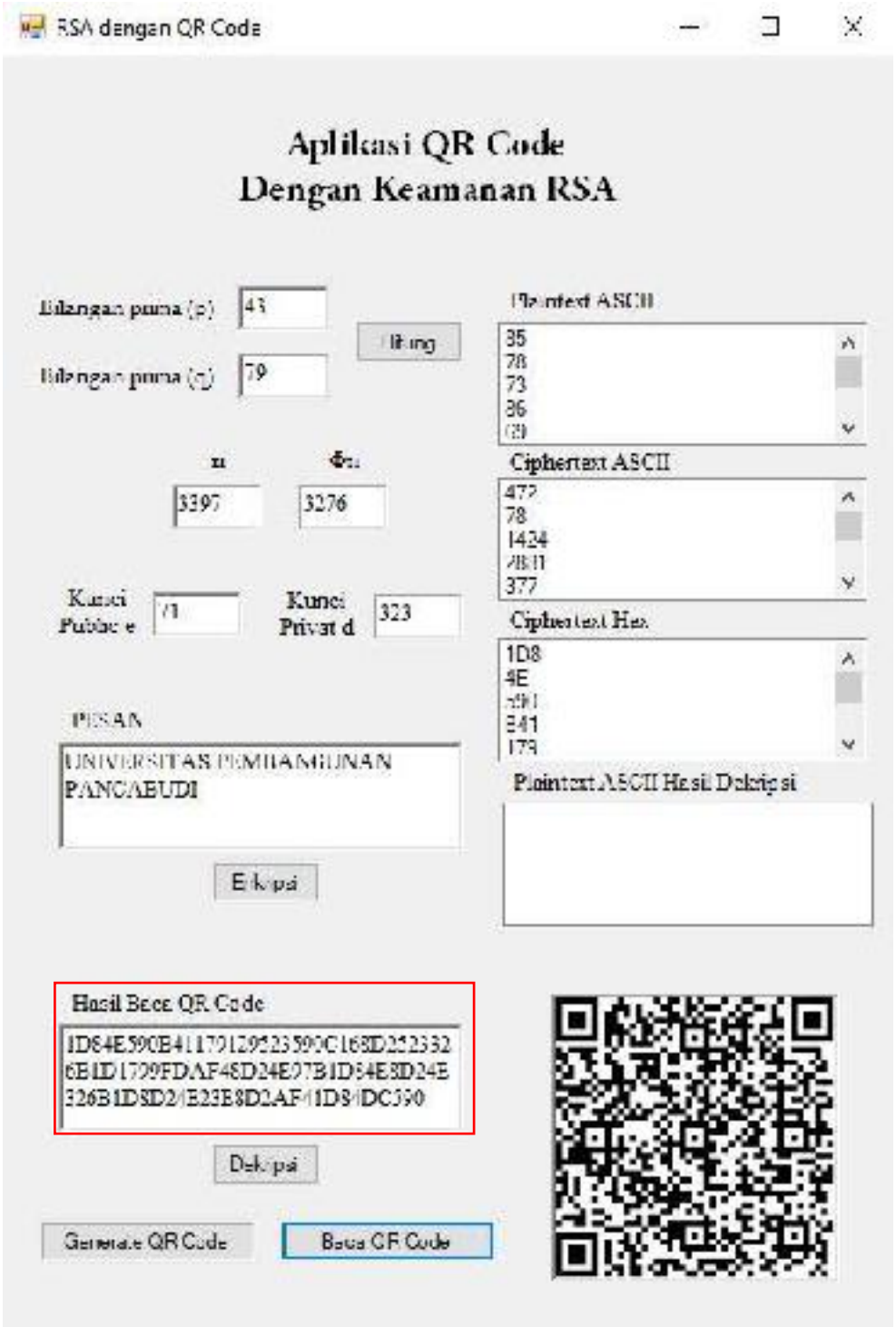
Gambar 4.4 Proses enkripsi pesan

Setelah proses enkripsi pesan dilakukan maka tahap selanjutnya adalah proses menghasilkan *QR Code*, dimana didalam *QR Code* terdapat pesan yang telah di enkripsi. Sehingga hasil dari *QR Code* berisi bilangan *hexadecimal* pada program akan tampil seperti pada gambar berikut:



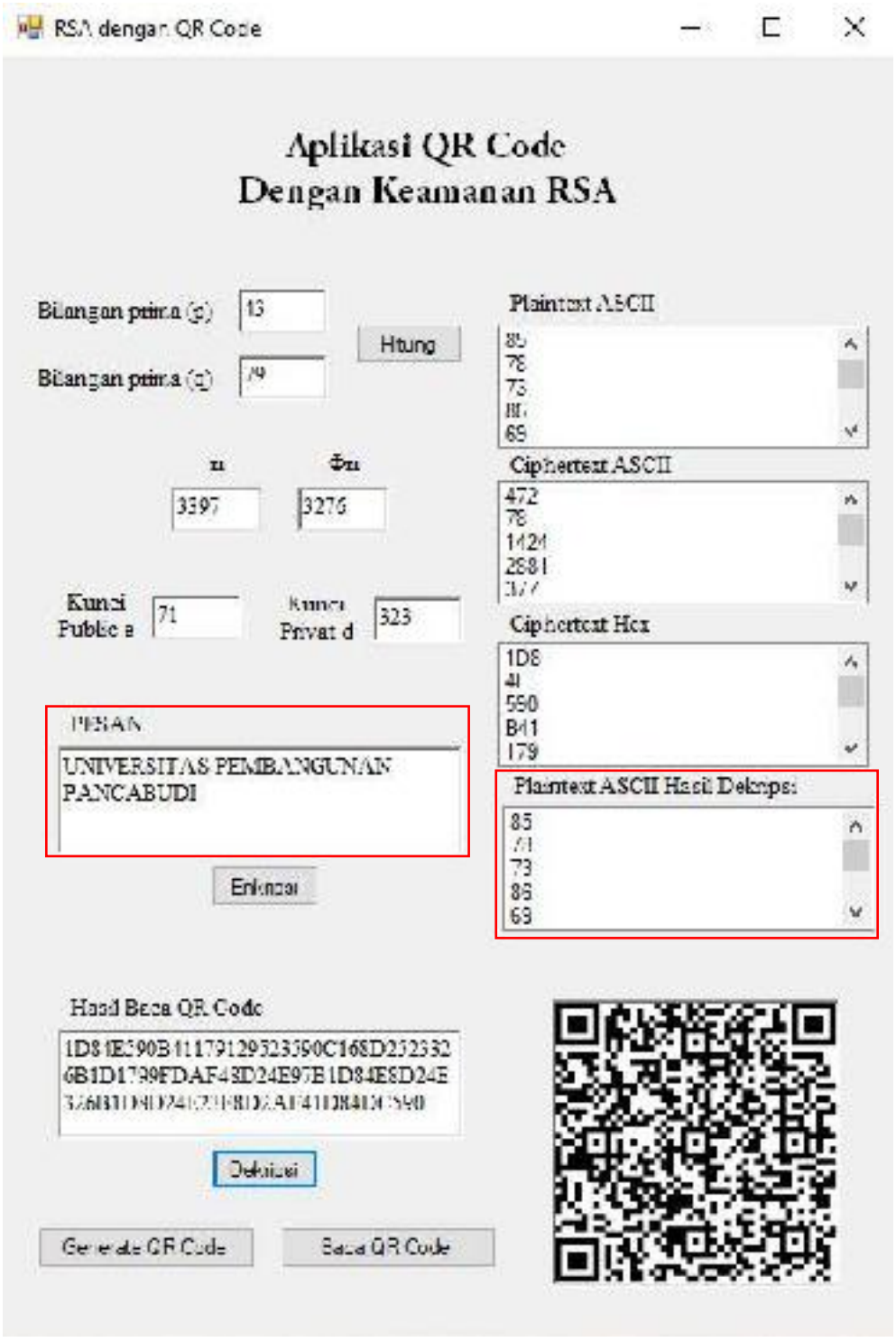
Gambar 4.5 Hasil *QR Code* pada program

Pada program yang dibuat, *QR Code* dapat dibaca pada tombol baca *QR Code*, yang dapat dilihat pada gambar sebagai berikut :



Gambar 4.6 Proses baca *QR Code*

Proses dekripsi dilakukan pada pengujian program dapat dilihat pada gambar berikut ini :



Gambar 4.7 Hasil dekripsi

4.2.3 Pembahasan Proses Enkripsi dan Dekripsi Algoritma RSA

a. Proses enkripsi

Pada pengujian enkripsi ini yang akan disimpan ke dalam *QR Code* adalah berupa pesan ataupun informasi. Pesan yang digunakan adalah sebagai berikut :

Plaintext = "UNIVERSITAS PEMBANGUNAN PANCABUDI"

1. p = 43 q = 79
2. n = p*q

   n = 43*79

   n = 3397
3. Φ(n) = (p-1)*(q-1)

   Φ(n) = (43-1)*79-1)

   Φ(n) = 3276
4. Kunci publik (e) = 71
5. kunci privat (d) = 323
6. *Plaintext* diubah ke format ASCII menjadi :

Tabel 4.1 Format ASCII *plaintext*

PT	U	N	I	V	E	R	S	I	T	A	S
ASCII PT	85	78	73	86	69	82	83	73	84	65	83
PT	_	P	E	M	B	A	N	G	U	N	A
ASCII PT	32	80	69	77	66	65	78	71	85	78	65
PT	N	_	P	A	N	C	A	B	U	D	I
ASCII PT	78	32	80	65	78	67	65	66	85	68	73

7. Melakukan proses enkripsi dengan rumus $C = P^e \bmod n$

$C_1 = 85^{71} \bmod 3397 = 472$

$C_2 = 78^{71} \bmod 3397 = 78$

$C_3 = 73^{71} \bmod 3397 = 1424$

$C_4 = 86^{71} \bmod 3397 = 2881$

$C_5 = 69^{71} \bmod 3397 = 377$

$C_6 = 82^{71} \bmod 3397 = 297$

$C_7 = 83^{71} \bmod 3397 = 1315$

$C_8 = 73^{71} \bmod 3397 = 1424$

$C_9 = 84^{71} \bmod 3397 = 3094$

$C_{10} = 65^{71} \bmod 3397 = 2258$

$C_{11} = 84^{71} \bmod 3397 = 1315$

$C_{12} = 32^{71} \bmod 3397 = 806$

$C_{13} = 80^{71} \bmod 3397 = 2845$

$C_{14} = 69^{71} \bmod 3397 = 377$

$C_{15} = 77^{71} \bmod 3397 = 2557$

$C_{16} = 66^{71} \bmod 3397 = 2804$

$C_{17} = 65^{71} \bmod 3397 = 2258$

$C_{18} = 78^{71} \bmod 3397 = 78$

$C_{19} = 71^{71} \bmod 3397 = 2427$

$C_{20} = 85^{71} \bmod 3397 = 472$

$C_{21} = 78^{71} \bmod 3397 = 78$

$C_{22} = 65^{71} \bmod 3397 = 2258$

$C_{23} = 78^{71} \bmod 3397 = 78$

$C_{24} = 32^{71} \bmod 3397 = 806$

$C_{25} = 80^{71} \bmod 3397 = 2845$

$C_{26} = 65^{71} \bmod 3397 = 2258$

$C_{27} = 78^{71} \bmod 3397 = 78$

$C_{28} = 67^{71} \bmod 3397 = 574$

$C_{29} = 65^{71} \bmod 3397 = 2258$

$C_{30} = 66^{71} \bmod 3397 = 2804$

$C_{31} = 85^{71} \bmod 3397 = 472$

$C_{32} = 68^{71} \bmod 3397 = 1244$

$C_{33} = 73^{71} \bmod 3397 = 1424$

Hasil Enkripsi dapat dilihat tabel dibawah ini pada baris CT (*ciphertext*)

Tabel 4.2 Hasil Enkripsi *ciphertext* ASCII

PT	U	N	I	V	E	R	S	I	T	A	S
ASCII PT	85	78	73	86	69	82	83	73	84	65	83
ASCII CT	**472**	**78**	**1424**	**2881**	**377**	**297**	**1315**	**1242**	**3094**	**2258**	**1315**
PT	_	P	E	M	B	A	N	G	U	N	A
ASCII PT	32	80	69	77	66	65	78	71	85	78	65
ASCII CT	**806**	**2845**	**377**	**2557**	**2804**	**2258**	**78**	**2427**	**472**	**78**	**2258**
PT	N	_	P	A	N	C	A	B	U	D	I
ASCII PT	78	32	80	65	78	67	65	66	85	68	73
ASCII CT	**78**	**806**	**2845**	**2258**	**78**	**574**	**2258**	**2804**	**472**	**1244**	**1424**

Berdasarkan tabel diatas ASCII CT merupakan hasil dari proses enkripsi $C = P^e \bmod n$ yang merupakan bilangan prima dari tabel ASCII. Untuk mendapatkan hasil enkripsi berupa *symbol* maka diperlukan suatu proses

mengubah nilai ASCII CT menjadi nilai *hexadecimal* dengan perhitungan sebagai berikut :

- ASCII CT_1 = 472

  DEC = 472 : 256 = 1

  472 – (1*256) = 216

  (1,216)

  HEX = 216 : 16 = 13 (D)

  216 – (13*16)

  = 216 – 208 = 8

  CT = (1 D8)

- ASCII CT_2 = 78

  HEX = 78 : 16 = 4

  78 – (4*16) = 14 (E)

  CT = (4E)

- ASCII CT_3 = 1424

  DEC = 1424 : 256 = 5

  1424 – (5*256) = 144

  (5,144)

  HEX = 144 : 16 = 9

  144 – (9*16)

  = 144 – 144 = 0

  CT = (5 90)

- ASCII CT_4 = 2881

  DEC = 2881 : 256 = 11(B)

  2881 – (11*256) = 65

  (11,65)

  HEX = 65 : 16 = 4

  65 – (4*16)

  = 65 – 64 = 1

  CT = (B 41)

- ASCII CT_5 = 377

  DEC = 377 : 256 = 1

  377 – (1*256) = 121

  (1,121)

  HEX = 121 : 16 = 7

  121 – (7*16)

  = 121 – 112 = 9

  CT = (1, 79)

  …….

- ASCII CT_{29} = 2258

  DEC = 2258 : 256 = 8

  2258 – (8*256) = 210

  (8,210)

HEX = 210 : 16 = 13

210 – (13*16)

= 210 – 208 = 2

CT = (8 D2)

- ASCII CT_{30} = 2804

DEC = 2804 : 256 = 10

2804 – (10*256) = 244

(10,244)

HEX = 244 : 16 = 15

244 – (15*16)

= 244 – 240 = 4

CT = (A F4)

- ASCII CT_{31} = 472

DEC = 472 : 256 = 1

472 – (1*256) = 216

(1,216)

HEX = 216 : 16 = 13 (D)

216 – (13*16)

= 216 – 208 = 8

CT = (1 D8)

- ASCII CT_{32} = 1244

DEC = 1244 : 256 = 4

1244 – (4*256) = 220

(5,144)

HEX = 220 : 16 = 13 (D)

220 – (13*16)

= 220 – 208 = 12 (C)

CT = (4 DC)

- ASCII CT_{33} = 1424

DEC = 1424 : 256 = 5

1424 – (5*256) = 144

(5,144)

HEX = 144 : 16 = 9

144 – (9*16)

= 144 – 144 = 0

CT = (5 90)

Dari proses perhitungan diatas maka hasil *hexadecimal* dapat diubah menjadi *symbol* yang tertera pada tabel ASCII. Agar lebih jelas dapat dilihat pada tabel hasil ciphertext dibawah ini :

Tabel 4.3 Hasil *ciphertext*

PT	U	N	I	V	E	R	S	I	T	A	S
ASCII PT	85	78	73	86	69	82	83	73	84	65	83
ASCII CT	**472**	**78**	**1424**	**2881**	**377**	**297**	**1315**	**1242**	**3094**	**2258**	**1315**
HEX CT	**1D8**	**4E**	**590**	**B41**	**179**	**129**	**523**	**4DA**	**C16**	**8D2**	**523**
CIPHERTEXT	**Ø**	**N**		**A**	**Y**	**)**	**#**	**Ú**		**Ò**	**#**
PT	_	P	E	M	B	A	N	G	U	N	A
ASCII PT	32	80	69	77	66	65	78	71	85	78	65
ASCII CT	**806**	**2845**	**377**	**2557**	**2804**	**2258**	**78**	**2427**	**472**	**78**	**2258**

HEX CT	**326**	**B1D**	**179**	**9FD**	**AF4**	**8D2**	**4E**	**97B**	**1D8**	**4E**	**8D2**
CIPHERTEXT	**&**		**y**	**ý**	**Ô**	**Ò**	**N**	**{**	**Ø**	**N**	**Ò**
PT	N	_	P	A	N	C	A	B	U	D	I
ASCII PT	78	32	80	65	78	67	65	66	85	68	73
ASCII CT	**78**	**806**	**2845**	**2258**	**78**	**574**	**2258**	**2804**	**472**	**1244**	**1424**
HEX CT	**4E**	**326**	**B1D**	**8D2**	**4E**	**23E**	**8D2**	**AF4**	**1D8**	**4DC**	**590**
CIPHERTEXT	**N**	**&**		**Ò**	**N**	**>**	**Ò**	**ô**	**Ø**	**Ü**	

Pada batasan masalah penulis telah menjelaskan bahwa *ciphertext* yang akan disimpan pada *QR Code* hanya berupa bilangan *hexadecimal*. Sehingga hasil dari *QR Code* dapat dilihat pada gambar dibawah ini.

Gambar 4.8 Hasil *QR Code*

Apabila *QR Code* dis*can* maka *QR Code* tersebut tetap menghasilkan pesan enkripsi (*ciphertext)* berupa bilangan *hexadecimal* seperti pada tebel 4.3 diatas. Adapun *ciphertext* yang berada pada *QR Code* adalah :

1D84E590B41179129523590C168D2523326B1D1799FDAF48D24E97B1D8

4E8D24E326B1D8D24E23E8D2AF41D84DC590

b. Proses dekripsi

Dekripsi dilakukan untuk mengubah pesan yang tidak bisa terbaca berupa *ciphertext* ke pesan asli (*plaintext*). Proses dekripsi menggunakan kunci d sebagai kunci privat untuk mengubah pesan rahasia menjadi pesan asli. Secara perhitungan manual, *ciphertext* berupa *symbol* dari bilangan *hexadecimal* akan dilakukan perhitungan menjadi bilangan *decimal* (ASCII CT) dan hasil ASCII CTlah yang akan diproses dengan rumus dekripsi RSA, $P = C^d \bmod n$. Adapun perhitungan dari HEX CT menjadi ASCII CT adalah sebagai berikut :

- HEX CT_1 = 1D8

  ASCII CT $= 1*16^2 + 13*16^1 + 8*16^0$

  $= 256 + 208 + 8$

  $= 472$

- HEX CT_2 = 4E

  ASCII CT $= 4*16^1 + 14*16^0$

  $= 64 + 14$

  $= 78$

- HEX CT_3 = 5 90

  ASCII CT $= 5*16^2 + 9*16^1 + 0*16^0$

  $= 1280 + 144 + 0$

  $= 1424$

- HEX CT_4 = B41

  ASCII CT $= 11*16^2 + 4*16^1 + 1*16^0$

= 2816 + 64 + 1

= 2881

- HEX CT_5 = 1 79

  ASCII CT = $1*16^2 + 7*16^1 + 9*16^0$

  = 256 + 112 + 9

  = 377

……..

- HEX CT_{30} = 8 D2

  ASCII CT = $8*16^2 + 13*16^1 + 2*16^0$

  = 2048 + 208 + 2

  = 2258

- HEX CT_{30} = A F4

  ASCII CT = $10*16^2 + 15*16^1 + 4*16^0$

  = 2560 + 240 + 4

  = 2804

- HEX CT_{31} = 1D8

  ASCII CT = $1*16^2 + 13*16^1 + 8*16^0$

  = 256 + 208 + 8

  = 472

- HEX CT_{32} = 4 DC

  ASCII CT = $4*16^2 + 13*16^1 + 12*16^0$

= 1024 + 208 + 12

= 1244

- HEX CT_{33} = 5 90

  ASCII CT = $5*16^2 + 9*16^1 + 0*16^0$

  = 1280 + 144 + 0

  = 1424

Tabel 4.4 Hasil perhitungan ASCII *ciphertext*

CIPHERTEXT	Ø	N		A	y	)	#	Ú		Ò	#
HEX CT	1D8	4E	590	B41	179	129	523	4DA	C16	8D2	523
ASCII CT	**472**	**78**	**1424**	**2881**	**377**	**297**	**1315**	**1242**	**3094**	**2258**	**1315**
CIPHERTEXT	&		y	ý	ô	Ò	N	{	Ø	N	Ò
HEX CT	326	B1D	179	9FD	AF4	8D2	4E	97B	1D8	4E	8D2
ASCII CT	**806**	**2845**	**377**	**2557**	**2804**	**2258**	**78**	**2427**	**472**	**78**	**2258**
CIPHERTEXT	N	&		Ò	N	>	Ò	ô	Ø	Ü	
HEX CT	4E	326	B1D	8D2	4E	23E	8D2	AF4	1D8	4DC	590
ASCII CT	**78**	**806**	**2845**	**2258**	**78**	**574**	**2258**	**2804**	**472**	**1244**	**1424**

Setelah perhitungan mengubaj *hexadecimal* menjadi bilangan ASCII CT maka proses dekripsi dilakukan. Adapun proses dekripsi dengan rumus :

$P = C^d \bmod n$

$P_1 = 472^{323} \bmod 3397 = 85$

$P_2 = 78^{323} \bmod 3397 = 78$

$P_3 = 1424^{323} \bmod 3397 = 73$

$P_4 = 2881^{323} \mod 3397 = 86$

$P_5 = 377^{323} \mod 3397 = 69$

$P_6 = 297^{323} \mod 3397 = 82$

$P_7 = 1315^{323} \mod 3397 = 83$

$P_8 = 1242^{323} \mod 3397 = 73$

$P_9 = 3094^{323} \mod 3397 = 84$

$P_{10} = 2258^{323} \mod 3397 = 65$

$P_{11} = 1315^{323} \mod 3397 = 84$

$P_{12} = 806^{323} \mod 3397 = 32$

$P_{13} = 2845^{323} \mod 3397 = 80$

$P_{14} = 377^{323} \mod 3397 = 69$

$P_{15} = 2557^{323} \mod 3397 = 77$

$P_{16} = 2804^{323} \mod 3397 = 66$

$P_{17} = 2258^{323} \mod 3397 = 65$

$P_{18} = 78^{323} \mod 3397 = 78$

$P_{19} = 2427^{323} \mod 3397 = 71$

$P_{20} = 472^{323} \mod 3397 = 85$

$P_{21} = 78^{323} \mod 3397 = 78$

$P_{22} = 2258^{323} \mod 3397 = 65$

$P_{23} = 78^{323} \mod 3397 = 78$

$P_{24} = 806^{323} \mod 3397 = 32$

$P_{25} = 2845^{323} \mod 3397 = 80$

$P_{26} = 2258^{323} \mod 3397 = 65$

$P_{27} = 78^{323} \mod 3397 = 78$

$P_{28} = 574^{323} \mod 3397 = 67$

$P_{29} = 2258^{323} \mod 3397 = 65$

$P_{30} = 2804^{323} \mod 3397 = 66$

$P_{31} = 472^{323} \mod 3397 = 85$

$P_{32} = 1244^{323} \mod 3397 = 68$

$P_{33} = 1424^{323} \mod 3397 = 73$

Maka hasil dari proses dekripsi dapat dilihat pada tabel berikut ini :

Tabel 4.5 Hasil Dekripsi *plaintext*

ASCII CT	472	78	1424	2881	377	297	1315	1242	3094	2258	1315
ASCII PT	**85**	**78**	**73**	**86**	**69**	**82**	**83**	**73**	**84**	**65**	**83**
PT	**U**	**N**	**I**	**V**	**E**	**R**	**S**	**I**	**T**	**A**	**S**
ASCII CT	806	2845	377	2557	2804	2258	78	2427	472	78	2258
ASCII PT	**32**	**80**	**69**	**77**	**66**	**65**	**78**	**71**	**85**	**78**	**65**
PT	**_**	**P**	**E**	**M**	**B**	**A**	**N**	**G**	**U**	**N**	**A**
ASCII CT	78	806	2845	2258	78	574	2258	2804	472	1244	1424
ASCII PT	**78**	**32**	**80**	**65**	**78**	**67**	**65**	**66**	**85**	**68**	**73**
PT	**N**	**_**	**P**	**A**	**N**	**C**	**A**	**B**	**U**	**D**	**I**

Dari hasil program serta pengujian dan pembahasan perhitunga diatas telah diketahui bahwa *QR Code* dapat menyimpan pesan dengan keamanan RSA. Dengan adanya algoritma RSA, maka pesan yang berada pada *QR Code* tidak dapat sembarangan dibaca dan dimodifikasi oleh orang yang tidak berkepentingan. Hal ini dikarenakan algoritma RSA memiliki dua kunci yang berbeda dan sulitnya

dalam memfaktorkan bilangan primanya. Mengamankan pesan dengan menggunakan algoritma RSA pada *QR Code* ini dapat berfungsi juga sebagai mengirim dan menerima pesan rahasia melalui *QR Code*.

BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Kesimpulan yang dapat diambil berdasarkan pembahasan mengenai implementasi *QR Code* menggunakan algoritma RSA dapat diambil kesimpulan sebagai berikut :

1. Algoritma kriptografi RSA dapat diimplementasikan pada *QR Code* untuk mengamankan pesan dan informasi yang ada di dalam *QR Code*
2. Pesan yang disimpan di dalam *QR Code* berupa *ciphertext* yang merupakan hasil enkripsi menggunakan algoritma kriptografi RSA, sehingga pihak yang tidak berwenang tidak dapat membaca dan memanipulasi pesan tersebut.
3. *QR Code* dapat menampung pesan yang sudah menjadi *ciphertext* tanpa mengubah isi *ciphertext* tersebut.
4. Semakin besar kunci public yang digunakan maka semakin kecil kemungkinan kunci privat untuk diketahui.
5. Keluaran yang dihasilkan memiliki panjang karakter yang berbeda dengan karakter yang dimasukkan (*plaintext*), ini disebabkan karena semakin besar bilangan prima yang digunakan maka semakin besar pula hasil dari proses enkripsi sehingga hasil proses enkripsi melebihi dari 256 karakter pada tabel ASCII.

5.2 Saran

Beberapa saran untuk penelitian dan pengembangan aplikasi selanjutnya adalah sebagai berikut:

1. Pengembangan aplikasi yang telah dilakukan masih perlu dilakukan studi, penyesuaian, dan perbaikan lebih lanjut.
2. Pada penelitian selanjutnya dapat melakukan pengembangan sistem agar sistem dapat mendekripsikan pesan pada *QR Code* dengan cara mens*can QR Code* secara langsung.

DAFTAR PUSTAKA

Albert, Ginting, R., Rizal, I., Ike, P, W. (2015) Implementasi Algoritma Kriptografi RSA Untuk Enkripsi dan Dekripsi Email. Vol.3 No.2 e-ISSN: 2238-0403. https://jtsiskom.undip.ac.id/index.php/jtsiskom/article/download/12009/11662

Ariyus, Dony. (2006). Kriptografi Keamanan Data Dan Komunikasi. Yogyakarta: Graha Ilmu.

Atika Sari, C., Hari Rachmawanto, Eko. (2014). Gabungan Algoritma Vernam Cipher dan End Of File untuk Keamanan Data. Vol.13, No.3. 150-157. https://publikasi.dinus.ac.id/index.php/technoc/article/download/565/334

Hidayat, A., Yogi, B., Paulus, E. 2017. Kriptografi Hillcipher Digunakan Dalam Sistem Keamanan Pada Tiket Dengan Teknologi *QR-CODE*. Jurnal Siliwangi. Vol.3 No.1 e-ISSN: 2477-3891. http://jurnal.unsil.ac.id/index.php/jssainstek/article/download/244/195

Sasmita, A. (2016, 27 Agustus). Makalah Aritmatika Modulo. Tulisan pada https://ayusasmitaweb.wordpress.com/2016/08/27/makalah-aritmetika-modulo/

Syaputra, H., Herdiyatmoko, H, F. 2012. Aplikasi Enkripsi Data Pada File Text Dengan Algoritma RSA. Jurusan Teknik Informatika. Sekolah Tinggi Teknik Musi, Palembang. Diakses dari http://eprints.dinus.ac.id/95/

Wibowo, Ivan dkk. 2009. Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data di Oracle. Fakultas Teknik. Universitas Kristen Duta Wacana. Diakses dari https://ti.ukdw.ac.id/ojs/index.php/informatika/article/view/68/32

Widiyanti Y.T. 2017. Aplikasi Teknologi QR (Quick Response) Code Implementasi Yang Universal. Komputaki. Vol.3 No.1. pp. 66-82 http://www.unaki.ac.id/ejournal/index.php/komputaki/article/download/154/166

Wikipedia. (2019). ASCII. Diakses 5 Maret 2019, dari https://id.wikipedia.org/wiki/ASCII

Wikipedia. (2019). Kode QR. Diakses 2 Maret 2019, dari https://id.wikipedia.org/wiki/Kode_QR

Zulkarnain, H, A., Munjiat, S.A., Herlina, H. 2019. Penerapan QR Code dan Vigenere Cipher Dalam Sistem Pelaporan Juru Parkir Ilegal. Jurnal Sistem Informasi. Vol.3 No.1 e-ISSN: 2579-5341 http://jurnal.uinsu.ac.id/index.php/query/article/download/4460/2199

Badawi, A. (2018). Evaluasi Pengaruh Modifikasi Three Pass Protocol Terhadap Transmisi Kunci Enkripsi.

Batubara, Supina. "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan." IT Journal Research and Development 2.1 (2017): 1-11.

Bahri, S. (2018). Metodologi Penelitian Bisnis Lengkap Dengan Teknik Pengolahan Data SPSS. Penerbit Andi (Anggota Ikapi). Percetakan Andi Ofsset. Yogyakarta.

Erika, Winda, Heni Rachmawati, and Ibnu Surya. "Enkripsi Teks Surat Elektronik (E-Mail) Berbasis Algoritma Rivest Shamir Adleman (RSA)." Jurnal Aksara Komputer Terapan 1.2 (2012).

Fitriani, W., Rahim, R., Oktaviana, B., & Siahaan, A. P. U. (2017). Vernam Encypted Text in End of File Hiding Steganography Technique. Int. J. Recent Trends Eng. Res, 3(7), 214-219.

Hardinata, R. S. (2019). Audit Tata Kelola Teknologi Informasi menggunakan Cobit 5 (Studi Kasus: Universitas Pembangunan Panca Budi Medan). Jurnal Teknik dan Informatika, 6(1), 42-45.

Hariyanto, E., Lubis, S. A., & Sitorus, Z. (2017). Perancangan prototipe helm pengukur kualitas udara. KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), 1(1).

Hariyanto, E., & Rahim, R. (2016). Arnold's cat map algorithm in digital image encryption. International Journal of Science and Research (IJSR), 5(10), 1363-1365.

Harumy, T. H. F., & Sulistianingsih, I. (2016). Sistem penunjang keputusan penentuan jabatan manager menggunakan metode mfep pada cv. Sapo durin. In Seminar Nasional Teknologi Informasi dan Multimedia (pp. 6-7).

Iqbal, M., Siahaan, A. P. U., Purba, N. E., & Purwanto, D. (2017). Prim's Algorithm for Optimizing Fiber Optic Trajectory Planning. Int. J. Sci. Res. Sci. Technol, 3(6), 504-509.

Marlina, L., Muslim, M., Siahaan, A. U., & Utama, P. (2016). Data Mining Classification Comparison (Naïve Bayes and C4. 5 Algorithms). Int. J. Eng. Trends Technol, 38(7), 380-383.

Muttaqin, Muhammad. "ANALISA PEMANFAATAN SISTEM INFORMASI E-OFFICE PADA UNIVERSITAS PEMBANGUNAN PANCA BUDI MEDAN DENGAN MENGGUNAKAN METODE UTAUT." Jurnal Teknik dan Informatika 5.1 (2018): 40-43.

Ramadhan, Z., Zarlis, M., Efendi, S., & Siahaan, A. P. U. (2018). Perbandingan Algoritma Prim dengan Algoritma Floyd-Warshall dalam Menentukan Rute Terpendek (Shortest Path Problem). JURIKOM (Jurnal Riset Komputer), 5(2), 135-139.

Rahim, R., Aryza, S., Wibowo, P., Harahap, A. K. Z., Suleman, A. R., Sihombing, E. E., ... & Agustina, I. (2018). Prototype file transfer protocol application for LAN and Wi-Fi communication. Int. J. Eng. Technol., 7(2.13), 345-347.

Wahyuni, Sri. "Implementasi Rapidminer Dalam Menganalisa Data Mahasiswa Drop Out." Jurnal Abdi Ilmu 10.2 (2018): 1899-1902.

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

rsitas : Universitas Pembangunan Panca Budi
tas : SAINS & TEKNOLOGI
n Pembimbing I : Andylala Adeta Utama Siahaan, S.Kom., M.Kom
n Pembimbing II : Hendry, S.Kom., M.Kom
Mahasiswa : ARIFFIN
an/Program Studi : Sistem Komputer
r Pokok Mahasiswa : 1514370078
ng Pendidikan : Strata Satu (S1)
Tugas Akhir/Skripsi : Implementasi QR Code Menggunakan Algoritma RSA.

ANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
7/2	Revisi Proposal / Judul		
28/2	Acc Seminar Judul		
3/3	Revisi Judul		
5/3	Revisi Bab I, II		
10/3	Revisi Bab III, IV		
12/3	Revisi Bab IV, Kesimpulan		
14	Acc Seminar Proposal		
15/6	Acc Sidang		
20/7	Acc Jilid		

Medan, 22 Februari 2019
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

t yang tidak perlu

FM-BPAA-2012-038

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

ersitas	: Universitas Pembangunan Panca Budi
ltas	: SAINS & TEKNOLOGI
en Pembimbing I	: Andysah Putera Utama Siahaan, S.Kom, M.Kom
en Pembimbing II	: Hendry, S.Kom, M.Kom
e Mahasiswa	: ARIFFIN
san/Program Studi	: Sistem Komputer
or Pokok Mahasiswa	: 1514370078
ang Pendidikan	: Strata Satu (S1)
l Tugas Akhir/Skripsi	: Implementasi QR Code Menggunakan Algoritma RSA.

ANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
-3. 2019	Acc Judul	[paraf]	
-3. 2019	Acc Seminar Proposal	[paraf]	
7. 2019	Acc Bab 1, lanjut Bab 2	[paraf]	
7. 2019	perbaiki penulisan sesuai panduan	[paraf]	
3. 2019	perbaiki Bab 2, tambahkan ...	[paraf]	
	sesuai dgn panduan skripsi	[paraf]	
3. 2019	Acc Bab 2, lanjut Bab 3	[paraf]	
o. 7. 2019	perbaiki Bab 3.	[paraf]	
3. 4. 2019	Acc Bab 3, lanjut Bab 4.	[paraf]	
4. 2019	Rev. Bab 4 & lanjut Bab 5	[paraf]	
	Acc Seminar Hasil	[paraf]	
8. 4. 2019		[paraf]	
6. 6. 2019	Acc Sidang	[paraf]	
1. 7. 2019	Acc Jilid		

Medan, 22 Februari 2019
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

ret yang tidak perlu

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km 4,5 Medan Fax. 061-8458077 PO BOX : 1099 MEDAN

PROGRAM STUDI TEKNIK ELEKTRO	(TERAKREDITASI)
PROGRAM STUDI TEKNIK ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

Saya yang bertanda tangan di bawah ini :

Nama Lengkap	: ARIFFIN
Tempat/Tgl. Lahir	: Medan / 10 Maret 1998
Nomor Pokok Mahasiswa	: 1514370078
Program Studi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Jumlah Kredit yang telah dicapai	: 141 SKS, IPK 3.70
Nomor Hp	: 081262176964
Dengan ini mengajukan judul sesuai bidang ilmu sebagai berikut	:

No.	Judul
1.	IMPLEMENTASI QR CODE MENGGUNAKAN ALGORITMA RSA

Catatan : Diisi Oleh Dosen Jika Ada Perubahan Judul

*Coret Yang Tidak Perlu

Medan, 05 April 2019

Pemohon,

(Ariffin)

Dekan,

(Ir. Iskandar Alamsyah, M.T., Ph.D.)

Tanggal : 16 April 2019

Disetujui oleh:

Dekan,

(Dr. Sahnidi Indra, S.T., M.Sc.)

Tanggal : .....

Disetujui oleh:

Dosen Pembimbing I :

(Andysah Putera Utama Siahaan, S.Kom., M.Kom)

Tanggal : 16 April 2019

Disetujui oleh:

Ka. Prodi Sistem Komputer

(MUHAMMAD IQBAL, S.Kom, M.Kom.)

Tanggal : .....

Disetujui oleh:

Dosen Pembimbing II:

(HENDRY, S.KOM., M.KOM.)

YAYASAN PROF. DR. H. KADIRUN YAHYA
UNIVERSITAS PEMBANGUNAN PANCA BUDI
LABORATORIUM KOMPUTER
Jl. Jend. Gatot Subroto Km 4,5 Sei Sikambing Telp. 061-8455571
Medan - 20122

KARTU BEBAS PRAKTIKUM

Yang bertanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

Nama	:	ARIFFIN
N.P.M.	:	1514370078
Tingkat/Semester	:	Akhir
Fakultas	:	SAINS & TEKNOLOGI
Jurusan/Prodi	:	Sistem Komputer

Benar-benar telah menyelesaikan urusan Administrasi di Laboratorium Komputer Universitas Pembangunan Panca Budi Medan

Medan, 27 Juni 2019

SOURCE CODE

```
Imports System.Numerics
Imports MessagingToolkit.QRCode.Codec
Imports MessagingToolkit.QRCode.Codec.Data

Public Class frmRA
    Dim p, q, n, t, k, nilai_e, nilai_d As BigInteger
    Dim QRCode As Bitmap

    Private Function GCD(ByVal m As BigInteger, ByVal n As BigInteger) As
BigInteger
        Dim r As BigInteger = n Mod m

        While (r <> 0)
            r = m Mod n
            m = n
            n = r
        End While

        Return m
    End Function

    Private Function HEX(ByVal dec As BigInteger) As String
        Dim r As String = ""
        Dim sb As Byte = 0
        Dim hb As BigInteger = dec

        While (hb > 0)

            sb = hb Mod 16
            hb = hb / 16

            Select Case sb
                Case 0 To 9
                    r = Convert.ToString(sb) & r
                Case 10
                    r = "A" & r
                Case 11
                    r = "B" & r
                Case 12
                    r = "C" & r
                Case 13
                    r = "D" & r
                Case 14
                    r = "E" & r
                Case 15
                    r = "F" & r
            End Select
        End While

        Return r
    End Function
```

```
    Private Sub btnHitung_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnHitung.Click
        p = txtP.Text
        q = txtQ.Text
        n = BigInteger.Multiply(p, q)
        t = BigInteger.Multiply(p - 1, q - 1)

        ' Mencari nilai E
        nilai_e = 70
        While (GCD(nilai_e, t) <> 1)
            nilai_e += 1
        End While

        'Mencari nilai D
        k = 1
        While ((t * k + 1) Mod nilai_e <> 0)
            k += 1
        End While

        nilai_d = (t * k + 1) / nilai_e

        txtN.Text = n.ToString()
        txtTotien.Text = t.ToString()
        txtE.Text = nilai_e.ToString()
        txtD.Text = nilai_d.ToString()
    End Sub

    Private Sub txtPT_TextChanged(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles txtPT.TextChanged
        lsbPT.Items.Clear()
        For i = 0 To txtPT.TextLength - 1
            lsbPT.Items.Add(Convert.ToByte(txtPT.Text(i)))
        Next
    End Sub

    Private Sub frmRA_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load
        txtPT.Text = ""
    End Sub

    Private Sub btnEnkrip_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnEnkrip.Click
        lsbHex.Items.Clear()

        For i = 0 To lsbPT.Items.Count - 1

lsbCT.Items.Add(BigInteger.ModPow(Convert.ToByte(lsbPT.Items(i)), nilai_e,
n))
            lsbHex.Items.Add(HEX(lsbCT.Items(i)))

        Next
    End Sub

    Private Sub btnDekrip_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnDekrip.Click
        Dim PT As String = ""
```

```
        For i = 0 To lsbCT.Items.Count - 1
            lsbDT.Items.Add(BigInteger.ModPow(lsbCT.Items(i), nilai_d, n))
            PT &=
Convert.ToChar(Convert.ToInt16(Convert.ToString(lsbDT.Items(i))))
        Next

        txtPT.Text = PT
    End Sub

    Private Sub btnGenQR_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnGenQR.Click
        Dim QRText As String = ""
        Dim QRCodeEnc As New QRCodeEncoder

        For i = 0 To lsbHex.Items.Count - 1
            QRText &= lsbHex.Items(i)
        Next

        QRCode = QRCodeEnc.Encode(QRText)
        pbQR.Image = QRCode
    End Sub

    Private Sub btnBacaQR_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnBacaQR.Click
        Dim QRCodeDec As New QRCodeDecoder
        txtDT.Text = QRCodeDec.decode(New QRCodeBitmapImage(QRCode))
    End Sub

End Class
```

Telah Diperiksa oleh LPMU
dengan Plagiarisme 25 %
Medan, 27 Juni 2019
Ka. LPMU
UNPAB
[illegible], S.Kom., M.Kom
[illegible], SE., MM

Hal : Permohonan Meja Hijau

FM-BPAA-2012-041

Medan, 26 Juni 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah di terima
berkas persyaratan
dapat di proses
Medan, 27 JUN 2019
Ka. BPAA
TEGUH WAHYONO, SE., MM.

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: ARIFFIN
Tempat/Tgl. Lahir	: Medan / 10 Maret 1998
Nama Orang Tua	: SYAHRAN
N. P. M.	: 1514370079
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 0812621 78964
Alamat	: Jl. [illegible]

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul IMPLEMENTASI QR CODE MENGGUNAKAN ALGORITMA RSA.
Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkipnya sebanyak 1 lembar.
7. Terlampir pelunasan kwitansi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 examplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 examplar untuk penguji (bentuk dan warna penjilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
9. Soft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
10. Terlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
11. Setelah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
12. Bersedia melunaskan biaya-biaya uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1.	[102] Ujian Meja Hijau	: Rp.	100.000
2.	[170] Administrasi Wisuda	: Rp.	1.500.000
3.	[202] Bebas Pustaka	: Rp.	100.000
4.	[221] Bebas LAB	: Rp.	5.000
	Total Biaya	: Rp.	~~1.605.000~~ 1.705.000

S-Uk. Tertunda Rp 2.650.000
4.355.000

Ukuran Toga : XL

Diketahui/Disetujui oleh :

Hamdani, S.T., M.Sc.
Dekan Fakultas SAINS & TEKNOLOGI

Hormat saya

ARIFFIN
1514370079

Catatan :
- 1.Surat permohonan ini sah dan berlaku bila ;
  - a. Telah dicap Bukti Pelunasan dari UPT Perpustakaan UNPAB Medan.
  - b. Melampirkan Bukti Pembayaran Uang Kuliah aktif semester berjalan
- 2.Dibuat Rangkap 3 (tiga), untuk - Fakultas - untuk BPAA (asli) - Mhs.ybs.

TANDA BEBAS PUSTAKA
No. 2491/Perp/BP/2019
Dinyatakan tidak ada sangkut paut dengan UPT. Perpustakaan
Medan, 27 JUN 2019
Ka. UPT. Perpustakaan
UNPAB INDONESIA UPT. PERPUSTAKAAN
[illegible] Hp. A.MP

Plagiarism Detector v. 1092 - Originality Report:

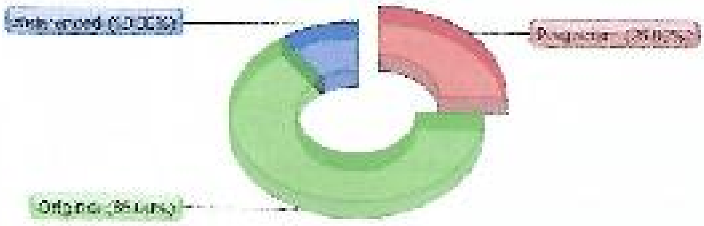
Analyzed document: 23/04/2019 09:26:49

"ARIFFIN_1514370078_SISTEM KOMPUTER.doc"

Licensed to: **Universitas Pembangunan Panca Budi_License4**

UNIVERSITAS PEMBANGUNAN PANCA BUDI

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 73	wrds: 7621	http://www.fileformat.info/info/charset/UTF-16/list.htm
% 25	wrds: 2013	https://en.wikipedia.org/wiki/Latin_Extended-A
% 17	wrds: 1029	http://www.ascii.ca/cp1250.htm

[Show other Sources:]

Processed resources details:

154 - Ok / 26 - Failed

[Show other Sources:]

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:
Wiki Detected!	[not detected]	[not detected]	[not detected]

Excluded Urls:

Included Urls:

Detailed document analysis:

IMPLEMENTASI QR CODE MENGGUNAKAN ALGORITMA RSA

SKRIPSI