Implementasi Kriptografi RSA pada Aplikasi Presensi dengan Teknologi *Quick Response Code* (Studi Kasus Stmik Indonesia Mandiri Bandung)

Dodi Dwitura
Program Studi Teknik Informatika
STMIK Indonesia Mandiri, Jl. Jakarta No.79 Bandung
Email : dodidwitura@gmail.com

ABSTRAK

Perkembangan teknologi informasi yang semakin maju dan pesat dewasa ini memberikan banyak sekali manfaat dan kemudahan di berbagai bidang. Hampir semua bidang saat ini tersentuh oleh teknologi tidak terkecuali bidang pendidikan. Satu dari berbagai pemanfaatan teknologi di bidang pendidikan atau bidang akademik yang menunjang kegiatan belajar mengajar mahasiswa adalah sistem pencatatan kehadiran. Pencatatan kehadiran atau sering dikenal dengan presensi memegang peranan penting dalam kegiatan perkuliahan. Melalui data presensi instansi dapat mengetahui informasi kedisiplinan dan keseriusan mahasiswa dalam mengikuti perkuliahan. Presensi juga menjadi salah satu parameter penilaian dosen dalam menentukan prestasi belajar mahasiswa. Pencatatan presensi pembelajaran tatap muka mahasiswa di STMIK Indonesia Mandiri saat ini masih dilakukan secara manual yaitu menggunakan kertas dan tulisan tanda tangan. Proses pengambilan data presensi secara manual ini dapat mengakibatkan terbukanya peluang manipulasi data kehadiran oleh mahasiswa. Ide yang muncul dari peneliti adalah merancang dan membangun aplikasi pencatatan presensi dengan teknologi *Quick Response Code (QR Code)* berbasis website. Dengan menggunakan aplikasi yang dibangun saat pembelajaran tatap muka mahasiswa harus menunjukan *QR Code* kepada dosen , kemudian dosen menscan *QR Code* yang diberikan oleh mahasiswa. *QR Code* yang ditampilkan yaitu berisi data nomor induk mahasiswa (NIM) yang sudah dienkripsi. Untuk mengenkripsi data peneliti mengimplementasikan kriptografi RSA (*Rivest Shamir Adleman*). RSA adalah algoritma asimetris yang menggunakan sepasang kunci yaitu kunci *public* dan kunci *privat* yang berbeda. Keamanan RSA terletak pada sulitnya memfaktorkan bilangan prima sehingga membuat data yang tersimpan pada *QR Code* menjadi lebih aman. Dari

hasil beberapa pengujian, aplikasi dapat melakukan enkripsi dan dekripsi data yang disimpan pada *QR Code* . Dengan adanya aplikasi ini dapat membantu mempermudah biro akademik dalam merekap dan mengecek data kehadiran serta dapat mengurangi resiko terjadinya kecurangan dan manipulasi data.

Kata Kunci: Kriptografi, algoritma RSA, *QR Code*

ABSTRACT

The development of information technology, which is increasingly advanced and rapidly grows, provides many benefits and develops in various fields. Almost all fields currently touched by technology, including education. One of the many uses of technology in the education or academic field that supports student teaching and learning activities is the attendance recording system. Attendance recording or often known as attendance plays an important role in lecture activities. Through agency data, it can see information on the discipline and seriousness of students in attending lectures. Attendance is also one of the parameters for lecturer fees in determining student achievement. The recording of student face-to-face learning attendance at STMIK Indonesia Mandiri is currently still done manually using paper and signature writing. This manual data collection process can open opportunities for data manipulation by students. The idea that emerged from the researcher was to design and build applications with website-based Quick Response Code (QR Code) technology. By using an application built during face-to-face learning, students must show the QR Code to the lecturer, then the lecturer scans the QR Code given by the student. QR Code that is written in a way that contains encrypted student ID number (NIM) data. To encrypt the data, the researcher implemented RSA (Rivest Shamir Adleman) cryptography. RSA is an asymmetric algorithm that uses a different key, namely the public and private keys. The security of RSA lies in the difficulty of factoring prime numbers so that it makes the data stored in the QR Code safer. From the results of several tests, the application can encrypt and decrypt the data contained in the QR Code. With this application, it can help make it easier for academics to recap and check the data that is present and can reduce the risk of fraud and data manipulation

***Keywords*:** *Cryptography, RSA algorithm, QR Code*

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang semakin maju dan pesat dewasa ini memberikan banyak sekali manfaat dan kemudahan di berbagai bidang. Hampir semua bidang saat ini tersentuh oleh teknologi tidak terkecuali bidang pendidikan . Satu dari berbagai pemanfaatan teknologi di bidang pendidikan atau bidang akademik yang menunjang kegiatan belajar mengajar mahasiswa adalah sistem pencatatan kehadiran. Pencatatan kehadiran atau sering dikenal dengan presensi memegang peranan penting dalam kegiatan perkuliahan. Melalui data presensi instansi dapat mengetahui informasi kedisiplinan dan keseriusan mahasiswa dalam mengikuti perkuliahan. Presensi juga menjadi salah satu parameter penilaian dosen dalam menentukan prestasi belajar mahasiswa.

Kegiatan belajar mengajar mahasiswa di STMIK Indonesia Mandiri dibagi menjadi pembelajaran tatap muka dan pembelajaran daring (e-learning). Saat ini proses pencatatan data presensi pembelajaran tatap muka mahasiswa di STMIK Indonesia Mandiri masih dilakukan secara manual yaitu menggunakan kertas dan tulisan tanda tangan. Proses pengambilan data presensi secara manual ini dapat mengakibatkan terbukanya peluang manipulasi data kehadiran oleh mahasiswa. Disamping itu pencatatan presensi saat ini juga menyulitkan dalam pemrosesan lebih lanjut karena data harus tetap diketik satu demi satu kemudian direkapitulasi manual dengan kehadiran data pembelajaran daring (e-learning) sehingga dirasa kurang efisien.

Berdasarkan masalah-masalah tersebut, ide yang muncul adalah membangun sistem presensi untuk mencatat dan mengelola presensi tatap muka dengan memanfaatkan teknologi *Quick Response Code* (QR Code) berbasis website. QR Code merupakan media yang digunakan dalam penyampaian informasi secara cepat dan mendapat response yang cepat tanpa melakukan input manual dengan cara mengetik. Informai yang dikodekan dalam QR Code dapat berupa URL, nomor telepon, pesan SMS, V-Card atau teks apapun (Ashford , 2020). Data yang tersimpan dalam *QR Code* adalah berupa data nomor induk mahasiswa (NIM). Untuk melakukan presensi dosen harus memindai *QR Code* yang ada pada web mahasiswa atau *QR Code* yang disimpan dalam

kartu tanda mahasiswa (NIM) yang sudah dienkripsi. Untuk menjaga kemanan dan kerahasiaan data, *QR Code* akan diamankan dengan menggunakan kriptografi RSA (*Rivest Shamir Adleman*). RSA adalah algoritma asimetris yang menggunakan sepasang kunci yaitu kunci *public* dan kunci *privat*. Keamanan RSA terletak pada sulitnya memfaktorkan bilangan prima. Sehingga dengan menggunakan kriptografi RSA ini akan membuat data yang tersimpan pada *QR Code* menjadi lebih aman.

1.2 Teori Pendukung

Quick Response Code

Quick Response Code atau sering disebut *QR Code* atau Kode QR adalah semacam simbol dua dimensi yang dikembangkan oleh Denso Wave yang merupakan anak perusahaan dari Toyota sebuah perusahaan Jepang pada tahun 1994. Tujuan dari QR Code ini adalah untuk menyampaikan informasi secara cepat dan juga mendapat tanggapan secara cepat. Pada awalnya *QR Code* digunakan untuk pelacakan bagian kendaraan untuk manufacturing. Namun sekarang, telah digunakan ntuk komersil yang ditujukan pada pengguna telepon seluler. *QR Code* adalah perkembangan dari barcode atau kode batang yang hanya mampu menyimpan informasi secara horizontal sedangkan *QR Code* mampu menyimpan informasi lebih banyak, baik secara horizontal maupun vertikal (Soleh, 2016).

GAMBAR : 2. 1 Contoh QR Code

Gambar 2.1 diatas adalah contoh sebuah *QR Code* yang apabila dipindai atau discan menampilkan data : “Saya adalah mahasiswa jurusan teknik informatika STMIK Indonesia Mandiri Bandung”. *QR Code* biasanya berbentuk persegi putih kecil dengan bentuk geometris hitam, meskipun sekarang banyak yang telah berwarna dan digunakan sebagai brand produk. Informasi yang dikodekan dalam *QR Code* dapat berupa URL, nomor telepon, pesan SMS, V-Card, atau teks apapun (Ashford,2010). *QR Code* telah

mendapatkan standarisasi internasional SO/IEC18004 dan Jepang JIS-X-0510 (Denso, 2011).

Algoritma

Algoritma adalah sebuah himpunan terhingga dari intruksi yang mempunyai karakteristik berikut ini:

1. Presisi (*precision*) , langkah-langkahnya dinyatakan dengan jelas.
2. Unik (*uniquiness)*, hasil lanjutan dari setiap langkah dari pelaksanaan. didefinisikan secara tunggal dan semata-mata bergantug pada masukan dan hasil dari langkah sebelumnya.
3. Terhingga (*finitness*), yaitu algoritma berhenti setelah beberapa intruksi terhingga dilaksanakan.
4. Masukan (*input*), yaitu algoritma memerlukan masukan.
5. Keluaran (*output*) ,yaitu algoritma menghasilkan keluaran.
6. Umum (*generallity*), yaitu algoritma berlaku pada himpunan masukan.

Algoritma juga diartikan sebagai metode langkah demi langkah dari pemecahan suatu masalah. Langkah-langkah dari suatu algoritma harus dinyatakan dengan jelas sehingga dapat ditulis dalam bahasa pemrograman dan dijalankan oleh komputer (Johnsonbaugh, 1985).

Kompleksitas dari suatu algoritma merupakan menggabarkan banyaknya komputasi yang dibutuhkan algoritma tersebut untuk menyelesaikan suatu masalah. Secara informal, algoritma yang sederhana dapat menyelesaikan masalah dalam waktu singkat, sementarta algoritma yang rumit atau kompleks membutuhkan waktu lama untuk menyelesaikan suatu masalah.

Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu *Crypto* dan *Graphia*. *Crypto* berarti rahasia dan *graphia* berarti tulisan. Secara terminologi kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Algoritma kriptografi terdiri dari tiga fungsi dasar yaitu enkripsi (penyandian), dekripsi(pembacaan sandi) dan kunci atau *key*. Keamanan dari kriptografi

modern didapat dengan menjaga kerahasiaan kunci yang dimiliki dari orang lain, tanpa harus merahasiakan algoritma itu sendiri.

Kunci memiliki fungsi yang sama dengan kata sandi. Jika keamanan keseluruhan algoritme bergantung pada kunci yang digunakan, orang lain dapat memublikasikan dan menganalisis algoritma. Jika algoritma yang dipublikasikan dapat diselesaikan oleh orang lain dalam waktu yang singkat berarti algoritma tersebut tidak aman digunakan (Ariyus, 2008).

Dalam bukunya Ariyus menuliskan tujuan dari kriptografi antara lain:

a. Kerahasiaan merupakan layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka maupun menghapus informasi yang telah disandi.
b. Integritas data yaitu berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan dan pensubstitusian data lain kedalam data yang sebenarnya.
c. Authentikasi yaitu berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, konten datanya, waktu pengiriman dan lain-lain.
d. *Non-repudiation* adalah upaya untuk mencegah pengirim atau produsen menolak untuk menyampaikan atau membuat informasi.

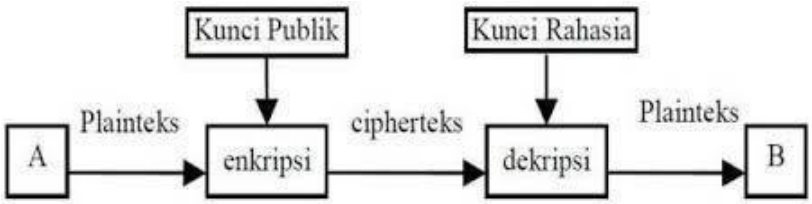
Kriptografi Simetris

Algoritma simetris atau biasa disebut algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses deskripsi. Algoritma ini dibagi menjadi dua kategori yaitu algoritma aliran (Stream Ciphers) dan algoritma blok (Block Ciphers). Pada algoritma aliran, proses penyandiannya akan beriorientasi pada satu *bit/byte* data. Sementara pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan *bit/byte* data (per blok). Adapun contoh algoritma kunci simetris adalah DES (*Data Encryption Standard*),

Blowfish, *Twofish*, *MARS*, *IDEA*, *3DES* (DES diaplikasikan 3 kali), AES (*Advanced Encryption Standard*) yang bernama asli Rijndael (abcdefghaniv, 2014).

Kriptografi Asimetris

Kriptografi asimetris adalah suatu algoritma yang menggunakan kunci yang berbeda pada proses enkripsi dan dekripsinya. Dimana kunci enkripsi dapat disebarkan kepada umum sehingga biasa disebut kunci publik (*public key*), sementara kunci dekripsi disimpan dan dirahasiakan untuk sendiri sehingga sebagai kunci pribadi (*private key*). Kriptografi ini dikenal pula dengan nama kriptografi kunci publik (public key cryptography) (Widiasari, 2014). Contoh algoritma yang menggunakan kriptografi asimetris diantaranya RSA (Riverst Shamir Adleman) dan ECC (Elliptic Curve Cryptography).



Algoritma RSA

Algoritma RSA diambil dari nama penciptanya yaitu Ron Rivest, Adi Shamir dan Len Adleman yang menciptakan metode ini pada tahun 1977. Teknologi dasar pertama kali ditemukan oleh Clifford Cock dari CESG (bagian dari British GCHQ) pada tahun 1973, tetapi dirahasiakan hingga tahun 1977. *Paten* dimiliki oleh RSA Labs dan telah expired (Hendra, 2012). Algoritma RSA adalah algoritma enkripsi dan otentikasi yang paling umum digunakan.

Algoritma RSA melibatkan perkalian dua bilangan prima besar, setelah kunci telah dibuat,bilangan prima asli tidak lagi penting dan dapat dibuang. Enkripsi dan dekripsi membutuhkan kunci publik dan kunci privat. Kunci publik digunakan untuk mengenkripsi pesan dan kunci ini tidak dirahasiakan, sementara kunci privat digunakan untuk proses dekripsi pesan dan kunci ini harus dirahasiakan.

Berikut besaran-besaran yang akan digunakan dalam algoritma kriptografi RSA:

1. p dan q bilangan prima (rahasia)

2. $n = p \times q$
3. $\Phi(n) = (p - 1)(q - 1)$
4. e = kunci enkripsi
5. d = kunci dekripsi
6. m = plainteks
7. c = cipherteks

Langkah pertama dalam algoritma kriptografi RSA adalah pembangkitan kunci (kunci publik dan kunci privat) yang nantinya akan digunakan untuk enkripsi dan dekripsi. Berikut adalah langkah-langkah pembangkitan kunci pada algoritma kriptografi RSA:

1. Pilihlah 2 bilangan prima, p dan q dimana $p \neq q$ dan nilai p dan q harus dirahasiakan.
2. Hitung nilai $n = p \times q$, nilai n tidak harus dirahasiakan.
3. Hitung $\Phi = (p - 1)(q - 1)$.
4. Pilihlah bilangan bulat sebagai kunci publik(e), dengan ketentuan $\Phi(1<e < \Phi)$ yang manabilangan tersebult adalah *coprime* dari Φ. kunci public tidak harus dirahasiakan.
5. Bangkitkan kunci privat dengan menggunakan persamaan $e \cdot d = 1 \pmod{\Phi(n)}$ kunci privat harus dirahasiakan.

Dari persamaan diatas dihasilkan kunci publik yaitu pasangan (e, n) dan kunci privat yaitu pasangan (e, d). setelah mendapatkan kunci public dan kunci privat kita bisa melakukan enkripsi dan dekripsi berikut langkah-langkahnya

Algoritma enkripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut:

1. Gunakan kunci publik penerima pesan, e, dan modulus n.
2. Susun plainteks m menjadi blok-blok m_1, m_2…., sedemikian sehingga setiap blok merepresentasikan nilai didalam selang [0, n – 1].
3. Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus $c_i = m_i^e \bmod n$.

Selanjutnya algoritma dekripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut:

1. Gunakan kunci privat untuk menghitung $m_i = c_i^d \bmod n$
2. Setiap blok cipherteks ci didekripsi kembali menjadi blok mi dengan rumus $m_i = c_i^d \bmod n$.

Sampai saat ini Algoritma RSA merupakan algoritma kunci publik yang paling popular diantara algoritma kunci public lainnya. Karna selain cukup ringan di memori algoritma RSA juga terkenal sangat aman.

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang efektif, maka selama itu pula keamanan algoritma RSA tetap terjamin (Munir, 2004).

1.3 Identifikasi Masalah

Berdasarkan latar belakang diatas, maka hal yang dapat diidentifikasikan adalah bagaimana mengatasi masalah keamanan pada aplikasi *QR Code* menggunakan algoritma kriptografi RSA. Penelitian ini dilakukan untuk mengetahui hasil dari implementasi algoritma kriptografi RSA untuk menjaga keamanan data pada *QR Code.*

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang cara mengenkripsi dan mendekripsi *QR Code* menggunakan algoritma kriptografi RSA.
2. Merancang dan membangun aplikasi presensi dengan *QR Code* berbasis website menggunakan algoritma kriptografi RSA

2. METODE PENELITIAN

Dalam menyelesaikan skripsi ini, penulis menggunakan metodologi penelitian sebagai berikut:

2.1 Pengumpulan Data

Adapun metodologi pengumpulan data yang digunakan adalah :

1. Observasi

   Penulis melakukan pengamatan secara langsung terhadap sistem yang sedang berjalan di lokasi penelitian untuk memperoleh data yang relevan dan akurat.
2. Studi Pustaka

Mencari sumber-sumber lain untuk memperkuat dasar teoritis melalui buku-buku, dokumen,serta bahan tulisan yang ada hubunganya dengan masalah yang diteliti.

2.2 Metode Pengembangan Perangkat Lunak

Metode yang digunakan untuk mengembangkan sistem ini adalah model *Waterfall*. Metode *Waterfall* adalah metode yang menyarankan pendekatan yang sistematis melalui berbagai tahapan yang ada pada SDLC untuk membangun sebuah perangkat lunak. Adapun tahapan metode *waterfall* diuraikan sebagai berikut:

a. Analisa Kebutuhan Software

Tahapan ini ini bertujuan untuk menganalisis semua persyaratan, termasuk menentukan dokumentasi dan antarmuka yang diperlukan untuk solusi perangkat lunak yang akan digunakan sebagai proses komputerisasi sistem.

b. Desain

Pada tahap ini, desain *database*, arsitektur perangkat lunak, dan desain antarmuka pengguna yang akan dibuat akan dilakukan sesuai dengan kebutuhan sistem. penggunaan Unified Modeling Language (UML) bertujuan untuk menjelaskan desain pemrograman dan desain database secara lebih detail.

c. Code Generation

Pada tahap ini, implementasi desain dibuat menjadi program perangkat lunak. Pada tahap ini dibuat sistem baru dengan menggunakan bahasa pemrograman php dengan Codeigniter sebagai *framework* dan MSQL untuk membuat *database*.

d. Testing

Tahap berikutnya adalah tahapan *testing* atau pengujian. Pada tahapan ini program diuji menggunakan *Black box* dengan menghasilkan sesuai dengan harapan yang telah dirancang sebelumnya. Penggunaan *Black box* akan memberikan penjelasan tentang kesesuaian program yang dibangun dengan harapan dalam pembuatan program.

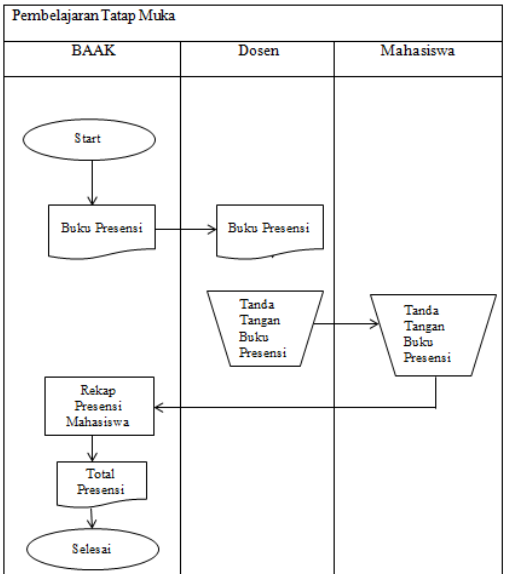
e. Maintenance

Dalam proses pemeliharaan ini penulis berupaya mengembangkan suatu sistem yang sudah dibuat berkaitan dengan perangkat lunak dan perangkat keras yang digunakan.

3. HASIL DAN PEMBAHASAN

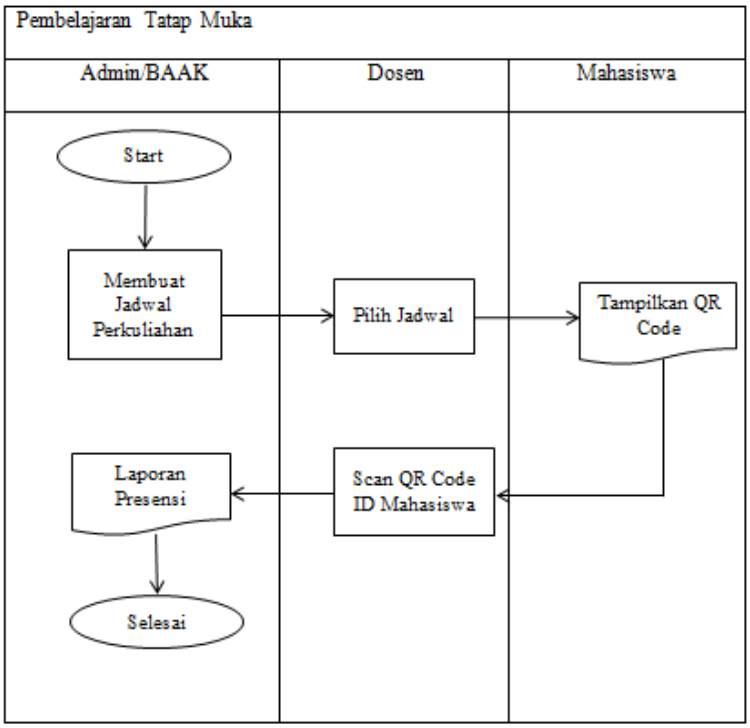
3.1 Proses Sistem Berjalan

.Berdasarkan hasil pengamatan yang dilakukan oleh penulis pengolahan data presensi tatap muka di STMIK Indonesia Mandiri saat ini masih belum terkomputerisasi atau masih secara manual yaitu dengan menggunakan kertas dan tulisan tanda tangan, Proses pencatatan presensi pembelajaran tatap muka yang berjalan saat ini diperlihatkan pada gambar dibawah ini:



Gambar 1 : Flowmap Sistem pencatatan presensi saat ini

Melihat dari proses pencatatan presensi saat ini dapat mengakibatkan terbukanya peluang manipulasi data kehadiran oleh mahasiswa saat pembelajaran tatap muka. Berikut adalah proses pencatatan presensi yang diusulkan menggunakan aplikasi berbasis web dengan memanfaatkan teknologi *Quick Response Code (QR Code):*



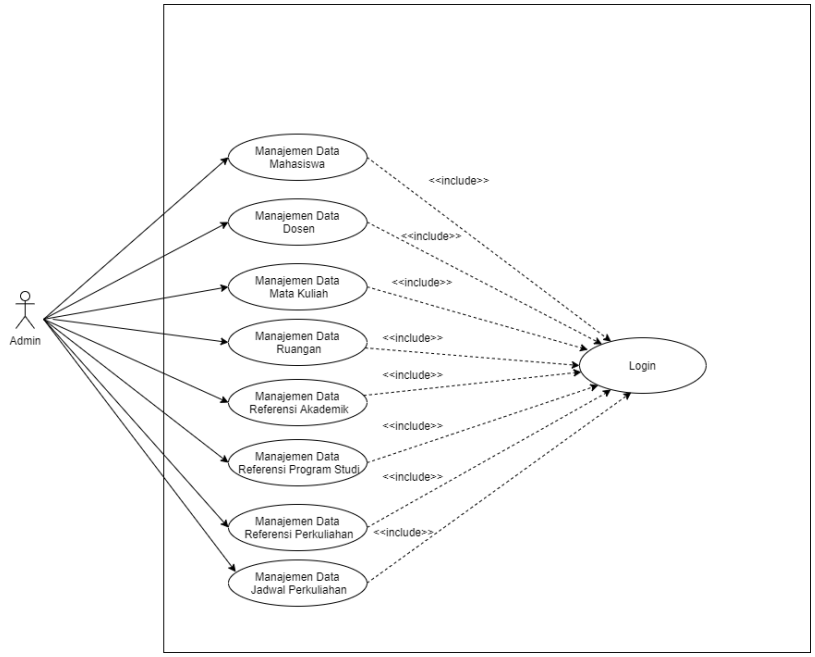
Gambar 2 : Flowmap Sistem pencatatan presensi yang diusulkan

Penjelasan *flowmap* aplikasi:

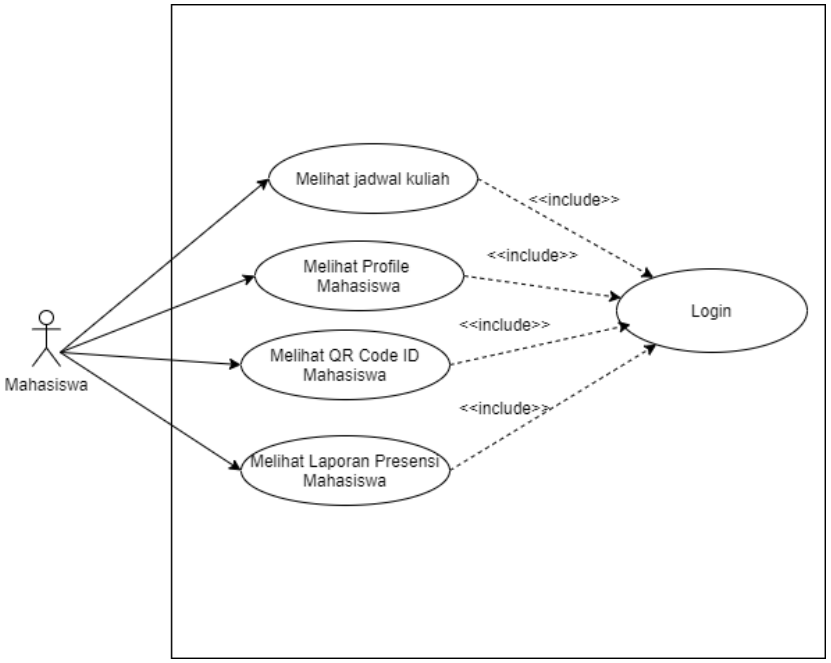
1. User admin atau BAAK melalui aplikasi mengelola data jadwal perkuliahan
2. Untuk mencatatat proses presensi , pada aplikasi dosen memilih menu jadwal
3. Mahasiswa menampilkan *QR Code* pada aplikasi atau pada Kartu Mahasiswa yang berisi nomor induk mahasiswa (NIM) telah telah dienkripsi
4. Dosen memilih scan QR dan menscan QR Code mahasiswa
5. Admin/BAAK dapat melihat laporan rekap presensi mahasiswa

3.2 *Use Case Diagram*

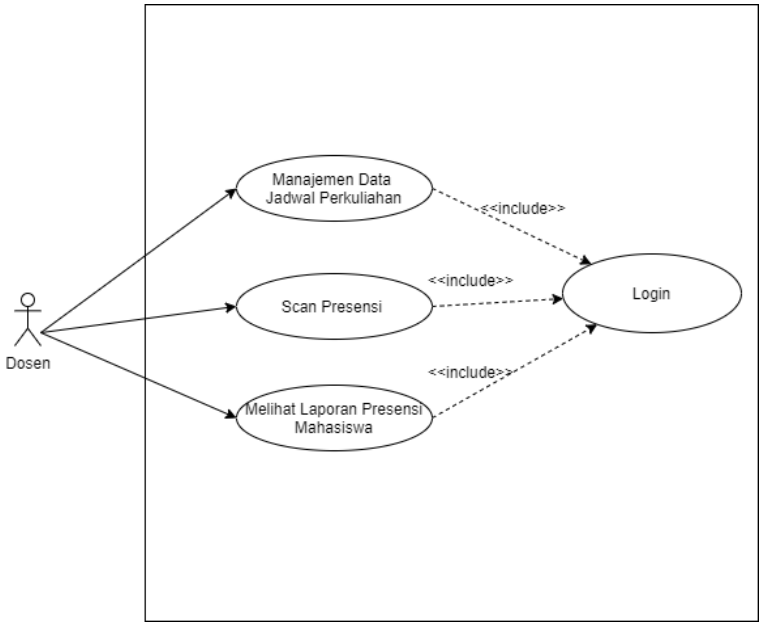
Pada aplikasi yang dikembangkan oleh peneliti ini melibatkan 3 aktor yaitu administrator (Biro Akademik) yang bertugas mengelola data yang dibutuhkan oleh aplikasi, dosen yang melakukan pemindaian dan mahasiswa yang menampilkan *QR Code*. *Use case diagram* aplikasi dijelaskan pada gambar dibawah ini :



Gambar 3 : *Use Case* Diagram Admin



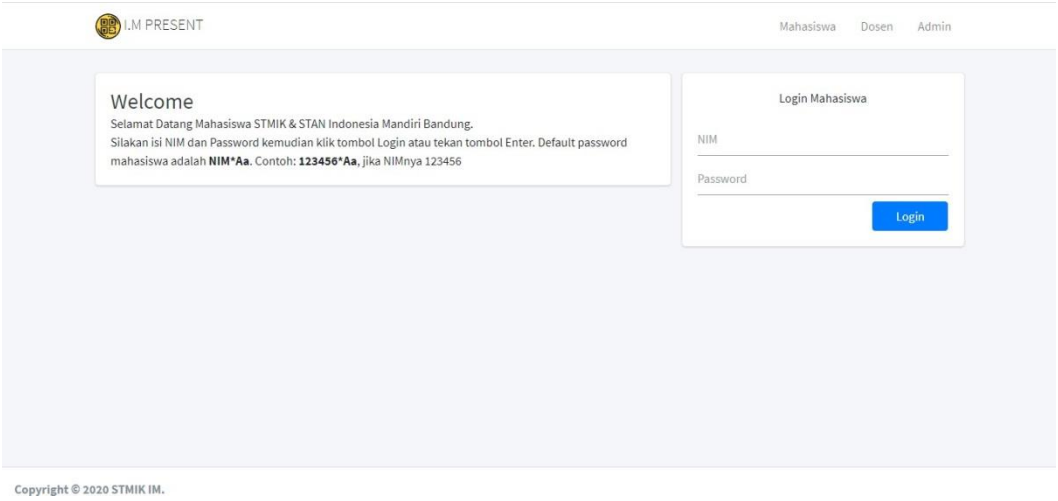
Gambar 4 : *Use Case* Diagram Mahasiswa



Gambar 5 : *Use Case Diagram* Dosen

3.2 Implementasi Sistem

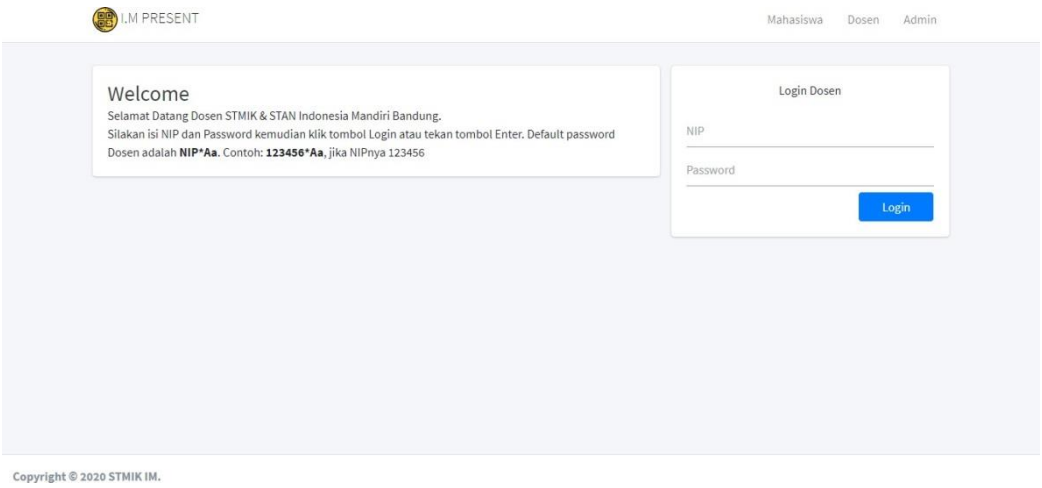
3.2.1 *Interface* Login Mahasiswa



Gambar 6 : Login Mahasiswa

Gambar 6 merupakan tampilan pertama ketika aplikasi dibuka. Sebelum masuk ke dalam sistem, mahasiswa harus login terlebih dahulu dengan memasukan NIM dan *password* dengan benar.

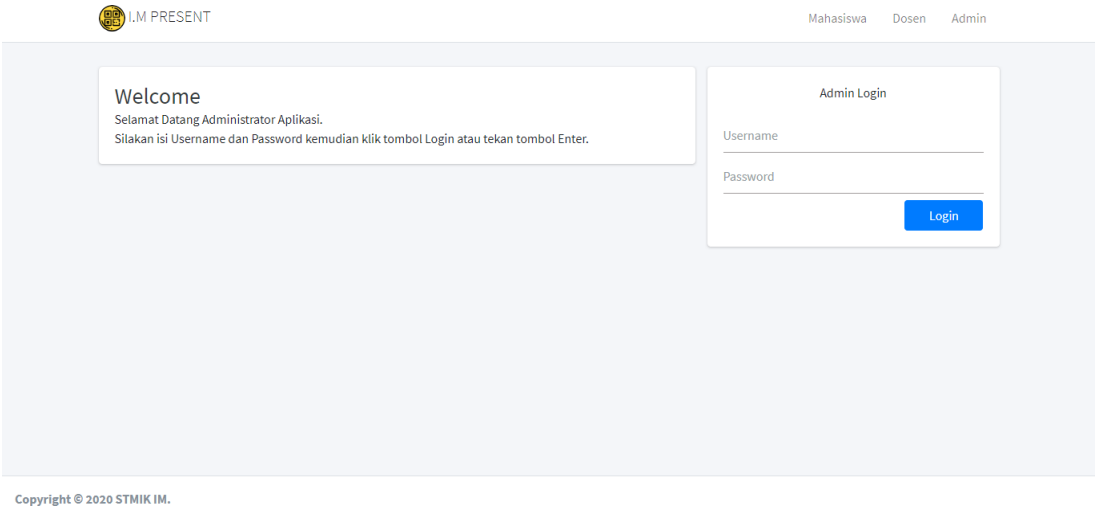
3.2.2 *Interface* Login Dosen



Gambar 7 : Login Dosen

Gambar 7 merupakan tampilan login dosen.. Untuk membuka menu ini klik Dosen pada bagian *header* halaman login .

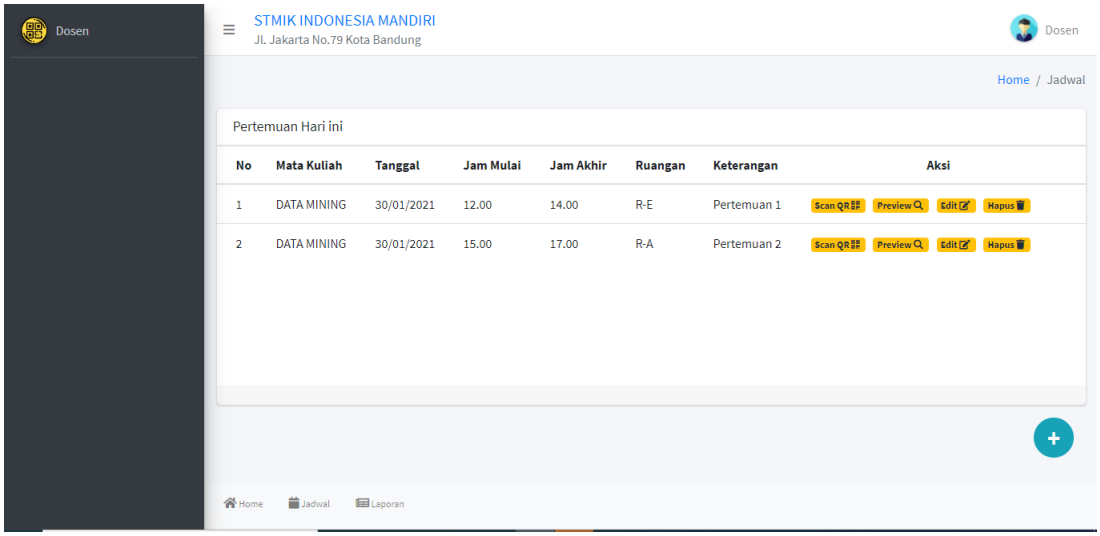
3.2.3 *Interface* Login Admin



Gambar 8 : Login Admin

Gambar 8 merupakan tampilan login admin.. Untuk membuka menu ini klik Admin pada bagian *header* halaman login .

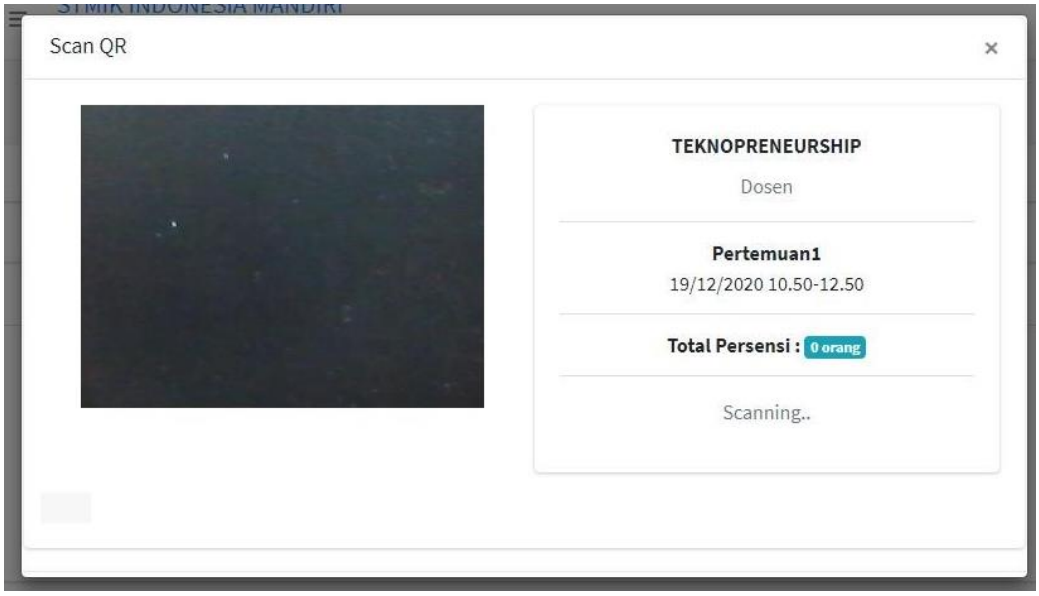
3.2.4 *Interface* Jadwal Dosen



Gambar 9 : Jadwal Dosen

Gambar 9 merupakan tampilan halaman jadwal halaman dosen. Halaman Jadwal menampilkan daftar jadwal perkuliahan yang telah disetting oleh administrator.

3.2.5 *Interface Scan* Presensi



Gambar 10 : *Scan* Presensi

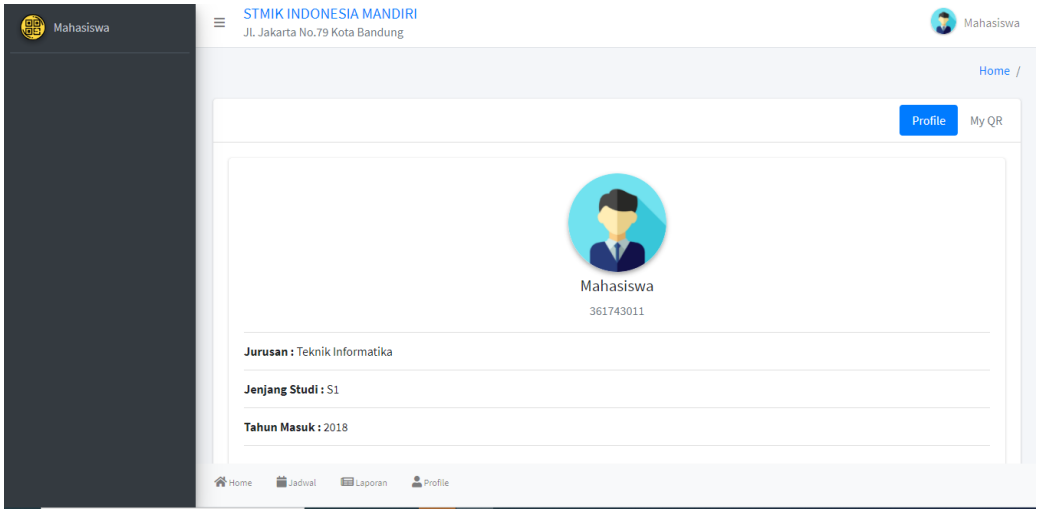
Gambar 10 merupakan tampilan halaman Scan Presensi. Halaman ini digunakan oleh dosen untuk menscan *QR Code* yang ditampilkan oleh mahasiswa saat pembelajaran tatap muka. Pada proses *scan* ini system mendekrip data yang terdapat

pada *QR Code* yang berisi ID mahasiswa yang telah dienkripsi. Untuk membuka menu ini dosen harus mengklik tombol *Scan* QR pada kolom aksi di halaman jadwal.

3.2.6 *Interface* Profile Mahasiswa

Pada halaman profile mahasiswa terdapat 2 halaman atau tab yaitu tab profile untuk menampilkan informasi data mahasiswa dan tab My QR untuk menampilkan *QR Code* mahasiswa.

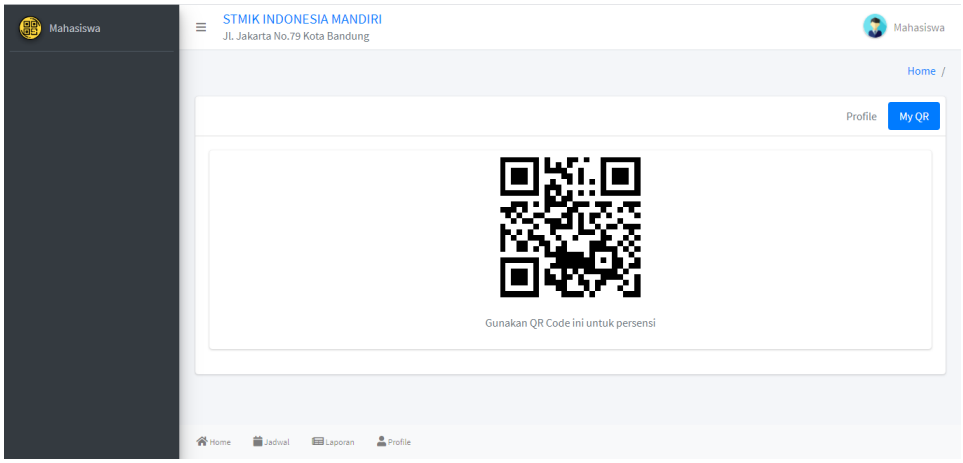
3.2.6.1 Tab Profile



Gambar 11 : Profile Mahasiswa

Gambar 11 merupakan halaman profile mahasiswa. Halaman ini menampilkan data informasi mahasiswa seperti nama,NIM, jurusan,program studi dan tahun masuk perkuliahan.

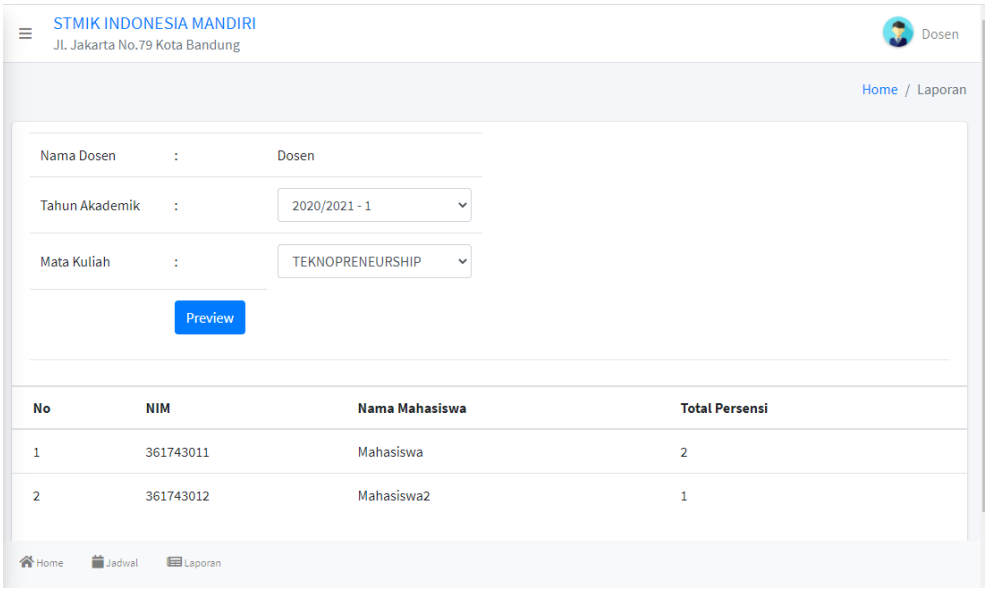
3.2.6.2 Tab QR Code



Gambar 12 : *QR Code* ID mahasiswa

Gambar 12 merupakan halaman untuk menampilkan QR Code mahasiswa. QR Code ini telah dienkripsi menggunakan algoritma kriptografi RSA.. Untuk menampilkan *QR Code* ini klik tab My QR pada halaman *profile*.

3.2.7 Halaman Laporan Presensi

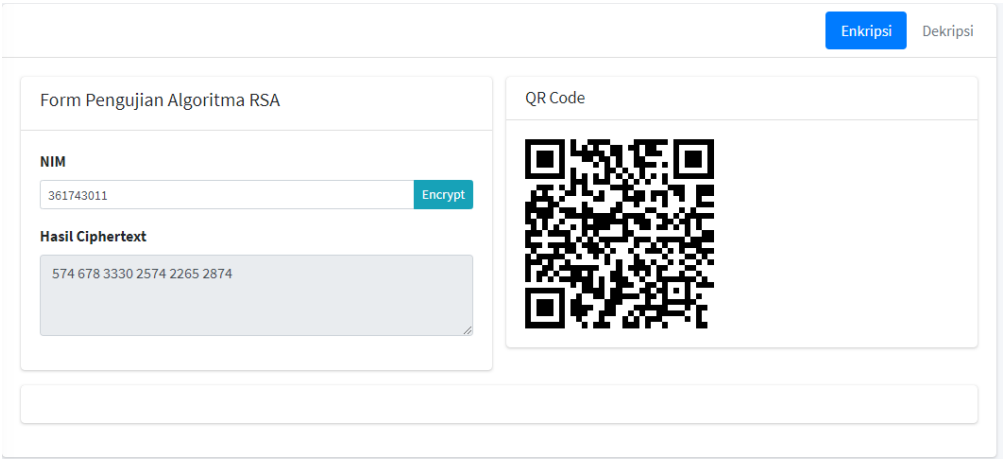


Gambar 13 : Laporan Presensi

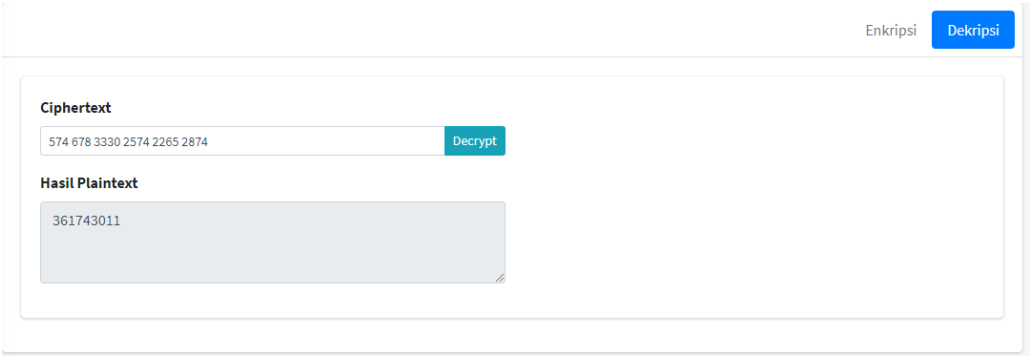
Gambar 13 merupakan halaman untuk menampilkan data laporan presensi tatap muka mahasiswa. Data rekap presensi dapat dipilih berdasarkan tahun akademik dan berdasarkan mata kuliah.

3.2.8 Hasil Pengujian Sistem

Berikut adalah form pengujian enkripsi dan dekripsi algoritma RSA yang terdapat pada aplikasi:



Gambar 14 : Pengujian Enkripsi RSA



Gambar 15 : Pengujian dekripsi RSA

Gambar 14 menunjukan pengujian sistem enkripsi terhadap suatu *plaintext*. Data yang dienkripsi merupakan data nomor induk mahasiswa (NIM) yang diinputkan kemudian digenerate menjadi sebuah *QR Code* . Sedangkan gambar 15 merupakan form dekripsi dari sebuah *ciphertext* yang merupkan hasil proses enkripsi yang berrfungsi untuk mengubah dan menampilkan kembali *ciphertext* kepada data aslinya (*plaintext).*

Berikut adalah hasil pengujian enkripsi data menggunakan algoritma RSA:

Tabel 1. Hasil Ujicoba Enkripsi

Data ujicoba	Jumlah Karakter	Hasil Enkripsi	Kesimpulan
36174301	8	574 678 3330 2574 2265 1605	[√] Sukses [ ] Gagal
36174302	8	574 678 3330 2574 1441 0	[√] Sukses [ ] Gagal
36174303	8	574 678 3330 2574 1441 1	[√] Sukses [ ] Gagal
36174304	8	574 678 3330 2574 1441 3139	[√] Sukses [ ] Gagal
36174305	8	574 678 3330 2574 1441 158	[√] Sukses [ ] Gagal
36174306	8	574 678 3330 2574 1441 2497	[√] Sukses [ ] Gagal
36174307	8	574 678 3330 2574 1441 270	[√] Sukses [ ] Gagal
36174308	8	574 678 3330 2574 1441 2086	[√] Sukses [ ] Gagal
36174309	8	574 678 3330 2574 1441 1254	[√] Sukses [ ] Gagal

36174310	8	574 678 3330 2574 907 2807	[√] Sukses [ ] Gagal

Tabel 2. Hasil Implementasi Enkripsi dan Dekripsi

No	Kelas Uji	Hasil yang Diharapkan	Hasil yang Diamati	Kesimpulan
1	Proses Enkripsi	Data dapat dienkripsi sehingga menghasilkan ouput *ciphertext*	Data berhasil dienkripsi tampil hasilenkripsi yaitu *ciphertext*	[√] Sukses [ ] Gagal
2	Proses Dekripsi	Data dapat didekripsi sehingga menghasilkan output *plaintext*	Data berhasil didekripsi tampil hasil dekripsi yaitu *plaintext*	[√] Sukses [ ] Gagal

4. SIMPULAN

4.1 Kesimpulan

Berdasarkan hasil pembahasan beserta penelitian yang telah dilakukan maka dapat diambil kesimpulan diantaranya:

1. Aplikasi sistem presensi telah dirancang dan dibangun dengan menggunakan 3 hak akses atau *role* dengan berbagai fitur. Hak akses pertama adalah hak akses admin yang dapat mengelola data dosen, data mahasiswa dan data referensi lain untuk memenuhi kebutuhan sistem. Hak akses kedua adalah Dosen yang dapat mimndai *QR Code* data mahasiswa untuk melakukan presensi tatap mukadan hak akses ker tiga adalah mahasiswa yang bertugas *menampilkan QR Code* saat proses pembelajaran tatap muka.
2. Dengan dibuatnya aplikasi presensi ini dapat mempermudah bagian biro akademik dalam merekap dan mengecek data kehadiran atau presensi.
3. Aplikasi presensi menggunakan *QR Code* ini juga dapat mengurangi resiko

terjadinya kecurangan dan manipulasi data karena data yang disimpan dalam *QR Code* sudah terenkripsi.

4.2 Saran

Dengan adanya kesimpulan diatas, ada beberapa saran yang dikemukan sebagai bahan pertimbangan lebih lanjut sehingga diharapkan dapat memberikan perbaikan dalam penelitian selanjutnya yaitu :

1. Untuk mengefektifitaskan data diperlukan adanya integrasi atau *Host to Host (H2H)* dengan sistem akademik.
2. Karena aplikasi ini dirancang hanya mencatat presensi tatap muka saja, maka diperlukan pengembangan aplikasi untuk mencatat presensi pembelajaran daring (*e-learning)*¸sehingga data lebih terintegrasi.

5. DAFTAR PUSTAKA

abcdefghaniv.(22 September 2014).Enkripsi Simetris dan Asimetris. Diakses dari https://www.hanivinside.net/2014/11/enkripsi-simetris-dan simetris.html#:~:text=Algoritma%20simetris%20atau%20sering%20disebut,algoritma%20blok%20(Block%20Ciphers) .

Ariyus, Dony (2008) . Pengantar Ilmu Kriptografi: Andi.

Ashford, Robin (2010, November 10). *QR Code and academic libraries eaching mobile users.*. Diakses dari http://crln.acrl.org/content/71/10/526.full .

Denso Wave Incorporated. (2013) . *Answer to your questions about the QR Code*. Diakses dari https://www.qrcode.com/en/ .

Hendra, S. (2012). Aplikasi Pengaman Pertukaran SMS pada Perangkat Android dengan Metode RSA.

Johnsonbaugh, R. (1998). Matematika Diskrit Edisi 4 Jilid 1. Jakrta : Prenhaliondo.

Soleh,M.L., dan L. A.(2016) . *Smart Persensi* Menggunakan QR Code dengan Enkripsi Vignere Cipher, 31-36.

Munir, Rinaldi (2004) . Algoritma RSA dan ElGamal, Bandung. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Algoritma%20RSA.pdf