Jurnal Smart Teknologi
Vol. 4, No. 3, Maret 2023, Halaman 390 – 395
ISSN: 2774-1702, http://jurnal.unmuhjember.ac.id/index.php/JST

Pengembangan Sistem Presensi Siswa menggunakan QR Code Dengan Kriptografi Triple DES Dan Caesar Cipher Yang Terintegrasi Sitem Informasi Akademik SMP Negeri 2 Pasirian

Development Of Student Pesence System Using QR Code With Triple DES And Caesar Cipher Cryptography Integrated Android-Based Academic Informaation System Of SMP Negeri 2 Pasirian

Prastyo Irwan Eka Susanto[1)], Deni Arifianto[2*)], Ari EKo Wardoyo[3)]
[1]Mahasiswa Program Studi Fakultas Teknik, Universitas Muhammadiyah Jember
Email : lli076439@gmail.com
[2]Dosen Fakultas Teknik, Univeritas Muhammadiyah Jember*Koresponden Author
Email : Deniarifianto@unmuhjember.ac.id
[3] Dosen Fakultas Teknik, Univeritas Muhammadiyah Jember
Email : Ariekowardoyo@unmuhjember.ac.id

Abstrak

Presensi merupakan suatu kegiatan yang penting dalam suatu pendidikan. Terdapat siswa yang harus dicatat keharirannya setiap hari, presensi pada pendidikan saat ini masih banyak yang mengunakan presensi manula dengan memanggil satu-persatu murid. Dengan adanya teknologi saat ini penulis mengembangkan presensi berbasis mobile dengan menggunakan QR Code dan dilengapi keamanan data yang terjamin aman. Dengan menggunakan Kriptografi Triple DES dan Caesar Cipher untuk keamanan datanya, data yang tersimpan pada data base tidak dapat di baca oleh orang lain yang tidak mengetahui kunci dari Kriptografi yang digunakan. Jadi yang dapat membaca hasil presensi pada data base hanya admin saja.

***Keywords**:* Kriptografi, Pressensi, QR Code, Android

Abstract

Attendance is an important activity in an education. There are students who must be recorded every day, attendance in education today is still many who use the presence of seniors by calling students one by one. With the current technology, the author develops a mobile-based presence using a QR Code and is equipped with data security that is guaranteed to be safe. By using Triple DES Cryptography and Caesar Cipher for data security, the data stored in the database cannot be read by other people who do not know the key to the cryptography used. So only admins can read the presence results in the database.

***Keywords**: Cryptography, Presses, QR Code*

1. PENDAHULUAN

Dalam perkembangan teknologi yang semakin maju dan pesat pada saat ini, sangat berpengaruh pada kemudahan-kemudahan yang diberikan dalam kehidupan sehari-hari terutama dalam bidang pemerintahan, perusahaan dan pendidikan, rumah sakit, universitas dan tempat lain. Sistem presensi ini dalam kegiatan belajar mengajar di suatu pendidikan, tentu memiliki siswa yang harus di catat kehadirannya setiap hari. Pencatatan kehadiran ini lebih sering disebut sebagai presensi. Maka dari itu presensi adalah salah satu faktor penting dalam dunia pendidikan.

Untuk mendapatkan data absensi siswa yang dilakukan di dalam kelas dimana sistem absensi yang ada saat ini masih di lakukan

secara manual, yaitu memanggil satu persatu murid yang berada di daftar absensi siswa. Sistem tersebut cukup memakan waktu, sehingga waktu, tidak menutup kemungkinan teknologi dapat membantu kegiatan absensi semakin cepat dan tidak memakan waktu pembelajaran. Dengan adanya telepon seluler dapat dimanfaatkan untuk membantu kegiatan absensi siswa.

Kehadiran peserta didik ketika mereka berpartisipasi dalam pembelajaran juga memegang peranan penting dalam proses belajar mengajar. Ponsel dengan sistem operasi dan akses internet adalah salah satu fungsi utama dari *smartphone*. Yang menarik dari *smartphone* adalah kemampuannya untuk menangkap, menyimpan dan melihat gambar, karena kebanyakan *smartphone* memiliki kamera. Ide ini menghasilkan penggunaan kode QR dan *smartphone* Android sebagai sistem tambahan, data siswa dapat disimpan sebagai gambar kode QR, dan kemudian disimpan di *smartphone* atau dicetak.

Beberapa hal ini lah yang mendorong pemikiran mengenai mengembangkan sistem yang dapat melakukan absensi siswa secara mobile, cepat, efektif dan efisien. Penelitian ini menggunakan Android. Untuk keamanan datanya menggunakan Kriptografi *Triple* DES, dan menggunakan *Caesar Cipher*. Kriptografi *Triple* DES merupakan salah satu sitem pengamanan data yang sangat ketat.

Dengan mengunakan *caesar chiper* data yang tersimpan di data base tetap terjaga Dengan melakukan enkripsi data dari hasil scan siswa menggunakan sistem ini lalu sistem memanggil link enkripsi agar dapat didekripsi dan dipilah dan dimasukkan kedalam database. Sedangkan *QR Code* merupakan sistem operasi mobile (OS) yang sangat populer dan banyak digunakan, Kode QR adalah sarana untuk memberikan informasi dengan cepat dan mendapatkan respon cepat tanpa input manual. Informasi yang dikodekan dalam kode QR dapat berupa alamat situs web, nomor telepon, pesan singkat, kartu nama, atau teks apa pun.

SMP Negeri 2 Pasirian menyediakan kuota wifi gratis yang dapat di pakai oleh semua siswa SMP Negeri 2 Pasirian. Dengan adanya jaringan wifi di SMP Negeri 2 Pasirian, penulis menambahkan untuk melakukan login pada aplikasi siswa, harus *connect* pada wifi lokal yang di sediakan khusus untuk siswa. Sehingga tidak akan ada yang bisa melakukan absensi di luar sekolah.

Pada penelitian Tugas Akhir yang berjudul "Pengembangan Sistem Presensi Siswa Menggunakan Qr *Code* Dengan Kriptografi *Triple* DES dan *Caesar Cipher* Yang Terintegrasi Sistem Informasi Akademik SMP Negeri 2 Pasirian Berbasis Android". penulis ingin melakukan pengujian keamanan data menggunakan Algoritma *Triple* DES dan *Enkripsi Caesar Cipher*.

2. TINJAUAN PUSTAKA

A. ANATOMI QR *CODE*

Beberapa penjelasan anatomi Qr *Code* Menurut Ariadi (2011) antara lain :

1. Finder Pattern berfungsi untuk identifikasi letak Qr *Code.*
2. Format Information berfungsi untuk informasi tentang error correction level dan mask pattern.
3. Data berfungsi untuk menyimpan data yang dikodekan.
4. Timing Pattern merupakan pola yang berfungsi untuk identifikasi koordinat pusat Qr *Code*, berbentuk modul hitam putih.

B. DATA ENCRYPTION STANDARD

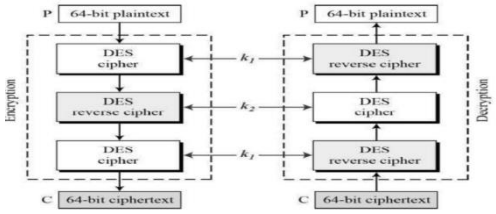
DES beroperasi pada ukuran blok 64-bit. DES mengenkripsikan 64-bit plainteks menjadi 64-bit cipherteks dengan menggunakan 56-bit kunci internal yang dibangkitkan dari kunci eksternal yang panjangnya 64-bit.

C. KRIPTOGRAFI *TRIPLE DES*

Triple DES (Triple Data Encryption Standard) merupakan suatu algoritma pengembangan dari algoritma DES (*Data Encryption Standard*). Pada dasarnya algoritma yang digunakan sama, hanya pada *Triple* DES dikembangkan dengan melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali. *Triple* DES memiliki tiga buah kunci yang berukuran 168-bit (tiga kali kunci 56-bit dari

Jurnal Smart Teknologi
Vol. 4, No. 3, Maret 2023, Halaman 390 – 395
ISSN: 2774-1702, http://jurnal.unmuhjember.ac.id/index.php/JST

DES). Pada algoritma *Triple* DES dibagi menjadi tiga tahap, setiap tahapnya merupakan implementasi dari algoritma DES.



Gambar 1. Cara Kerja Dari *Triple* DES
Sumber: Sumber Penelitian

Ukuran kunci meningkat di *Triple* DES untuk memastikan keamanan tambahan melalui kemampuan enkripsi. Setiap blok berisi 64 bit data. Tiga kunci yang disebut sebagai bundel kunci dengan 56 bit per kunci. Ada tiga keying Pilihan dalam standar enkripsi data:

a. Semua kunci menjadi independen.
b. Kunci 1 dan kunci 2 menjadi kunci independen.
c. Semua tiga kunci yang identic.

D. CAESAR CIPHER

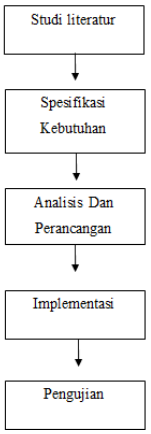
Caesar Cipher merupakan salah satu algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi. *Caesar cipher* merupakan salah satu jenis *cipher* substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada *chiperteks*. Teknik seperti ini disebut juga sebagai chiper abjad tunggal.Algoritma *kriptografi Caesar Cipher* sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama.

Algoritma dari *Caesar Cipher* adalah C = E (P) = (P + K) mod 26 untuk fungsi enkripsi. Sedangkan untuk fungsi dekripsi adalah P = D (C) = (C - K) mod 26.

Gambar 2. Tabel Subtitusi *Caesar Cipher*
Sumber: Sumber Penelitian

3. METODE PENELITIAN

Dalam tugas akhir ini harus dilakukan langkah-langkah untuk memastikan kegiatan penelitian mencapai hasil yang maksimal. Untuk itu penulis memberikan langkah-langkah untuk memaksimalkan pengerjaan Tugas Akhir ini. Langkah-langkah ini adalah sebagai berikut:



Gambar 3. Tahap Penelitian
Sumber: Sumber Penelitian

A. STUDI LITERATUR

Penelitian ini dimulai dengan melakukan studi literatur, yaitu proses pengumpulan data sebagai bahan referensi baik dari buku, artikel, jurnal, makalah, atau situs internet yang berkaitan dengan presensi, android, eclipse, QR *Code* dan Algoritma *Triple* DES.

B. SPESIFIKASI KEBUTUHAN

Pada tahap ini di ambil pada alat dalam proses membuat aplikasi. Untuk data yang di uji diambil pada data guru dan siswa SMP Negeri 2 Pasirian untuk dilakukan proses presensi.

C. ANALISA DAN PERANCANGAN

Masalah yang ada pada sistem presensi saat ini adalah saat proses presensi siswa yang masih menggunakan presensi manual. Data yang tercatat masih rentan hilang atau rusak. Jadi penilis mengembangkan system presensi yang datanya di amankan oleh *Algoritma*

Jurnal Smart Teknologi
Vol. 4, No. 3, Maret 2023, Halaman 390 – 395
ISSN: 2774-1702, http://jurnal.unmuhjember.ac.id/index.php/JST

Triple DES dan *Enkripsi Caesar Chipher*.

D. IMPLEMENTASI

Pada bab ini akan membahas mengenai penerapan dari hasil perancangan pada bab sebelumnya dan juga memberikan contoh peerhitungan pada *Algoritma Triple* DES dan dilanjutkan dengan enkripsi *Caesar Cipher*.

E. PENGUJIAN

Pada tahap ini diakukan pengujian keamanan menggunakan tools online yang terdapat di WEB. Hasil dari enkripsi 2 metode tersebut akan di uji dengan tools online. jika pada pengujian menggunakan tools online menghasilkan plainteks yang sama pada system WEB *History* presensi berarti keamanan dua metode tersbut gagal.

F. KESIMPULAN DAN SARAN

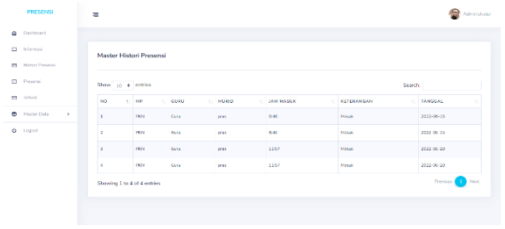
Pada tahap kesimpulan diambil untuk menjawab rumusan masalah yang telah ditentukan sebelumnya, dan saran diambil untuk pertimbangan pengembangan penelitian ini.

4. HASIL DAN PEMBAHASAN

A. IMPLEMENTASI SISTEM

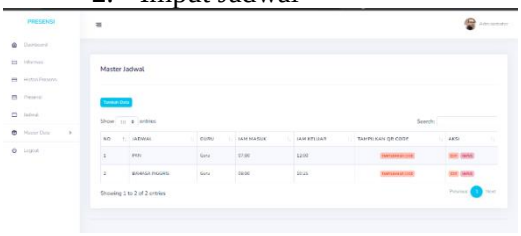
Setelah mengembangkan system presensi siswa menggunakan QR Code dengan Algorima *Triple* DES dan *Caesar Cipher*, tahap selanjutnya yaitu menguji keamanan Algoritma *Triple* DES dan *Caesar Cipher*. Tahap pengujian ini dilakukan agar mengetahui apakah Algoritma *Triple* DES$_c$. dan *Caesar Cipher* dapat mengamankan data presensi siswa.

a. Tampilan WEB Admin
   1. *History* Presensi



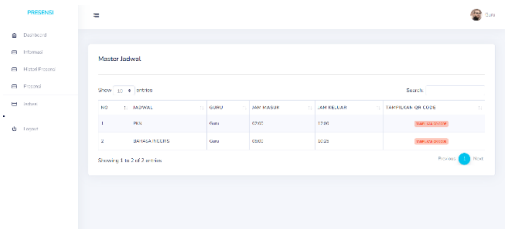
Gambar 4. *History* Presensi
Sumber: Sumber Tatap Muka

2. Imput Jadwal



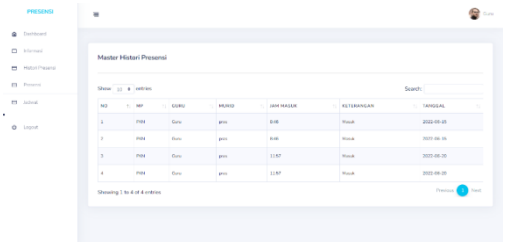
Gambar 5. Input Jadwal
Sumber: Sumber Tatap Muka

b. Tampilan WEB Gru
   1. Cetak *QR Code* Untuk Presensi



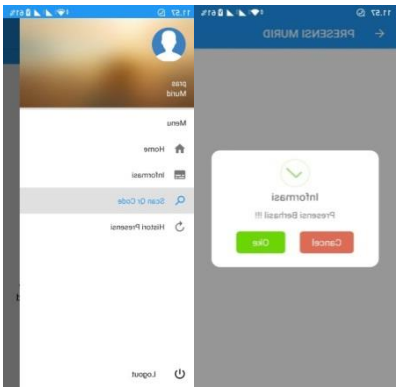
Gambar 6. Cetak QR *Code* Untuk Presensi
Sumber: Sumber Tatap Muka

2. Cek Data Presensi



Gambar 7. Cek Data Presensi
Sumber: Sumber Tatap Muka

Tampilan Android Siswa



Gambar 8. Scan QR *Code*
Sumber: Sumber Tatap Muka

Jurnal Smart Teknologi
Vol. 4, No. 3, Maret 2023, Halaman 390 – 395
ISSN: 2774-1702, http://jurnal.unmuhjember.ac.id/index.php/JST

B. PENGUJIAN

Pada pengujian keamanan data presensi, penulis menggunakan *Tools Deskripsi Triple* DES pada link *(https://tripledes.herokuapp.com/decrypt)* dan *Tools online Deskripsi Caesar Cipher* pada link (https://www.dcode.fr/caesar-cipher) untuk menguji *Algoritma Triple* DES dan *Caesar Cipher*.

Tabel 1. Pengujian Chiperteks menggunakan tools online *Triple* DES

NO	Chipertek	Key	Tools	Plainteks	Hasil
1	YwO5 duolvxh=	nmuhjembe	Triple DES	â-Jæ6 Á~Å	Gagal
2	t+VRd Q+2D9h=			›+®X x@¯	Gagal

Sumber: Hasil Pengujian

Tabel 2. Pengujian Chiperteks menggunakan tools online Caesar Cipher
Sumber: Hasil Pengujian

Pengujian dengan menggunakan kedua *tools Triple* DES dan *Caaesar Chipher* menghasilkan *Plainteks* yang berbeda tidak seperti pada halaman history presensi. Jadi kesimpulannya dengan menggunakan kombinasi 2 metode dapat mengamankan data pada data base.

5. KESIMPULAN DAN SARAN

A. KESIMPULAN

Berdasar kanpenelitian yang telah dilakukan, dapat diambil kesimpulan yaitu data yang hasil presensi yang tersimpan dalam data base dapat di amankan dengan menggunakan *Algoritma Triple DES* dan *Caesar Cipher*.

B. SARAN

Berdasarkan pada penelitian yang sudah dilakukan, adapun beberapa saran yang bisa dikembangkan pada penelitian berikutnya adalah seperti bertikut :

1. Untuk Penelitian selanjutnya bisa menggunakan algoritma yang lebih baru

NO	Chiperteks	Key	Tools	Plainteks	Hasil
1	YwO5d uolvxh=	5	Caesa Ciphe	ÞbT5izt qacm=	Gagal
2	t+VRdQ +2D9h=			y+Awi V+2I9m	Gagal

contohnya Algoritma AES.

2. Untuk Penelitian berikutnya dapat menggunakan lebih kombinas metode untuk keamanan data

6. DAFTAR PUSTAKA

[1] Budiyanto, G. (2020). Implementasi Teknologi Geofencing untuk Sistem Lokasi Dosen (Silodes) di Universitas PGRI Yogyakarta Berbasis Android. *http://prosiding.senadi.upy.ac.id/index.php/senadi/article/view/162*.

[2] Alasi, T.S & Siahaan, A.T.A.A. (2020). Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database. *http://ojs.logika.ac.id/index.php/jikl/article/view/52*.

[3] Arista, M.K. (2021). RANCANG BANGUN APLIKASI PRESENSI DENGAN METODE LOCAL BINARY PATTERN HISTOGRAMS DAN GEOFENCING BERBASIS MOBILE PADA UNIVERSITAS DINAMIKA. *https://repository.dinamika.ac.id/id/eprint/5521/13/17410100135-2021-UNIVERSITASDINAMIKA.pdf*.

[4] Damayanti, I. (2016). PENGEMBANGAN SiS+ KONSULTASI MENGGUNAKAN QR CODE SCANNER SEBAGAI MEDIA KONSULTASI. *https://widuri.raharja.info/index.php?title=SI1212474171*.

[5] fauzi, A. (2017). Analisis

PerbandinganFull Vigenère Chiper, Auto-key Vigenère Chiper dan Running key Vigenère Chiper. *https://docplayer.info/73065440-Analisis-perbandingan-full-vigenere-chiper-auto-key-vigenere-chiper-dan-running-key-vigenere-chiper.html*.

[6] Hardita, V.C & Sholeha, E.W. (2021). PENERAPAN KOMBINASI METODE VIGENERE CIPHER, CAESAR CIPHER DAN SIMBOL BACA DALAM MENGAMANKAN PESAN. *https://ojs.stmikplk.ac.id/index.php/saintekom/article/view/202*.

[7] Hasan, S & Muhammad, N. (2020). SISTEM INFORMASI PEMBAYARAN BIAYA STUDI BERBASIS WEB PADA POLITEKNIK SAINS DAN TEKNOLOGI WIRATAMA MALUKU.

[8] Hasmoro, S.A & Saufik, I. (2017). SISITEM INFORMASI GEGRAFI LOKAL OLEH-OLEH KHAS KOTA SEMARANG BERBASIS MOBILE ANDROID. *https://media.neliti.com/media/publications/209551-sistem-informasi-geografi-lokasi-oleh-a.pdf*.

[9] Hernawati, K. (2017). Implementasi Cipher Viginere pada kode ASCII dengan Memanfaatkan Digit Desimal Bilangan Seuler . *http://staffnew.uny.ac.id/upload/132309677/penelitian/Implementasi+Cipher+Viginere+pada+kode+ASCII.pdf*.

[10] Hidayah, M. (2017, Juni). Arsitektur Android. *https://medium.com/@muhammad30hidayah696/arsitektur-android-6cfbc3dd8cd3*.

[11] Kurniawan, F. (2017). Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost. *file:///C:/Users/ADMIN/Downloads/247-1-1061-1-10-20170615.pdf*.

[12] Maulana, T. (2020). PEMBANGUNAN APLIKASI MEDIA PELATIHAN ATLET KFBC SERANG MENGGUNAKAN TEKNOLOGI SENSOR DETAK JANTUNG, SUHU, ACCELEROMETER DAN GEOFENCING. *https://elibrary.unikom.ac.id/id/eprint/4165/1/UNIKOM_Tezar%20Maulana_Cover.pdf*.

[13] Muara, P & Sipahutar. (2018). BERBAGAI KASUS PENYERANGAN TERHADAP KRIPTOGRAFI. *https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1/Makalah1-060.pdf*.