JURNAL BUFFER INFORMATIKA p-ISSN : 2527-4856, e-ISSN : 2614-5413
Volume 5 Nomor 1, April 2019 https://journal.uniku.ac.id/index.php/buffer

IMPLEMENTASI ALGORITMA CAESAR CIPHER UNTUK KEAMANAN DATA PADA KARTU UJIAN (Studi Kasus : SMK Model Patriot IV Ciawigebang Kab.Kuningan)

Andriyanto[1]
[1]SMK MODEL PATRIOT IV CIAWIGEBANG - KUNINGAN
E-mail: *[1]**andriyanto@gmail.**com

Abstrak

Saat ini, semua kegiatan sudah berbasis digital hal ini menimbulkan sebuah permasalahan baru dimana kejahatan sudah beralih menjadi kejahatan digital. Keamanan data berperan penting dalam menjaga kerahasiaan informasi agar tidak jatuh ke tangan yang salah. SMK Patriot Model IV Ciawigebang memiliki data yang cukup banyak untuk diolah salah satunya data akademik siswa dimana data tersebut sebetulnya sudah menggunakan komputer. Akan tetapi pada pelaksanaan proses ujian masih dilakukan secara semi-manual dimana peserta diberikan sebuah kertas ujian yang berisi identitas siswa tersebut sedangkan jadwal ujian harus mereka lihat pada papan pengumuman. Hal ini dirasakan kurang efisien dalam segi waktu dan kurang optimal dikarenakan penggunaan space/tempat untuk menempelkan jadwal. Kertas Ujian yang diberikan kepada siswa pun rentan akan adanya pemalsuan karena tidak adanya penanda khusus yang tidak mudah ditiru. Oleh sebab itu, pada penelitian ini dikembangkan kartu ujian dimana pada kartu tersebut berisi qr code yang telah diekripsi menggunakan Algoritma Caesar Cipher. Ketika siswa/guru ingin melihat data siswa maupun jadwal ujian, mereka melakukan scan qrcode melalui android dengan cara kerja qr code tersebut akan digenerate oleh sistem dan dideskripsikan menggunakan algoritma Caesar Cipher kemudian dicocokan dengan data yang berada di database, jika cocok maka akan menampilkan data siswa beserta jadwal ujiannya. Sedangkan dari sisi backend, admin dapat mengelola data siswa dan jadwal ujian menggunakan aplikasi web. Sistem ini dirancang menggunakan UML kemudian diimplementasikan ke dalam web dan android. Hasil akhir dari aplikasi ini diharapkan dapat membantu pihak sekolah maupun siswa dalam mengelola data siswa serta data ujian.

Kata Kunci— *Kartu Ujian,QrCode, Enkripsi, Algoritma Caesar Cipher*

Abstract

At present, all activities are digital based, this raises a new problem where crime has turned into digital crime. Data security plays an important role in maintaining the confidentiality of information so it does not fall into the wrong hands. Ciawigebang Model IV Patriot Vocational School has quite a lot of data to be processed, one of which is student academic data where the data is actually already using a computer. However, the implementation of the examination process is still done semi-manually where participants are given an examination paper containing the student's identity while the exam schedule must be seen on the notice board. This is felt to be less efficient in terms of time and less than optimal due to the use of space / place to stick to the schedule. Paper Exams given to students are also vulnerable to forgery because there are no special markers that are not easily imitated. Therefore, in this study an examination card was developed in which the card contained a qr code that had been encrypted using the Caesar Cipher Algorithm. When students / teachers want to see student data and exam schedules, they do a qrcode scan through Android by way of working the qr code will be generated by the system and described using the Caesar Cipher algorithm and then matched to the data in the database, if suitable it will display student data along with the exam schedule. While from the backend side, the admin can manage student data

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

and exam schedules using a web application. This system is designed using UML and then implemented into the web and android. The final results of this application are expected to help the school and students in managing student data and exam data.

Keywords*— Exam Card, Qr Code, Encription, Caesar Cipher Algorithm*

1. PENDAHULUAN

SMK Patriot Model IV Ciawigebang adalah salah satu SMK unggulan dalam bidang teknologi, hal ini dapat dilihat dari adanya program studi yang Teknik Komputer dan Jaringan (TKJ) dan Aplikasi Perkantoran (AP).

Dalam pengelolaan data di sekolah tersebut masih banyak yang dilakukan secara semi manual salah satunya dalam proses ujian dimana data peserta ujian besserta jadwal ujian masih dicetak dalam kertas sehingga tidak efisien dari segi waktu dan tidak optimal dikarenakan penggunaan kertas yang banyak serta membutuhkan tempat yang luas.

Penggunaan kertas sebagai identitas peserta ujian pun rentan terjadinya pemalsuan dikarenakan belum adanya penanda khusus dalam kartu tersebut sehingga mudah untuk ditiru. Padahal keamanan data dan informasi sangatlah penting.

Keamanan data tidak hanya bergantung dari keamanan storage dimana data tersebut berada, melainkan proses transfer data dari suatu media ke media lainnya. Banyak orang yang tidak menyadari ketika mereka melakukan pengiriman data, ada peluang untuk mencuri atau mengubah informasi dari data yang akan dikirim tersebut, sehingga data tersebut tidak asli lagi. Oleh sebab itu, keamanan dalam pengiriman data juga menjadi hal sangat vital apalagi jika di dalamnya terdapat informasi yang sifatnya sangat penting dan rahasia (Ariyus, 2009)

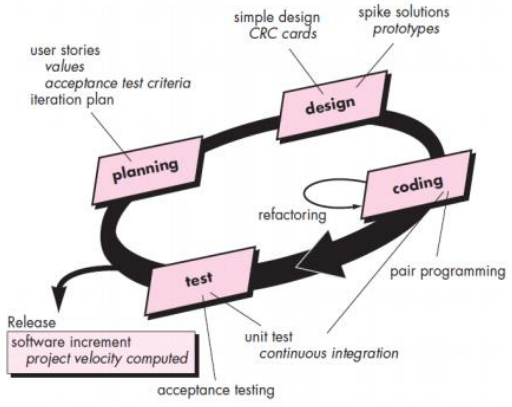
Untuk mengatasi permasalahan diatas maka penulis melakukan penelitian dengan judul "Implementas Algoritma Caesar Cipher untuk Keamanan Data Pada Kartu Ujian (studi kasus pada SMK Model Patriot IV Ciawigebang Kab. Kuningan).

2. METODE PENELITIAN

2.1. Extreme Programming

Menurut Pressman (2010, p. 72), Extreme Programming (XP) adalah salah satu metode pengembangan software yang termasuk dalam metode agile. [2]

Dalam Extreme Programming, terdapat 4 (empat) kerangka kerja yang dilakukan yaitu planning, design, coding dan testing.



Gambar 1 XP[2]

Berikut merupakan proses Extreme Programming menurut Pressman [2]:

a. Planning, aktifitas yang juga disebut sebagai the planning game dimulai dengan "mendengarkan" yaitu sebuah aktifitas mengumpulkan kebutuhan yang memungkinkan para anggota teknikal dari tim XP untuk memahami

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

konteks bisnis untuk perangkat lunak dan untuk mendapatkan broad feel untuk output yang dibutuhkan dan fitur utama serta fungsionalitas. Pada tahap ini, stakeholder dan programmer bekerjasama untuk menentukkan bagaimana mengelompokkan cerita ke dalam rilis berikutnya atau peningkatan perangkat lunak selanjutnya, yang akan dibangun oleh tim XP.

b. Design, menyediakan panduan implementasi untuk proses seperti yang sudah dituliskan. Gagasan pusat di dalam XP adalah design terjadi sebelum dan setelah coding dimulai
c. Coding, menterjemahkan penjabaran yang sudah dilakukan pada tahap penulisan kode program.
d. Testing, pada tahap ini unit test yang dikreasikan harus diimplementasikan menggunakan framework yang memungkinkan mereka menjadi otomatis (karenanya, dapat dieksekusi dengan mudah dan berulang-ulang). Hal ini mendorong strategi regresi testing ketika kode dimodifikasi

2.1.1. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah :

a. Wawancara, melakukan sesi tanya jawab kepada pihak-pihak yang terkait dengan penelitian
b. Observasi, dilakukan dengan melakukan pengamatan secara langsung di objek penelitian.
c. Studi Literatur, melakukan studi terhadap dokumen-dokumen yang dibutuhkan dalam penelitian

2.1.2. Algoritma Caesar Cipher

Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (plaintext) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet.

Ini adalah algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga caesar chiper), untuk menyandikan pesan yang ia kirim kepada para gubernurnya. Caranya adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet). Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan abjad. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu k = 3). Dengan mengkodekan setiap huruf abjad dengan integer sebagai berikut: A = 0, B = 1, …,Z = 25, maka secara matematis caesar chiper menyandikan plainteks pi menjadi ci dengan aturan (enkripsi):

$$c_i = E(p_i) = (p_i + k) \bmod 26$$

Deskripsi :

$$p_i = D(c_i) = (c_i - k) \bmod 26$$

Karena hanya ada 26 huruf abjad, maka pergeseran huruf yang mungkin dilakukan adalah dari 0 sampai 25. Setiap huruf yang sama digantikan oleh huruf yang sama di sepanjang pesan, sehingga sandi Caesar digolongkan kepada, substitusi monoalfabetik. [3].

2.1.3. UML

Unified Modeling Language (UML) adalah salah satu standar bahasa yang banyak digunakan di dunia industri untuk mendefinisikan requirement, membuat analisis dan desain, serta menggambarkan arsitektur dalam pemrograman berorientasi objek. UML merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung.

UML hanya berfungsi untuk melakukan pemodelan. Jadi penggunaan UML tidak terbatas pada metodologi tertentu, meskipun pada kenyataannya UML paling banyak digunakan pada metodologi berorientasi objek [4]

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

Dibawah ini merupakan penjelasan sigkat mengenai diagram-diagram UML [4]:

a. Use Case Diagram merupakan pemodelan untuk kelakuan (behavior) sistem informasi yang akan dibuat.
b. Activity Diagram menggambarkan workflow (aliran kerja) atau aktivitas dari sebuah sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak
c. Class Diagram menggambarkan struktur sistem dari segi pendefinisian kelas-kelas yang akan dibuat untuk membangun sistem
d. Sequence Diagram menggambarkan kelakuan objek pada use case dengan mendeskripsikan waktu hidup objek dengan massage yang dikirimkan dan diterima antar objek.

3. HASIL DAN PEMBAHASAN

Adapun hasil dan pembahasan dari penelitian ini adalah:

a. Pengumpulan Data

- Wawancara, melakukan sesi tanya jawab kepada Wakil Kepala Sekolah Bidang Kesiswaan, adapun yang diperoleh berdasarkan hasil wawancara adalah sistem yang berjalan pada saat pencetakan kartu ujian, data yang terdapat pada kartu ujian serta jadwal yang ujian yang ditempel.
- Observasi, melakukan pengamatan secara langsung pada saat persiapan dan pada saat ujian dilaksanakan.
- Studi Pustaka, mempelajari literatur yang terkait penelitian seperti buku mengenai php dan mysqli, android, qr code, algoritma caesar cipher.

b. Algoritma Caesar Cipher

Tabel 1. Tabel deret Alphabeth

A	B	C	D	E	F	G
0	1	2	3	4	5	6

H	I	J	K	L	M	N
7	8	9	10	11	12	13

O	P	Q	R	S	T	U
14	15	16	17	18	19	20

V	W	X	Y	Z
21	22	23	24	25

Contoh :
id peserta ujian dalam bentuk Plaintext (Pi) : XTKJIVIXIXXV
Sedangkan Jumlah Deret Substitusi : 10
Kemudian menentukan index dari Plaintext (Pi) berdasarkan tabel 1.

Tabel 2. Hasil konversi index dari Pi

Pi	X	T	K	J	I	V
I	23	19	10	9	8	21

Pi	I	X	I	X	X	V
i	8	23	8	23	23	21

Lalu Enkripsi Plaintext (Tabel 2) menjadi Cipher Text menggunakan Algoritma Caesar Cipher.

Tabel 3. Perhitungan Enkripsi Dengan Caesar Chiper

Cipher Text	Caesar Cipher		Result
	(Pi+k)mod 26	=	
C[1]	(23+10)mod 26	7	H
C[2]	(19+10)mod 26	3	D
C[3]	(10+10)mod 26	20	U
C[4]	(9+10)mod 26	19	T
C[5]	(8+10)mod 26	18	S
C[6]	(21+10)mod 26	5	F
C[7]	(8+10)mod 26	18	S
C[8]	(23+10)mod 26	7	H
C[9]	(8+10)mod 26	18	S
C[10]	(23+10)mod 26	7	H
C[11]	(23+10)mod 26	7	H
C[12]	(21+10)mod 26	5	F

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

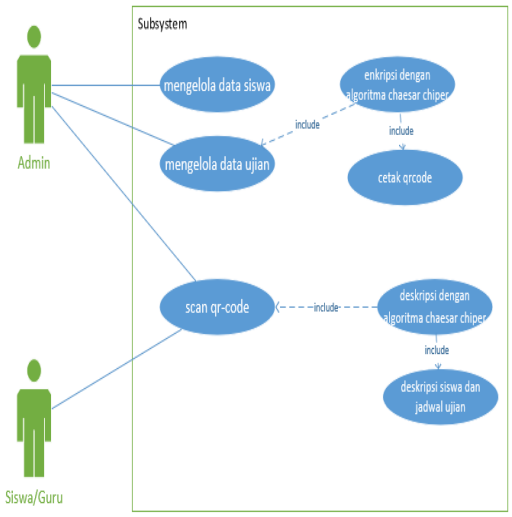
Untuk merubah kembali Cipher Text menjadi Plaintext, dilakukan proses deskripsi menggunakan Algoritma Caesar Cipher

Tabel 4. Perhitungan Deskripsi Dengan Caesar Chiper

Plain Text	Caesar Cipher		Result
	(Ci-k)mod 26	=	
P[1]	(7-10)mod 26	23	X
P[2]	(3-10)mod 26	19	T
P[3]	(20-10)mod 26	10	K
P[4]	(19-10)mod 26	9	J
P[5]	(18-10)mod 26	8	I
P[6]	(5-10)mod 26	21	V
P[7]	(18-10)mod 26	8	I
P[8]	(7-10)mod 26	23	X
P[9]	(18-10)mod 26	8	I
P[10]	(7-10)mod 26	23	X
P[11]	(7-10)mod 26	23	X
P[12]	(5-10)mod 26	21	V

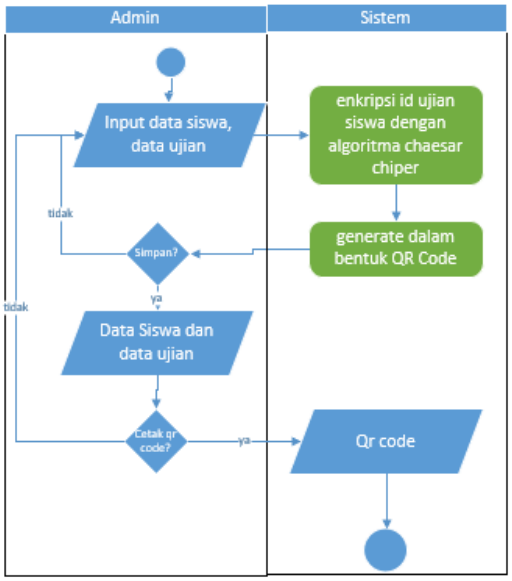
c. Perancangan Sistem

- Use Case Diagram



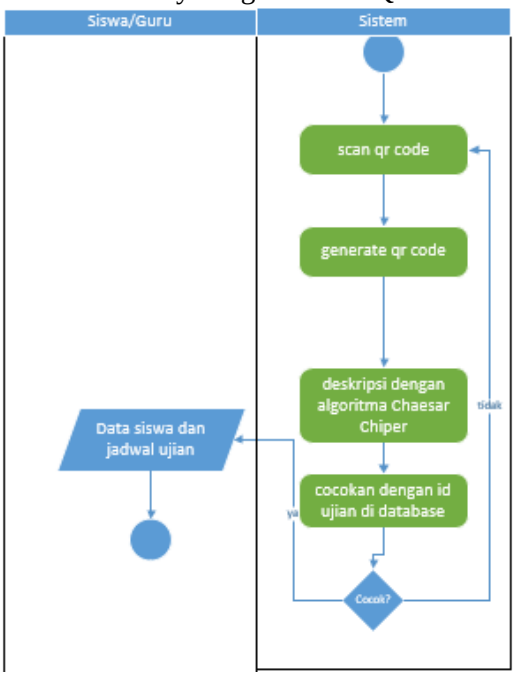
Gambar 2. Use Case Diagram

- Activity Diagram Mengelola Peserta Ujian



Gambar 3. Activity Diagram Peserta Ujian

- Activity Diagram Scan QR Code



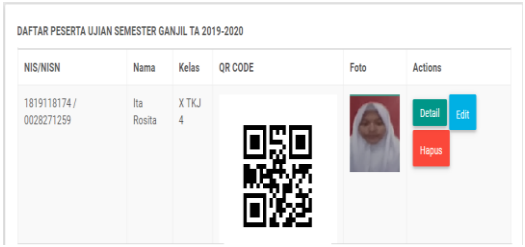
Gambar 4. Activity Diagram Scan QR Code

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

d. Implementasi

Admin :

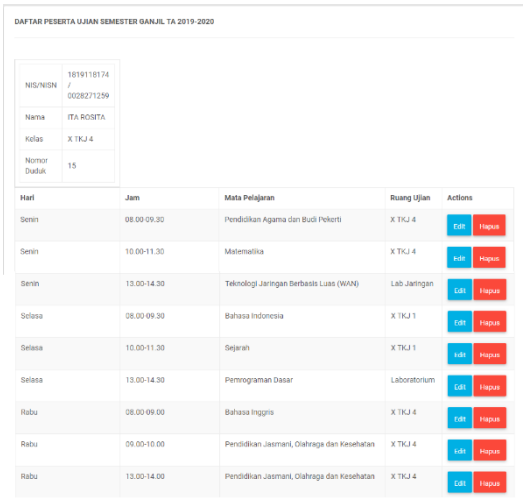
- Data Peserta Ujian



Gambar 5. Data Peserta Ujian

Pada backend interface ini, admin dapat melakukan pengelolaan data peserta ujian : menambah, melihat, mengupdate, menghapus.

- Mengelola Jadwal Ujian Peserta



Gambar 6. Detail Jadwal Ujian Peserta

Pengguna :

- Menu Utama

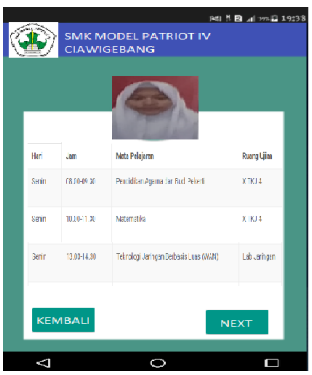
Gambar 7. Menu Utama Android

- Scan QR Code

Gambar 8. Scan Qr Code

Jika ingin melihat jadwal ujian, peserta ujian menekan tombol NEXT

- Detail Jadwal Peserta Ujian



Gambar 9. Detail Jadwal Peserta Ujian

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

4. KESIMPULAN

Adapun kesimpulan dari penelitian ini adalah:

1. Penelitian ini dapat mengelola data peserta ujian/siswa beserta jadwal ujiannya.
2. Penelitian ini dapat menjaga kerahasiaan data karena id peserta ujian telah dienkripsi menggunakan Algoritma Caesar Cipher dan digenerate dalam bentuk Qr Code.

5. SARAN

Agar penelitian yang dihasilkan lebih optimal, maka diharapkan :

1. Adanya pengembangan lebih lanjut mengenai algoritma untuk keamanan data.
2. Qr Code diprint pada media yang tahan air agar dapat tahan lama.
3. Untuk pengembangan selanjutnya, siswa dibuatkan kartu tanda pengenal yang didalamnya sudah berisi Qr Code, sehingga dapat menghilangkan media kertas sebagai identitas peserta.

UCAPAN TERIMA KASIH

Serta penulis mengucapakan terima kasih kepada semua pihak yang telah membantu sehingga penelitian ini dapat selesai tepat pada waktunya.

DAFTAR PUSTAKA

[1] Ariyus, D. 2009. Keamanan Multimedia. Yogyakarta: Andi.

[2] Pressman, R.S. (2010), Software Engineering : a practitioner's approach,. McGraw-Hill, New York, 68

[3] Santosa, Egar Dika. Implementasi Algoritma Caesar Cipher dan Hill Cipher pada Database Sistem Inventori TB Mitra Jepara. Semarang: Fakultas Ilmu Komputer, Universitas Dian Nuswantoro.

[4] A. S., Rosa dan Shalahuddin, M. 2013. Rekayasa Perangkat Lunak Terstruktur. Dan Berorientasi Objek. Informatika. Bandung