

IMPLEMENTASI ALGORITMA VIGENERE CHIPER UNTUK KEAMANAN TANGGAL KADALUARSA (Studi Kasus : Toko Kemuning Depok – Prov. Jawa Barat)

Yani Suryani¹

¹PT. Indonesia TRC Industry – Cikarang

E-mail: *¹yani.suryani@gmail.com

Abstrak

Makanan adalah salah satu hal penting dalam kehidupan masyarakat. Semakin berkualitas suatu makanan maka dapat menghasilkan sumber daya manusia yang berkualitas juga. Akan tetapi maraknya pemalsuan salah satunya pemalsuan tanggal kadaluarsa mengakibatkan masyarakat harus jeli dan teliti dalam memilih produk. Salah satu makanan yang digemari masyarakat adalah jenis kue dan bolu. Toko Kemuning salah satu toko yang banyak memproduksi jenis-jenis kue tersebut untuk didistribusikan dan dijual sendiri di tokonya. Oleh karena itu, untuk meningkatkan kepercayaan masyarakat terhadap kualitas produk yang dihasilkan oleh Toko Kemuning maka pada penelitian ini dibuat sebuah aplikasi untuk mengelola data produk, dimana konsumen dapat mengecek tanggal kadaluarsa melalui android dengan cara scan qr code yang terdapat dalam kemasan kue. Adapun yang digenerate ke dalam bentuk qr code adalah id produk, id tersebut berisi string unik yang dienkripsi menggunakan algoritma vigenere chipper sehingga tidak mudah dideteksi oleh orang lain. Admin dapat melakukan pengelolaan data produk sehingga ketika toko memproduksi kue, data dapat tersimpan di database dan qr code dapat dicetak. Dengan penelitian ini diharapkan dapat meningkatkan kepercayaan konsumen serta menjaga kualitas produk dari toko kemuning.

Kata Kunci— Kue, Enkripsi, Algoritma Vigenere Chipper

Abstract

Food is one of the important things in people's lives. The more quality a food can produce quality human resources as well. However, the rise of counterfeiting, one of which is falsification of expiration date, causes the public to be observant and careful in choosing products. One of the foods that are favored by the public is a type of cake and sponge cake. Kemuning Shop is one shop that produces many types of cakes to be distributed and sold alone in the store. Therefore, to increase public trust in the quality of products produced by the Kemuning Shop, an application is made to manage product data, where consumers can check the expiration date via android by scanning the qr code contained in the cake packaging. As for what is generated in the form of qr code is a product id, the id contains a unique string that is encrypted using the vigenere chipper algorithm so that it is not easily detected by others. Admins can manage product data so that when a shop produces cookies, data can be stored in a database and the QR code can be printed. With this research it is expected to increase consumer confidence and maintain product quality from kemuning shops.

Keywords— Cake, Encryption, Vigenere Chipper Algorithm

1. PENDAHULUAN

Pangan merupakan salah satu bagian terpenting dalam kehidupan manusia karena salah satu faktor penentu kualitas sumber daya manusia adalah kualitas pangan yang masuk ke dalam tubuh manusia. Sehingga masyarakat menjadi lebih selektif dalam memilih makanan yang berkualitas. Salah satu hasil olahan pangan yang banyak diminati masyarakat adalah kue sehingga semakin banyak produsen-produksi makanan yang bermunculan, salah satunya Toko Kemuning yang terletak di Depok Provinsi Jawa Barat.

Toko kemuning memproduksi kue per 3 hari, dimana kue yang dihasilkan tidak hanya untuk dijual sendiri tetapi juga untuk didistribusikan ke toko-toko retail. Pada sistem yang berjalan terdapat beberapa permasalahan yaitu ketika konsumen ingin mengetahui tanggal kadaluarsa dari suatu kue harus menanyakan langsung kepada penjaga toko, hal ini tidak efisien waktu. Sedangkan jika tanggal kadaluarsa dalam bentuk cap, rentan terjadi pemalsuan data yang nantinya akan berakibat pada menurunnya kepercayaan masyarakat terhadap produk toko tersebut.

Untuk mengatasi permasalahan diatas maka penulis melakukan penelitian dengan judul “Implementasi Algoritma Vigenere Cipher untuk Keamanan Tanggal Kadaluarsa (studi kasus pada Toko Kemuning Depok – Jawa Barat)”

2. METODE PENELITIAN

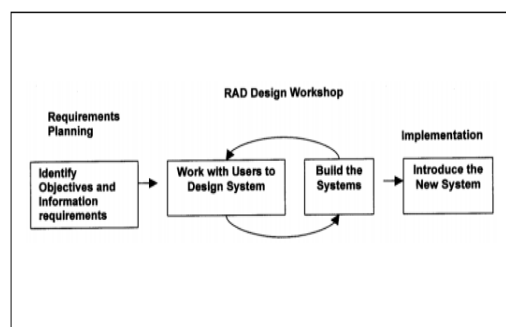
2.1. RAD Application

Menurut Martin (dalam Pressman, 2002), *Rapid Application Development (RAD)* adalah sebuah model proses

pengembangan perangkat lunak sekuensial linear yang menekankan siklus pengembangan yang sangat pendek.[1]

Model RAD ini merupakan pengembangan dari metode sekuensial linier di mana perkembangan cepat dicapai dengan menggunakan model pendekatan berbasis komponen. Jika kebutuhan user dapat dipahami dengan baik, proses RAD memungkinkan pengembangan sistem dalam periode waktu yang lebih singkat.

Metode RAD memiliki 3 tahapan utama dalam pengembangannya (Noertjahyana, 2002) :



Gambar 1. RAD [2]

- Rencana Kebutuhan (*Requirement Planning*). Pada tahap ini, dilakukan pertemuan dengan user untuk melakukan identifikasi tujuan dari aplikasi atau sistem dan melakukan identifikasi kebutuhan informasi untuk mencapai tujuan
- Proses Desain (*Design Workshop*). Pada tahap ini adalah melakukan proses desain dan melakukan perbaikan-perbaikan apabila masih terdapat ketidaksesuaian desain antara user dan analis.
- Implementasi (*Implementation*). Setelah desain dari sistem yang akan dibuat sudah disetujui baik itu oleh user maka pada tahap ini programmer mengembangkan prototype menjadi suatu program.

2.1.1. Teknik

2.1.2. 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

2.1.3. Algoritma Vigenere Chiper

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau pada tahun 1586. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553. Cara kerja dari Vigenère cipher ini mirip dengan Caesar cipher, yaitu mengenkripsi plaintext pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet.

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjadmajemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti Caesar cipher yang menerapkan metode substitusi abjadtunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama (Hallim, 2010).[3]

Rumus matematik proses enkripsi dengan vigenere chiper :

$$Ci \rightarrow (Pi + Ki) \text{Mod } 65 \quad \dots\dots\dots (2.1)$$

Keterangan :

Ci : Nilai ciphertext

Pi : Nilai Plaintext

Ki : Nilai Kunci

Mod 65 : Modulus 65 Karakter

Proses Deskripsi :

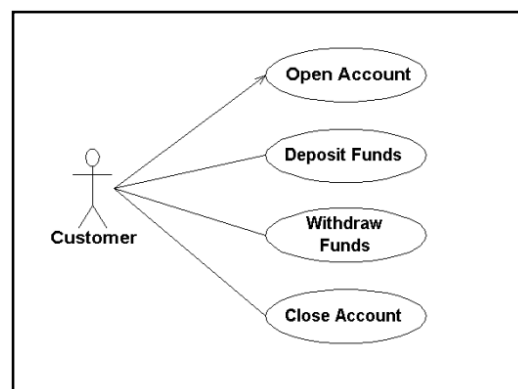
$$Pi \rightarrow (Ci - Ki) \text{Mod } 65 \quad \dots\dots\dots (2.2)$$

2.1.4. UML

Unified Modeling Language (UML) adalah sebuah bahasa pemodelan visual yang dirancang khusus untuk pengembangan dan analisis sistem berorientasi objek dan desain. UML pertama kali dikembangkan oleh Grady Booch, Jim Rumbaugh, dan Ivars Jacobson pada pertengahan tahun 1990. (Journal of Database Management: Keng Siau and Qing Cao, 2001:26) [4]

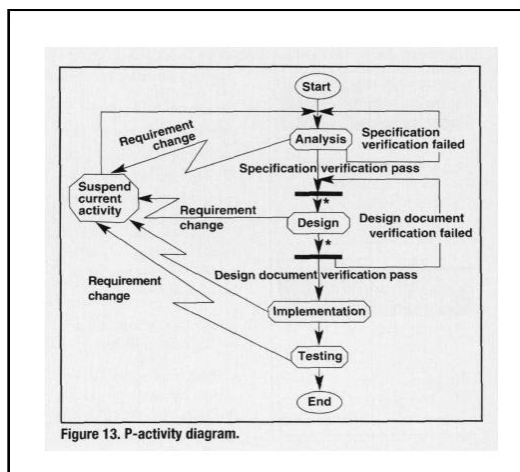
Dibawah ini merupakan penjelasan singkat mengenai diagram-diagram UML The Elements of UML 2.0: Scott W.Ambler (2005:35)

- a. Use Case Diagram adalah sebuah diagram yang menunjukkan hubungan antara actors dan use cases.



Gambar 2. Use Case Diagram

b. Activity Diagram adalah suatu diagram yang menggambarkan konsep aliran data/kontrol, aksi terstruktur serta dirancang dengan baik dalam suatu sistem. (Journal of Object Technology:Conrad Bock, 2003:45)



Gambar 3. Activity Diagram

Sumber: Journal of Object - Oriented Programming : Shih-Chien Chou and Jen-Yen Jason Chen (2000:25)

3. HASIL DAN PEMBAHASAN

Adapun hasil dan pembahasan dari penelitian ini adalah:

- a. Pengumpulan Data
 - Wawancara, melakukan sesi tanya jawab kepada pemilik toko beserta pegawai yang bertugas sebagai *chef* serta penjaga toko. Yang diperoleh adalah : pada sistem yang berjalan tanggal kadaluarsa belum dicantumkan pada produk. Jenis kue yang dihasilkan antara lain kue ulang tahun dan kue pengantin.
 - Observasi, melakukan pengamatan secara langsung ketika terjadi transaksi pembelian, dimana pembeli mengetahui tanggal kadaluarsa dengan bertanya secara langsung kepada pemilik toko.

- Studi Pustaka, mempelajari literatur yang terkait penelitian seperti buku mengenai php dan mysql, android, qr code, algoritma vigenere chipper.

b. Algoritma Vigenere Chipper
Contoh soal : buah CARICA

Tabel 1. Contoh id kue dalam bentuk Plaintext : CAUTBAA

Pi	C	A	U	T	B	A	A	
Ki	k	e	m	u	n	i	n	g
	0	1	2	3	4	5	6	7

Sedangkan Kata Kunci ditentukan default oleh sistem : kemuning

Tabel 2. Perhitungan Enkripsi Dengan Vigenere Chipper

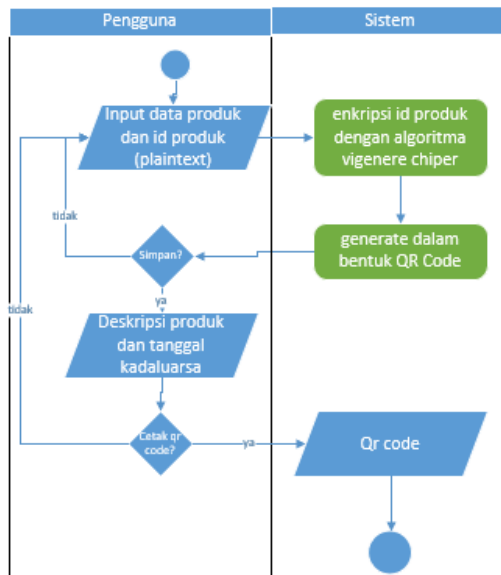
		Result
$(C+k) \text{ mod } 65 =$	$(2+10) = 12$	M
$(A+e) \text{ mod } 65 =$	$(0+4) = 4$	E
$(U+m) \text{ mod } 65 =$	$(20+12) = 32$	G
$(T+u) \text{ mod } 65 =$	$(19+20) = 39$	N
$(B+n) \text{ mod } 65 =$	$(1+13) = 14$	O
$(A+i) \text{ mod } 65 =$	$(0+8) = 8$	I
$(A+n) \text{ mod } 65 =$	$(0+13) = 13$	N

Tabel 3. Perhitungan Deskripsi Dengan Vigenere Chipper

		Result
$(M-k) \text{ mod } 65 =$	$(12-10) = 2$	C
$(E-e) \text{ mod } 65 =$	$(4-4) = 0$	A
$(G-m) \text{ mod } 65 =$	$(6-12) = -6$	U
$(N-u) \text{ mod } 65 =$	$(13-20) = -7$	T
$(O-n) \text{ mod } 65 =$	$(14-13) = 1$	B
$(I-i) \text{ mod } 65 =$	$(8-8) = 0$	A
$(N-n) \text{ mod } 65 =$	$(13-13) = 0$	A

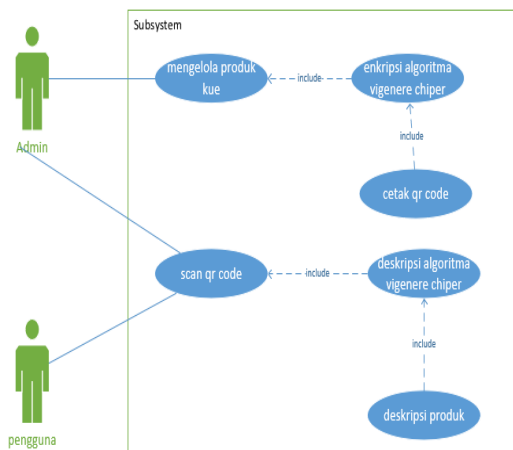
Tabel 4 Substitusi Vigenere Chiper

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z



Gambar 5. Activity Diagram Mengelola Produk

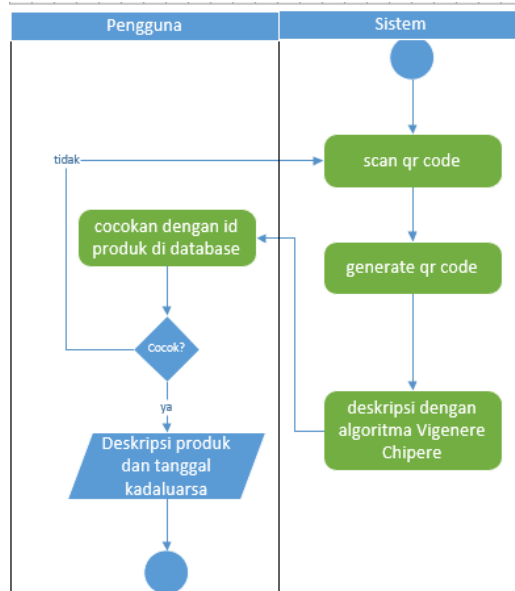
- c. Perancangan Sistem
- Use Case Diagram



Gambar 4. Use Case Diagram













- Activity Diagram Mengelola Produk

- Activity Diagram Scan QR Code



Gambar 6. Activity Diagram Scan QR Code

- d. Implementasi Admin :
- Data Kue

No	Nama	Deskripsi	Ukuran dan Harga	Tanggal Produksi	Tanggal Kadaluarsa	Gambar	QR CODE	Actions
1	Cake Ulang Tahun Buah	Cake blackforest rasa coklat, dibagian tengah dilapisi selai strawberry dilapisi sesuai keinginan, di bagian luar dilapisi whipped cream dan coklat leleh. Di bagian atas ditaburi buah-buahan dapat disesuaikan dengan permintaan. Dapat diberi ucapan	20 = Rp. 150.000 22 = Rp. 180.000 24 = Rp. 200.000 28 = Rp. 220.000 30 = Rp. 250.000	2019-08-01	2019-08-03			 
2	Cake Ulang Tahun Karakter	Kue blackforest, dilapisi pondant/whipped cream, diberi gambar karakter.	20 = Rp. 180.000 22 = Rp. 200.000 24 = Rp. 250.000 30 = Rp. 300.000	2019-08-01	2019-08-03			 
3	Cake Ulang Tahun	Kue Ulang Tahun Blackforest Rasa Coklat, pada tengah kue dilapisi selai strawberry (dapat disesuaikan dengan permintaan).	20 = Rp. 120.000 22 = Rp. 150.000 24 = Rp. 180.000 28 = Rp. 200.000 30 = Rp. 250.000	2019-08-01	2019-08-03			 

Gambar 7. Data Kue

Pada backend interface ini, admin dapat melakukan pengelolaan data produk(kue) : menambah, melihat, mengupdate, menghapus.

Pengguna :

- Menu Utama



Gambar 8. Menu Utama Android

- Jenis Kue



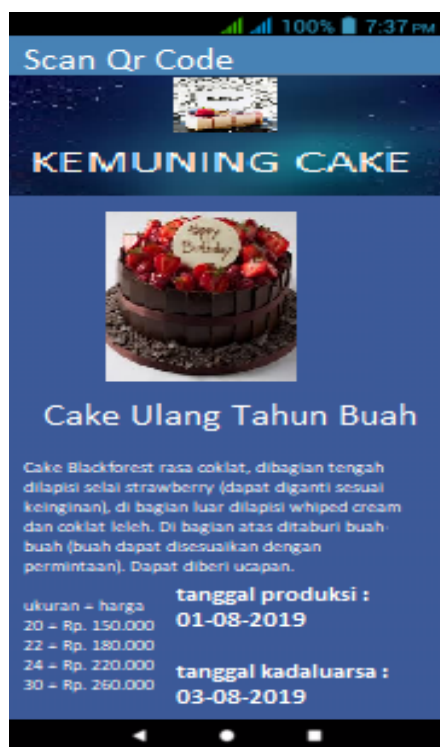
Gambar 9. Jenis Kue

- Detail Kue



Gambar 10. Detail Kue

- Hasil Scan QR-Code



Gambar 11. Hasil Scan QR Code

4. KESIMPULAN

Adapun kesimpulan dari penelitian ini adalah:

1. Penelitian ini mampu menampilkan tanggal kadaluarsa dengan lebih aman dikarenakan sudah dienkripsi menggunakan Algoritma Vigenere Cipher.
2. Aplikasi ini dapat mengelola produk kue oleh admin dan dapat menampilkan deskripsi kue melalui scan qr code secara lebih mudah oleh pengguna karena sudah berbasis android.

5. SARAN

Agar penelitian yang dihasilkan lebih optimal, maka diharapkan :

1. Adanya pengembangan lebih lanjut mengenai algoritma untuk keamanan data.
2. Dapat dikembangkan ke dalam bentuk 3Dimensi agar menjadi lebih menarik.

UCAPAN TERIMA KASIH

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

DAFTAR PUSTAKA

- [1] Roger S. Pressman, 2002. *Rekayasa Perangkat Lunak Pendekatan Praktisi* (Buku. Satu), ANDI Yogyakarta
- [2] Noertjahyana, 2002. *Studi Analisis Rapid Application Development Sebagai Salah Satu Alternatif Metode Pengembangan Perangkat Lunak*. Jurnal Informatika.
- [3] Hallim. Abd, dkk. 2010. "Pembuatan Perangkat Lunak Media Pembelajaran Kriptografi Klasik". Institut Teknologi Sepuluh November.
- [4] Siau, Keng Cao, Qing/ *Journal of Database Management/ Unified Modelling Language/ Jan-Mar 2001; 12, 1; ABI/INFORM Research pg.26*
- [5] Conrad Bock, "Journal of Object Technology", 2003: 45