BUFFER INFORMATIKA
Volume 6 Nomor 1, April 2020
p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

Implementasi Algoritma *El Gamal* Pada Aplikasi Pengaman Produk CV. Rimba 99 Meubeul Menggunakan *Qr Code*

Firman Faturohman[1)], Aji Permana M.Kom[2)], Tito Sugiharto M.Eng[3)]
PT. Berkah Kuningan Jawa Barat[1)], Fakultas Ilmu Komputer, Universitas Kuningan[2,3)]
Jl. Cut Nyak Dhien, Cijoho, Kuningan
Email : 2015081043@student.uniku.ac.id[1)], aji@uniku.ac.id[2], tito@uniku.ac.id[3)]

ABSTRAK

Industri Mebel adalah sebuah industri yang mengolah bahan baku atau bahan setengah jadi dari kayu, rotan, dan bahan baku lainnya untuk dijadikan produk mebel yang mempunyai nilai tambah dan menjadi lebih tinggi manfaatnya dari sebelumnya. CV. Rimba 99 Meubel sebagai produsen mebel jati memiliki beberapa masalah diantaranya konsumen sulit membedakan produk yang dibuat CV. Rimba 99 Meubel dengan perusahaan mebel yang lain, banyaknya produk mebel yang menyerupai produk CV. Rimba 99 Meubel yang di distribusikan ke toko–toko mebel dengan kualitas yang buruk. Berdasarkan permasalahan berikut menjadi dasar penulis untuk mengambil judul penelitian "Implementasi Algoritma El Gamal Pada Aplikasi Pengaman Produk CV. Rimba 99 Meubel Menggunakan *QR Code*". Aplikasi yang dibuat dapat mengecek keaslian produk mebel CV. Rimba 99 Meubel oleh konsumen pada toko-toko mebel yang di distribusikan menggunakan *QR Code* agar mudah digunakan dan dapat menyimpan data yang banyak. Untuk masalah keamanan data maka digunakan algoritma kriptografi El Gamal pada bagian enkripsi dan deskripsi data agar data produk aman dan sulit di palsukan. Aplikasi ini dikembangkan dengan menggunakan metode *Rational Unified Process* (RUP) dimana tahapan pembuatan sistem atau aplikasi akan lebih jelas dan terstruktur dengan baik. Hasil dari penelitian ini adalah sebuah aplikasi berbasis *client server* dimana pada *client* adalah sebuah aplikasi android dengan fitur utama *scan QR Code* khusus yang berfungsi untuk menampikan data produk mebel dan dari sisi *server* adalah aplikasi untuk memanajemen data produk mebel dalam bentuk *QR Code* pada proses enskripsi dan deskripsi data.

Kata Kunci : *Mebel, El Gamal, QR Code, Android, Rational Unified Process*

ABSTRACT

Furniture industry is an industry that processes raw materials or semi-finished materials from wood, rattan, and other raw materials to be used as furniture products that have added value and it has higher benefit than before. CV. Rimba 99 Meubel as a teak furniture producer has several problems including the difficulty for consumers to differentiate products made by CV. Rimba 99 Meubel with other furniture companies, many furniture products that resemble with CV products. Rimba 99 Furniture distributed to furniture shops with poor quality. Based on the following problems the author is based to take the title of the research "Implementation of the El Gamal Algorithm in the Product Safety Application CV. Rimba 99 Meubel Using QR Code ". The application that is made can check the authenticity of furniture products from CV. Rimba 99 Meubel by consumers in furniture stores distributed using QR Code so that it is easy to use and it can store a lot of data. For data security issues, El Gamal cryptographic algorithm is used in the data encryption and description section so that product data is safe and difficult to fake. This application was developed using the Rational Unified Process (RUP) method where the stages of making a system or application will be clearer and well structured. The results of this study are a client server based application where the client is an android

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

application with the main feature of a special QR Code scan that serves to display furniture product data and from the server side is an application for managing furniture product data in the form of QR Code in the encryption process and data description.

Keywords : *Furniture, El Gamal, QR Code, Android, Rational Unified Process*

1. PENDAHULUAN

Industri Mebel adalah sebuah industri yang mengolah bahan baku atau bahan setengah jadi dari kayu, rotan, dan bahan baku lainnya untuk dijadikan produk mebel yang mempunyai nilai tambah dan menjadi lebih tinggi manfaatnya dari sebelumnya. Dimana sebuah industri mebel dituntut untuk mampu bersaing dengan industri mebel lainnya dalam menghasilkan produk yang berkualitas sesuai dengan keinginan konsumen.

CV. Rimba 99 Meubel memiliki beberapa masalah diantaranya konsumen sulit membedakan produk yang dibuat CV. Rimba 99 Meubel dengan perusahaan mebel yang lain, banyaknya produk mebel yang menyerupai produk CV. Rimba 99 Meubel yang di distribusikan ke toko–toko mebel dengan kualitas yang buruk dan belum adanya aplikasi untuk mempermudah dalam mengecek produk CV. Rimba 99 Meubel.

Maka dari permasalahan itu perlunya sebuah media atau sistem yang dimana masyarakat atau konsumen dapat mengecek keaslian dari produk mebel tersebut dengan praktis, mudah dan terpercaya berdasarkan data dari produsen terkait. Algoritma kriptografi kunci publik *El Gamal* merupakan algoritma blok *chipper* yaitu algoritma yang melakukan proses enkripsi pada blok-blok *plaintext* yang kemudian menghasilkan blok-blok *chipertext*, yang nantinya blok-blok *chipertext* tersebut akan dideskripsi kembali dan hasilnya kemudian digabungkan menjadi *plaintext* semula.

Quick Response Code sering di sebut *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. *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 vertical (Ashford, 2010).

Dengan memanfaatkan teknologi *Quick Response Code* (*QR Code*) yang di kombinasikan dengan algoritma Kriptografi *El Gamal* yang di kembangkan dalam aplikasi android, cara kerjanya cukup sederhana yakni dengan menempelkan *QR Code* pada produk mebel, dimana QR Code tersebut mengandung informasi yang dienkripsi oleh algoritma *El Gamal,* algoritma tersebut akan diterapkan pada *QR Code* kemudian kita dapat melakukan pengecekan secara *Realtime* dengan melakukan *scanning* dengan aplikasi android yang dikembangkan kemudian aplikasi akan melakukan pemindaian dan mendeskripsikan data tersebut, setelah itu akan melakukan *checking* ke *server* apakah data yang ada pada *QR Code* tersebut valid atau tidak, kemudian aplikasi akan menampilkan informasi produk tersebut asli buatan produsen tersebut, dengan aplikasi tersebut tentunya akan ada beberapa elemen yang terbantu, baik itu dari konsumen ataupun dari produsen.

2. METODE PENELITIAN

2.1. Metode Pengembangan Sistem

Metode penelitian yang di pakai pada pengembangan aplikasi ini menggunakan metode *Rational Unified Process* (RUP), metode ini penulis gunakan karena konsep *object oriented* yang cocok dengan konsep aplikasi yang akan dibangun, berikut 4 fase tahapan :

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

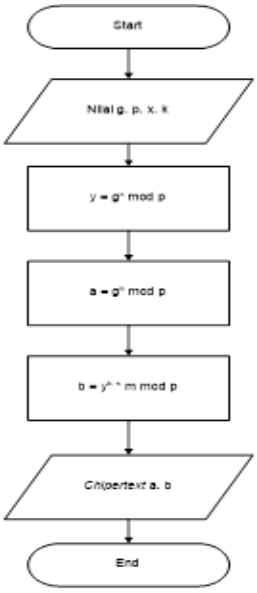
1) Inception
   Pada tahap ini lebih memodelkan proses bisnis yang di butuhkan (*business modelling*) dan mendifinisikan kebutuhan sistem yang akan dibuat (*requirements*). Dalam hal ini penulis melakukan pengumpulan data dengan cara melakukan observasi mengenai CV. Rimba 99 Meubel serta melakukan wawancara terkait informasi mengenai bagaimana proses pembuatan dan penjualan produk. Data tersebut kemudian di analisis sebagai pemenuhan kebutuhan untuk melakukan perancangan aplikasi yang dibuat.
2) Elaboration
   Tahap untuk melakukan desain secara lengkap berdasarkan hasil analisis ditahap *inception.* Aktivitas yang dilakukan pada tahap ini antara lain mencakup pembuatan desain arsitektur subsistem (*architecture pattern*), desain komponen sistem, desain format data (protokol komunikasi), desain antarmuka/tampilan, desain peta aliran tampilan, penentuan *design pattern* yang digunakan, pemodelan diagram UML (*Unified Modelling Language*) dan pembuatan dokumentasi.
3) Construction
   Tahap ini fokus pada pengembangan komponen dan fitur-fitur sistem, implementasi kode program dan pengujian perangkat lunak. Pada tahap ini penulis mulai melakukan penulisan kode program (*coding)* degan menggunakan bahasa pemrograman java untuk android (c*lient*), PHP untuk sisi web (server) dan MySQL untuk pembuatan *database.*
4) Transition
   Pada tahap ini dilakukan pengujian, penyerahan dan pelatihan penggunaan aplikasi kepada *user* serta pemeliharaan penggunaannya. Pengujian pada aplikasi ini dilakukan dengan menggunakan *blackbox testing* dan *whitebox testing* untuk memastikan sistem berjalan dengan baik. *Maintenance* atau pemeliharaan dilakukan untuk memastikan agar aplikasi tetap berjalan dengan semestinya.

2.2. Metode Penyelesaian Masalah

Metode pemecahan masalah yang digunakan dalam penelitian ini adalah dengan menggunakan algoritma *El Gamal.* Kriptografi *El Gamal* pertama kali dipublikasikan oleh Taher El Gamal pada tahun 1985. Kriptografi *El Gamal* pada mulanya digunakan untuk *digital signature*, namun kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan deskripsi. Kriptografi *El Gamal* digunakan kedalam perangkat lunak sekuriti yang dikembangkan oleh GNU, program PGP, dan pada sistem sekuriti lainnya. Kriptografi *El Gamal* tidak dipatenkan oleh pembuatnya melainkan didasarkan atau penyempurnaan dari pada kriptografi *Diffei-Hellman*, yaitu sebuah kriptografi kunci publik yang dikenalkan oleh Whitfield Diffie dan Martin Hellman. Sehingga hak paten kriptografi *Diffie-Hellman* mencakup kriptografi *El Gamal.* Dan hak paten ini telah berakhir pada tahun 1997 sehingga mulai saat itu kriptografi *El Gamal* dapat di komersilkan secara umum.

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

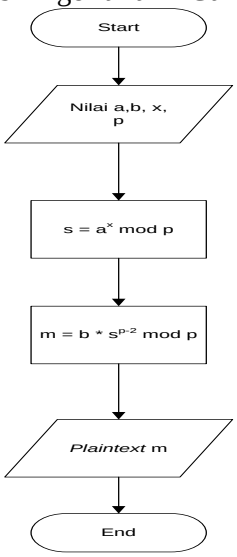
1) Enkripsi Algoritma El Gamal



Gambar 1. Flowchart Enkripsi Algoritma El Gamal

Flowchart pada gambar 1 menggambarkan proses enkripsi algoritma el gamal dengan menentukan nilai g, p, x dan k yang memiliki beberapa proses yaitu pertama membuat pembangkit kunci dengan mencari nilai y dan kemudian menentukan *chipertext* a dan b.

2) Deskripsi Algoritma El Gamal



Gambar 2. Flowchart Deskripsi Algoritma El Gamal

Flowchart pada gambar 2 menggambarkan proses deskripsi algoritma el gamal dengan menentukan nilai a, b, p dan x yang memiliki beberapa proses yaitu pertama mencari nilai s dan kemudian mencari nilai m yang hasilnya akan di rubah ke bentuk plaintext atau karakter asli.

3) Perhitungan Algoritma El Gamal

Proses ini dilakukan oleh penerima pesan (Receiver). *Receiver* membangkitkan kunci publik dan privatnya. Namun sebelum itu tentukan dulu *plaintext*, kunci publik dan kunci privat yang akan diterapkan:

Pesan (*plaintext*) : MKS20190001
Nilai (p,g,y,x): (257, 7, 86, 3)
Nilai k_1 = 2, k_2 = 2, k_3 = 2, k_4 = 3, k_5 = 3, k_6= 3, k_7 = 4, k_8 = 4, k_9 = 4, k_{10} = 5, k_{11} = 5.

Kemudian hitung $y = g^x \ mod \ p = 7^3 \ mod$ 257 = 86. Diperoleh kunci publik (y,g,p) = (86,7,257) dan kunci privatnya x = 3. Kunci publik (86,7,257) inilah yang diberikan penerima kepada pemberi pesan. Kunci rahasia tetap dipegang oleh penerima dan tidak boleh ada yang mengetahui selain dirinya sendiri.

Langkah selanjutnya penyelesaian proses enkripsi sebagai berikut :

Diketahui :
Plaintext : "MKS20190001".
Nilai p = 257, g = 7 dan y = 86.
Nilai k_1 = 2, k_2 = 2, k_3 = 2, k_4 = 3, k_5 = 3, k_6= 3, k_7 = 4, k_8 = 4, k_9 = 4, k_{10} = 5, k_{11} = 5.

Penyelesaian : Ubah pesan asli (*plaintext*) ke dalam ASCII
M=77, K=75, S=83, 2=50, 0=48, 1=49, 9=57, 0=48, 0=48, 0=48, 1=49.

Sehingga nilai pesan ASCII adalah sebagai berikut :
m_1=77, m_2=75, m_3=83, m_4=50, m_5=48, m_6=49, m_7=57, m_8=48, m_9=48, m_{10}=48, M_{11}=49.

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

Hitung enkripsi a dengan rumus $a = g^k \bmod p$

$a_1 = 7^2 \bmod 257 = 49$
$a_2 = 7^2 \bmod 257 = 49$
$a_3 = 7^2 \bmod 257 = 49$
$a_4 = 7^3 \bmod 257 = 86$
$a_5 = 7^3 \bmod 257 = 86$
$a_6 = 7^3 \bmod 257 = 86$
$a_7 = 7^4 \bmod 257 = 88$
$a_8 = 7^4 \bmod 257 = 88$
$a_9 = 7^4 \bmod 257 = 88$
$a_{10} = 7^5 \bmod 257 = 102$
$a_{11} = 7^5 \bmod 257 = 102$

Hitung enkripsi b dengan rumus $b = y^k.m \bmod p$

$b_1 = 86^2 .77 \bmod 257 = 237$
$b_2 = 86^2 .75 \bmod 257 = 94$
$b_3 = 86^2 .83 \bmod 257 = 152$
$b_4 = 86^3 .50 \bmod 257 = 78$
$b_5 = 86^3 .48 \bmod 257 = 116$
$b_6 = 86^3 .49 \bmod 257 = 97$
$b_7 = 86^4 .57 \bmod 257 = 153$
$b_8 = 86^4 .48 \bmod 257 = 210$
$b_9 = 86^4 .48 \bmod 257 = 210$
$b_{10} = 86^5 .48 \bmod 257 = 70$
$b_{11} = 86^5 .49 \bmod 257 = 125$

Setelah mendapatkan nilai enkripsi a dan b, hasil perhitungan tersebut disusun dengan pola sebagai berikut :
a1, b1, a2, b2,a3, b3, a4, b4, a5, b5, a6, b6, a7, b7, a8, b8, a9, b9, a10, b10, a11, b11.

Sehingga membentuk *ciphertext* :
49, 237, 49, 94, 49, 152, 86, 78, 86, 116, 86, 97, 88, 153, 88, 210, 88, 210, 102, 70, 102, 125.

Langkah terakhir penyelesaian proses deskripsi sebagai berikut :

Diketahui :
ciphertext : **49, 237, 49, 93, 49, 37, 86, 78, 86, 116, 86, 97, 88, 153, 88, 210, 88, 210, 102, 70, 102, 125.**
Nilai p = 257, x = 3.

Penyelesaian : pisahkan nilai a dan b pada pesan rahasia (*ciphertext*).
Hitung s dengan rumus : $s = a^x \bmod p$

$s_1 = 49^3 \bmod 257 = 200$
$s_2 = 49^3 \bmod 257 = 200$
$s_3 = 49^3 \bmod 257 = 200$
$s_4 = 86^3 \bmod 257 = 238$
$s_5 = 86^3 \bmod 257 = 238$
$s_6 = 86^3 \bmod 257 = 238$
$s_7 = 88^3 \bmod 257 = 165$
$s_8 = 88^3 \bmod 257 = 165$
$s_9 = 88^3 \bmod 257 = 165$
$s_{10} = 102^3 \bmod 257 = 55$
$s_{11} = 102^3 \bmod 257 = 55$

Hitung m (pesan asli) dengan rumus : $m = b. S^{(p-2)} \bmod p$

$m_1 = 237 . 200^{(257-2)} \bmod 257 = 77$
$m_2 = 94 . 200^{(257-2)} \bmod 257 = 75$
$m_3 = 152 . 200^{(257-2)} \bmod 257 = 83$
$m_4 = 78 . 238^{(257-2)} \bmod 257 = 50$
$m_5 = 116 . 238^{(257-2)} \bmod 257 = 48$
$m_6 = 97 . 238^{(257-2)} \bmod 257 = 49$
$m_7 = 153 . 165^{(257-2)} \bmod 257 = 57$
$m_8 = 210 . 165^{(257-2)} \bmod 257 = 48$
$m_9 = 210 . 165^{(257-2)} \bmod 257 = 48$
$m_{10} = 70 . 55^{(257-2)} \bmod 257 = 48$
$m_{11} = 125 . 55^{(257-2)} \bmod 257 = 49$

Setelah mendapatkan nilai m_n, masing-masing nilai m hasil dari dekripsi diubah kembali menjadi bilangan ASCII (plainteks). Dengan hasil sebagai berikut :
M = m_1 = 77, K = m_2 = 75, S = m_3 =83, 2 = m_4 = 50, 0 = m_5 = 48, 1 = m_6 = 49, 9 = m_7 = 57, 0 = m_8 = 48, 0 = m_9 = 48, 0 = m_{10} = 48, 1 = m_{11} = 49.

Setelah proses deskripsi berhasil yaitu MKS20190001 maka sistem akan menampilkan data mebel sesuai kode produk yaitu nama produk, kategori produk, kualitas kayu jati, tanggal produksi dan foto produk.

3. HASIL DAN PEMBAHASAN

3.1. Analisis Sistem

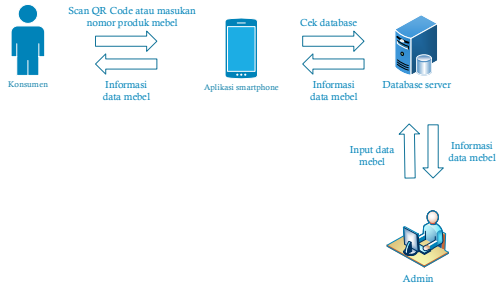
1). Analisis Sistem Yang Sedang Berjalan
Analisis sistem yang sedang berjalan sekarang untuk proses pengecekan produk mebel buatan CV. Rimba 99 Meubel yang masih dilakukan dengan cara manual. Dapat di lihat pada gambar 3.

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

Gambar 3. *Rich Picture Diagram* Sistem yang sedang berjalan

2). Analisis Sistem Yang Diusulkan

Sistem yang diusulkan akan mempermudah konsumen dalam pengecekan produk mebel buatan CV. Rimba 99 Meubel. Konsumen cukup melakukan *scan QR Code* yang ada pada produk mebel menggunakan *smartphone android*, lalu data informasi mebel akan muncul secara cepat, mudah dan aman.

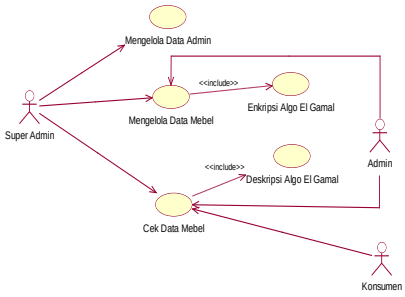


Gambar 4. *Rich Picture Diagram* Sistem yang diusulkan

3.2. Perancangan Sistem

Metode perancangan atau pemodelan perangkat lunak yang digunakan dalam penelitian ini yaitu metode perancangan *Unified Modeling Process* (UML).

A. Use Case Diagram



Gambar 5. *Use Case Diagram Sistem*

Gambar 5 menjelaskan *use case diagram* pada aplikasi pengaman produk mebel dari CV. Rimba 99 Meubel

B. Implementasi Desain Antar Muka

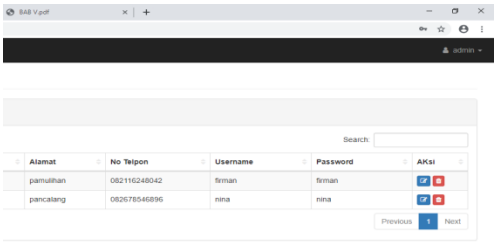
1). Interface WEB Server

a. Halaman Beranda

Gambar 6. Halaman Beranda

Gambar 6 adalah tampilan admin pada halaman beranda.

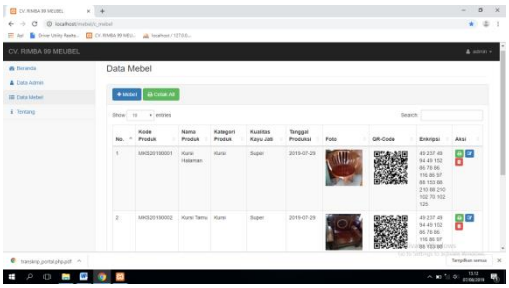
b. Halaman Data Admin



Gambar 7. Halaman Data Admin

Gambar 7 adalah tampilan admin pada halaman data admin.

c. Halaman Data Mebel



Gambar 8. Halaman Data Mebel

Gambar 8 adalah tampilan admin pada halaman data mebel.

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

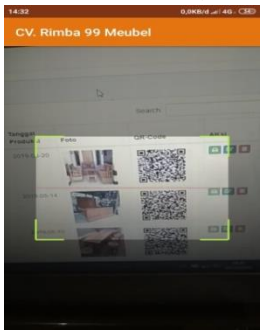
2). Interface Aplikasi Mobile

a. Halaman Beranda Mobile

Gambar 9. Halaman Beranda *Mobile*

Gambar 9 adalah tampilan *user* pada halaman beranda di aplikasi *mobile scanner*.

b. Halaman Menu Scan QR Code



Gambar 10. Halaman Menu *Scan QR Code*

Gambar 10 adalah tampilan *user* pada halaman menu *scan QR Code* di aplikasi *mobile*.

c. Halaman Hasil Scan

Gambar 11. Halaman Hasil *Scan*

Gambar 11 adalah tampilan *user* pada halaman hasil *scan* di aplikasi *mobile*.

4. KESIMPULAN

Berdasarkan rumusan masalah, penulis memperoleh kesimpulan yang dapat diambil dari penelitian ini sebagai berikut.

1. Aplikasi pengaman produk mebel pada CV. Rimba 99 Meubel dibuat dengan bahasa pemrograman java yaitu dengan *software* android studio untuk sisi *client* dan bahasa pemrograman PHP untuk sisi *server*.
2. Aplikasi pengaman produk mebel dibuat berbasis *mobile* untuk pengecekan produk mebel dengan *QR Code* yang digunakan oleh konsumen dengan mudah, praktis dan aman sedangkan untuk pengelolaan mebel dari CV. Rimba 99 Meubel dibuat berbasis web dengan mudah dan aman dalam kelola produk mebel.
3. Algoritma *El Gamal* pada aplikasi ini berfungsi sebagai salah satu solusi keamanan data produk mebel yang mengenskripsi kode produk pada *database*. Sehingga menjamin keaslian data produk. Implementasi algoritma *El Gamal* yang dienkripsi di simpan pada *QR Code* menjamin kamanan dalam pengecekan produk mebel.

5. SARAN

Berdasarkan hasil penelitian yang diperoleh, maka ada beberapa saran yang peneliti ajukan sebagai berikut.

1. Penelitian ini dapat dikembangkan bukan hanya dapat menampilkan gambar produk saat scan produk namun juga tampil dengan desain 3D atau lebih nyata agar konsumen lebih percaya dengan kualitas dan pelayanan dari CV. Rimba 99 Meubel.
2. Penambahan fitur pada saat upload gambar mebel jika sudah ada gambar yang sama maka akan ada pemberitahuan “gambar sudah ada!”.
3. Penambahan fitur yang mampu menerima krtitik dan masukan konsumen.

DAFTAR PUSTAKA

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

[1]. A.S Rosa dan Salahuddin M, 2015. Modul Pembelajaran Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek), Modula, Bandung.
[2]. Aribowo, Eko. (2008). Aplikasi Pengaman Dokumen Office Dengan Algoritma Kriptografi Kunci Asimetris El Gamal, Jurnal Informatika.Volume 2 No 2.
[3]. Fazlur Rochman, Fatich, 2016. Implementasi QR Code Dan Digital Signature Untuk Menentukan Keabsahan Dokumen KRS dan KHS (Studi Kasus Fakultas Sains Dan Teknologi Universitas Airlangga).
[4]. Munir, Rinaldi. 2006. Kriptografi Algoritma RSA & ElGamal. Dapartemen Teknik Informatika, ITB : Bandung.
[5]. Mauluddin, Amras, M Aditya. 2018. Pengembangan Perangkat Lunak Pemilihan Ketua Umum Berbasis Web Pada Organisasi IPMKN.
[6]. Rahmawati, Anita dan Rahman, Arif. (2011), Sistem Pengamanan Keaslian Ijasah Menggunakan QR-Code dan Algoritma Base64. Volume 1 No 2 ISSN 2087-8737.
[7]. Rahmawati, A. D. 2012. Analisis Persebaran Toko Mebel Kayu Di Kabupaten Jepara Provinsi Jawa Tengah. Semarang : Universitas Diponegoro.
[8]. Widyartono, Agustinus. (2011). Algoritma ElGamal Untuk Enkripsi Data Menggunakan GnuPG. Volume 1 No 1.