

Penerapan Algoritma MD5 dan Caesar Cipher Untuk Mengamankan Database Pada Aplikasi Pengaduan Masyarakat Pada Kantor Kepala Desa Bulu Cina

Implementation of MD5 Algorithm and Caesar Cipher to Secure Database in Public Complaints Application at Bulu Cina Village Head Office

Muhammad Hqmal^{a,1}, Linda Wahyuni^{b,2}

^aInformatika, Universitas Potensi Utama, Medan 20241, Sumatera Utara, Indonesia

^bSistem Informasi, Universitas Potensi Utama, Medan 20241, Sumatera Utara, Indonesia

Email: muhammadhiqmal31@gmail.com¹, lindawahyuni391@gmail.com²

ABSTRAK

Perkembangan teknologi komputer telah membawa dampak signifikan dalam meningkatkan efisiensi pelayanan publik, termasuk dalam sistem pengaduan masyarakat. Namun, keamanan data pengguna dan isi pengaduan menjadi tantangan utama yang perlu diperhatikan. Penelitian ini bertujuan untuk mengembangkan aplikasi pengaduan masyarakat berbasis mobile dengan menerapkan algoritma kriptografi guna meningkatkan keamanan data. Algoritma MD5 digunakan untuk mengenkripsi password pengguna, sedangkan Caesar Cipher diterapkan untuk mengamankan teks isi pengaduan. Penggunaan kedua algoritma ini diharapkan dapat melindungi data dari risiko kebocoran atau penyalahgunaan oleh pihak yang tidak berwenang. Aplikasi ini dikembangkan menggunakan bahasa pemrograman PHP dan Kotlin, dengan basis data MySQL, serta dilengkapi fitur input pengaduan dan sistem login. Hasil penelitian menunjukkan bahwa penerapan enkripsi pada database dapat meningkatkan keamanan informasi sekaligus memudahkan masyarakat dalam menyampaikan pengaduan secara digital. Dengan demikian, aplikasi ini tidak hanya meningkatkan efisiensi pelayanan di Kantor Kepala Desa Bulu Cina tetapi juga menjamin kerahasiaan data pengguna.

Kata Kunci : MD5, Caesar Cipher, Keamanan Data, Aplikasi Pengaduan Masyarakat, Enkripsi Database.

ABSTRACT

The development of computer technology has significantly improved the efficiency of public services, including public complaints systems. However, the security of user data and complaint content remains a major challenge. This study aims to develop a mobile-based public complaints application by implementing cryptographic algorithms to enhance data security. The MD5 algorithm is used to encrypt user passwords, while Caesar Cipher is applied to secure the complaint text. The use of these two algorithms is expected to protect data from the risk of leakage or misuse by unauthorized parties. This application was developed using the PHP and Kotlin programming languages, with a MySQL database, and is equipped with complaint input and login features. The results of the study indicate that the application of encryption to the database can improve information security while making it easier for the public to submit complaints digitally. Thus, this application not only improves service efficiency at the Bulu Cina Village Head's Office but also ensures the confidentiality of user data.

Keywords : MD5, Caesar Cipher, Data Security, Public Complaint Application, Database Encryption.

Disubmit:

Info Artikel :
Direview:

Diterima :

Copyright © 2025 - senadimu. All rights reserved.

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini tidak lepas dari pesatnya perkembangan teknologi komputer, karena komputer merupakan media yang dapat memberikan kemudahan bagi manusia dalam menyelesaikan suatu pekerjaan [1]. Keberadaan teknologi tidak bisa dipungkiri sangat mempengaruhi kehidupan manusia. Pemanfaatannya dalam berbagai hal dari mulai yang sederhana sampai mencakup lingkup yang besar jelas sangat membantu, meringankan, memudahkan, praktis, dan lainnya dalam konteks yang positif [2]. Teknologi saat ini berkembang pesat seiring berjalannya waktu, banyak penyampaian informasi yang menggunakan teknologi sehingga informasi yang disampaikan lebih tepat sasaran [3]. Sistem informasi merupakan suatu sistem didalam suatu organisasi yang mendukung operasi, bersifat manajerial menyediakan pihak luar tertentu dengan laporan-laporan yang dibutuhkan [4]. Sistem dapat didefinisikan sebagai sekumpulan objek-objek yang saling berelasi dan berinteraksi, serta hubungan antar objek bisa dilihat sebagai satu kesatuan yang dirancang untuk mencapai satu tujuan yang telah ditetapkan [5].

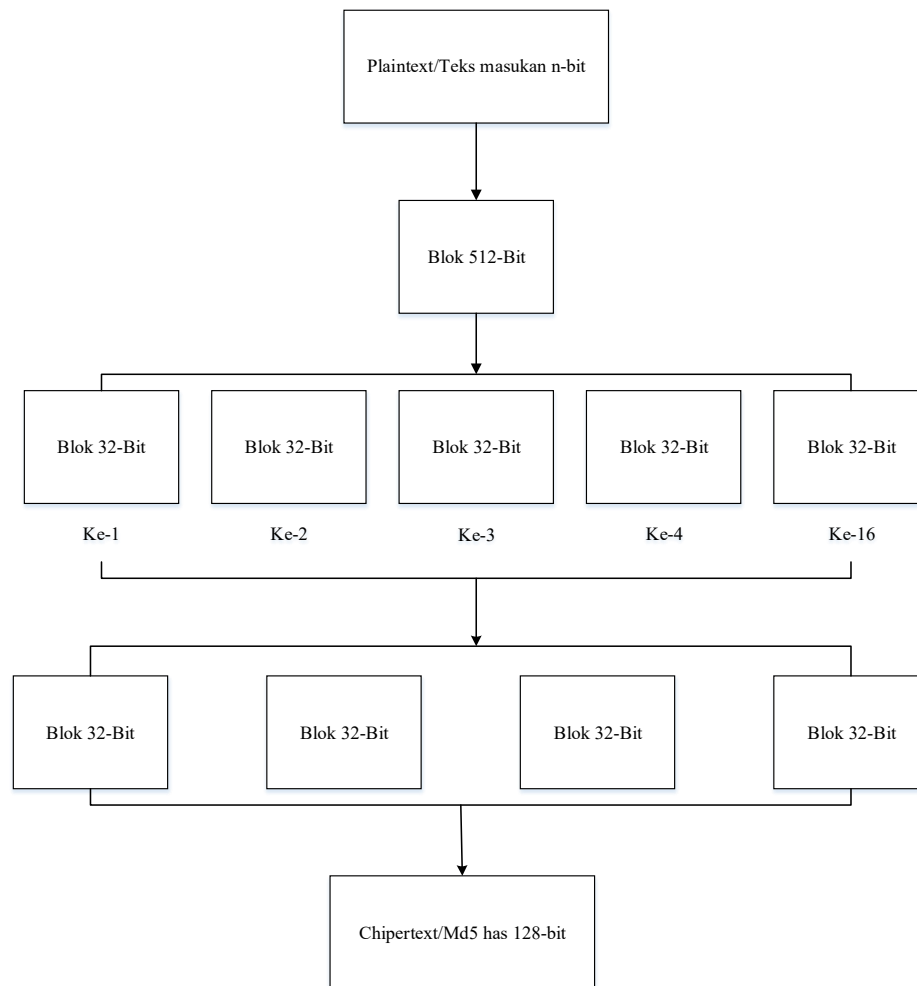
Dalam penelitian ini, pengamanan data pengguna dan data isi pengaduan menjadi perhatian utama dalam pengembangan sistem pengaduan masyarakat. Pengamanan dilakukan pada dua aspek penting, yaitu autentikasi pengguna (login) dan isi laporan pengaduan. Untuk melindungi informasi akun pengguna, khususnya password, digunakan algoritma MD5 (Message Digest 5). MD5 (Message Digest 5) merupakan salah satu algoritma kriptografi hash yang berfungsi untuk menghasilkan nilai hash atau message digest berukuran tetap [6]. Metode ini digunakan untuk memverifikasi integritas data, karena setiap perubahan sekecil apa pun pada data asli akan menghasilkan nilai hash yang sangat berbeda [7]. Meskipun tergolong cepat dan efisien, metode MD5 saat ini dianggap kurang aman untuk aplikasi kriptografi modern karena telah ditemukan beberapa kelemahan berupa kemungkinan terjadinya *collision* (dua input berbeda menghasilkan hash yang sama) [8].

Selain itu, isi pengaduan masyarakat yang dikirimkan melalui sistem juga dapat mengandung informasi sensitif yang perlu dijaga kerahasiaannya. Oleh karena itu, diterapkan pula algoritma Caesar Cipher. Caesar Cipher merupakan salah satu algoritma kriptografi klasik yang termasuk dalam jenis substitution cipher, di mana setiap huruf pada teks asli (plaintext) digantikan oleh huruf lain yang memiliki jarak atau pergeseran tertentu dalam alfabet [9]. Metode ini bekerja dengan prinsip sederhana yaitu melakukan pergeseran karakter berdasarkan jumlah kunci tertentu [10]. Meskipun tergolong sederhana dan mudah diterapkan, Caesar Cipher memiliki tingkat keamanan yang rendah karena ruang kunci yang terbatas dan dapat dengan mudah dipecahkan melalui analisis frekuensi huruf atau brute force attack [11].

Penelitian “Pengembangan Aplikasi Keamanan Data Agen Kapal Dengan Menggunakan Metode MD5 Berbasis Web”. keamanan data tidak diterapkan maka informasi dalam data tersebut dapat bocor. Ini mengkhawatirkan nama pemilik data agen kapal. Ia takut identitasnya diambil alih oleh orang lain [12]. Penelitian “Algoritma Sequential Search Dan MD5 Pada Aplikasi Inventory Barang Berbasis Web”. Hasil penelitian ini adalah dengan adanya aplikasi sistem inventory ini lebih memudahkan dalam proses penyimpanan, mengurangi resiko dalam proses pencarian produk dan keamanan data lebih terjamin [13]. Penelitian “Implementasi Algoritma Vigenere Cipher dan Caesar Cipher Untuk Pengamanan Password Dalam Penerimaan Siswa Baru”. Algoritma kriptografi vigenere cipher, caesar cipher dan dikombinasikan dengan regular expression sebagai keamanan dimana password yang di input oleh user akan di enkripsi untuk melindungi data password serta membantu calon siswa dalam membuat password yang kuat [14]. Penelitian “Implementasi Kriptografi Hybrid Menggunakan Caesar Cipher dan Affine Cipher Untuk Keamanan Teks”. Melalui analisis mendalam terhadap kombinasi kedua teknik ini, diharapkan dapat ditemukan solusi yang lebih baik dalam menghadapi tantangan keamanan informasi di era digital yang terus berkembang [15].

2. METODE

MD5 termasuk dalam kategori algoritma *hash function*, yang berarti hasil enkripsi MD5 tidak bisa dikembalikan ke bentuk semula. Informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. MD5 sering digunakan sebagai *digital signature* dari sebuah *file*, atau sebagai bentuk pengamanan dari *password* yang tersimpan dalam *database*. MD5 mengolah teks masukan n bit yang dipadatkan ke bentuk blok 512 bit. Lalu blok ini dibagi dalam 16 bentuk sub-blok yang masing-masing berukuran 32 bit dan diproses menggunakan operasi-operasi pada algoritma MD5. Keluaran terdiri dari 4 blok berukuran 32 bit, yang digabungkan menjadi panjang 128 bit. Gambaran proses ini bisa dilihat pada gambar berikut :



Gambar 1 Diagram MD5
(Sumber : Zebua dkk., 2022)

Keterangan tahapan dapat dijelaskan sebagai berikut :

1. *Plaintext/Teks Masukan (n-bit)*
Ini adalah data awal atau teks yang ingin diubah menjadi hash MD5. Ukuran data bisa bervariasi.
2. Blok 512-bit
MD5 bekerja dengan membagi *input* menjadi blok-blok berukuran 512-bit. Jika panjang pesan tidak kelipatan 512-bit, maka dilakukan padding untuk menyesuaikan panjangnya.
3. Pembagian Blok 512-bit Menjadi 16 Sub-Blok 32-bit
Setiap blok 512-bit dibagi menjadi 16 bagian dengan masing-masing bagian berukuran 32-bit. Blok-blok ini diberi label Ke-1 hingga Ke-16.

4. Proses Transformasi (4 Ronde)
Setiap blok 32-bit akan diproses melalui empat *ronde* operasi *non-linear* menggunakan fungsi logika (F, G, H, I) yang berbeda di setiap *ronde*. Setiap *ronde* terdiri dari 16 operasi transformasi berdasarkan konstanta yang telah ditentukan.
5. Proses Kombinasi Blok 32-bit
Setelah melalui proses transformasi, nilai-nilai 32-bit tersebut dikombinasikan kembali untuk membentuk hasil akhir.
6. *Ciphertext*/MD5 Hash 128-bit
Setelah semua proses selesai, keluaran akhirnya adalah hash MD5 berukuran 128-bit. Biasanya hash ini ditampilkan dalam format *hexadecimal* 32 karakter.

3. HASIL DAN PEMBAHASAN

Analisis masalah dalam penelitian ini dimulai dari kenyataan bahwa Kantor Kepala Desa Bulu Cina belum memiliki sistem pengaduan masyarakat berbasis digital yang dapat diakses secara daring. Selama ini, proses pengaduan masih dilakukan secara konvensional, di mana masyarakat harus datang langsung ke kantor desa untuk menyampaikan keluhan, saran, atau laporan. Kondisi tersebut tidak hanya menyulitkan masyarakat dari sisi waktu dan tenaga, tetapi juga memperlambat respon dan tindak lanjut dari pihak desa dalam menangani pengaduan yang masuk.

Selain dari segi aksesibilitas, aspek keamanan data pengguna dan informasi pengaduan juga menjadi permasalahan penting. Belum diterapkannya sistem autentikasi yang aman membuat data kredensial pengguna, seperti *password login*, berisiko disimpan dalam bentuk teks asli (*plain text*), yang dapat dengan mudah disalahgunakan apabila terjadi kebocoran data. Di sisi lain, isi dari pengaduan masyarakat yang bersifat sensitif juga perlu mendapatkan perlindungan agar tidak mudah diakses atau dimanipulasi oleh pihak yang tidak berwenang.

Sebagai solusi atas permasalahan tersebut, penelitian ini mengusulkan pengembangan aplikasi pengaduan masyarakat berbasis mobile dan web, dengan menerapkan dua mekanisme pengamanan utama, yaitu:

1. Algoritma MD5 pada proses *login* untuk mengenkripsi *password* pengguna menjadi kode *hash* satu arah yang tidak dapat dikembalikan ke bentuk aslinya, guna meningkatkan keamanan autentikasi.
2. Algoritma *Caesar Cipher* untuk melakukan enkripsi terhadap isi teks pengaduan yang dikirimkan oleh pengguna, agar informasi yang bersifat privat atau sensitif tidak tersimpan dalam bentuk asli di dalam *database*.

Pengembangan sistem ini dilakukan menggunakan bahasa pemrograman

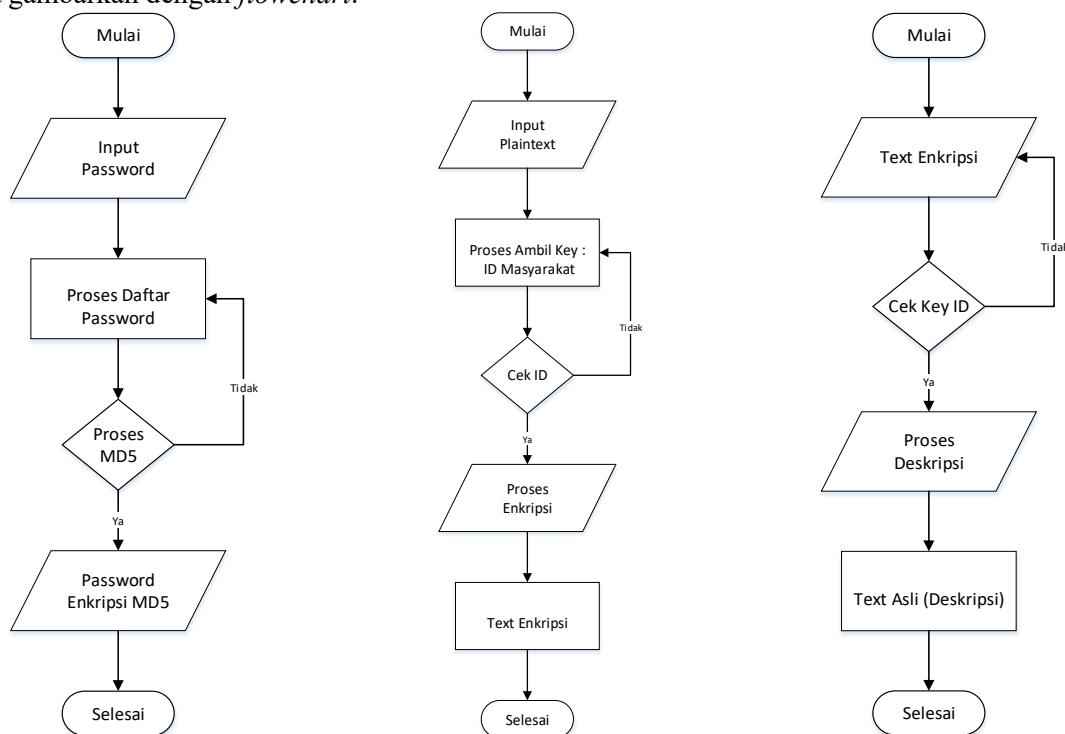
Kotlin untuk aplikasi mobile, serta PHP dan MySQL untuk pengelolaan data dan proses server-side. Dengan pendekatan ini, diharapkan sistem dapat diakses dengan fleksibel oleh masyarakat melalui perangkat mobile, sekaligus menjamin keamanan data melalui metode enkripsi ganda.

Dengan demikian, penelitian ini tidak hanya berfokus pada pengembangan sistem pengaduan digital yang mempercepat dan mempermudah proses penyampaian laporan, tetapi juga memberikan perhatian serius terhadap keamanan data pengguna dan isi pengaduan, guna mendukung pelayanan publik yang lebih modern, efisien, dan terpercaya di lingkungan Kantor Kepala Desa Bulu Cina.

3.1 Flowchart Metode

Flowchart metode merupakan diagram alir yang menggambarkan urutan atau langkah-langkah proses kerja secara sistematis dalam suatu metode penelitian atau perancangan sistem. *Flowchart* berfungsi sebagai alat bantu visual yang menunjukkan hubungan logis antara setiap tahap kegiatan, mulai dari proses awal hingga hasil akhir yang diinginkan. Dalam konteks penelitian dan pengembangan sistem, *flowchart* metode digunakan untuk memvisualisasikan alur tahapan penelitian atau proses pengembangan perangkat lunak agar lebih mudah dipahami oleh peneliti maupun pembaca. Setiap simbol pada *flowchart* memiliki arti tertentu, seperti proses, keputusan, *input*, *output*, serta arah aliran

data yang menggambarkan jalannya proses secara terstruktur. Artinya setiap bentuk prosedural bisa Anda gambarkan dengan *flowchart*.



Gambar 2 *Flowchart* Metode

3.2 Penerapan Metode MD5

1. Representasi Input

Setiap karakter dikonversikan ke nilai Binary yang direpresentasikan sebagai berikut:

Tabel 1 Representasi Input

Karakter	ASCII Decimal	Hex	Biner 8-bit
T	84	0x54	1010100
e	101	0x65	1100101
k	107	0x6B	1101011
n	110	0x6E	1101110
i	105	0x69	1101001
k	107	0x6B	1101011

Total Bit: $6 \times 8 = 48$ bit

Tabel 2 Padding hingga 448-bit (mod 512)

Deskripsi	Nilai Biner
Teks "Teknik"	01010100 01100101 01101011 01101110 01101001 01101011
Bit '1' Padding	10000000
Padding '0'	343 bit (sampai total 448 bit)

MD5 menggunakan 4 buffer 32-bit dengan nilai awal, adapun nilai awal yang digunakan dijelaskan pada table berikut.

Tabel 3 Buffer Inisialisasi

Register	Nilai Hex	Nilai Desimal (Signed)
A	0x67452301	1732584193
B	0xefcdab89	-271733879
C	0x98badcfe	-1732584194

D	0x10325476	271733878
---	------------	-----------

Karena 4 putaran MD5 masing-masing 16 operasi kompleks (melibatkan rotasi bit, fungsi *non-linear*, dan konstanta $T[i]$), maka hanya disarankan merepresentasikan nilai hasil akhir tiap putaran, Setiap putaran melakukan 16 operasi dengan fungsi yang berbeda:

- a. Putaran 1: Fungsi $F(X,Y,Z) = (X \text{ AND } Y) \text{ OR } (\text{NOT } X \text{ AND } Z)$

Nilai awal:

A = 0x860E6DA5

B = 0xAEB817D2

C = 0x2A7DA70A

D = 0x0DB3C535

- b. Putaran 2: Fungsi $G(X,Y,Z) = (X \text{ AND } Z) \text{ OR } (Y \text{ AND } \text{NOT } Z)$

Nilai:

A = 0xE95256C1

B = 0x918403C2

C = 0xD9BC5668

D = 0x01AFDD94

- c. Putaran 3: Fungsi $H(X,Y,Z) = X \text{ XOR } Y \text{ XOR } Z$

Nilai:

A = 0xF646A063

B = 0xB6BCB3C1

C = 0x6C321F46

D = 0x045BCC16

- d. Putaran 4: Fungsi $I(X,Y,Z) = Y \text{ XOR } (X \text{ OR } \text{NOT } Z)$

Nilai akhir putaran:

AA = 0x4F58DF57

BB = 0x9B463249

CC = 0xB333C93F

DD = 0x7BEB62B5

Tabel 4 Operasi Putaran

Putaran	Fungsi	A	B	C	D
1	$F(X,Y,Z)$	0x860E6DA5	0xAEB817D2	0x2A7DA70A	0x0DB3C535
2	$G(X,Y,Z)$	0xE95256C1	0x918403C2	0xD9BC5668	0x01AFDD94
3	$H(X,Y,Z)$	0xF646A063	0xB6BCB3C1	0x6C321F46	0x045BCC16
4	$I(X,Y,Z)$	0x4F58DF57	0x9B463249	0xB333C93F	0x7BEB62B5

Hasil dari 4 putaran ditambahkan ke buffer awal:

A = A + AA = 0x67452301 + 0x4F58DF57 = 0xB69E0258

B = B + BB = 0xefcdab89 + 0x9B463249 = 0x8B13DDD2

C = C + CC = 0x98badcfe + 0xB333C93F = 0x4BEEA6D3

D = D + DD = 0x10325476 + 0x7BEB62B5 = 0x8C1DB72B

Tabel 5 Penambahan Buffer Akhir

Register	Nilai Awal	Hasil Putaran	Penjumlahan Akhir
A	0x67452301	0x4F58DF57	0xB69E0258
B	0xefcdab89	0x9B463249	0x8B13DDD2
C	0x98badcfe	0xB333C93F	0x4BEEA6D3
D	0x10325476	0x7BEB62B5	0x8C1DB72B

Nilai akhir diambil sebagai *concatenation* dari A, B, C, D dalam *little-endian*: A = B69E0258 → 58 02 9E B6

B = 8B13DDD2 → D2 DD 13 8B

C = 4BEEA6D3 → D3 A6 EE 4B

D = 8C1DB72B → 2B B7 1D 8C

Tabel 6 Hasil Akhir

Register	Nilai Akhir	Little-Endian
A	B69E0258	58 02 9E B6
B	8B13DDD2	D2 DD 13 8B
C	4BEEA6D3	D3 A6 EE 4B
D	8C1DB72B	2B B7 1D 8C

Digabungkan menjadi: 58029EB6D2DD138B3DA6EE4B2BB71D8C Hasil hash MD5 untuk "Teknik": 58029eb6d2dd138b3da6ee4b2bb71d8c.

3.3 Penerapan Metode Caesar Chiper

Key : 3

Plain Text : D E S A B U L U C I N A

1. Proses Enkripsi

Adapun proses enkripsi *caesar chiper* dapat dijelaskan pada tabel berikut ini:

Tabel III7 Enkripsi

No	Asli	ASCII	Posisi	Perhitungan	Posisi	Hasil
1	D	68	3	$(3 + 3) \% 26 = 6$	6	G
2	E	69	4	$(4 + 3) \% 26 = 7$	7	H
3	S	83	18	$(18 + 3) \% 26 = 21$	21	V
4	A	65	0	$(0 + 3) \% 26 = 3$	3	D
5	(spasi)		-	Tidak dihitung	-	(spasi)
6	B	66	1	$(1 + 3) \% 26 = 4$	4	E
7	U	85	20	$(20 + 3) \% 26 = 23$	23	X
8	L	76	11	$(11 + 3) \% 26 = 14$	14	O
9	U	85	20	$(20 + 3) \% 26 = 23$	23	X
10	(spasi)		-	Tidak dihitung	-	(spasi)
11	C	67	2	$(2 + 3) \% 26 = 5$	5	F
12	I	73	8	$(8 + 3) \% 26 = 11$	11	L
13	N	78	13	$(13 + 3) \% 26 = 16$	16	Q
14	A	65	0	$(0 + 3) \% 26 = 3$	3	D

Chiper Text : G H V D E X O X F L Q D

2. Proses Deskripsi

Adapun proses deskripsi *caesar chiper* dapat dijelaskan pada tabel berikut ini:

Tabel 8 Deskripsi

No	Enkripsi	ASCII	Posisi	Perhitungan	Posisi	Asli
1	G	71	6	$(6 - 3 + 26) \% 26 = 3$	3	D
2	H	72	7	$(7 - 3 + 26) \% 26 = 4$	4	E
3	V	86	21	$(21 - 3 + 26) \% 26 = 18$	18	S
4	D	68	3	$(3 - 3 + 26) \% 26 = 0$	0	A
5	(spasi)		-	Tidak dihitung	-	(spasi)
6	E	69	4	$(4 - 3 + 26) \% 26 = 1$	1	B
7	X	88	23	$(23 - 3 + 26) \% 26 = 20$	20	U
8	O	79	14	$(14 - 3 + 26) \% 26 = 11$	11	L
9	X	88	23	$(23 - 3 + 26) \% 26 = 20$	20	U
10	(spasi)		-	Tidak dihitung	-	(spasi)
11	F	70	5	$(5 - 3 + 26) \% 26 = 2$	2	C
12	L	76	11	$(11 - 3 + 26) \% 26 = 8$	8	I
13	Q	81	16	$(16 - 3 + 26) \% 26 = 13$	13	N
14	D	68	3	$(3 - 3 + 26) \% 26 = 0$	0	A

Plain Text : D E S A B U L U C I N A

3.4 Tampilan Hasil

Berikut ini dijelaskan tentang tampilan hasil dari perancangan sistem yang dibangun dapat dilihat sebagai berikut :

1. Tampilan Menu Utama

Tampilan menu utama pada sistem terlihat pada gambar berikut :

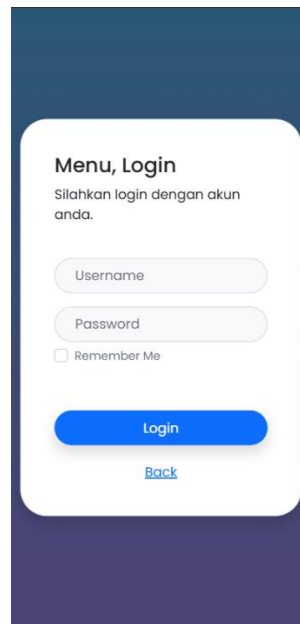


Gambar 3 Tampilan Menu Utama

Tampilan Menu Utama adalah halaman pertama yang muncul saat aplikasi dijalankan. Halaman ini dapat diakses oleh tiga jenis pengguna, yaitu Admin, Masyarakat, dan Kepala Desa (Kades). Pada tampilan ini, terdapat dua tombol utama, yaitu Login dan Register. Tombol *Login* digunakan oleh semua pengguna (Admin, Masyarakat, dan Kades) untuk masuk ke sistem sesuai dengan hak akses masing-masing. Sementara itu, tombol *Register* hanya tersedia untuk Masyarakat saja, karena admin dan kades didaftarkan secara internal oleh sistem. Tampilan ini dirancang sederhana dan intuitif agar mudah digunakan oleh semua pihak.

2. Tampilan Menu *Login*

Tampilan menu *login* pada sistem terlihat pada gambar berikut :

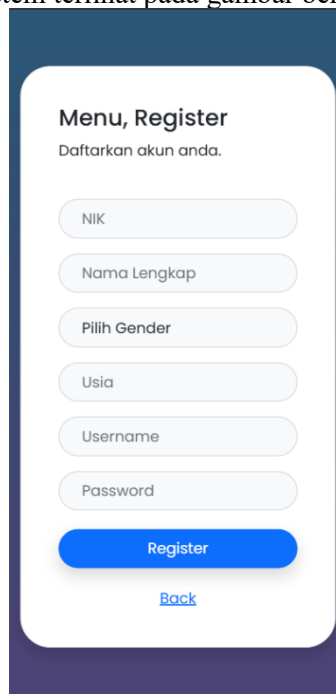
The image shows a mobile application interface for a login screen. It features a dark blue header and a white rounded rectangle in the center. Inside the rectangle, the title "Menu, Login" is at the top, followed by the instruction "Silahkan login dengan akun anda." Below this are two input fields labeled "Username" and "Password". There is a checkbox labeled "Remember Me" and a blue "Login" button. At the bottom of the white rectangle is a blue link labeled "Back".

Gambar 4 Tampilan Menu *Login*

Tampilan Menu *Login* dapat diakses oleh Admin, Masyarakat, dan Kades untuk masuk ke dalam sistem. Pada halaman ini, pengguna diminta mengisi *username* dan *password* sebelum menekan tombol *Login*. Untuk keamanan, *password* yang dimasukkan oleh pengguna dienkripsi menggunakan algoritma MD5 sebelum dikirim ke *server*, sehingga data sensitif tetap terlindungi dari potensi kebocoran. Tampilan ini dirancang sederhana namun fungsional, memastikan proses autentikasi berjalan lancar bagi semua jenis pengguna.

3. Tampilan Menu *Register*

Tampilan menu *register* pada sistem terlihat pada gambar berikut :

The image shows a mobile application interface for a register screen. It features a dark blue header and a white rounded rectangle in the center. Inside the rectangle, the title "Menu, Register" is at the top, followed by the instruction "Daftarkan akun anda." Below this are several input fields: "NIK", "Nama Lengkap", "Pilih Gender", "Usia", "Username", and "Password". There is a blue "Register" button and a blue link labeled "Back" at the bottom of the white rectangle.

Gambar 5 Tampilan Menu *Register*

Tampilan Menu *Register* hanya dapat diakses oleh masyarakat yang ingin membuat akun baru. Pada halaman ini, pengguna diminta mengisi beberapa data, seperti NIK (Nomor Induk Kependudukan), nama lengkap, usia, jenis kelamin, *username* dan *password*. Ketika tombol *Register* ditekan, *password* akan otomatis dienkripsi menggunakan MD5 sebelum disimpan ke *database*, sehingga keamanan data pengguna tetap terjaga. Tampilan ini dirancang sederhana dan mudah digunakan, memastikan proses pendaftaran berjalan lancar bagi masyarakat.

4. Tampilan Menu Dashboard

Tampilan menu dashboard pada sistem terlihat pada gambar berikut :

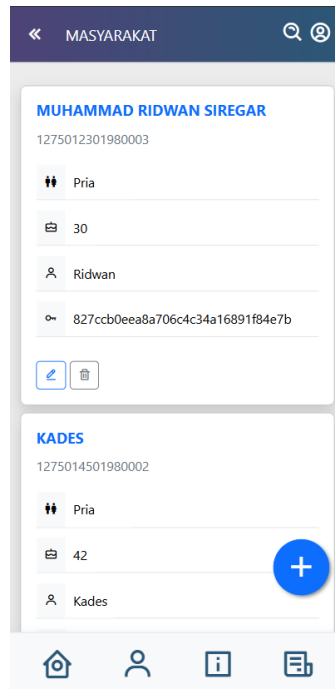


Gambar 6 Tampilan Menu Dashboard

Tampilan Menu *Dashboard* menyesuaikan fitur berdasarkan jenis pengguna yang *login*. Admin memiliki akses penuh, termasuk mengelola akun, data masyarakat, data pengaduan, dan laporan pengaduan. Pimpinan (Kades) hanya dapat mengakses akun dan laporan pengaduan untuk memantau progress tanpa mengedit data. Sementara masyarakat bisa mengelola akun pribadi, mengajukan proses pengaduan, serta melihat riwayat pengaduan yang pernah mereka laporkan. Tampilan ini dirancang intuitif dengan menu yang berbeda sesuai peran, memastikan setiap pengguna hanya mengakses fitur yang relevan.

5. Tampilan Data Masyarakat

Tampilan data masyarakat pada sistem terlihat pada gambar berikut :

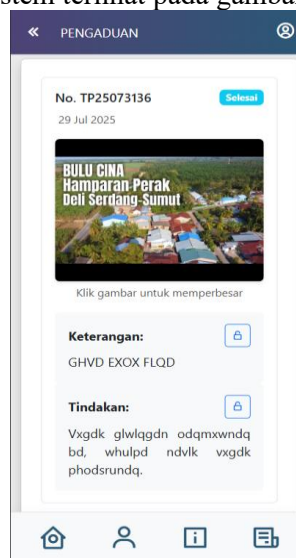


Gambar 7 Tampilan Data Masyarakat

Tampilan Data Masyarakat merupakan fitur eksklusif yang hanya dapat diakses oleh Admin. Pada menu ini, admin memiliki kemampuan penuh untuk mengelola data masyarakat, termasuk menambahkan data baru (tambah data), memperbarui informasi (ubah), atau menghapus data (hapus). Data yang ditampilkan mencakup NIK, nama lengkap, usia, jenis kelamin, *username*, dan *password* (yang secara otomatis terenkripsi dengan MD5 saat disimpan). Tampilan ini disajikan dalam format tabel dengan tombol aksi untuk memudahkan admin dalam melakukan operasi CRUD (*Create, Read, Update, Delete*). Desain antarmuka dibuat sederhana namun fungsional untuk memastikan efisiensi dalam pengelolaan data warga.

6. Tampilan Data Pengaduan

Tampilan data pengaduan pada sistem terlihat pada gambar berikut :

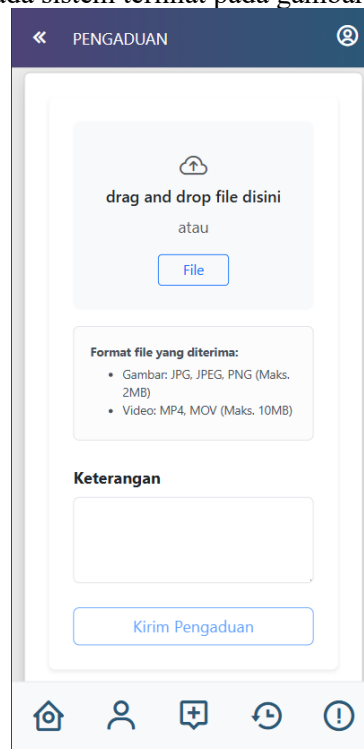


Gambar 8 Tampilan Data Pengaduan

Tampilan Data Pengaduan merupakan fitur khusus Admin dan Kades untuk mengelola laporan dari Masyarakat. Admin dapat mengelola semua, sedangkan Kades hanya dapat melihat atau memonitoring setiap pengaduan yang masuk. Menu ini menampilkan daftar pengaduan yang berisi deskripsi masalah (yang dienkripsi menggunakan metode *Caesar Cipher* untuk keamanan data sensitif), status penanganan, dan detail lainnya. Admin dapat melakukan beberapa aksi seperti memverifikasi status penanganan ("diproses", "selesai"), menghapus data pengaduan. Data pengaduan berasal dari *input* masyarakat yang telah mengisi *form* pengaduan sebelumnya. Tampilan dirancang dengan antarmuka tabel yang dilengkapi filter dan tombol aksi untuk memudahkan administrasi.

7. Tampilan Proses Pengaduan

Tampilan proses pengaduan pada sistem terlihat pada gambar berikut :

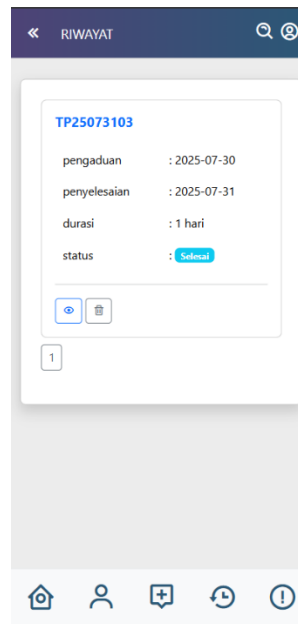


Gambar 9 Tampilan Proses Pengaduan

Tampilan Proses Pengaduan merupakan fitur khusus masyarakat untuk melaporkan masalah atau keluhan. Pada menu ini, pengguna dapat mengunggah bukti berupa foto atau video serta menuliskan keterangan pengaduan yang akan otomatis dienkripsi menggunakan *Caesar Cipher* untuk keamanan data. Setelah melengkapi informasi, masyarakat dapat mengirimkan laporan dengan menekan tombol Kirim Pengaduan. Tampilan ini dirancang sederhana namun efektif, memastikan proses pelaporan berjalan mudah sementara data pribadi tetap terlindungi. Setelah dikirim, pengaduan akan masuk ke sistem untuk ditindaklanjuti oleh admin.

8. Tampilan Riwayat Pengaduan

Tampilan riwayat pengaduan pada sistem terlihat pada gambar berikut :

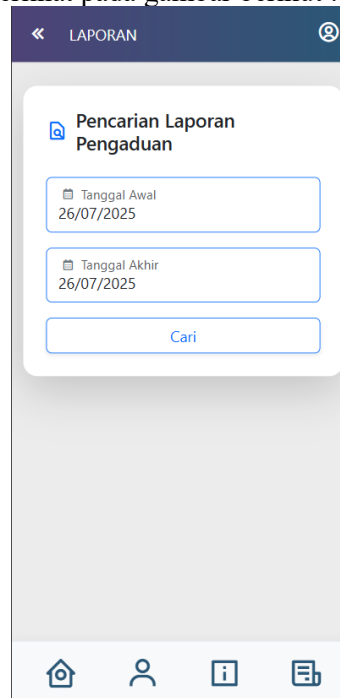


Gambar 10 Tampilan Riwayat Pengaduan

Tampilan Riwayat Pengaduan merupakan menu khusus masyarakat untuk melacak semua pengaduan yang pernah di laporkan. Pada halaman ini, ditampilkan informasi penting seperti tanggal pengaduan dan status penanganan ("diproses", atau "selesai"). Masyarakat juga memiliki opsi untuk menghapus riwayat pengaduan jika diperlukan. Tampilan dirancang dalam bentuk daftar yang rapi, memudahkan pengguna untuk melacak perkembangan laporan. Fitur ini memberikan transparansi sekaligus kontrol bagi masyarakat atas pengaduan-pengaduan yang telah di *submit* sebelumnya.

9. Tampilan Laporan

Tampilan laporan pada sistem terlihat pada gambar berikut :



Gambar 11 Tampilan Laporan

Tampilan Laporan dapat diakses oleh Admin dan Kades untuk menghasilkan rekapan data pengaduan berdasarkan periode tertentu. Pada menu ini, pengguna dapat memilih tanggal awal dan tanggal akhir, lalu menekan tombol Cari untuk memproses permintaan. Jika data tersedia, sistem akan secara otomatis mengunduh *file* laporan dalam format PDF yang berisi rangkuman pengaduan dalam rentang waktu yang ditentukan. Fitur ini memudahkan Admin dan Kades dalam mendapatkan data terstruktur untuk keperluan dokumentasi atau evaluasi tanpa perlu konversi manual. Tampilan dirancang minimalis dengan fokus pada fungsi filter tanggal sebagai parameter utama pembuatan laporan.

4. KESIMPULAN

1. Aplikasi pengaduan masyarakat berbasis mobile yang dikembangkan berhasil meningkatkan efisiensi pelayanan publik di Kantor Kepala Desa Bulu Cina dengan menyediakan sistem yang dapat diakses secara online.
2. Penerapan algoritma MD5 pada sistem login terbukti mampu meningkatkan keamanan autentikasi pengguna, karena password tidak disimpan dalam bentuk teks asli (plain text).
3. Penggunaan Caesar Cipher sebagai metode enkripsi teks pengaduan memberikan lapisan perlindungan tambahan terhadap isi pengaduan, dan enkripsi ini mencegah teks pengaduan terbaca secara langsung jika terjadi kebocoran data atau akses tidak sah.

UCAPAN TERIMA KASIH

Sebagai penutup, penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah memberikan kesempatan dan dukungan dalam penyelesaian Karya Tulis Ilmiah (KTI) ini. Penulis juga menyampaikan apresiasi kepada dosen pembimbing, para pengajar, serta seluruh pihak yang telah memberikan arahan, motivasi, dan bantuan selama proses penyusunan karya ini.

REFERENSI

- [1] M. H. Akmal and L. Wahyuni, "Sistem Informasi Kegagalan Produksi Berbasis WEB Pada PT. Jui Shin Indonesia," *Jurnal Info Digit (JID)*, no. 3, pp. 1746–1760, 2024, [Online]. Available: <https://kti.potensi-utama.org/index.php/JID/article/view/1537%0Ahttps://kti.potensi-utama.org/index.php/JID/article/download/1537/586>
- [2] Z. Siregar and L. Wahyuni, "Jurnal Sains dan Teknologi Widyaloka SISTEM INFORMASI PENGADAAN BAHAN Jurnal Sains dan Teknologi Widyaloka," *Jurnal Sains dan Teknologi Widyaloka*, vol. 3, pp. 91–104, 2024.
- [3] R. Teguh Pradana and L. Wahyuni, "Perancangan Aplikasi Bimbingan Konseling Kesulitan Belajar Siswa Menggunakan Metode Backward Chaining Berbasis Android Pada Sekolah PAB 2 Helvetia Counseling Guidance Application for Student Learning Difficulties Using Android-Based Backward Chaining Meth," *JID (Jurnal Info Digit)*, no. 2, p. 263, 2024, [Online]. Available: <http://kti.potensi-utama.ac.id/index.php/JID>
- [4] M. Rio Rivalda and L. Wahyuni, "Perancangan Sistem Informasi Karyawan Outsourcing Menggunakan Metode Naive Bayes Berbasis Android Pada PT. Dapensi Trio Usaha Design of Outsourced Employee Information System Using The Android Based Naive Bayes Method At

- PT. Dapensi Trio Usaha,” *JID (Jurnal Info Digit)*, no. 3, pp. 1055–1069, 2024, [Online]. Available: <http://kti.potensi-utama.ac.id/index.php/JID>
- [5] M. Darusman and L. Wahyuni, “Analisa Dan Perancangan Sistem Informasi Tracer Study Alumni Berbasis Android Pada SMK BINA SATRIA Medan,” *JID (Jurnal Info Digit)*, no. 3, 2024.
- [6] A. Z. F. Rangkuti and H. Fahmi, “Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5,” *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 3, no. 2, pp. 170–175, 2020, doi: 10.32672/jnkti.v3i2.2384.
- [7] I. Inayatullah, Antonius Wahyu Sudrajat, Nyimas Sabilina Cahyani, and U. Ubaidillah, “Rancang Bangun Aplikasi Pengamanan Akta Notaris Menggunakan Md5 Pada Kantor Notaris Taufiqurrachman, S.H.,” *Klik - Jurnal Ilmu Komputer*, vol. 3, no. 1, pp. 1–11, 2022, doi: 10.56869/klik.v3i1.316.
- [8] E. Setyawati, C. E. Widjayanti, R. R. Siraiz, and H. Wijoyo, “Pengujian keamanan komputer kriptografi pada surat elektronik berbasis website dengan enkripsi metode MD5,” *Jurnal Manajemen Informatika Jayakarta*, vol. 1, no. 1, p. 56, 2021, doi: 10.52362/jmijayakarta.v1i1.367.
- [9] F. Harris and R. E. Sari, “Meningkatkan Keamanan Source Code Web Melalui Teknik Enkripsi dan Dekripsi Dengan Metode Reverse Cipher dan Caesar Cipher Improving Web Source Code Security Through Encryption and Decryption Techniques Using Reverse Cipher and Caesar Cipher Methods,” *JID (Jurnal Info Digit)*, no. 2, p. 405, 2024, [Online]. Available: <http://kti.potensi-utama.ac.id/index.php/JID>
- [10] A. Latiep and N. Syahputri, “Rancang Bangun Aplikasi Keamanan Data Penjualan Berbasis Web Menggunakan Metode Caesar Cipher Dan Base64 Pada Pabrik Tahu SS,” *JID (Jurnal Info Digit)*, no. 3, pp. 952–964, 2024.
- [11] S. L. Parhusip and R. E. Sari, “Pesan yang Dirahasiakan Menggunakan Algoritma Feal dan Caesar Chiper Disisipkan ke Dalam Gambar Menggunakan Metode Least Signifigan Bit (LSB),” *JID (Jurnal Info Digit)*, vol. 2, no. 2, pp. 694–708, 2024.
- [12] R. Oktari Batubara, “Pengembangan Aplikasi Keamanan Data Agen Kapal Dengan Menggunakan Metode MD5 Berbasis Web Development Of Ship Agent Data Security Application Using Web-Based MD5 Method,” *Jurnal Widya*, vol. 4, no. 1, pp. 87–96, 2023, [Online]. Available: <https://jurnal.amikwidyaloka.ac.id/index.php/awl>
- [13] D. Alfiyan, S. Andryana, and I. D. Sholihati, “Algoritma Sequential Search Dan MD5 Pada Aplikasi Inventory Barang Berbasis Web,” *Smatika Jurnal*, vol. 13, no. 02, pp. 199–211, 2023, doi: 10.32664/smatika.v13i02.902.
- [14] M. K. Fauzi and A. Setiawan, “Implementasi Algoritma Vigenere Chiper dan Caesar Chiper Untuk Pengamanan Password Dalam Penerimaan Siswa Baru,” *JID (Jurnal Info Digit)*, vol. 2, no. 3, p. 1083, 2024, [Online]. Available: <http://kti.potensi-utama.ac.id/index.php/JID>
- [15] J. Jureksi and A. Zulkarnain Hasibuan, “Implementasi Kriptografi Hybrid Menggunakan Caesar Cipher dan Affine Cipher Untuk Kemanan Teks Hybrid Cryptography Implementation Using Caesar Cipher and Affine Cipher for Text Security,” *Jurnal JUREKSI (Jurnal ReKayasa Sistem)*,

vol. 2, no. 3, pp. 2240–2250, 2024, [Online]. Available: <https://kti.potensi-utama.ac.id/index.php/%7C>

- [16] B. Zebua, P. Herwanto, and R. Rosida, “Penggunaan Encripsi MD5 Untuk Pencegahan SQL Injection Pada Aplikasi Berbasis Web,” *Prosiding Seminar Nasional Inovasi dan Adopsi Teknologi (INOTEK)*, vol. 2, no. 1, pp. 22–31, 2022, doi: 10.35969/inotek.v2i1.206.