

**UJIAN AKHIR SEMESTER**  
**DESAIN DAN PEMROGRAMAN APLIKASI MOBILE**  
**APLIKASI ENKRIPSI DAN DEKRIPSI PESAN SEDERHANA**  
**MENGGUNAKAN HILL CIPHER**



**Kelompok : TI4A**

**Anggota :**

- **Han Lie (2111500077)**
- **Martua Denny Natalius Sitanggang (2311500002)**
- **Rizky Oktoreza (2311500001)**
- **Harmin Abdul Maryanto (2311500099)**

## Kata Pengantar

Puji syukur kehadiran Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas terakhir sekaligus Ujian Akhir Semester untuk mata kuliah *Desain Pemrograman Mobile* yang diampu oleh Bapak Tri Sugihartono, M.Kom.

Tugas ini merupakan proyek pengembangan prototipe aplikasi startup mobile menggunakan Flutter. Dalam pengembangannya, proyek ini juga mengintegrasikan konsep dari mata kuliah lain, yaitu *Aljabar Linear dan Matriks*, khususnya dalam topik *Kriptografi Hill Cipher*.

Laporan ini disusun untuk mendokumentasikan seluruh proses pengembangan, mulai dari ide awal hingga terbentuknya prototipe akhir. Penulis berharap laporan ini dapat memberikan inspirasi dan mendorong minat pembaca untuk ikut belajar dan mengembangkan aplikasi atau perangkat lunak, seiring dengan pesatnya perkembangan teknologi saat ini.

Penulis menyadari bahwa laporan ini masih jauh dari sempurna. Oleh karena itu, segala bentuk kritik dan saran yang membangun sangat diharapkan demi perbaikan di masa mendatang.

Akhir kata, semoga laporan ini dapat memberikan manfaat bagi siapa pun yang membacanya.

Pangkalpinang, 3 Juli 2025

Penulis

## LATAR BELAKANG

### Sekilas tentang Kriptografi

*Kriptografi* atau Kriptologi , merupakan keahlian dan ilmu dari cara-cara untuk komunikasi aman pada kehadirannya di pihak ketiga. Secara umum kriptografi ialah tentang mengkonstruksi dan menganalisis protokol komunikasi yang dapat memblokir lawan. Berbagai aspek dalam keamanan informasi seperti data rahasia, integritas data, autentikasi, dan non-repudansi merupakan pusat dari kriptografi modern. Kriptografi modern terjadi karena terdapat titik temu antara disiplin ilmu matematika, ilmu komputer dan teknik elektro. Aplikasi dari kriptografi termasuk ATM, password komputer, dan E-Commerce. (Sumber : Wikipedia)

### Hill Cipher

Hill Cipher adalah sandi substitusi poligrafik yang didasarkan pada aljabar linear. Diciptakan oleh Lester S. Hill pada tahun 1929, sandi ini merupakan sandi poligrafik pertama yang praktis (meskipun sulit) untuk dioperasikan pada lebih dari tiga simbol sekaligus.

(Sumber : Wikipedia)

### Ide Awal Aplikasi

Awalnya, penulis masih menampung berbagai ide dari anggota kelompok lain. Namun, serupa dengan penulis, mereka pun belum mampu memberikan gagasan yang konkret. Oleh karena itu, penulis kemudian mengusulkan sebuah ide yang berdasarkan pada materi yang telah dipelajari dalam mata kuliah *Aljabar Linear dan Matriks*, yakni penerapan konsep matriks dalam proses enkripsi dan dekripsi menggunakan algoritma *Hill Cipher*. Materi tersebut dirasa sangat menarik dan menantang, sehingga menumbuhkan semangat lebih bagi penulis untuk menjadikannya sebagai dasar proyek UAS ini.

Gagasan ini juga dilatarbelakangi oleh maraknya kasus pembajakan akun WhatsApp, Telegram, dan berbagai media sosial lainnya. Banyak pengguna yang merasa khawatir apabila informasi-informasi penting yang bersifat pribadi, profesional, atau sensitif jatuh ke tangan pihak yang tidak bertanggung jawab. Berangkat dari kekhawatiran tersebut, penulis berinisiatif untuk menerapkan pengetahuan yang diperoleh di kelas ke dalam pengembangan sebuah prototipe aplikasi yang mampu mengenkripsi dan mendekripsi pesan sebagai bentuk kontribusi terhadap peningkatan keamanan komunikasi digital.

## DESKRIPSI FITUR APLIKASI

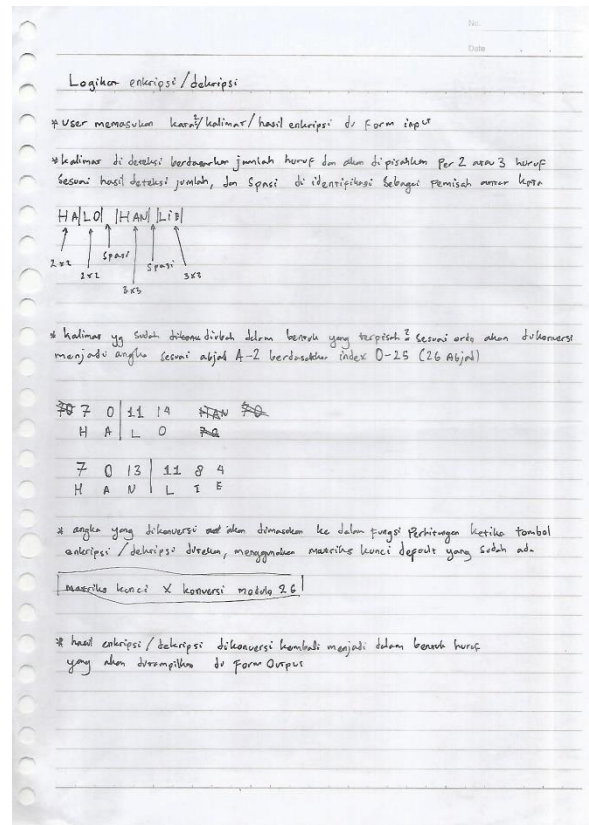
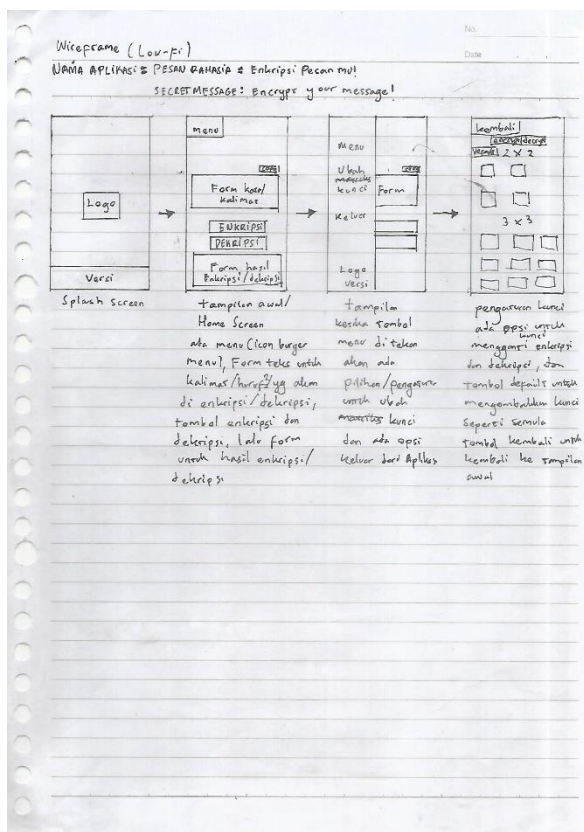
Aplikasi ini dirancang dengan konsep yang sederhana namun fungsional. Terdapat beberapa komponen utama, seperti *form* input untuk memasukkan pesan asli (plaintext) yang akan dienkripsi maupun ciphertext yang akan didekripsi, serta *form* output untuk menampilkan hasil dari proses enkripsi atau dekripsi.

Untuk melakukan proses enkripsi dan dekripsi, disediakan dua tombol utama yang masing-masing menjalankan fungsi sesuai kebutuhan pengguna. Selain itu, aplikasi juga memungkinkan pengguna untuk mengatur sendiri matriks kunci enkripsi serta matriks kunci dekripsi (yang merupakan invers dari matriks kunci enkripsi) sesuai kesepakatan antar pihak. Hal ini dirancang agar pengguna dapat saling bertukar informasi sensitif secara aman, mirip dengan sistem komunikasi rahasia dalam dunia intelijen atau pertukaran data terenkripsi antar lembaga.

Sebagai tambahan, aplikasi ini menyediakan tombol “Default” pada pengaturan matriks kunci. Tombol ini dapat digunakan oleh pengguna yang belum memahami cara menentukan matriks kunci atau invers-nya secara manual, sehingga tetap dapat menggunakan aplikasi dengan lancar tanpa hambatan teknis.

### Desain awal serta konsep yang dijadikan referensi

Penulis pertama-tama menjabarkan urutan logika secara garis besar dan juga menggambar wireframe low-fidelity secara manual di kertas.





Penulis juga menggunakan referensi berupa Soal dari tugas mata kuliah Aljabar Linear dan Matriks.

3. Budi mengirimkan pesan kepada temannya yaitu "SEMANGAT BELAJAR UNTUK MASA DEPAN" enkripsi dan dekripsi. Ken dengan Hill Cipher kalimat yang dikirimkan Budi tersebut (Cord 2x2) dan 3x3) matriks kunci gander seperti contoh Lathia

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

ENKRIPSI

matriks kunci (2x2)

3	3
2	5

matriks kunci (3x3)

6	2	4
13	16	10
20	17	15

SEM 18 AUG 0 AT 0 BEL 1 AJ 0 AR 0

4	13	19	4	0	9	17
12	6			11		

UNT = 20 UK 20 MA 12 SA 18 DEP 3 AN 0

13	10	0	0	4	13
19				15	

D : 14 SEM : 6 24 1 18 6x18+24x9+1x12 216 mod 26 8 I

13	16	10	13	13x18+16x9+10x12 268 mod 26 2 C
20	17	15	12	20x10+17x9+15x12 301 mod 26 10 K

Q : 15 AUG : 6 24 1 0 6x0+24x13+1x6 318 mod 26 6 G

20	17	15	6	13x0+16x13+10x6 268 mod 26 8 I
				20x0+17x13+15x6 301 mod 26 10 K

U : 20 AT 33 0 3x0+3x19 57 mod 26 5 F

25	19	2x0+5x19 95 mod 26 17 R
----	----	-------------------------

Z : 25 UNT 6 24 1 20 6x20+24x13+1x19 351 mod 26 9 J

13	16	10	13	13x20+16x13+10x19 350 mod 26 8 I
20	17	15	19	20x20+17x13+15x19 306 mod 26 12 M

UK 33 0 3x20+3x10 90 mod 26 12 M

25	10	2x20+5x10 90 mod 26 12 M
----	----	--------------------------

Name: \_\_\_\_\_  
Date: \_\_\_\_\_

---

$K_1 = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$

$\Rightarrow$

$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

  
$$K_{k1} = \begin{bmatrix} 16 & 19 \\ 17 & 15 \end{bmatrix} = 1 \cdot (16 \times 15 - 17 \times 10) = -\cancel{10} \quad 70$$
$$K_{k2} = \begin{bmatrix} 13 & 10 \\ 20 & 15 \end{bmatrix} = -1 \cdot (13 \times 15 - 20 \times 10) = 5$$
$$K_{k3} = \begin{bmatrix} 12 & 16 \\ 20 & 17 \end{bmatrix} = 1 \cdot (13 \times 17 - 20 \times 16) = -99$$
$$K_{k4} = \begin{bmatrix} 24 & 1 \\ 12 & 15 \end{bmatrix} = -1 \cdot (24 \times 15 - 17 \times 1) = -343$$
$$K_{k5} = \begin{bmatrix} 6 & 1 \\ 20 & 15 \end{bmatrix} = 1 \cdot (6 \times 15 - 20 \times 1) = 70$$
$$K_{k6} = \begin{bmatrix} 6 & 24 \\ 20 & 17 \end{bmatrix} = -1 \cdot (6 \times 17 - 20 \times 24) = -\cancel{378} \quad 378$$
$$K_{k7} = \begin{bmatrix} 24 & 1 \\ 16 & 10 \end{bmatrix} = 1 \cdot (24 \times 10 - 16 \times 1) = 224$$
$$K_{k8} = \begin{bmatrix} 6 & 1 \\ 13 & 10 \end{bmatrix} = -1 \cdot (6 \times 10 - 13 \times 1) = -47$$
$$K_{k9} = \begin{bmatrix} 6 & 24 \\ 13 & 16 \end{bmatrix} = 1 \cdot (6 \times 16 - 13 \times 24) = -216$$
  

$\begin{matrix} \text{korraktor} \\ \begin{bmatrix} 70 & 5 & -99 \\ -343 & 70 & 378 \\ 224 & -47 & -216 \end{bmatrix} \end{matrix}$

 $\Rightarrow$

$\begin{matrix} \text{Algor} \\ \begin{bmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{bmatrix} \end{matrix}$

 $= 25 \times$

$\begin{bmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{bmatrix}$

 $\stackrel{\text{mod } 26}{=} \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$

  
$$\det K = \begin{vmatrix} 6 \times 70 + 24 \times 5 + 1 \times (-99) \end{vmatrix} = 941 \pmod{26}$$
$$941 \not\equiv 1 \pmod{26}$$

$\frac{941}{26} = 36 \text{ R } 5$

No. \_\_\_\_\_  
 Date \_\_\_\_\_

$$\text{BEL} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 1 & 6 \times 1 + 24 \times 4 + 1 \times 11 \\ 4 & 13 \times 3 + 16 \times 4 + 10 \times 11 \\ 11 & 20 \times 1 + 17 \times 4 + 15 \times 11 \end{bmatrix} \begin{bmatrix} 113 \text{ mod } 26 \\ 182 \\ 253 \end{bmatrix} \begin{bmatrix} 9 \\ 5 \\ 19 \end{bmatrix} \begin{bmatrix} J \\ F \\ T \end{bmatrix}$$

$$\text{AJ} = \begin{bmatrix} 3 & 3 \\ 25 \end{bmatrix} \begin{bmatrix} 0 \\ 9 \end{bmatrix} \begin{bmatrix} 3 \times 0 + 3 \times 9 \\ 2 \times 0 + 5 \times 9 \end{bmatrix} \begin{bmatrix} 27 \text{ mod } 26 \\ 45 \end{bmatrix} \begin{bmatrix} 1 \\ 19 \end{bmatrix} \begin{bmatrix} B \\ T \end{bmatrix}$$

$$\text{AR} = \begin{bmatrix} 3 & 3 \\ 25 \end{bmatrix} \begin{bmatrix} 0 \\ 17 \end{bmatrix} \begin{bmatrix} 3 \times 0 + 3 \times 17 \\ 2 \times 0 + 5 \times 17 \end{bmatrix} \begin{bmatrix} 51 \text{ mod } 26 \\ 85 \end{bmatrix} \begin{bmatrix} 25 \\ 7 \end{bmatrix} \begin{bmatrix} Z \\ H \end{bmatrix}$$

$$\text{MA} = \begin{bmatrix} 3 & 3 \\ 25 \end{bmatrix} \begin{bmatrix} 12 \\ 0 \end{bmatrix} \begin{bmatrix} 3 \times 12 + 3 \times 0 \\ 2 \times 12 + 5 \times 0 \end{bmatrix} \begin{bmatrix} 36 \text{ mod } 26 \\ 24 \end{bmatrix} \begin{bmatrix} 10 \\ 29 \end{bmatrix} \begin{bmatrix} K \\ Y \end{bmatrix}$$

$$\text{SA} = \begin{bmatrix} 3 & 3 \\ 25 \end{bmatrix} \begin{bmatrix} 18 \\ 0 \end{bmatrix} \begin{bmatrix} 3 \times 18 + 3 \times 0 \\ 2 \times 18 + 5 \times 0 \end{bmatrix} \begin{bmatrix} 54 \text{ mod } 26 \\ 36 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \begin{bmatrix} C \\ K \end{bmatrix}$$

$$\text{DEP} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 3 & 6 \times 3 + 24 \times 4 + 1 \times 15 \\ 13 \times 3 + 16 \times 4 + 10 \times 15 \\ 20 \times 3 + 17 \times 4 + 15 \times 15 \end{bmatrix} \begin{bmatrix} 129 \text{ mod } 26 \\ 253 \\ 353 \end{bmatrix} \begin{bmatrix} 25 \\ 19 \\ 15 \end{bmatrix} \begin{bmatrix} Z \\ T \\ D \end{bmatrix}$$

$$\text{AN} = \begin{bmatrix} 3 & 3 \\ 25 \end{bmatrix} \begin{bmatrix} 0 \\ 13 \end{bmatrix} \begin{bmatrix} 3 \times 0 + 3 \times 13 \\ 2 \times 0 + 5 \times 13 \end{bmatrix} \begin{bmatrix} 39 \text{ mod } 26 \\ 65 \end{bmatrix} \begin{bmatrix} 13 \\ 13 \end{bmatrix} \begin{bmatrix} N \\ N \end{bmatrix}$$

SEMANGAT BELAJAR UNTUK MASA DEPAN  
 ICKGIZFR JFTBTZ JIWNM KYCK ZTPUN

DEKRIPS:

$$\begin{bmatrix} 3 & 3 \\ 25 \end{bmatrix} \begin{matrix} \text{adjoin } K \\ \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \end{matrix} \text{mod } 26 = \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix}$$

$$\det(K) = (3 \times 5) - (3 \times 2) = 15 - 6 = 9$$

$$9 \times X \equiv 1 \text{ mod } 26$$

$$9 \times 3 \equiv 27 \equiv 1 \text{ mod } 26$$

$$\text{invers det}(K) = 3$$

$$\text{invers } K \text{ (mod } 26)$$

$$\text{invers det}(K) \times \text{adjoin mod } 26$$

$$= 3 \times \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} \text{mod } 26$$

$$= \begin{bmatrix} 15 & 69 \\ -2 & 9 \end{bmatrix} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

15	17	8	5	10
20	9	21	8	21
		21	12	8

ICKGIZFR JFTGTZH  
JIWMM KYCK ZTPNN

ICK =  $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$

GIZ =  $\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 8 \\ 6 \\ 8 \\ 25 \end{bmatrix}$

FR =  $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 5 \\ 17 \end{bmatrix}$

JFT =  $\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 9 \\ 5 \\ 19 \end{bmatrix}$

BT =  $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 1 \\ 19 \end{bmatrix}$

ZH =  $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 25 \\ 7 \end{bmatrix}$

JIW =  $\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 9 \\ 22 \\ 22 \end{bmatrix}$

MM =  $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 12 \\ 12 \end{bmatrix}$

KY =  $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 10 \\ 24 \end{bmatrix}$

CK =  $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

SEMANAKAT =  $\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 15 \\ 15 \end{bmatrix}$

NN =  $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 13 \\ 13 \end{bmatrix}$

$\begin{bmatrix} 8 \times 8 + 5 \times 2 + 10 \times 0 \\ 21 \times 8 + 8 \times 2 + 21 \times 0 \\ 21 \times 8 + 12 \times 2 + 8 \times 0 \end{bmatrix} = \begin{bmatrix} 174 \\ 394 \\ 272 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \\ 26 \end{matrix} = \begin{bmatrix} 18 \\ 4 \\ 12 \end{bmatrix} \begin{matrix} S \\ E \\ M \end{matrix}$

$\begin{bmatrix} 8 \times 6 + 5 \times 8 + 10 \times 25 \\ 21 \times 6 + 8 \times 8 + 21 \times 25 \\ 21 \times 6 + 12 \times 8 + 8 \times 25 \end{bmatrix} = \begin{bmatrix} 338 \\ 745 \\ 826 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \\ 26 \end{matrix} = \begin{bmatrix} 0 \\ 13 \\ 6 \end{bmatrix} \begin{matrix} A \\ N \\ G \end{matrix}$

$\begin{bmatrix} 15 \times 5 + 17 \times 17 \\ 20 \times 5 + 9 \times 17 \end{bmatrix} = \begin{bmatrix} 364 \\ 253 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \end{matrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix} \begin{matrix} A \\ T \end{matrix}$

$\begin{bmatrix} 8 \times 9 + 5 \times 5 + 10 \times 19 \\ 21 \times 9 + 8 \times 5 + 21 \times 19 \\ 21 \times 9 + 12 \times 5 + 8 \times 19 \end{bmatrix} = \begin{bmatrix} 287 \\ 688 \\ 401 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \\ 26 \end{matrix} = \begin{bmatrix} 0 \\ 4 \\ 11 \end{bmatrix} \begin{matrix} A \\ E \\ L \end{matrix}$

$\begin{bmatrix} 15 \times 1 + 17 \times 19 \\ 20 \times 1 + 9 \times 19 \end{bmatrix} = \begin{bmatrix} 338 \\ 201 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \end{matrix} = \begin{bmatrix} 0 \\ 9 \end{bmatrix} \begin{matrix} A \\ J \end{matrix}$

$\begin{bmatrix} 15 \times 25 + 17 \times 7 \\ 20 \times 25 + 9 \times 7 \end{bmatrix} = \begin{bmatrix} 449 \\ 563 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \end{matrix} = \begin{bmatrix} 0 \\ 17 \end{bmatrix} \begin{matrix} A \\ R \end{matrix}$

$\begin{bmatrix} 8 \times 9 + 5 \times 8 + 10 \times 22 \\ 21 \times 9 + 8 \times 8 + 21 \times 22 \\ 21 \times 9 + 12 \times 8 + 8 \times 22 \end{bmatrix} = \begin{bmatrix} 332 \\ 715 \\ 461 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \\ 26 \end{matrix} = \begin{bmatrix} 20 \\ 13 \\ 19 \end{bmatrix} \begin{matrix} U \\ N \\ T \end{matrix}$

$\begin{bmatrix} 15 \times 12 + 17 \times 12 \\ 20 \times 12 + 9 \times 12 \end{bmatrix} = \begin{bmatrix} 384 \\ 348 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \end{matrix} = \begin{bmatrix} 10 \\ 20 \end{bmatrix} = \begin{matrix} U \\ K \end{matrix}$

$\begin{bmatrix} 15 \times 10 + 17 \times 24 \\ 20 \times 10 + 9 \times 24 \end{bmatrix} = \begin{bmatrix} 558 \\ 416 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \end{matrix} = \begin{bmatrix} 12 \\ 0 \end{bmatrix} \begin{matrix} M \\ A \end{matrix}$

$\begin{bmatrix} 15 \times 2 + 17 \times 10 \\ 20 \times 2 + 9 \times 10 \end{bmatrix} = \begin{bmatrix} 200 \\ 130 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \end{matrix} = \begin{bmatrix} 18 \\ 0 \end{bmatrix} \begin{matrix} S \\ A \end{matrix}$

$\begin{bmatrix} 8 \times 25 + 5 \times 19 + 10 \times 15 \\ 21 \times 25 + 8 \times 19 + 21 \times 15 \\ 21 \times 25 + 12 \times 19 + 8 \times 15 \end{bmatrix} = \begin{bmatrix} 445 \\ 492 \\ 873 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \\ 26 \end{matrix} = \begin{bmatrix} 3 \\ 4 \\ 15 \end{bmatrix} \begin{matrix} D \\ E \\ P \end{matrix}$

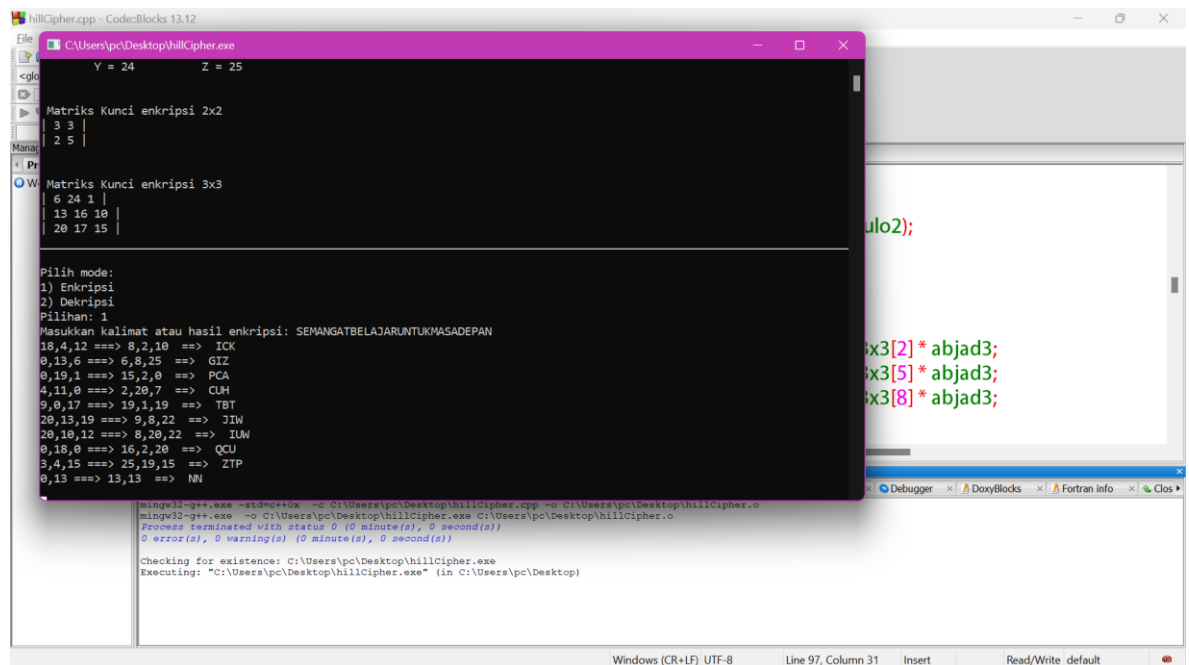
$\begin{bmatrix} 15 \times 13 + 17 \times 13 \\ 20 \times 13 + 9 \times 13 \end{bmatrix} = \begin{bmatrix} 416 \\ 371 \end{bmatrix} \begin{matrix} \text{mod } 26 \\ 26 \end{matrix} = \begin{bmatrix} 0 \\ 13 \end{bmatrix} \begin{matrix} A \\ N \end{matrix}$

ICKGIZFR JFTGTZH JIWMM KYCK ZTPNN  
SEMANAKAT BELAJAR UNTUK MASA DEPAN

## Pengujian logika menggunakan C++ di CodeBlocks

Sourcecode C++ ini bisa didapatkan di repository proyek ini. :

<https://github.com/johan99999/Pesan-Rahasia-Enkripsi-Pesan-mu/blob/development/hillCipher.cpp>



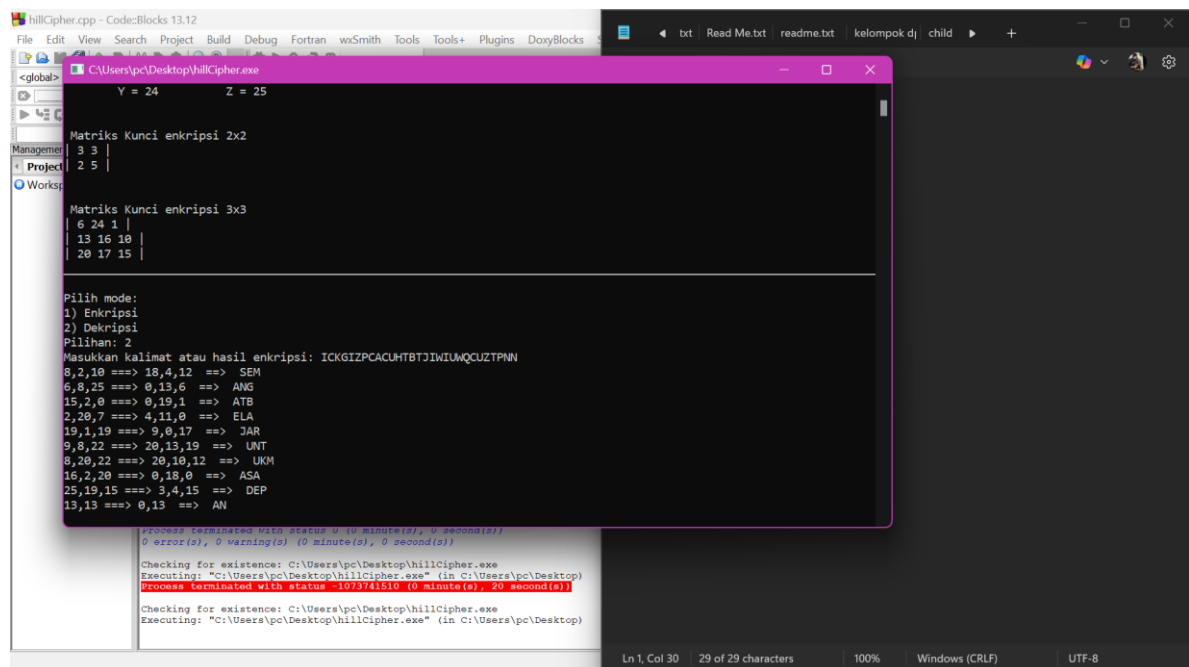
```
Y = 24      Z = 25

Matriks Kunci enkripsi 2x2
| 3 3 |
| 2 5 |

Matriks Kunci enkripsi 3x3
| 6 24 1 |
| 13 16 10 |
| 20 17 15 |

Pilih mode:
1) Enkripsi
2) Dekripsi
Pilihan: 1
Masukkan kalimat atau hasil enkripsi: SEMANGATBELAJARUNTUKMASADEPAN
18,4,12 ==> 8,2,10 ==> ICK
0,13,6 ==> 6,8,25 ==> GIZ
0,19,1 ==> 15,2,0 ==> PCA
4,11,0 ==> 2,20,7 ==> CUH
9,0,17 ==> 19,1,19 ==> TBT
20,13,19 ==> 9,8,22 ==> JIW
20,10,12 ==> 8,20,22 ==> IUW
0,18,0 ==> 16,2,20 ==> QCU
3,4,15 ==> 25,19,15 ==> ZTP
0,13 ==> 13,13 ==> NN

Process terminated with status 0 (0 minute(s), 0 second(s))
0 error(s), 0 warning(s) (0 minute(s), 0 second(s))
Checking for existence: C:\Users\pc\Desktop\hillCipher.exe
Executing: "C:\Users\pc\Desktop\hillCipher.exe" (in C:\Users\pc\Desktop)
```



```
Y = 24      Z = 25

Matriks Kunci enkripsi 2x2
| 3 3 |
| 2 5 |

Matriks Kunci enkripsi 3x3
| 6 24 1 |
| 13 16 10 |
| 20 17 15 |

Pilih mode:
1) Enkripsi
2) Dekripsi
Pilihan: 2
Masukkan kalimat atau hasil enkripsi: ICKGIZPCACUHTBTJINIUMQCUZTPNN
8,2,10 ==> 18,4,12 ==> SEM
6,8,25 ==> 0,13,6 ==> ANG
15,2,0 ==> 0,19,1 ==> ATB
2,20,7 ==> 4,11,0 ==> ELA
19,1,19 ==> 9,0,17 ==> JAR
9,8,22 ==> 20,13,19 ==> UNT
8,20,22 ==> 20,10,12 ==> UKM
16,2,20 ==> 0,18,0 ==> ASA
25,19,15 ==> 3,4,15 ==> DEP
13,13 ==> 0,13 ==> AN

Process terminated with status 0 (0 minute(s), 0 second(s))
0 error(s), 0 warning(s) (0 minute(s), 0 second(s))
Checking for existence: C:\Users\pc\Desktop\hillCipher.exe
Executing: "C:\Users\pc\Desktop\hillCipher.exe" (in C:\Users\pc\Desktop)
Process terminated with status -1073741510 (0 minute(s), 20 second(s))
Checking for existence: C:\Users\pc\Desktop\hillCipher.exe
Executing: "C:\Users\pc\Desktop\hillCipher.exe" (in C:\Users\pc\Desktop)
```



## DESAIN UI/UX APLIKASI

Desain di figma hanya dibuat sebagai referensi pengerjaan di flutter, jadi hanya dilakukan sedikit prototyping di bagian menu drawer.

Link desain figma :

<https://www.figma.com/design/4nFJZ4iAwwGJxMaAM8eJuu/Pesan-Rahasia-Enkripsi-Pesan-mu?node-id=0-1&t=XBz9U4T2mnW8LpiZ-1>



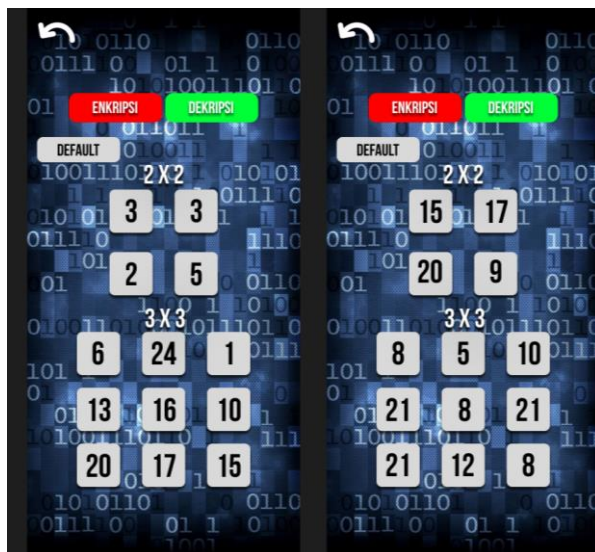
Splash Screen



Tampilan Awal



Tampilan Tentang



Tampilan setelan matriks kunci



Tampilan Menu Drawer

## DOKUMENTASI TEKNIS DAN ARSITEKTUR APLIKASI EVALUASI HASIL DAN PENGUJIAN

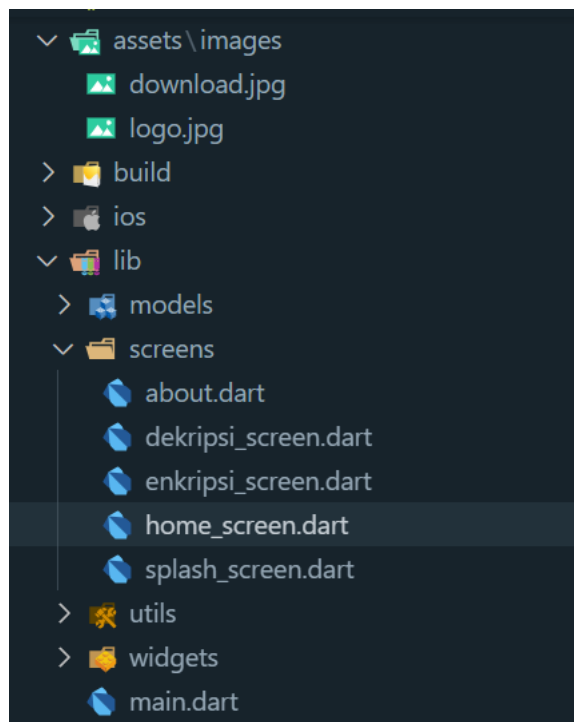
Link Repository :

<https://github.com/johan99999/Pesan-Rahasia-Enkripsi-Pesan-mu>

Teknologi yang digunakan selama pengembangan :

- Flutter 3.32.4
- Microsoft Visual Studio Code
- Android Studio 2024.3.2
- Figma

Struktur Proyek :



Seluruh tampilan dibuat di directory baru bernama “screens”, isinya adalah splash screen, home screen, setelan matriks kunci enkripsi, setelan matriks kunci dekripsi serta halaman tentang / about. Navigasi menggunakan Navigasi Drawer.



## LOGIKA PEMROGRAMAN

1. Pengguna memasukkan kata-kata, kalimat, atau hasil enkripsi pada form input.
2. Kalimat di deteksi berdasarkan jumlah huruf dan akan dipisahkan per 2 atau 3 huruf sesuai hasil deteksi.
  - SEMANGAT BELAJAR UNTUK MASA DEPAN
  - SEMANGATBELAJARUNTUKMASADEPAN
  - SEM|ANG|ATB|ELA|JAR|UNT|UKM|ASA|DEP|AN
3. Kalimat yang sudah diubah dalam bentuk yang terpisah-pisah sesuai ordo (2x2 atau 3x3) akan dikonversi menjadi dalam bentuk angka sesuai abjad AZ berdasarkan indeks 0-25 (26 Abjad).
  - SEM|ANG|ATB|ELA|JAR|UNT|UKM|ASA|DEP|AN
  - 18,4,12|0,13,6|0,19,1|4,11,0|9,0,17|20,13,19|20,10,12|0,18,0|3,4,15|0,13
4. Angka yang dikonversi akan dimasukkan ke dalam fungsi perhitungan ketika tombol enkripsi/dekripsi ditekan, menggunakan matriks kunci default yang sudah ada.
  - (Matriks kunci x Konversi) modulo 26
  - 18,4,12|0,13,6|0,19,1|4,11,0|9,0,17|20,13,19|20,10,12|0,18,0|3,4,15|0,13
  - 8,2,10|6,8,25|15,2,0|2,20,7|19,1,19|9,8,22|8,20,22|16,2,20|25,19,15|13,13
5. Hasil enkripsi/dekripsi konversi Kembali menjadi dalam bentuk huruf yang akan ditampilkan dalam bentuk output.
  - ICKGIZPCACUHTBTJIWIUWQCUZTPNN
  - SEMANGATBELAJARUNTUKMASADEPAN

## RUMUS ENKRIPSI DAN DEKRIPSI

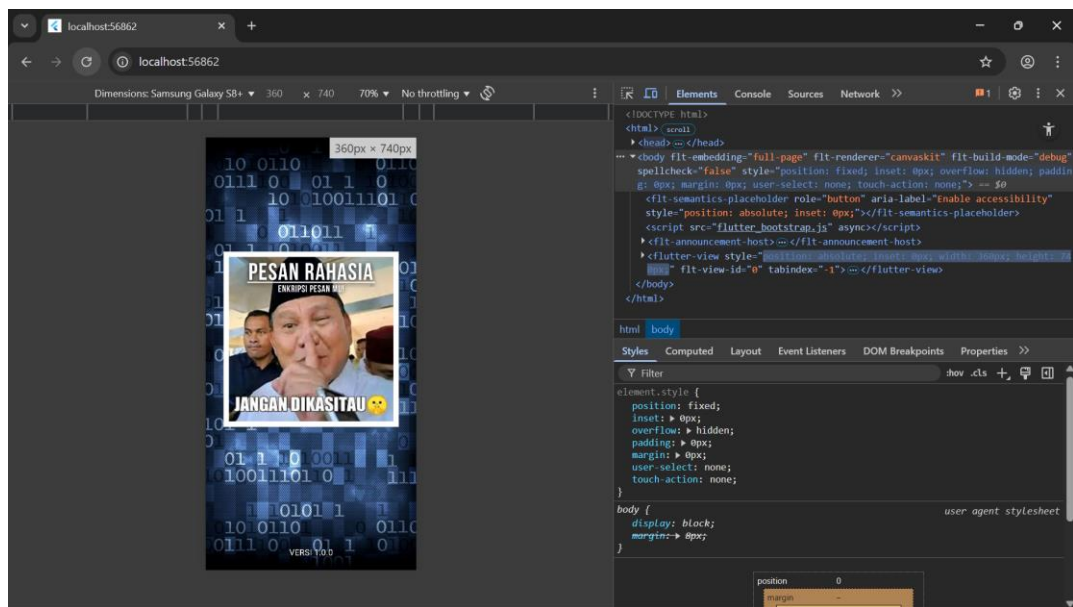
### Matriks Kunci x Matriks Plain Text Modulo 26

$$\begin{array}{cc} a & b \\ c & d \end{array} \cdot \begin{array}{c} a \\ b \end{array} \text{ mod } 26 \text{ (ordo } 2 \times 2)$$

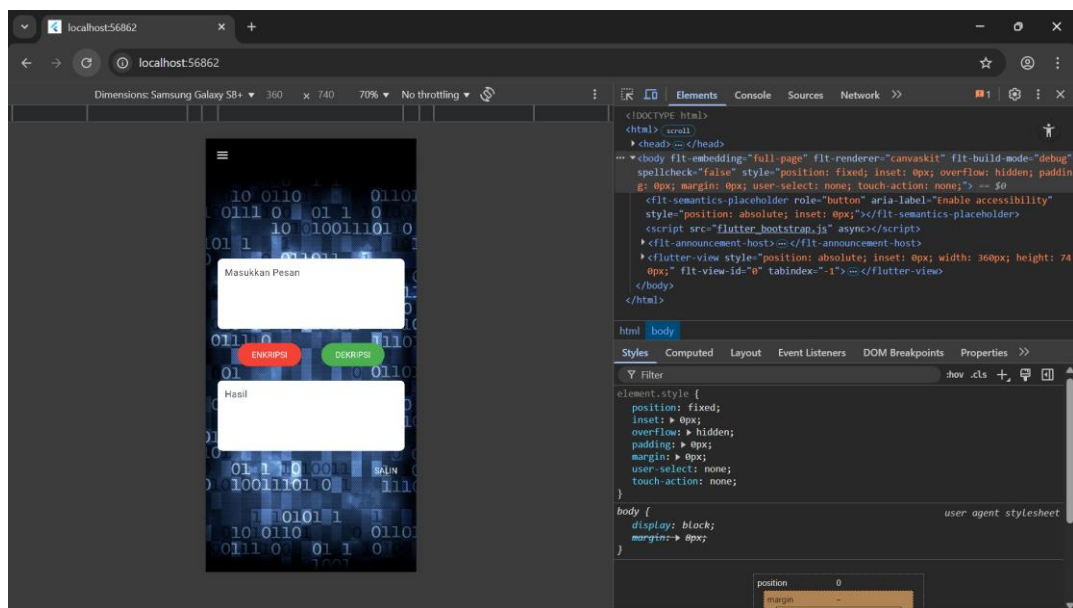
$$\begin{array}{ccc} a & b & c \\ d & e & f \\ g & h & i \end{array} \cdot \begin{array}{c} a \\ b \\ c \end{array} \text{ mod } 26 \text{ (ordo } 3 \times 3)$$

Lebih lengkapnya bisa dilihat di lampiran referensi yang diambil dari tugas mata kuliah aljabar.

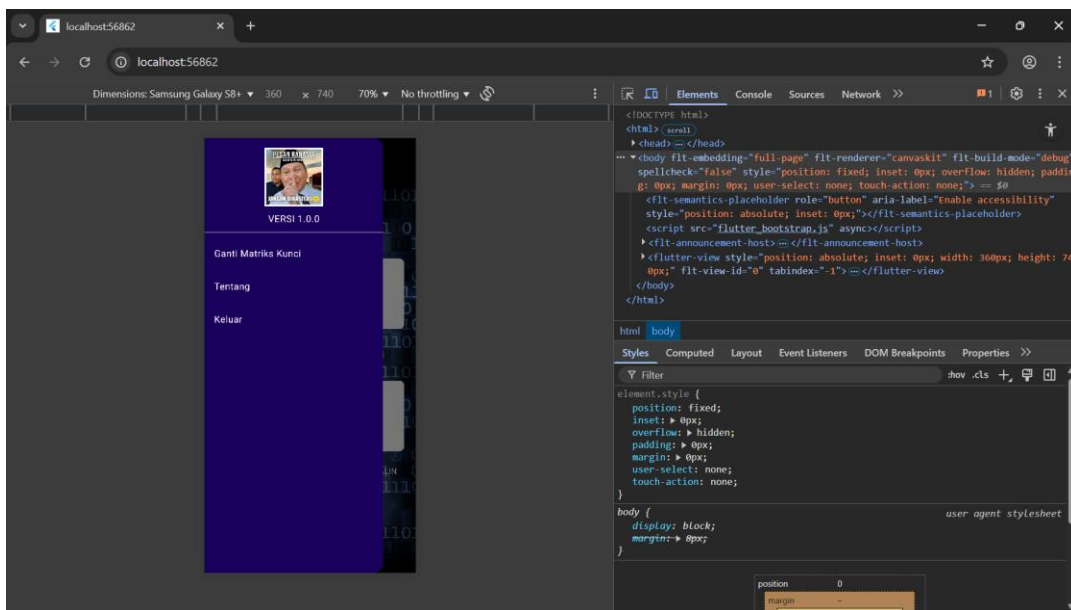
## HASIL IMPLEMENTASI DESAIN DAN LOGIKA SERTA PENGUJIAN



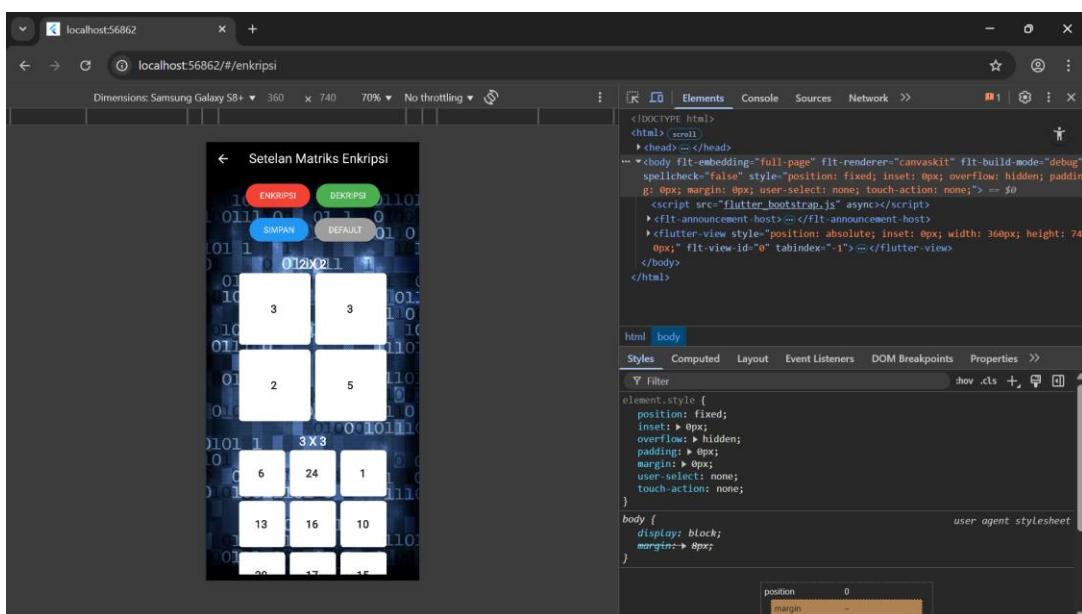
Tampilan Splash Screen



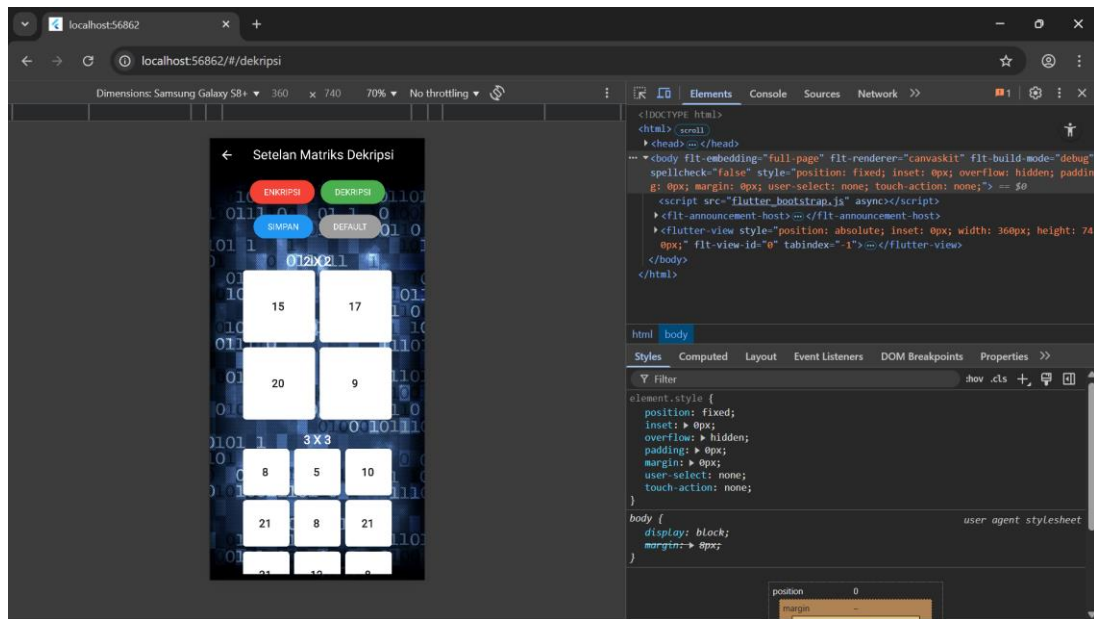
Tampilan awal aplikasi



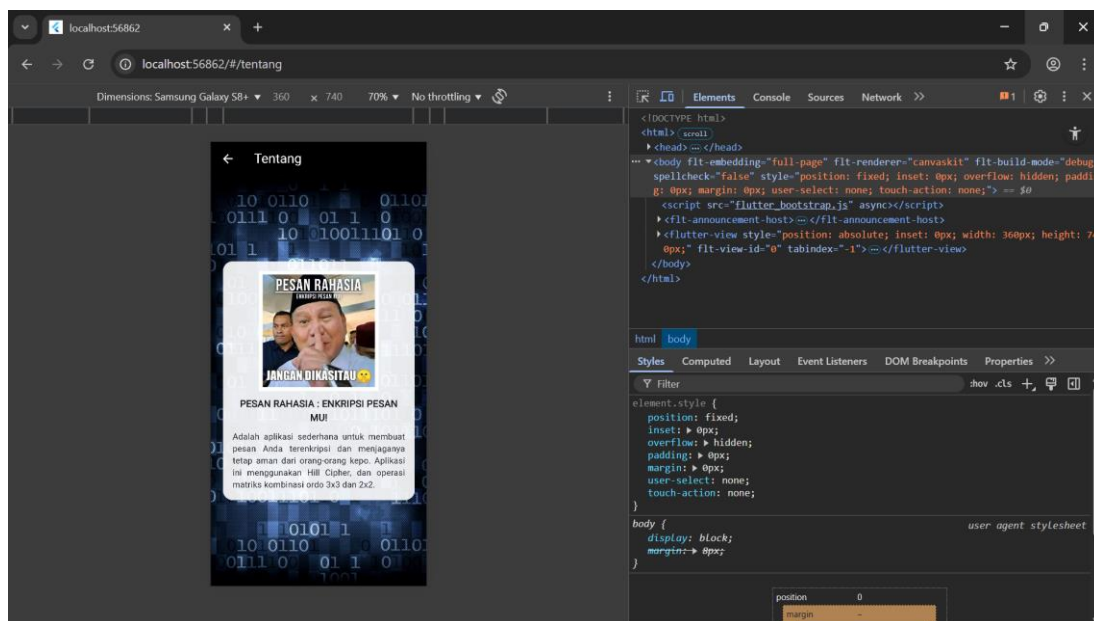
Tampilan Menu Drawer



Tampilan Pengaturan Matriks Kunci (Enkripsi)

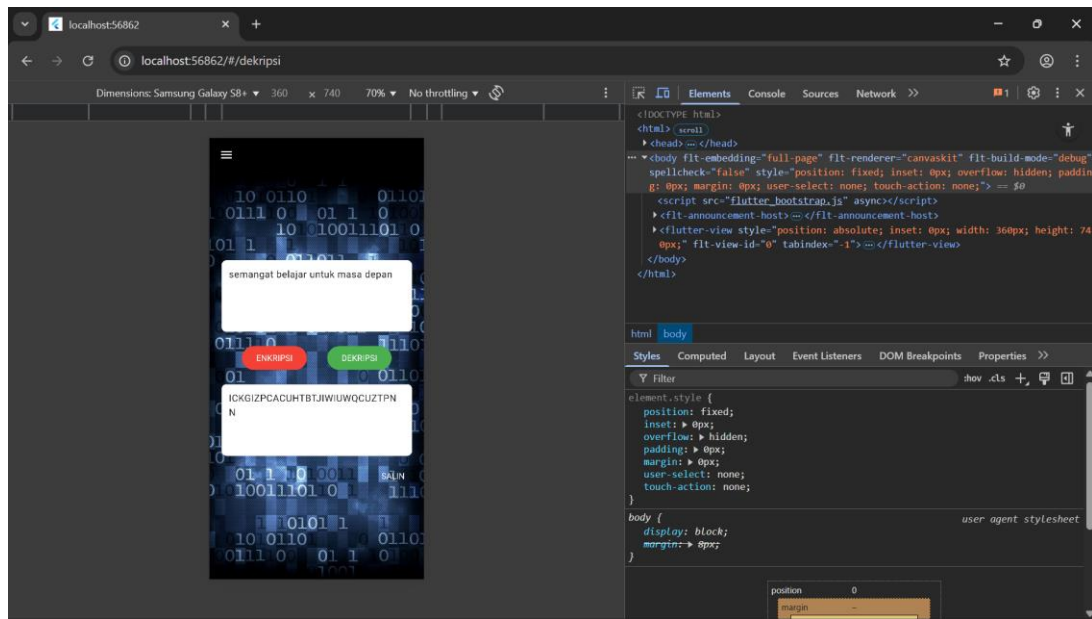


Tampilan Pengaturan Matriks Kunci (Dekripsi)

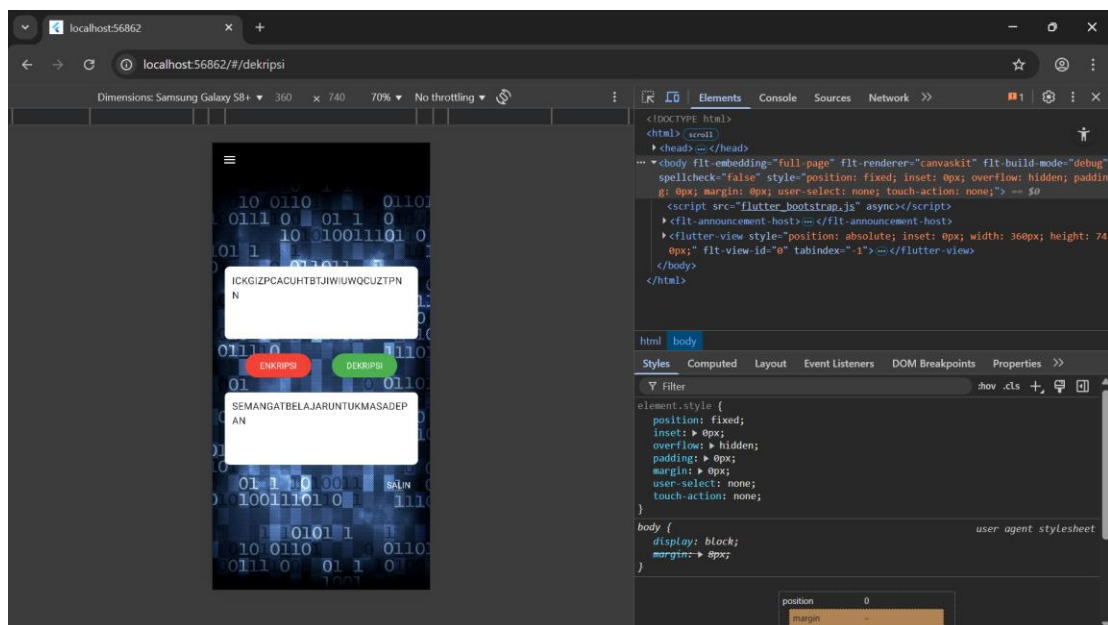


Tampilan tentang / about





### Hasil Pengujian Enkripsi



### Hasil Pengujian Dekripsi

## HASIL EVALUASI

Pengujian aplikasi telah dilakukan dan berjalan dengan baik serta lancar. Proses enkripsi dan dekripsi terbukti selaras dan akurat, salah satunya saat dilakukan pengujian menggunakan kalimat “*semangat belajar untuk masa depan*”. Hasil dekripsi berhasil mengembalikan pesan terenkripsi ke bentuk aslinya tanpa kesalahan.

### Kekurangan

Meskipun fungsi utama aplikasi berjalan dengan baik, terdapat beberapa kekurangan yang perlu diperhatikan:

- Matriks kunci yang tersedia masih terbatas dan belum beragam; aplikasi saat ini hanya menggunakan matriks default.
- Proses enkripsi dan dekripsi belum mendukung karakter simbol, angka, serta spasi. Pesan harus terdiri dari huruf alfabet saja agar proses berjalan lancar.
- Validasi input dan pengelolaan error masih bisa ditingkatkan untuk menghadapi berbagai kemungkinan penggunaan nyata (*real-world usage*).

### Saran Pengembangan

Apabila proyek ini dikembangkan lebih lanjut, berikut beberapa saran pengembangan:

- **Peningkatan UI/UX:** Antarmuka pengguna masih sederhana dan belum optimal secara estetika maupun kenyamanan pengguna (*user experience*).
- **Pembuatan Matriks Kunci Otomatis:** Fitur yang memungkinkan pengguna membuat sendiri matriks kunci enkripsi dan invers dekripsinya secara otomatis, baik secara acak maupun berdasarkan algoritma tertentu.
- **Integrasi ke API/Chatbot:** Penulis juga mempertimbangkan pengembangan aplikasi ini ke dalam bentuk *chatbot* yang dapat diintegrasikan dengan platform komunikasi seperti WhatsApp, sehingga pengguna dapat mengirim dan menerima pesan terenkripsi secara langsung melalui obrolan.

## KESIMPULAN DAN PENUTUP

Melalui tugas akhir semester ini, penulis berhasil merancang dan mengembangkan sebuah prototipe aplikasi mobile sederhana yang mampu melakukan proses enkripsi dan dekripsi menggunakan algoritma *Hill Cipher*. Aplikasi ini dibangun menggunakan Flutter dan memanfaatkan konsep matriks dari mata kuliah *Aljabar Linear dan Matriks*, sehingga tidak hanya memenuhi capaian pembelajaran mata kuliah *Desain Pemrograman Mobile*, tetapi juga menerapkan integrasi antar disiplin ilmu.

Hasil pengujian menunjukkan bahwa aplikasi mampu menjalankan fungsi utama dengan baik dan konsisten, terutama dalam mengubah pesan teks menjadi bentuk terenkripsi dan mengembalikannya ke bentuk semula. Aplikasi ini dapat menjadi cikal bakal dari sistem komunikasi aman berbasis kriptografi yang sederhana, dan bermanfaat untuk menjaga kerahasiaan pesan pengguna.

Namun demikian, aplikasi ini masih memiliki keterbatasan, di antaranya belum mendukung karakter selain huruf alfabet, serta pengaturan matriks kunci yang masih terbatas pada nilai default. Dari sini, terbuka ruang pengembangan lebih lanjut, seperti peningkatan UI/UX, otomatisasi pembuatan matriks kunci, hingga integrasi dalam bentuk chatbot atau API untuk digunakan pada platform komunikasi populer seperti WhatsApp.

Sebagai penutup, penulis berharap proyek ini dapat menjadi langkah awal dalam membangun ketertarikan mahasiswa terhadap pengembangan aplikasi mobile yang tidak hanya interaktif, tetapi juga memiliki nilai fungsional dan keamanan informasi. Kritik dan saran yang membangun sangat penulis harapkan demi penyempurnaan proyek ini di masa mendatang.