

## PENGAMANAN KATA SANDI AKUN DENGAN METODE *AFFINE CIPHER*

### *ACCOUNT PASSWORD SECURITY WITH AFFINE CIPHER METHOD*

Ade Novia Rahma<sup>1</sup>

<sup>1</sup>Program Studi Matematika, Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau  
[Email: [adenoviarahma\\_mufti@yahoo.co.id](mailto:adenoviarahma_mufti@yahoo.co.id)]

Received Sep 6<sup>th</sup> 2022; Accepted Dec 30<sup>th</sup> 2022; Published Dec 30<sup>th</sup> 2022;

#### Abstrak

Pada saat ini kesadaran keamanan akun sangat minim. Keahlian para hacker saat ini juga semakin berkembang. Metode *Affine Cipher* merupakan metode yang tepat untuk mengamankan kata sandi akun dan menjadikan kata sandi akun tidak mudah dikenal. Hasil akhir dari penelitian ini pasangan huruf yang sudah terbentuk tidak ada kemungkinan lain yang akan terbentuk, sehingga meningkatkan keamanan akun.

**Kata Kunci:** *Cipherteks, Plainteks, Affine Cipher, Kata Sandi*

#### Abstract

*At this time, the awareness of account security is minimal. The expertise of hackers is currently also growing. The Affine Cipher's Method is the proper method for securing making account password not easily recognized. The results of this research is that the letter pairs that have been formed are unlikely to be formed, thereby increasing account security.*

**Keywords:** *Cryptography, Affine Cipher, Password*

## 1. Pendahuluan

Dalam penggunaan penyimpanan aplikasi dengan menggunakan akun saat ini diperlukan kata sandi yang sulit untuk dikenal dan dilacak. Penggunaan kata sandi dengan kata-kata yang mudah ditebak sangat berbahaya untuk keamanan akun dan keamanan file yang penting atau dokumen yang disimpan oleh pihak tertentu.

Dokumen penting atau hasil karya orang lain yang jika diketahui oleh orang lain

dikhawatirkan akan disalah gunakan dan terjadi pemalsuan data yang dapat dilakukan oleh para hacker.

Menurut [1], *dictionary attack* adalah salah satu cara hacker untuk mengetahui password penting yang di miliki. *Dictionary attack* adalah suatu cara pencarian password menggunakan bantuan komputer dengan mencoba segala kemungkinan kombinasi huruf dan angka. Untuk

mempercepat penyerangan atau pencarian sandi, kombinasi huruf dan angka akan dirancang sesuai dengan kata-kata yang sering muncul sehingga membentuk suatu rumus.

Untuk menghindari hacker tersebut diperlukan metode untuk membuat kata sandi yang sulit dan tidak mudah dikenal yang dapat digunakan untuk kata samaran dalam penggunaan kata sandi. Metode itu adalah metode affine cipher. Menurut [2] affine cipher merupakan salah satu metode pada kriptografi. Affine cipher adalah metode yang mudah untuk menentukan kata samaran pada pesan dan tidak mudah dikenali oleh hacker.

Penelitian terdahulu yang berkaitan dengan metode affine cipher yaitu Pada tahun 2011, [3] membahas tentang implementasi kombinasi caesar dan affine cipher untuk keamanan data teks. Kemudian penelitian juga dibahas oleh [4] membahas sistem kriptografi untuk *text message* menggunakan metode affine cipher. Selanjutnya tahun 2013 [5] membahas *caesar cipher* dengan judul peran algoritma *caesar cipher* dalam membangun karakter akan kesadaran keamanan informasi. Pada tahun 2018, Fiqriardhi Kurniawan dan Rizky Pradana, membahas tentang algoritma affine cipher dalam pengamanan transfer data pada chatting berbasis android. [6]

Dari beberapa penelitian diatas, penulis tertarik melanjutkan penggunaan affine cipher dengan menggunakan karakter-karakter yang terdiri dari alfabet yang berjumlah 26 (dari A,B,C,D,...,Z) dan angka yang berjumlah 10 (dari 0,1,2,3,...,9) sehingga jumlah karakter yang digunakan adalah sebanyak 36.

## 2. Metode

Penelitian ini dilakukan untuk menentukan cara penggunaan kata samaran dalam password agar tidak mudah dikenal dan menjadikan akun dan file lebih aman. Metode yang digunakan adalah *Affine Cipher*, Adapun istilah penting dan rumus yang penulis gunakan dalam menyusun penelitian ini adalah :

**Definisi 1.** [1] Pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks (plaintext) atau teks jelas maknanya. Bentuk pesan yang tersandi disebut cipherteks (ciphertext) atau kriptogram (cryptogram).

**Definisi 2.** [1] Pengirim (sender) adalah entitas yang mengirim pesan kepada entita lainnya. Penerima (receiver) adalah entitas yang menerima pesan.

**Definisi 3.** [1] Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (encryption) atau *enciphering* (standard nama menurut ISO 7498-2) dan proses mengembalikan cipherteks menjadi plainteks semula dinamakan deskripsi (*description*) atau *deciphering* (standard nama menurut ISO 7498-2).

**Definisi 4.** [2] Algoritma kriptografi disebut juga *cipher* yaitu aturan untuk *eniphering* dan *dechipering*, atau fungsi matematika yang digunakan untuk enkripsi dan deskripsi. Kunci (*key*) adalah parameter yang digunakan untuk transformasi *eniphering* dan *dechipering*.

**Definisi 5.** [2] Sistem kriptografi (*cryptosystem*) adalah kumpulan yang terdiri dari algoritma

kriptografi, semua plainteks dan cipherteks yang mungkin, dan kunci (SCH96).

**Definisi 6.** [2] Penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan.

**Definisi 7.** [2] Kriptanalisis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalisis.

**Definisi 8.** [1] *Affine Cipher* adalah perluasan dari *Caesar Cipher*, yang mengalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran. Secara matematis enkripsi plainteks  $X$  menghasilkan cipherteks  $C$  dinyatakan dengan fungsi kongruen :

$$C \equiv ax + b \pmod{N}$$

Yang dalam hal ini  $n$  adalah ukuran alphabet,  $a$  adalah bilangan bulat yang harus relatif prima dengan  $n$  (jika tidak relatif prima, maka deskripsi tidak bisa dilakukan) dan  $b$  adalah jumlah pergeseran (*Caesar cipher* adalah khusus dari *affine cipher* dengan  $m = 1$ ). Untuk melakukan deskripsi, rumus diatas harus dipecahkan untuk memperoleh  $P$ . Solusi kekongruenan tersebut hanya ada jika inversi  $a \pmod{n}$ , dinyatakan  $a^{-1}$ , ada. Jika  $a^{-1}$  ada maka deskripsi dilakukan dengan persamaan

$$P \equiv a^{-1}(C - b) \pmod{n}$$

Keterangan :

$C$  = Chiperteks

$P$  = Plaintext

$a$  = bilangan bulat prima

$b$  = pergeseran

$N$  = jumlah total karakter ( batasi 36 karakter (A-Z, 0-9)

### 3. Hasil Dan Pembahasan

*Affine Cipher* untuk kata sandi merupakan kombinasi ide dari caesar cipher dan affine cipher. *Affine Cipher* yang digunakan untuk kata sandi bertujuan agar kata sandi tidak mudah dikenal dan tidak mudah di ambil oleh para hacker untuk disalah gunakan. Penggunaan karakter pada *Affine Cipher* itu tidak terbatas sehingga dapat digunakan berbagai macam karakter untuk pembentukan kata sandi. Disini akan menggunakan karakter-karakter yang terdiri dari alfabet yang berjumlah 26 (dari A,B,C,D,...,Z) dan angka yang berjumlah 10 (dari 0,1,2,3,...,9). Sehingga jumlah karakter yang digunakan adalah sebanyak 36.

Tabel 1. Penomoran Plaintext

Karakter	Urutan (Plaintext)	Karakter	Urutan (Plaintext)
A	0	0	26
B	1	1	27
C	2	2	28
D	3	3	29
E	4	4	30
F	5	5	31
G	6	6	32
H	7	7	33
I	8	8	34
J	9	9	35
K	10		
L	11		

M	12		
N	13		
O	1		
P	15		
Q	16		
R	17		
S	18		
T	19		
U	20		
V	21		
W	22		
X	23		
Y	24		
Z	25		

Dalam pembahasan ini akan diambil  $b = 5$  dan  $a = 5$  karna penggunaan affine cipher ini bilangan bulat yang harus relatif prima dimana  $b$  adalah jumlah pergeseran huruf dan  $a$  adalah bilangan bulat prima. Perlu diingat bahwa dalam penggunaan affine cipher ini dapat dimodifikasi dengan mengubah bilangan bulat prima (bukan hanya 5) dan jumlah pergeseran (bukan hanya 5) tetapi bisa menggunakan jumlah pergeseran yang lain dan bilangan prima yang lain.

$$N = 36$$

$$a = 5$$

$$b = 5$$

$$x = \text{Plaintext}$$

Berikut adalah pasangan huruf yang akan terbentuk antara huruf yang sebenarnya dengan huruf yang disamarkan dengan rumus Cipherteks yaitu :

$$C \equiv ax + b \pmod{N}$$

Rumus diatas digunakan untuk perluasan dari *Caesar Cipher* , yang mengalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran.

$$A \rightarrow X_1 = 0 \rightarrow C_1 \equiv 5.0 + 5$$

$$\pmod{36} \equiv 5 \pmod{36} \equiv 5 \text{ F}$$

$$B \rightarrow X_2 = 1 \rightarrow C_2 \equiv 5.1 + 5$$

$$\pmod{36} \equiv 10 \pmod{36} \equiv 10 \text{ K}$$

$$C \rightarrow X_3 = 2 \rightarrow C_3 \equiv 5.2 + 5$$

$$\pmod{36} \equiv 15 \pmod{36} \equiv 15 \text{ P}$$

$$D \rightarrow X_4 = 3 \rightarrow C_4 \equiv 5.3 + 5$$

$$\pmod{36} \equiv 20 \pmod{36} \equiv 20 \text{ U}$$

$$E \rightarrow X_5 = 4 \rightarrow C_5 \equiv 5.4 + 5$$

$$\pmod{36} \equiv 25 \pmod{36} \equiv 25 \text{ Z}$$

$$F \rightarrow X_6 = 5 \rightarrow C_6 \equiv 5.5 + 5$$

$$\pmod{36} \equiv 30 \pmod{36} \equiv 30 \text{ 4}$$

$$G \rightarrow X_7 = 6 \rightarrow C_7 \equiv 5.6 + 5$$

$$\pmod{36} \equiv 35 \pmod{36} \equiv 35 \text{ 9}$$

$$H \rightarrow X_8 = 7 \rightarrow C_8 \equiv 5.7 + 5$$

$$\pmod{36} \equiv 40 \pmod{36} \equiv 4 \text{ E}$$

$$I \rightarrow X_9 = 8 \rightarrow C_9 \equiv 5.8 + 5$$

$$\pmod{36} \equiv 45 \pmod{36} \equiv 9 \text{ J}$$

$$J \rightarrow X_{10} = 9 \rightarrow C_{10} \equiv 5.9 + 5$$

$$\pmod{36} \equiv 50 \pmod{36} \equiv 14 \text{ O}$$

$$K \rightarrow X_{11} = 10 \rightarrow C_{11} \equiv 5.10 + 5$$

$$\pmod{36} \equiv 55 \pmod{36} \equiv 19 \text{ T}$$

$$L \rightarrow X_{12} = 11 \rightarrow C_{12} \equiv 5.11 + 5$$

$$\pmod{36} \equiv 60 \pmod{36} \equiv 24 \text{ Y}$$

$$M \rightarrow X_{13} = 12 \rightarrow C_{13} \equiv 5.12 + 5$$

$$\pmod{36} \equiv 65 \pmod{36} \equiv 29 \text{ 3}$$

$$N \rightarrow X_{14} = 13 \rightarrow C_{14} \equiv 5.13 + 5$$

$$\pmod{36} \equiv 70 \pmod{36} \equiv 34 \text{ 8}$$

$O \rightarrow X_{15} = 14 \rightarrow C_{15} \equiv 5.14 + 5$   
 $(\text{mod } 36) \equiv 75 (\text{mod } 36) \equiv 3D$   
 $P \rightarrow X_{16} = 15 \rightarrow C_{16} \equiv 5.15 + 5$   
 $(\text{mod } 36) \equiv 80 (\text{mod } 36) \equiv 8I$   
 $Q \rightarrow X_{17} = 16 \rightarrow C_{17} \equiv 5.16 + 5$   
 $(\text{mod } 36) \equiv 85 (\text{mod } 36) \equiv 13N$   
 $R \rightarrow X_{18} = 17 \rightarrow C_{18} \equiv 5.17 + 5$   
 $(\text{mod } 36) \equiv 90 (\text{mod } 36) \equiv 18S$   
 $S \rightarrow X_{19} = 18 \rightarrow C_{19} \equiv 5.18 + 5$   
 $(\text{mod } 36) \equiv 95 (\text{mod } 36) \equiv 23X$   
 $T \rightarrow X_{20} = 19 \rightarrow C_{20} \equiv 5.19 + 5$   
 $(\text{mod } 36) \equiv 100 (\text{mod } 36) \equiv 28 2$   
 $U \rightarrow X_{21} = 20 \rightarrow C_{21} \equiv 5.20 + 5$   
 $(\text{mod } 36) \equiv 105 (\text{mod } 36) \equiv 33 7$   
 $V \rightarrow X_{22} = 21 \rightarrow C_{22} \equiv 5.21 + 5$   
 $(\text{mod } 36) \equiv 110 (\text{mod } 36) \equiv 2 C$   
 $W \rightarrow X_{23} = 22 \rightarrow C_{23} \equiv 5.22 + 5$   
 $(\text{mod } 36) \equiv 115 (\text{mod } 36) \equiv 7H$   
 $X \rightarrow X_{24} = 23 \rightarrow C_{24} \equiv 5.23 + 5$   
 $(\text{mod } 36) \equiv 120 (\text{mod } 36) \equiv 12M$   
 $Y \rightarrow X_{25} = 24 \rightarrow C_{25} \equiv 5.24 + 5$   
 $(\text{mod } 36) \equiv 125 (\text{mod } 36) \equiv 17R$   
 $Z \rightarrow X_{26} = 25 \rightarrow C_{26} \equiv 5.25 + 5$   
 $(\text{mod } 36) \equiv 130 (\text{mod } 36) \equiv 2W$   
 $0 \rightarrow X_{27} = 26 \rightarrow C_{27} \equiv 5.26 + 5$   
 $(\text{mod } 36) \equiv 135 (\text{mod } 36) \equiv 27 1$   
 $1 \rightarrow X_{28} = 27 \rightarrow C_{28} \equiv 5.27 + 5$   
 $(\text{mod } 36) \equiv 140 (\text{mod } 36) \equiv 32 6$   
 $2 \rightarrow X_{29} = 28 \rightarrow C_{29} \equiv 5.28 + 5$   
 $(\text{mod } 36) \equiv 145 (\text{mod } 36) \equiv 1 B$   
 $3 \rightarrow X_{30} = 29 \rightarrow C_{30} \equiv 5.29 + 5$   
 $(\text{mod } 36) \equiv 150 (\text{mod } 36) \equiv 6 G$   
 $4 \rightarrow X_{31} = 30 \rightarrow C_{31} \equiv 5.30 + 5$   
 $(\text{mod } 36) \equiv 155 (\text{mod } 36) \equiv 11 L$   
 $5 \rightarrow X_{32} = 31 \rightarrow C_{32} \equiv 5.31 + 5$

$(\text{mod } 36) \equiv 160 (\text{mod } 36) \equiv 16 Q$   
 $6 \rightarrow X_{33} = 32 \rightarrow C_{33} \equiv 5.32 + 5$   
 $(\text{mod } 36) \equiv 165 (\text{mod } 36) \equiv 21 V$   
 $7 \rightarrow X_{34} = 33 \rightarrow C_{34} \equiv 5.33 + 5$   
 $(\text{mod } 36) \equiv 170 (\text{mod } 36) \equiv 26 0$   
 $8 \rightarrow X_{35} = 34 \rightarrow C_{35} \equiv 5.34 + 5$   
 $(\text{mod } 36) \equiv 175 (\text{mod } 36) \equiv 31 5$   
 $9 \rightarrow X_{36} = 35 \rightarrow C_{36} \equiv 5.35 + 5$   
 $(\text{mod } 36) \equiv 180 (\text{mod } 36) \equiv 0 A$

Setelah mendapatkan Cipherteks akan dicari Plainteks untuk mengetahui apa huruf yang sebenarnya dari huruf yang disamarkan tersebut.

Dengan menggunakan rumus yaitu :

$$P \equiv m^{-1}(C - b) (\text{mod } n)$$

$F = C_1 = 5 \rightarrow P_1 \equiv 29(5-5)$   
 $(\text{mod } 36) = 0 = 0 (\text{mod } 36) = A$   
 $K = C_2 = 10 \rightarrow P_2 \equiv 29(10-5)$   
 $(\text{mod } 36) = 145 = 1 (\text{mod } 36) = B$   
 $P = C_3 = 15 \rightarrow P_3 \equiv 29(15-5)$   
 $(\text{mod } 36) = 290 = 2 (\text{mod } 36) = C$   
 $U = C_4 = 20 \rightarrow P_4 \equiv 29(20-5)$   
 $(\text{mod } 36) = 435 = 3 (\text{mod } 36) = D$   
 $Z = C_5 = 25 \rightarrow P_5 \equiv 29(25-5)$   
 $(\text{mod } 36) = 580 = 4 (\text{mod } 36) = E$   
 $4 = C_6 = 30 \rightarrow P_6 \equiv 29(30-5)$   
 $(\text{mod } 36) = 725 = 5 (\text{mod } 36) = F$   
 $9 = C_7 = 35 \rightarrow P_7 \equiv 29(35-5)$   
 $(\text{mod } 36) = 870 = 6 (\text{mod } 36) = G$   
 $E = C_8 = 4 \rightarrow P_8 \equiv 29(4-5)$   
 $(\text{mod } 36) = -29 = 7 (\text{mod } 36) = H$   
 $J = C_9 = 9 \rightarrow P_9 \equiv 29(9-5)$   
 $(\text{mod } 36) = 116 = 8 (\text{mod } 36) = I$   
 $O = C_{10} = 14 \rightarrow P_{10} \equiv 29(14-5)$   
 $(\text{mod } 36) = 261 = 9 (\text{mod } 36) = J$

$T=C_{11}=19 \rightarrow P_{11} \equiv 29(19-5)$   
 $(\text{mod } 36)=406=10(\text{mod } 36)= K$   
 $Y=C_{12}=24 \rightarrow P_{12} \equiv 29(24-5)$   
 $(\text{mod } 36)=551=11(\text{mod } 36)= L$   
 $3=C_{13}=29 \rightarrow P_{13} \equiv 29(29-5)$   
 $(\text{mod } 36)=696=12(\text{mod } 36)= M$   
 $8=C_{14}=34 \rightarrow P_{14} \equiv 29(34-5)$   
 $(\text{mod } 36)=841=13(\text{mod } 36)= N$   
 $D=C_{15}=3 \rightarrow P_{15} \equiv 29(3-5)$   
 $(\text{mod } 36)=-58=14(\text{mod } 36)= O$   
 $I=C_{16}=8 \rightarrow P_{16} \equiv 29(8-5)$   
 $(\text{mod } 36)=87=15(\text{mod } 36)= P$   
 $N=C_{17}=13 \rightarrow P_{17} \equiv 29(13-5)$   
 $(\text{mod } 36)=232=16(\text{mod } 36)= Q$   
 $S=C_{18}=18 \rightarrow P_{18} \equiv 29(18-5)$   
 $(\text{mod } 36)=377=17(\text{mod } 36)= R$   
 $X=C_{19}=23 \rightarrow P_{19} \equiv 29(23-5)$   
 $(\text{mod } 36)=522=18(\text{mod } 36)= S$   
 $2=C_{20}=28 \rightarrow P_{20} \equiv 29(28-5)$   
 $(\text{mod } 36)=667=19(\text{mod } 36)= T$   
 $7=C_{21}=33 \rightarrow P_{21} \equiv 29(33-5)$   
 $(\text{mod } 36)=812=20(\text{mod } 36)= U$   
 $C=C_{22}=2 \rightarrow P_{22} \equiv 29(2-5)$   
 $(\text{mod } 36)=-87=21(\text{mod } 36)= V$   
 $H=C_{23}=7 \rightarrow P_{23} \equiv 29(7-5)$   
 $(\text{mod } 36)=58=22(\text{mod } 36)= W$   
 $M=C_{24}=12 \rightarrow P_{24} \equiv 29(12-5)$   
 $(\text{mod } 36)=203=23(\text{mod } 36)= X$   
 $R=C_{25}=17 \rightarrow P_{25} \equiv 29(17-5)$   
 $(\text{mod } 36)=348=24(\text{mod } 36)= Y$   
 $W=C_{26}=22 \rightarrow P_{26} \equiv 29(22-5)$   
 $(\text{mod } 36)=493=25(\text{mod } 36)= Z$   
 $1=C_{27}=27 \rightarrow P_{27} \equiv 29(27-5)$   
 $(\text{mod } 36)=638=26(\text{mod } 36)= 0$   
 $6=C_{28}=32 \rightarrow P_{28} \equiv 29(32-5)$

$(\text{mod } 36)=783=27(\text{mod } 36)= 1$   
 $B=C_{29}=1 \rightarrow P_{29} \equiv 29(1-5)$   
 $(\text{mod } 36)=-116=28(\text{mod } 36)= 2$   
 $G=C_{30}=29 \rightarrow P_{30} \equiv 29(30-5)$   
 $(\text{mod } 36)=29=29(\text{mod } 36)= 3$   
 $L=C_{31}=29 \rightarrow P_{31} \equiv 29(31-5)$   
 $(\text{mod } 36)=174=30(\text{mod } 36)= 4$   
 $Q=C_{32}=29 \rightarrow P_{32} \equiv 29(32-5)$   
 $(\text{mod } 36)=319=31(\text{mod } 36)= 5$   
 $V=C_{33}=29 \rightarrow P_{33} \equiv 29(33-5)$   
 $(\text{mod } 36)=464=32(\text{mod } 36)= 6$   
 $0=C_{34}=29 \rightarrow P_{34} \equiv 29(34-5)$   
 $(\text{mod } 36)=609=33(\text{mod } 36)= 7$   
 $5=C_{35}=29 \rightarrow P_{35} \equiv 29(35-5)$   
 $(\text{mod } 36)=754=34(\text{mod } 36)= 8$   
 $A=C_{36}=29 \rightarrow P_{136} \equiv 29(36-5)$   
 $(\text{mod } 36)=-145=35(\text{mod } 36)= 9$

Dari hasil diatas diperoleh Cipherteks dan Plainteks. Cipherteks adalah huruf yang disamarkan kemudian Plainteks adalah mengembalikan huruf yang sudah disamarkan menjadi huruf yang sebenarnya. Perlu diingat bahwa A sudah pasti F, B sudah pasti K, C sudah pasti P, D sudah pasti U, E sudah pasti Z dan seterusnya, begitupun kebalikannya. Dalam pasangan huruf yang sudah terbentuk tidak ada kemungkinan lain yang akan terbentuk dengan ketetapan bahwa a adalah 5 dan b adalah 5 maka dari 36 karakter itu hanya akan terbentuk pasangan huruf seperti diatas.

Contoh 1 :

Password yang belum dienskripsi :

MATHUSR18C2019

Password yang sudah dienskripsi :  
3F2E7XS65B16A

Berikut adalah bentuk dari Cipherteks.

$$\begin{aligned}
 M \rightarrow X_{13} = 12 &\rightarrow C_{13} \\
 &\equiv 5.12 + 5 \pmod{36} \\
 &\equiv 65 \pmod{36} \equiv 29 = 3 \\
 A \rightarrow X_1 = 0 &\rightarrow C_1 \equiv 5.0 + 5 \pmod{36} \\
 &\equiv 5 \pmod{36} \equiv 5 = F \\
 T \rightarrow X_{20} = 19 &\rightarrow C_{20} \\
 &\equiv 5.19 + 5 \pmod{36} \\
 &\equiv 100 \pmod{36} \equiv 28 \\
 &= 2 \\
 H \rightarrow X_8 = 7 &\rightarrow C_8 \equiv 5.7 + 5 \pmod{36} \\
 &\equiv 40 \pmod{36} \equiv 4 = E \\
 U \rightarrow X_{21} = 20 &\rightarrow C_{21} \\
 &\equiv 5.20 + 5 \pmod{36} \\
 &\equiv 105 \pmod{36} \equiv 33 \\
 &= 7 \\
 S \rightarrow X_{19} = 18 &\rightarrow C_{19} \\
 &\equiv 5.18 + 5 \pmod{36} \\
 &\equiv 95 \pmod{36} \equiv 23 = X \\
 R \rightarrow X_{18} = 17 &\rightarrow C_{18} \\
 &\equiv 5.17 + 5 \pmod{36} \\
 &\equiv 90 \pmod{36} \equiv 18 = S \\
 1 \rightarrow X_{28} = 27 &\rightarrow C_{28} \\
 &\equiv 5.27 + 5 \pmod{36} \\
 &\equiv 140 \pmod{36} \equiv 32 \\
 &= 6 \\
 8 \rightarrow X_{35} = 34 &\rightarrow C_{35} \\
 &\equiv 5.34 + 5 \pmod{36} \\
 &\equiv 175 \pmod{36} \equiv 31 \\
 &= 5 \\
 2 \rightarrow X_{29} = 28 &\rightarrow C_{29} \\
 &\equiv 5.28 + 5 \pmod{36} \\
 &\equiv 145 \pmod{36} \equiv 1 = B
 \end{aligned}$$

$$\begin{aligned}
 0 \rightarrow X_{27} = 26 &\rightarrow C_{27} \\
 &\equiv 5.26 + 5 \pmod{36} \\
 &\equiv 135 \pmod{36} \equiv 27 \\
 &= 1 \\
 1 \rightarrow X_{28} = 27 &\rightarrow C_{28} \\
 &\equiv 5.27 + 5 \pmod{36} \\
 &\equiv 140 \pmod{36} \equiv 32 \\
 &= 6 \\
 9 \rightarrow X_{36} = 35 &\rightarrow C_{36} \\
 &\equiv 5.35 + 5 \pmod{36} \\
 &\equiv 180 \pmod{36} \equiv 0 = A
 \end{aligned}$$

Berikut adalah bentuk dari Plainteks.

$$\begin{aligned}
 3 = C_{13} = 29 &\rightarrow P_{13} \\
 &\equiv 29(29 - 5) \pmod{36} \\
 &= 696 = 12 \pmod{36} \\
 &= M \\
 F = C_1 = 5 &\rightarrow P_1 \\
 &\equiv 29(5 - 5) \pmod{36} \\
 &= 0 = A \\
 2 = C_{20} = 28 &\rightarrow P_{20} \\
 &\equiv 29(28 - 5) \pmod{36} \\
 &= 667 = 19 \pmod{36} \\
 &= T \\
 E = C_8 = 4 &\rightarrow P_8 \\
 &\equiv 29(4 - 5) \pmod{36} \\
 &= -29 = 7 \pmod{36} = H \\
 7 = C_{21} = 33 &\rightarrow P_{21} \\
 &\equiv 29(33 - 5) \pmod{36} \\
 &= 812 = 20 \pmod{36} \\
 &= U \\
 X = C_{19} = 23 &\rightarrow P_{19} \\
 &\equiv 29(23 - 5) \pmod{36} \\
 &= 522 = 18 \pmod{36} \\
 &= S
 \end{aligned}$$

$$\begin{aligned} S = C_{18} = 18 &\rightarrow P_{18} \\ &\equiv 29(18 - 5) \pmod{36} \\ &= 377 = 17 \pmod{36} \\ &= R \end{aligned}$$

$$\begin{aligned} 6 = C_{28} = 32 &\rightarrow P_{28} \\ &\equiv 29(32 - 5) \pmod{36} \\ &= 783 = 27 \pmod{36} \\ &= 1 \end{aligned}$$

$$\begin{aligned} 5 = C_{35} = 29 &\rightarrow P_{35} \\ &\equiv 29(35 - 5) \pmod{36} \\ &= 754 = 34 \pmod{36} \\ &= 8 \end{aligned}$$

$$\begin{aligned} B = C_{29} = 1 &\rightarrow P_{29} \\ &\equiv 29(1 - 5) \pmod{36} \\ &= -116 = 28 \pmod{36} \\ &= 2 \end{aligned}$$

$$\begin{aligned} 1 = C_{27} = 27 &\rightarrow P_{27} \\ &\equiv 29(27 - 5) \pmod{36} \\ &= 638 = 26 \pmod{36} \\ &= 0 \end{aligned}$$

$$\begin{aligned} 6 = C_{28} = 32 &\rightarrow P_{28} \\ &\equiv 29(32 - 5) \pmod{36} \\ &= 783 = 27 \pmod{36} \\ &= 1 \end{aligned}$$

$$\begin{aligned} A = C_{36} = 29 &\rightarrow P_{136} \\ &\equiv 29(36 - 5) \pmod{36} \\ &= -145 = 35 \pmod{36} \\ &= 9 \end{aligned}$$

Contoh 2 :

Password yang belum dienkripsi :

KONSTANTA357

Password yang sudah dienkripsi :

TD8X2F82FGQ0

Berikut adalah bentuk dari Cipherteks.

$$\begin{aligned} K \rightarrow X_{11} = 10 &\rightarrow C_{11} \\ &\equiv 5.10 + 5 \pmod{36} \\ &\equiv 55 \pmod{36} \equiv 19 = T \end{aligned}$$

$$\begin{aligned} O \rightarrow X_{15} = 14 &\rightarrow C_{15} \\ &\equiv 5.14 + 5 \pmod{36} \\ &\equiv 75 \pmod{36} \equiv 3 = D \end{aligned}$$

$$\begin{aligned} N \rightarrow X_{14} = 13 &\rightarrow C_{14} \\ &\equiv 5.13 + 5 \pmod{36} \\ &\equiv 70 \pmod{36} \equiv 34 = 8 \end{aligned}$$

$$\begin{aligned} S \rightarrow X_{19} = 18 &\rightarrow C_{19} \\ &\equiv 5.18 + 5 \pmod{36} \\ &\equiv 95 \pmod{36} \equiv 23 \\ &= X \end{aligned}$$

$$\begin{aligned} T \rightarrow X_{20} = 19 &\rightarrow C_{20} \\ &\equiv 5.19 + 5 \pmod{36} \\ &\equiv 100 \pmod{36} \equiv 28 \\ &= 2 \end{aligned}$$

$$\begin{aligned} A \rightarrow X_1 = 0 &\rightarrow C_1 \\ &\equiv 5.0 + 5 \pmod{36} \\ &\equiv 5 \pmod{36} \equiv 5 = F \end{aligned}$$

$$\begin{aligned} N \rightarrow X_{14} = 13 &\rightarrow C_{14} \\ &\equiv 5.13 + 5 \pmod{36} \\ &\equiv 70 \pmod{36} \equiv 34 \\ &= 8 \end{aligned}$$

$$\begin{aligned} T \rightarrow X_{20} = 19 &\rightarrow C_{20} \\ &\equiv 5.19 + 5 \pmod{36} \\ &\equiv 100 \pmod{36} \equiv 28 \\ &= 2 \end{aligned}$$

$$\begin{aligned} A \rightarrow X_1 = 0 &\rightarrow C_1 \\ &\equiv 5.0 + 5 \pmod{36} \\ &\equiv 5 \pmod{36} \equiv 5 \\ &= F \end{aligned}$$

$$\begin{aligned} 3 \rightarrow X_{30} = 29 &\rightarrow C_{30} \\ &\equiv 5.29 + 5 \pmod{36} \\ &\equiv 150 \pmod{36} \equiv 6 = G \end{aligned}$$



$$\begin{aligned} 5 \rightarrow X_{32} = 31 \rightarrow C_{32} \\ &\equiv 5.31 + 5 \pmod{36} \\ &\equiv 160 \pmod{36} \equiv 16 \\ &= Q \end{aligned}$$

$$\begin{aligned} 7 \rightarrow X_{34} = 33 \rightarrow C_{34} \\ &\equiv 5.33 + 5 \pmod{36} \\ &\equiv 170 \pmod{36} \equiv 26 \\ &= 0 \end{aligned}$$

Berikut adalah bentuk dari Plainteks.

$$\begin{aligned} T = C_{11} = 19 \rightarrow P_{11} \\ &\equiv 29(19 - 5) \pmod{36} \\ &= 406 = 10 \pmod{36} \\ &= K \end{aligned}$$

$$\begin{aligned} D = C_{15} = 3 \rightarrow P_{15} \\ &\equiv 29(3 - 5) \pmod{36} \\ &= -58 = 14 \pmod{36} \\ &= 0 \end{aligned}$$

$$\begin{aligned} 8 = C_{14} = 34 \rightarrow P_{14} \\ &\equiv 29(34 - 5) \pmod{36} \\ &= 841 = 13 \pmod{36} \\ &= N \end{aligned}$$

$$\begin{aligned} X = C_{19} = 23 \rightarrow P_{19} \\ &\equiv 29(23 - 5) \pmod{36} \\ &= 522 = 18 \pmod{36} \\ &= S \end{aligned}$$

$$\begin{aligned} 2 = C_{20} = 28 \rightarrow P_{20} \\ &\equiv 29(28 - 5) \pmod{36} \\ &= 667 = 19 \pmod{36} \\ &= T \end{aligned}$$

$$\begin{aligned} F = C_1 = 5 \rightarrow P_1 \\ &\equiv 29(5 - 5) \pmod{36} \\ &= 0 = 0 \pmod{36} = A \end{aligned}$$

$$\begin{aligned} 8 = C_{14} = 34 \rightarrow P_{14} \\ &\equiv 29(34 - 5) \pmod{36} \\ &= 841 = 13 \pmod{36} \\ &= N \end{aligned}$$

$$\begin{aligned} 2 = C_{20} = 28 \rightarrow P_{20} \\ &\equiv 29(28 - 5) \pmod{36} \\ &= 667 = 19 \pmod{36} \\ &= T \end{aligned}$$

$$\begin{aligned} F = C_1 = 5 \rightarrow P_1 \\ &\equiv 29(5 - 5) \pmod{36} \\ &= 0 = 0 \pmod{36} = A \end{aligned}$$

$$\begin{aligned} G = C_{30} = 29 \rightarrow P_{30} \\ &\equiv 29(30 - 5) \pmod{36} \\ &= 29 = 29 \pmod{36} = 3 \end{aligned}$$

$$\begin{aligned} Q = C_{32} = 29 \rightarrow P_{32} \\ &\equiv 29(32 - 5) \pmod{36} \\ &= 319 = 31 \pmod{36} \\ &= 5 \end{aligned}$$

$$\begin{aligned} 0 = C_{34} = 29 \rightarrow P_{34} \\ &\equiv 29(34 - 5) \pmod{36} \\ &= 609 = 33 \pmod{36} \\ &= 7 \end{aligned}$$

Contoh 3 :

Password yang belum dienkripsi :

VARIABELXYZ

Password yang sudah dienkripsi :

CFSJFKZYMRW

Berikut adalah bentuk dari Cipherteks.

$$\begin{aligned} V \rightarrow X_{22} = 21 \rightarrow C_{22} \\ &\equiv 5.21 + 5 \pmod{36} \\ &\equiv 110 \pmod{36} \equiv 2 = C \end{aligned}$$

$$\begin{aligned}
A \rightarrow X_1 = 0 \rightarrow C_1 & \\
& \equiv 5.0 + 5 \pmod{36} \\
& \equiv 5 \pmod{36} \equiv 5 = F \\
R \rightarrow X_{18} = 17 \rightarrow C_{18} & \\
& \equiv 5.17 + 5 \pmod{36} \\
& \equiv 90 \pmod{36} \equiv 18 = S \\
I \rightarrow X_9 = 8 \rightarrow C_9 & \\
& \equiv 5.8 + 5 \pmod{36} \\
& \equiv 45 \pmod{36} \equiv 9 = J \\
A \rightarrow X_1 = 0 \rightarrow C_1 & \\
& \equiv 5.0 + 5 \pmod{36} \\
& \equiv 5 \pmod{36} \equiv 5 = F \\
B \rightarrow X_2 = 1 \rightarrow C_2 & \\
& \equiv 5.1 + 5 \pmod{36} \\
& \equiv 10 \pmod{36} \equiv 10 = K \\
E \rightarrow X_5 = 4 \rightarrow C_5 & \\
& \equiv 5.4 + 5 \pmod{36} \\
& \equiv 25 \pmod{36} \equiv 25 = Z \\
L \rightarrow X_{12} = 11 \rightarrow C_{12} & \\
& \equiv 5.11 + 5 \pmod{36} \\
& \equiv 60 \pmod{36} \equiv 24 = Y \\
X \rightarrow X_{24} = 23 \rightarrow C_{24} & \\
& \equiv 5.23 + 5 \pmod{36} \\
& \equiv 120 \pmod{36} \equiv 12 \\
& = M \\
Y \rightarrow X_{25} = 24 \rightarrow C_{25} & \\
& \equiv 5.24 + 5 \pmod{36} \\
& \equiv 125 \pmod{36} \equiv 17 \\
& = R \\
Z \rightarrow X_{26} = 25 \rightarrow C_{26} & \\
& \equiv 5.25 + 5 \pmod{36} \\
& \equiv 130 \pmod{36} \equiv 2 \\
& = W
\end{aligned}$$

Berikut adalah bentuk dari Plainteks.

$$\begin{aligned}
C = C_{22} = 2 \rightarrow P_{22} & \\
& \equiv 29(2 - 5) \pmod{36} \\
& = -87 = 21 \pmod{36} \\
& = V \\
F = C_1 = 5 \rightarrow P_1 & \\
& \equiv 29(5 - 5) \pmod{36} \\
& = 0 = 0 \pmod{36} = A \\
S = C_{18} = 18 \rightarrow P_{18} & \\
& \equiv 29(18 - 5) \pmod{36} \\
& = 377 = 17 \pmod{36} \\
& = R \\
J = C_9 = 9 \rightarrow P_9 & \\
& \equiv 29(9 - 5) \pmod{36} \\
& = 116 = 8 \pmod{36} = I \\
F = C_1 = 5 \rightarrow P_1 & \\
& \equiv 29(5 - 5) \pmod{36} \\
& = 0 = 0 \pmod{36} = A \\
K = C_2 = 10 \rightarrow P_2 & \\
& \equiv 29(10 - 5) \pmod{36} \\
& = 145 = 1 \pmod{36} = B \\
Z = C_5 = 25 \rightarrow P_5 & \\
& \equiv 29(25 - 5) \pmod{36} \\
& = 580 = 4 \pmod{36} = E \\
Y = C_{12} = 24 \rightarrow P_{12} & \\
& \equiv 29(24 - 5) \pmod{36} \\
& = 551 = 11 \pmod{36} \\
& = L \\
M = C_{24} = 12 \rightarrow P_{24} & \\
& \equiv 29(12 - 5) \pmod{36} \\
& = 203 = 23 \pmod{36} \\
& = X
\end{aligned}$$

$$\begin{aligned}
 R = C_{25} = 17 &\rightarrow P_{25} \\
 &\equiv 29(17 - 5) \pmod{36} \\
 &= 348 = 24 \pmod{36} \\
 &= Y
 \end{aligned}$$

$$\begin{aligned}
 W = C_{26} = 22 &\rightarrow P_{26} \\
 &\equiv 29(22 - 5) \pmod{36} \\
 &= 493 = 25 \pmod{36} \\
 &= Z
 \end{aligned}$$

Contoh 4 :

Password yang belum dienkripsi :

DIFFERENSIALPQ

Password yang sudah dienkripsi :

UJ44ZSZ8XJFYIN

Berikut adalah bentuk dari Cipherteks.

$$\begin{aligned}
 D \rightarrow X_4 = 3 &\rightarrow C_4 \\
 &\equiv 5.3 + 5 \pmod{36} \\
 &\equiv 20 \pmod{36} \equiv 20 = U
 \end{aligned}$$

$$\begin{aligned}
 I \rightarrow X_9 = 8 &\rightarrow C_9 \\
 &\equiv 5.8 + 5 \pmod{36} \\
 &\equiv 45 \pmod{36} \equiv 9 = J
 \end{aligned}$$

$$\begin{aligned}
 F \rightarrow X_6 = 5 &\rightarrow C_6 \\
 &\equiv 5.5 + 5 \pmod{36} \\
 &\equiv 30 \pmod{36} \equiv 30 = 4
 \end{aligned}$$

$$\begin{aligned}
 F \rightarrow X_6 = 5 &\rightarrow C_6 \\
 &\equiv 5.5 + 5 \pmod{36} \\
 &\equiv 30 \pmod{36} \equiv 30 = 4
 \end{aligned}$$

$$\begin{aligned}
 E \rightarrow X_5 = 4 &\rightarrow C_5 \\
 &\equiv 5.4 + 5 \pmod{36} \\
 &\equiv 25 \pmod{36} \equiv 25 = Z
 \end{aligned}$$

$$\begin{aligned}
 R \rightarrow X_{18} = 17 &\rightarrow C_{18} \\
 &\equiv 5.17 + 5 \pmod{36} \\
 &\equiv 90 \pmod{36} \equiv 18 = S
 \end{aligned}$$

$$\begin{aligned}
 E \rightarrow X_5 = 4 &\rightarrow C_5 \\
 &\equiv 5.4 + 5 \pmod{36} \\
 &\equiv 25 \pmod{36} \equiv 25 = Z
 \end{aligned}$$

$$\begin{aligned}
 N \rightarrow X_{14} = 13 &\rightarrow C_{14} \\
 &\equiv 5.13 + 5 \pmod{36} \\
 &\equiv 70 \pmod{36} \equiv 34 = 8
 \end{aligned}$$

$$\begin{aligned}
 S \rightarrow X_{19} = 18 &\rightarrow C_{19} \\
 &\equiv 5.18 + 5 \pmod{36} \\
 &\equiv 95 \pmod{36} \equiv 23 = X
 \end{aligned}$$

$$\begin{aligned}
 I \rightarrow X_9 = 8 &\rightarrow C_9 \\
 &\equiv 5.8 + 5 \pmod{36} \\
 &\equiv 45 \pmod{36} \equiv 9 = J
 \end{aligned}$$

$$\begin{aligned}
 A \rightarrow X_1 = 0 &\rightarrow C_1 \\
 &\equiv 5.0 + 5 \pmod{36} \\
 &\equiv 5 \pmod{36} \equiv 5 = F
 \end{aligned}$$

$$\begin{aligned}
 L \rightarrow X_{12} = 11 &\rightarrow C_{12} \\
 &\equiv 5.11 + 5 \pmod{36} \\
 &\equiv 60 \pmod{36} \equiv 24 = Y
 \end{aligned}$$

$$\begin{aligned}
 P \rightarrow X_{16} = 15 &\rightarrow C_{16} \\
 &\equiv 5.15 + 5 \pmod{36} \\
 &\equiv 80 \pmod{36} \equiv 8 = I
 \end{aligned}$$

$$\begin{aligned}
 Q \rightarrow X_{17} = 16 &\rightarrow C_{17} \\
 &\equiv 5.16 + 5 \pmod{36} \\
 &\equiv 85 \pmod{36} \equiv 13 = N
 \end{aligned}$$

Berikut adalah bentuk dari Plainteks.

$$\begin{aligned}
 U = C_4 = 20 &\rightarrow P_4 \\
 &\equiv 29(20 - 5) \pmod{36} \\
 &= 435 = 3 \pmod{36} = D
 \end{aligned}$$

$$\begin{aligned}
 J = C_9 = 9 &\rightarrow P_9 \\
 &\equiv 29(9 - 5) \pmod{36} \\
 &= 116 = 8 \pmod{36} = I
 \end{aligned}$$

$$\begin{aligned}
4 = C_6 = 30 &\rightarrow P_6 \\
&\equiv 29(30 - 5) \pmod{36} \\
&= 725 = 5 \pmod{36} = F \\
4 = C_6 = 30 &\rightarrow P_6 \\
&\equiv 29(30 - 5) \pmod{36} \\
&= 725 = 5 \pmod{36} = F \\
Z = C_5 = 25 &\rightarrow P_5 \\
&\equiv 29(25 - 5) \pmod{36} \\
&= 580 = 4 \pmod{36} = E \\
S = C_{18} = 18 &\rightarrow P_{18} \\
&\equiv 29(18 - 5) \pmod{36} \\
&= 377 = 17 \pmod{36} \\
&= R \\
Z = C_5 = 25 &\rightarrow P_5 \\
&\equiv 29(25 - 5) \pmod{36} \\
&= 580 = 4 \pmod{36} = E \\
8 = C_{14} = 34 &\rightarrow P_{14} \\
&\equiv 29(34 - 5) \pmod{36} \\
&= 841 = 13 \pmod{36} \\
&= N \\
X = C_{19} = 23 &\rightarrow P_{19} \\
&\equiv 29(23 - 5) \pmod{36} \\
&= 522 = 18 \pmod{36} \\
&= S \\
J = C_9 = 9 &\rightarrow P_9 \\
&\equiv 29(9 - 5) \pmod{36} \\
&= 116 = 8 \pmod{36} = I \\
F = C_1 = 5 &\rightarrow P_1 \\
&\equiv 29(5 - 5) \pmod{36} \\
&= 0 = 0 \pmod{36} = A \\
Y = C_{12} = 24 &\rightarrow P_{12} \\
&\equiv 29(24 - 5) \pmod{36} \\
&= 551 = 11 \pmod{36} \\
&= L
\end{aligned}$$

Contoh 5 :

Password yang belum dienskripsi :  
GULAJAWA46

Password yang sudah dienskripsi :  
97YFOFHFLV

Berikut adalah bentuk dari Cipherteks.

$$\begin{aligned}
G \rightarrow X_7 = 6 &\rightarrow C_7 \\
&\equiv 5.6 + 5 \pmod{36} \\
&\equiv 35 \pmod{36} \equiv 35 = 9 \\
U \rightarrow X_{21} = 20 &\rightarrow C_{21} \\
&\equiv 5.20 + 5 \pmod{36} \\
&\equiv 105 \pmod{36} \equiv 33 \\
&= 7 \\
L \rightarrow X_{12} = 11 &\rightarrow C_{12} \\
&\equiv 5.11 + 5 \pmod{36} \\
&\equiv 60 \pmod{36} \equiv 24 = Y \\
A \rightarrow X_1 = 0 &\rightarrow C_1 \\
&\equiv 5.0 + 5 \pmod{36} \\
&\equiv 5 \pmod{36} \equiv 5 = F \\
J \rightarrow X_{10} = 9 &\rightarrow C_{10} \\
&\equiv 5.9 + 5 \pmod{36} \\
&\equiv 50 \pmod{36} \equiv 14 = O \\
A \rightarrow X_1 = 0 &\rightarrow C_1 \\
&\equiv 5.0 + 5 \pmod{36} \\
&\equiv 5 \pmod{36} \equiv 5 = F \\
W \rightarrow X_{23} = 22 & \\
&\rightarrow C_{235.22} + 5 \pmod{36} \\
&\equiv 115 \pmod{36} \equiv 7 = H \\
A \rightarrow X_1 = 0 &\rightarrow C_1 \\
&\equiv 5.0 + 5 \pmod{36} \\
&\equiv 5 \pmod{36} \equiv 5 = F \\
4 \rightarrow X_{31} = 30 &\rightarrow C_{31} \\
&\equiv 5.30 + 5 \pmod{36} \\
&\equiv 155 \pmod{36} \equiv 11 \\
&= L
\end{aligned}$$

$$\begin{aligned}
 6 \rightarrow X_{33} = 32 \rightarrow C_{33} \\
 &\equiv 5 \cdot 32 + 5 \pmod{36} \\
 &\equiv 165 \pmod{36} \equiv 21 \\
 &= V
 \end{aligned}$$

Berikut adalah bentuk dari Plainteks.

$$\begin{aligned}
 9 = C_7 = 35 \rightarrow P_7 \\
 &\equiv 29(35 - 5) \pmod{36} \\
 &= 870 = 6 \pmod{36} = G
 \end{aligned}$$

$$\begin{aligned}
 7 = C_{21} = 33 \rightarrow P_{21} \\
 &\equiv 29(33 - 5) \pmod{36} \\
 &= 812 = 20 \pmod{36} \\
 &= U
 \end{aligned}$$

$$\begin{aligned}
 Y = C_{12} = 24 \rightarrow P_{12} \\
 &\equiv 29(24 - 5) \pmod{36} \\
 &= 551 = 11 \pmod{36} \\
 &= L
 \end{aligned}$$

$$\begin{aligned}
 F = C_1 = 5 \rightarrow P_1 \\
 &\equiv 29(5 - 5) \pmod{36} \\
 &= 0 = 0 \pmod{36} = A
 \end{aligned}$$

$$\begin{aligned}
 O = C_{10} = 14 \rightarrow P_{10} \\
 &\equiv 29(14 - 5) \pmod{36} \\
 &= 261 = 9 \pmod{36} = J
 \end{aligned}$$

$$\begin{aligned}
 F = C_1 = 5 \rightarrow P_1 \\
 &\equiv 29(5 - 5) \pmod{36} \\
 &= 0 = 0 \pmod{36} = A
 \end{aligned}$$

$$\begin{aligned}
 H = C_{23} = 7 \rightarrow P_{23} \\
 &\equiv 29(7 - 5) \pmod{36} \\
 &= 58 = 22 \pmod{36} = W
 \end{aligned}$$

$$\begin{aligned}
 F = C_1 = 5 \rightarrow P_1 \\
 &\equiv 29(5 - 5) \pmod{36} \\
 &= 0 = 0 \pmod{36} = A
 \end{aligned}$$

$$\begin{aligned}
 L = C_{31} = 29 \rightarrow P_{31} \\
 &\equiv 29(31 - 5) \pmod{36} \\
 &= 174 = 30 \pmod{36} \\
 &= 4
 \end{aligned}$$

$$\begin{aligned}
 V = C_{33} = 29 \rightarrow P_{33} \\
 &\equiv 29(33 - 5) \pmod{36} \\
 &= 464 = 32 \pmod{36} \\
 &= 6
 \end{aligned}$$

Penggunaan *Affine Cipher* ini dapat dimodifikasi dengan mengubah bilangan bulat prima, jumlah karakter dan jumlah pergeseran. Namun, pada pembahasan ini menggunakan bilangan bulat prima 5, jumlah karakter 36 dan jumlah pergeseran 5 karna untuk memudah hasil kongruen. Dari hasil diatas dapat diketahui bahwa pasangan huruf yang belum di enkripsi dan yang sudah dienkripsi sudah mempunyai pasangan yang sesuai dan tidak ada kemungkinan pasangan huruf yang lain.

#### 4. Kesimpulan Dan Saran

Dari pembahasan diperoleh Cipherteks dan Plainteks. Cipherteks adalah huruf yang disamarkan kemudian Plainteks adalah mengembalikan huruf yang sudah disamarkan menjadi huruf yang sebenarnya, dimana bahwa A sudah pasti F, B sudah pasti K, C sudah pasti P, D sudah pasti U, E sudah pasti Z dan seterusnya, begitupun kebalikannya. Dalam pasangan huruf yang sudah terbentuk tidak ada kemungkinan lain yang akan terbentuk dengan ketetapan bahwa a adalah 5 dan b adalah 5 maka dari 36 karakter itu hanya akan terbentuk pasangan huruf seperti

dipembahasakan sehingga hacker dizaman ini sangat sulit mengenal kata sandi dan akan meningkatkan keamanan akun.

## Daftar Pustaka

- [1] R. Munir, “Kriptografi,” *Informatika, Bandung*, 2006.
- [2] R. Sadikin, “Kriptografi untuk keamanan jaringan,” 2020.
- [3] D. Rachmawati dan A. Candra, “Implementasi Kombinasi Caesar dan Affine Cipher untuk Keamanan Data Teks,” *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, vol. 1, no. 2, Nov 2015, doi: 10.26418/jp.v1i2.12587.
- [4] A. Septiarini dan H. Hamdani, “Sistem Kriptografi Untuk Text Message Menggunakan Metode Affine,” *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, vol. 6, no. 1, hlm. 50–53, 2016.
- [5] D. Seftyanto, M. Apriani, dan T. Haryanto, “Peran Algoritma Caesar Cipher Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi,” dalam *Seminar Nasional Matematika dan Pendidikan Matematika FMIPA UNY*, 2012, hlm. 883–890.
- [6] F. Kurniawan dan R. Pradana, “ALGORITMA AFFINE CIPHER DAN AES 256 DALAM PENGAMANAN TRANSFER DATA PADA CHATTING BERBASIS ANDROID,” *SKANIKA*, vol. 1, no. 1, hlm. 1–7, 2018.
- [7] M. P. Sukirman, “Teori Himpunan”.
- [8] T. Limbong, P. Manullang, dan E. Napitupulu, “Dikte Test Applications (IMLA) Using Computer Assisted Instruction (CAI) Model,” *Int. J. Eng. Res. Technol*, vol. 6, no. 10, hlm. 384–388, 2017.