No.: Date.:

KSA (Key Scheduling Algorithm)

Inisialisasi : $S_0 = S_1 \cdots S_{255} = 255$

Key = Saputra1 → length key = 8

Iterasi ke - 0

$i = 0, j = 0, S = 115$

$j = (j + S[i] + K[i \bmod \text{length}(K)]) \bmod 256$

$= (0 + 0 + K[0 \bmod 8]) \bmod 256$

$= (0 + K[0]) \bmod 256$

$= (0 + 115) \bmod 256$

$= 115 \bmod 256$

$= 115$

Swap = S[i], S[j] = S[0], S[115]

S = 115, 2, 3, 4, 5, 6, 7 ..., 114, 0, 116, ..., 255

Iterasi ke - 1

$i = 1, j = 115, a = 97$

$j = (j + S[i] + K[i \bmod \text{length}(K)]) \bmod 256$

$= (115 + 1 + K[i \bmod \text{length } 8]) \bmod 256$

$= (116 + K[i]) \bmod 256$

$= (116 + 97) \bmod 256$

$= 213 \bmod 256$

$= 213$

No. :

Date. :

Swap = S[i], S[j] = S[1], S[213]

S = 115, 213, 3, 4, 5 ..., 114, 0, 116, ..., 212, 1, 214, ... 255

Iterasi ke-2

i = 2, j = 213, P = 112

j = (j + S[i] + K[i mod length[K]]) mod 256

= (213 + 2 + K[2 mod length 8]) mod 256

= (215 + K[2]) mod 256

= (215 + 112) mod 256

= 327 mod 256

= 327 ⇒ j = 71

Swap = S[i], S[j] = S[2], S[71]

S = 115, 213, 71, 3, 4, 5 ..., 70, 2, 72, ... 114, 0, 116, ..., 212, 1, 214 ... 255

No.: Date.:

PRGA (Pseudo Random Generation Algorithm)

Plaintext = 200gg

* Iterasi ke-1

i = 0, j = 0

for idx = 0 to length (P) - 1 do
= 0 to len (S) - 1 do
= 0 to 4 do

i = (i + 1) mod 256
= (0 + 1) mod 256
= 1

j = (j + S[i]) mod 256
= (0 + 213) mod 256
= 213 mod 256
= 213

swap = S[i], S[j] = S[1], S[213]
t = (S[i] + S[j]) mod 256
= (1 + 213) mod 256
= 214 mod 256
= 214

u = S[t] => S[214]

No. : Date. :

C = u ⊕ p(0)
= 214 ⊕ 2
⇒ Binary ⇒ 214 ⇒ 11010110
2 ⇒ 00110010 ⊕
11100100 ⇒ 228
⇒ ä

* Iterasi Ke-2

i = 1, j = 213

for index = 0 to 4
i = (i + 1) mod 256
= (1+1) mod 256
= 2 mod 256
= 2

j = (j + S[i]) mod 256
= (213 + S[2]) mod 256
= (213 + 71) mod 256
= 284 mod 256
= 284

t = (S[i] + S[j]) mod 256
= (S[2] + S[284]) mod 256
= (71 + 284) mod 256
= 99 mod 256

No. :

Date. :

$$
\begin{aligned}
4 &= S(t) \\
&= S[99] \\
&= 99
\end{aligned}
$$

$$
\begin{aligned}
C &= 4 \oplus P[1] \\
&= 99 \oplus 0 \\
&\Rightarrow 01100011 \\
&\quad\ 00110000 \ \oplus \\
&\quad\ 01010011 \rightarrow \text{Chr} \Rightarrow S \text{ (kapital)}
\end{aligned}
$$