

Nama : Arya Pratama

NIM : F1620061

Kelas : Ganjil

Kriptografi

Algoritma : key scheduling Algoritma (KSA)

Kunci : saputra1, $\text{len}(k) = 8$

Array S : [0, 1, 2, 3, 4, 5, 6, 7, 8, ..., 100, 101, 102, 103, ..., 253, 254, 255]

\Rightarrow literasi Pertama $\rightarrow i = 0$ [0, 08, 80, ..., 8, 32, 12, 8, ..., 100, 101, 102, 103] = 2 posisi

$j = 0$

$\Rightarrow j = (j + s[i] + k[i \bmod \text{len}(k)]) \bmod 256$

$$= (0 + 0 + k[0 \% 8]) \% 256$$

$$= (k[0]) \% 256$$

$= ("s") \% 256 \Rightarrow$ nilai desimal dari "s" = 115

$$= 115 \% 256$$

$$j = 115$$

swap ($s[i], s[j]$)

swap ($s[0], s[115]$)

Array S = [115, 1, 2, 3, 4, 5, 6, 7, ..., 110, 111, 112, 113, 114, 0, 116, ..., 199, 200, 201, 202, 203, 204, 205, ..., 250, 251, 252, 253, 254, 255]

\Rightarrow literasi kedua $\rightarrow i = 1$

$j = 115, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255]$

$\Rightarrow j = (j + s[i] + k[i \% \text{len}(k)]) \% 256$

$$= (115 + s[1] + k[1 \% 8]) \% 256$$

$$= (115 + 1 + k[1]) \% 256$$

$= (115 + 1 + 97) \% 256 = (116 + 97) \% 256 \Rightarrow$ desimal dm "a" = 97

$$= (116 + 97) \% 256$$

$$= 213 \% 256$$

$$j = 213$$

swap ($s[i], s[j]$)

swap ($s[1], s[213]$)

Array S = [115, 213, 1, 2, 3, 4, 5, 6, 7, ..., 112, 113, 114, 0, 116, 117, ..., 210, 211, 212, 213, 214, ..., 250, 251, 252, 253, 254, 255]

\Rightarrow literasi ketiga $\rightarrow i = 2$

$$j = 213$$

$$\begin{aligned} \Rightarrow j &= (j + s[i] + k[i \% \text{len}(k)]) \% 256 \\ &= (213 + s[2] + k[2 \% 8]) \% 256 \\ &= (213 + 2 + k[2]) \% 256 \\ &= (215 + "p") \% 256 \Rightarrow \text{desimal dari } "p" = 112 \\ &= (215 + 112) \% 256 \\ &= 327 \% 256 \end{aligned}$$

$$j = 71$$

swap $(s[i], s[j])$

swap $(s[2], s[7])$

Array $s = [115, 213, 71, 3, A, 5, 6, 7, \dots, 69, 70, 2, 72, \dots, 112, 113, 114, 0, 116, \dots, 216, 211, 212, 1, 214, \dots, 250, 251, 252, 253, 254, 255]$

\Rightarrow literasi keempat $\rightarrow i = 3$

$$j = 71$$

$$\begin{aligned} \Rightarrow j &= (j + s[i] + k[i \% \text{len}(k)]) \% 256 \\ &= (71 + s[3] + k[3 \% 8]) \% 256 \\ &= (71 + 3 + k[3]) \% 256 \\ &= (74 + "u") \% 256 \Rightarrow \text{desimal dari } "u" = 117 \\ &= (74 + 117) \% 256 \\ &= 191 \% 256 \end{aligned}$$

$$j = 191$$

swap $(s[i], s[j])$

swap $(s[3], s[17])$

Array $s = [115, 213, 71, 191, 4, 5, 6, 7, \dots, 69, 70, 2, 72, 73, \dots, 112, 113, 114, 0, 116, \dots, 189, 190, 3, 192, \dots, 210, 211, 212, 1, 214, 215, 250, 251, 252, 253, 254, 255]$

\Rightarrow literasi kelima $\rightarrow i = 4$

$$j = 191$$

$$\begin{aligned} \Rightarrow j &= (j + s[i] + k[i \% \text{len}(k)]) \% 256 \\ &= (191 + s[4] + k[4 \% 8]) \% 256 \\ &= (191 + 4 + k[4]) \% 256 \\ &= (195 + "t") \% 256 \Rightarrow \text{desimal } "t" = 16 \\ &= (195 + 16) \% 256 \\ &= 211 \% 256 \\ &= 55 \end{aligned}$$

~~swap $(s[i], s[j])$~~

Swar ($s[i], s[j]$)

Sweat ($s[0], s[55]$)

Array $s = [115, 213, 71, 191, 55, 174, 6, 7, 8, \dots, 83, 59, 4, 56, 57, \dots, 69, 70, 2, 72, 73, \dots, 113, 114, 0, 116, 117, \dots, 189, 190, 3, 192, \dots, 211, 212, 1, 214, \dots, 250, 251, 252, 253, 254, 255]$

\Rightarrow literasi keenam $\rightarrow i = 5$

$$j = 55$$

$$\Rightarrow j = (j + s[i] + k[i \% \text{len}(k)]) \% 256$$

$$= (55 + s[5] + k[5 \% 8]) \% 256$$

$$= (55 + 5 + k[5]) \% 256$$

$$= (60 + "r") \% 256 \Rightarrow \text{desimal } "r" = 114$$

$$= (60 + 114) \% 256$$

$$= 174 \% 256$$

$$= 174$$

Array $s = [115, 213, 71, 191, 55, 174, 6, 7, 8, \dots, 83, 59, 4, 56, 57, \dots, 69, 70, 2, 72, 73, \dots, 113, 114, 0, 116, 117, \dots, 172, 173, \cancel{174}, 5, 175, 176, \dots, 189, 190, 3, 192, 193, \dots, 211, 212, 1, 214, 215, \dots, 250, 251, 252, 253, 254, 255]$

\Rightarrow literasi ketujuh $\rightarrow i = 6$

$$j = 174$$

$$\Rightarrow j = (j + s[i] + k[i \% \text{len}(k)]) \% 256$$

$$= (174 + s[6] + k[6 \% 8]) \% 256$$

$$= (174 + 6 + k[6]) \% 256$$

$$= (180 + \cancel{a}) \% 256 \Rightarrow \text{desimal } "a" = 97$$

$$= (180 + 97) \% 256$$

$$= 277 \% 256$$

$$= 21$$

Sweat ($s[i], s[j]$)

Sweat ($s[0], s[21]$)

Array $s = [115, 213, 71, 191, 55, 174, 21, 7, 8, \dots, 19, 20, 6, 22, 23, \dots, 83, 82, 59, 4, 56, 57, \dots, 69, 70, 2, 72, 73, \dots, 113, 114, 0, 116, 117, \dots, 172, 173, 5, 175, 176, \dots, 189, 190, 3, 192, 193, \dots, 211, 212, 1, 214, 215, \dots, 250, 251, 252, 253, 254, 255]$

\Rightarrow literasi kodingan $\rightarrow i = 7$ $([E]2 \cdot [J]2) \text{ now}$
 $j = 21$ $([T]2 \cdot [A]2) \text{ now}$
 $\Rightarrow j = (j + s[i] + k[i \% \ln(1e)]) \% 256$ $[0, 255] \rightarrow [0, 255]$
 $= (21 + s[7] + k[7 \% 8]) \% 256$ $[0, 255]$
 $= (21 + 7 + k[7]) \% 256$ $[0, 255]$
 $= (20 + "1") \% 256 \Rightarrow \text{desimal "1"} = 49$
 $= (20 + 49) \% 256$ $70 \leftarrow \text{marvel}$
 $= 77 \% 256$ $77 = 0$
 $= 77$ $228 \leftarrow [m] \text{ now } 87 \leftarrow [t]2 + 0 = 87$
 Swap ($s[i]$, $s[j]$)
 Swap ($s[7]$, $s[77]$)

Array $s = [115, 213, 71, 191, 85, 21, 77, 0, \dots, 19, 20, 6, 22, 23, \dots, 53, 54, 41, 56,$
 $57, \dots, 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, 0, 113, 114, 0, 116, 117, \dots,$
 $172, 173, 8, 175, 176, \dots, 109, 190, 3, 192, 193, 194, 211, 212, 1, 214, 215, \dots$
 $280, 281, 282, 283, 284, 285]$

$\Rightarrow i = \text{debut} - \text{now} \leftarrow$
 $i = 6$
 $228 \leftarrow [([0] \text{ now } 87)4 + [t]2 + 0] = 64$
 $228 \leftarrow ([0 \text{ now } 87]4 + [t]2 + 0) =$
 $228 \leftarrow [0]4 + 0 + 0 = 0$
 $sp = 2^0 \leftarrow \text{debut} (= 228 \leftarrow [0]4 + 0) = 1$
 $228 \leftarrow [0]4 + 0 = 0$
 $228 \leftarrow 0 = 0$

$([E]2 \cdot [J]2) \text{ now}$

$([E]2 \cdot [J]2) \text{ now}$

$([E]2 \cdot [J]2) \text{ now}$