KSA

KEY = saputra 1

index	Value	Tabe ascii
0	s	115
1	a	97
2	p	112
3	u	117
4	t	116
5	r	114
6	a	97
7	1	49

S = [0, 1, 2, 3, 4, 5, 6, ..., 256, 255]

untuk i = 0, J = 0

J = (i + S[i] + k[i mod length(k)]) mod 256

= (0 + 0 + k[0 mod 8]) mod 256

= (0 + k[0]) mod 256

= (0 + 115) mod 256

= 115 mod 256 = 115

Swap(S[i], S[J]) = Swap(S[0], S[115])

S = [115, 1, 2, 3, ..., 114, 0, 116, ..., 255]

Date

untuk i = 1, J = 115

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

= (115 + 1 + K*[1 mod 0.] mod 256

= (116 + K[1]) mod 256

= (116 + 97) mod 256

= 213 mod 256 = 213

swap (S[1], S[J]) = swap [S[1], S[213]])

S = [115, 213, 2, 3, ..., 212, ~~1~~ 214, ..., 256]

untuk i = 2, J = 213

J = (J + S[i] + k[i mod length(k)]] mod 256

= [213 + 2 + k[2 mod 0] mod 256

= (~~213~~ 215 + k[2]) mod 256

= (215 + 112) mod 256

= 327 mod 256 = 71

swap (S[2], S[71])

S = [115, 213, 71, 3, ... 70, 2, ~~72~~, 255] untuk i = 3, J = 71

J = (J + S[i] + k[i mod length(k)]) mod 256

= (71 + 3 + k(3 mod 8)) mod 256

= (74 + k[3]) mod 256

= (74 + 117) mod 256

= 191 mod 256 = 191

swap (S[3], S[191])

S = [115, 213, 71, 191, 4, ... , 190, 3, 192, .. 255]

untuk i = 4, J = 191

J = (191 + 4 + k(4 mod 8)) mod 256

= (195 + k[4]) mod 256

= (195 + 116) mod 256

= 311 mod 256 = 55

swap (S[4], S[55])

S = [115, 213, 71, 191, 55, 5, ... , 54, 4, 56, ... , 255]

untuk i = 5, J = 55

J = (55 + 5 + k[5 mod 8]) mod 256

= (60 + 114) mod 256

= 174 mod 256 = 174

Date

swap (s[i], s[j] = swap [s[5], S[179]]

untuk i = 6, j = 174

j = (174 + 6 + k[6 mod 0]) mod 256

= (180 + 97) mod 256

= 277 mod 256 = 21

swap (s[6], s[21])

S = [115, 213, 71, 191, 55, 174, 21, 7, ... , 246, 22,

255]

untuk i = 7, j = 21

j = (21 + 7 + k[7 mod 0) mod 256

= (28 + 49) mod 256

= 77 mod 256 = 77

swap (S[7] S [77])

S = [115, 213, 71, 199, 55, 174, 21, 77, 8, ...

76, 7, 78, ... , 255]

lakukan iterasi hingga iterasi k 255,
sehingga :

s = [115, 213, 71, 45, 31, 174, 20, 74, 235, 105, 17,
44, 211, 101, 150, 244, 93, 207, 121, 129, 59,
144, 79, 119, 35, 34, 39, 13, 156, 2, 14, 99,
165, 187, 186, 118, 6, 113, 169, 171, 15, 47,
255, 134, 250, 32, 57, 8, 117, 106, 109, 29, 3
143, 64, 100, 42, 18, 30, 56, 9, 7, 196, 0, 173,
242, 205, 78, 137, 133, 249, 176, 87, 83, 194,
204, 22, 40, 132, 196, 233, 193, 195, 189, 89, 96
212, 159, 103, 28, 23, 124, 230, 236, 188, 72
85, 82, 164, 46, 225, 44, 56, 247, 192, 86, 142
123, 1, 181, 149, 116, 215, 227, 198, 131, 231
184, 177, 36, 76, 180, 107, 130, 140, 251, 127,
95, 7, 51, 60, 259, 158, 102, 237, 98, 69
226, 26, 191, 38, 138, 139, 122, 16, 62, 19, 77
220, 153, 33, 152, 154, 9, 168, 21, 216,
232, 249 88, 148, 209, 228, 218, 175, 199
53 155, 178, 243, 234, 91, 166, 52, 239, 197
183, 254, 65, 157, 12, 120, 170, 224, 47, 60,
222, 108, 61, 160, 98, 14, 91, 126, 190, 68
125, 145, 27, 151, 163, 228, 223, 203, 85
45, 252, 192, 170, 172, 246, 63, 210, 238, 95

201, 81, 182, 219 162, 221, 110, 167, 141, 83,
179, 206, 245, 93, 241, 58, 147, 219, 53, 67
138, 37, 24, 109, 104, 168, 191, 120, 142, [84
11, 202, 240, 90, 80, 5, 73, 56 208, 200 25]

PRGA

Plaintext = 2086

Index	value	decimal
0	2	50
1	0	48
2	8	56
3	6	54

untuk i=0, j=0

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

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

= (0+S[1]) mod 256

= (0+S 213) mod 256

= 213

swap (S[i], S[j]) = swap(S[1], S[213])

S = [115, 201, 71, ..., 75, 213, 81, ..., 25]

t = S[i] + S[j] = 158

u = S[t] = 198

c = u $\oplus$ P[index] = 168 = i

untuk i = 1, J = 213

i = (i+1) mod 256 = (1+1) mod 256 = 2

J = (J + S[i]) mod 256

= (213 + S[2]) mod 256

= (213 + 71) mod 256

= 284 mod 256 = 28

swap (S[i], S[J]) = swap (S[2], S[28])

S = [115, 201, 156, 49, ..., 13, 71, ..., 25]

t = S[i] + S[J] = 227

u = S[t] = 241

c = u $\oplus$ P[index] = 193 = Á

untuk i = 2, J = 28

i = (i+1) mod 256 = (2+1) mod 256 = 3

J = (28 + 49) mod 256

= (~~28+~~ 77) mod 256 = 77

swap (S[49], S[77])

S = [115, 201, 156, 146, 31, ..., 132, 49, 23, ... , 25]

t = S[i] + S[J] = 195

U = S[t] = 145

C = U ⊕ P [index] = 165 = ¥

untuk i = 3, J = 77

i = (i + 1) mod 256 (3+1) mod 256 = 4

J = (J + S[i]) mod 256

= (77 + S[4]) mod 256

= 108 mod 256 = 08

=

Swap (S[4], S[108])

S = [115, 201, 156, 146, 149, ..., 181, 31, 116, ..., 25]

t = S[i] + S[J] = 186

U = S[t] = 70

C = U ⊕ P[index] = 116 = t