

# 128비트 블록 암호알고리즘 (SEED)

1998년 10월 29일



한국정보보호센터

# 128비트 블록 암호알고리즘(SEED)

## 1. 연산기호의 정의

- $a \oplus b$  : a Exclusive-Or b
- $\boxplus$  :  $(a+b) \bmod 2^{32}$

## 2. 알고리즘 전체 구성도

128비트 블록을 2개의 64비트 블록 ( $L_0(64), R_0(64)$ )으로 나누어 16라운드를 수행한 후 최종 128비트 출력을 ( $L_{16}(64), R_{16}(64)$ )라 하자.

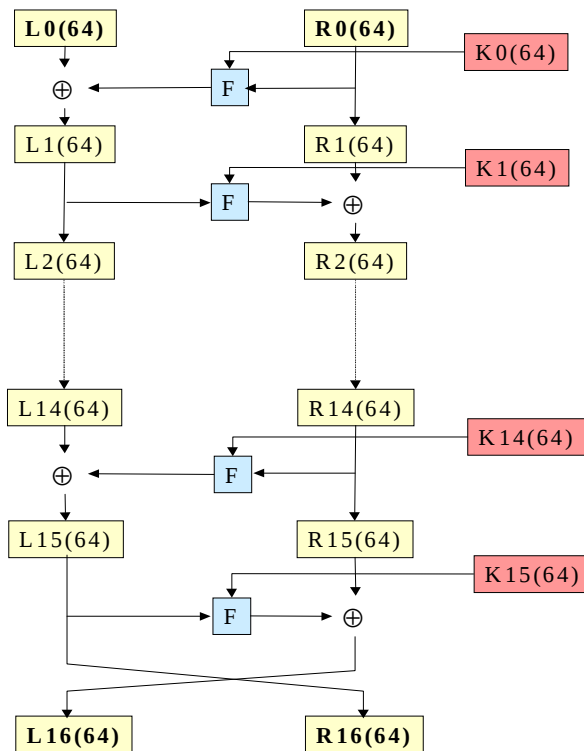


그림 2 > 전체 구조도

### 3. F함수

$$A' = C$$

$$B' = D$$

$$C' = G[G\{(C \oplus K_0) \oplus (D \oplus K_1)\} \oplus G\{(D \oplus K_1) \oplus G\{(C \oplus K_0) \oplus (D \oplus K_1)\}\}]$$

$$D' = G[G\{(C \oplus K_0) \oplus (D \oplus K_1)\} \oplus G\{(D \oplus K_1) \oplus G\{(C \oplus K_0) \oplus (D \oplus K_1)\}\}] \oplus G[(D \oplus K_1) \oplus G\{(C \oplus K_0) \oplus (D \oplus K_1)\}]$$

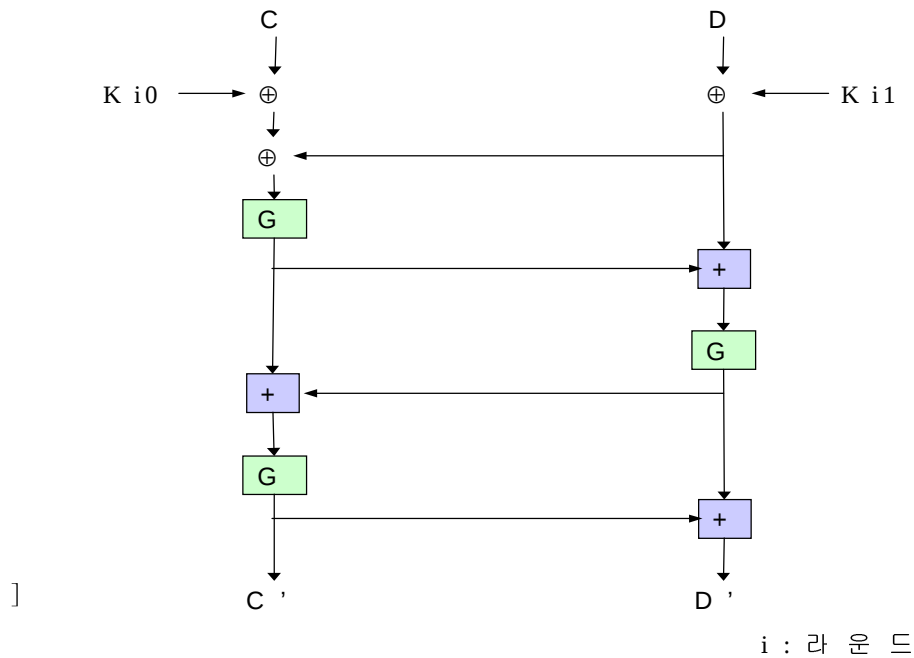


그림 3 > F-함수 구조도

### 4. G 함수

G함수의 입력 32비트를 4개의 8비트 블록으로  $(X_3, X_2, X_1, X_0)$ 으로 분할하여 2개의 S Box를  $(S_2, S_1, S_2, S_1)$  순서로 적용시키고, 4비트 왼쪽 회전변환 후, 4개의 8비트 블록  $(Z_3, Z_2, Z_1, Z_0)$ 을 생성한다.

$$\begin{aligned} Y_3 &= (Y_{31}, Y_{30}) = S_2(X_3) & Z_3 &= (Y_{30}, Y_{21}) \\ Y_2 &= (Y_{21}, Y_{20}) = S_1(X_2) & Z_2 &= (Y_{20}, Y_{11}) \\ Y_1 &= (Y_{11}, Y_{10}) = S_2(X_1) & Z_1 &= (Y_{10}, Y_{01}) \\ Y_0 &= (Y_{01}, Y_{00}) = S_1(X_0) & Z_0 &= (Y_{00}, Y_{31}) \end{aligned}$$

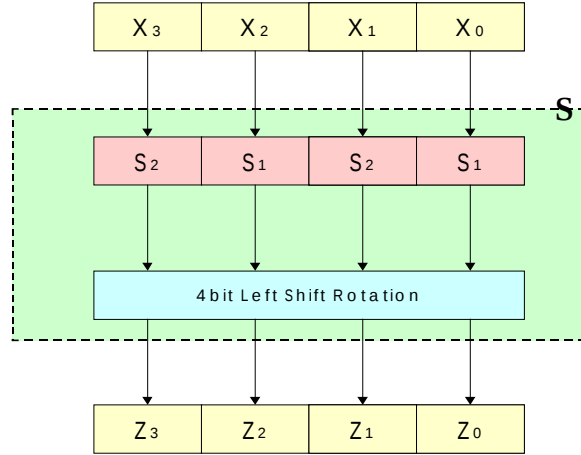


그림 4 > G-함수 구조도

## 5. S-Box들에 사용된 부울함수

진단사함수  $x^n$ ,  $0 \leq n \leq 255$ 에서 DC 및 LC 특성이 가장 우수한 2개의  $n = 247, 251$ 을 선택하고,  $GF(2^8)$ 상에서의 지수승을 구하기 위해  $GF(2^8)$ 상에서의 모든 원소를 원시원소 (primitive element)  $\alpha$ 의 멱승으로 표현하자.

(사용된 원시원소는  $\alpha = p(x) = x^8 + x^6 + x^5 + x + 1$ )

### 5.1 선형변환

지수함수의 입력  $x=0$ 이 출력 0,  $x=1$ 이 출력 1으로 고정되는 것을 방지하기 위하여 지수함수를  $y = Ax^n \oplus b$ 로 선형변환한다.

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

각 S-Box에 사용된 행렬은 A의 두 행을 교환하여  $A^{(1)}$ ,  $A^{(2)}$  사용한다.

( $A^{(1)}$  = A의 2와 6행을 교환,  $A^{(2)}$  = A의 1와 8행을 교환)

$$S_1(x) = A^{(1)} x^{247} \oplus b_1$$

$$b_1 = (1, 0, 0, 1, 0, 1, 0, 1)^T, b_2 = (0, 0, 0, 1, 1, 1, 0, 0)^T \text{라 하고, } S_2(x) = A^{(2)} x^{251} \oplus b_2$$

| $i$ | $x^{247}$ | $i$ | $x^{247}$ | $i$ | $x^{247}$ | $i$ | $x^{247}$ | $i$ | $x^{247}$ | $i$ | $x^{247}$ | $i$ | $x^{247}$ | $i$ | $x^{247}$ |
|-----|-----------|-----|-----------|-----|-----------|-----|-----------|-----|-----------|-----|-----------|-----|-----------|-----|-----------|
| 0   | 169       | 1   | 133       | 2   | 214       | 3   | 211       | 4   | 84        | 5   | 29        | 6   | 172       | 7   | 37        |
| 8   | 93        | 9   | 67        | 10  | 24        | 11  | 30        | 12  | 81        | 13  | 252       | 14  | 202       | 15  | 99        |
| 16  | 40        | 17  | 68        | 18  | 32        | 19  | 157       | 20  | 224       | 21  | 226       | 22  | 200       | 23  | 23        |
| 24  | 165       | 25  | 143       | 26  | 3         | 27  | 123       | 28  | 187       | 29  | 19        | 30  | 210       | 31  | 238       |
| 32  | 112       | 33  | 140       | 34  | 63        | 35  | 168       | 36  | 50        | 37  | 221       | 38  | 246       | 39  | 116       |
| 40  | 236       | 41  | 149       | 42  | 11        | 43  | 87        | 44  | 92        | 45  | 91        | 46  | 189       | 47  | 1         |
| 48  | 36        | 49  | 28        | 50  | 115       | 51  | 152       | 52  | 16        | 53  | 204       | 54  | 242       | 55  | 217       |
| 56  | 44        | 57  | 231       | 58  | 114       | 59  | 131       | 60  | 155       | 61  | 209       | 62  | 134       | 63  | 201       |
| 64  | 96        | 65  | 80        | 66  | 163       | 67  | 235       | 68  | 13        | 69  | 182       | 70  | 158       | 71  | 79        |
| 72  | 183       | 73  | 90        | 74  | 198       | 75  | 120       | 76  | 166       | 77  | 18        | 78  | 175       | 79  | 213       |
| 80  | 97        | 81  | 195       | 82  | 180       | 83  | 65        | 84  | 82        | 85  | 125       | 86  | 141       | 87  | 8         |
| 88  | 31        | 89  | 153       | 90  | 0         | 91  | 25        | 92  | 4         | 93  | 83        | 94  | 247       | 95  | 225       |
| 96  | 253       | 97  | 118       | 98  | 47        | 99  | 39        | 100 | 176       | 101 | 139       | 102 | 14        | 103 | 171       |
| 104 | 162       | 105 | 110       | 106 | 147       | 107 | 77        | 108 | 105       | 109 | 124       | 110 | 9         | 111 | 10        |
| 112 | 191       | 113 | 239       | 114 | 243       | 115 | 197       | 116 | 135       | 117 | 20        | 118 | 254       | 119 | 100       |
| 120 | 222       | 121 | 46        | 122 | 75        | 123 | 26        | 124 | 6         | 125 | 33        | 126 | 107       | 127 | 102       |
| 128 | 2         | 129 | 245       | 130 | 146       | 131 | 138       | 132 | 12        | 133 | 179       | 134 | 126       | 135 | 208       |
| 136 | 122       | 137 | 71        | 138 | 150       | 139 | 229       | 140 | 38        | 141 | 128       | 142 | 173       | 143 | 223       |
| 144 | 161       | 145 | 48        | 146 | 55        | 147 | 174       | 148 | 54        | 149 | 21        | 150 | 34        | 151 | 56        |
| 152 | 244       | 153 | 167       | 154 | 69        | 155 | 76        | 156 | 129       | 157 | 233       | 158 | 132       | 159 | 151       |
| 160 | 53        | 161 | 203       | 162 | 206       | 163 | 60        | 164 | 113       | 165 | 17        | 166 | 199       | 167 | 137       |
| 168 | 117       | 169 | 251       | 170 | 218       | 171 | 248       | 172 | 148       | 173 | 89        | 174 | 130       | 175 | 196       |
| 176 | 255       | 177 | 73        | 178 | 57        | 179 | 103       | 180 | 192       | 181 | 207       | 182 | 215       | 183 | 184       |
| 184 | 15        | 185 | 142       | 186 | 66        | 187 | 35        | 188 | 145       | 189 | 108       | 190 | 219       | 191 | 164       |
| 192 | 52        | 193 | 241       | 194 | 72        | 195 | 194       | 196 | 111       | 197 | 61        | 198 | 45        | 199 | 64        |
| 200 | 190       | 201 | 62        | 202 | 188       | 203 | 193       | 204 | 170       | 205 | 186       | 206 | 78        | 207 | 85        |
| 208 | 59        | 209 | 220       | 210 | 104       | 211 | 127       | 212 | 156       | 213 | 216       | 214 | 74        | 215 | 86        |
| 216 | 119       | 217 | 160       | 218 | 237       | 219 | 70        | 220 | 181       | 221 | 43        | 222 | 101       | 223 | 250       |
| 224 | 227       | 225 | 185       | 226 | 177       | 227 | 159       | 228 | 94        | 229 | 249       | 230 | 230       | 231 | 178       |
| 232 | 49        | 233 | 234       | 234 | 109       | 235 | 95        | 236 | 228       | 237 | 240       | 238 | 205       | 239 | 136       |
| 240 | 22        | 241 | 58        | 242 | 88        | 243 | 212       | 244 | 98        | 245 | 41        | 246 | 7         | 247 | 51        |
| 248 | 232       | 249 | 27        | 250 | 5         | 251 | 121       | 252 | 144       | 253 | 106       | 254 | 42        | 255 | 154       |

Figure 1:  $S_1$ -Box

| $i$ | $x^{251}$ | $i$ | $x^{251}$ | $i$ | $x^{251}$ | $i$ | $x^{251}$ | $i$ | $x^{251}$ | $i$ | $x^{251}$ | $i$ | $x^{251}$ | $i$ | $x^{251}$ |
|-----|-----------|-----|-----------|-----|-----------|-----|-----------|-----|-----------|-----|-----------|-----|-----------|-----|-----------|
| 0   | 56        | 1   | 232       | 2   | 45        | 3   | 166       | 4   | 207       | 5   | 222       | 6   | 179       | 7   | 184       |
| 8   | 175       | 9   | 96        | 10  | 85        | 11  | 199       | 12  | 68        | 13  | 111       | 14  | 107       | 15  | 91        |
| 16  | 195       | 17  | 98        | 18  | 51        | 19  | 181       | 20  | 41        | 21  | 160       | 22  | 226       | 23  | 167       |
| 24  | 211       | 25  | 145       | 26  | 17        | 27  | 6         | 28  | 28        | 29  | 188       | 30  | 54        | 31  | 75        |
| 32  | 239       | 33  | 136       | 34  | 108       | 35  | 168       | 36  | 23        | 37  | 196       | 38  | 22        | 39  | 244       |
| 40  | 194       | 41  | 69        | 42  | 225       | 43  | 214       | 44  | 63        | 45  | 61        | 46  | 142       | 47  | 152       |
| 48  | 40        | 49  | 78        | 50  | 246       | 51  | 62        | 5   | 165       | 53  | 249       | 54  | 13        | 55  | 223       |
| 56  | 216       | 57  | 43        | 58  | 102       | 69  | 122       | 60  | 39        | 61  | 47        | 62  | 241       | 63  | 114       |
| 64  | 66        | 65  | 212       | 66  | 65        | 67  | 192       | 68  | 115       | 69  | 103       | 70  | 172       | 71  | 139       |
| 72  | 247       | 73  | 173       | 74  | 128       | 75  | 31        | 76  | 202       | 77  | 44        | 78  | 170       | 79  | 52        |
| 80  | 210       | 81  | 11        | 82  | 238       | 83  | 233       | 84  | 93        | 85  | 148       | 86  | 24        | 87  | 248       |
| 88  | 87        | 89  | 174       | 90  | 8         | 91  | 197       | 82  | 19        | 93  | 205       | 94  | 134       | 95  | 185       |
| 96  | 255       | 97  | 125       | 98  | 193       | 99  | 49        | 100 | 245       | 101 | 138       | 102 | 106       | 103 | 177       |
| 104 | 209       | 105 | 32        | 106 | 215       | 107 | 2         | 108 | 34        | 109 | 4         | 110 | 104       | 111 | 113       |
| 112 | 7         | 113 | 219       | 114 | 157       | 115 | 153       | 116 | 97        | 117 | 190       | 118 | 230       | 119 | 89        |
| 120 | 221       | 121 | 81        | 122 | 144       | 123 | 220       | 124 | 154       | 125 | 163       | 126 | 171       | 127 | 208       |
| 128 | 129       | 129 | 15        | 130 | 71        | 131 | 26        | 132 | 227       | 133 | 236       | 134 | 141       | 135 | 191       |
| 136 | 150       | 137 | 123       | 138 | 92        | 139 | 162       | 140 | 161       | 141 | 99        | 142 | 35        | 143 | 77        |
| 144 | 200       | 145 | 158       | 146 | 156       | 147 | 58        | 148 | 12        | 149 | 46        | 150 | 186       | 151 | 110       |
| 152 | 159       | 153 | 90        | 154 | 242       | 155 | 146       | 156 | 243       | 157 | 73        | 158 | 120       | 159 | 204       |
| 160 | 21        | 161 | 251       | 162 | 112       | 163 | 117       | 164 | 127       | 165 | 53        | 166 | 16        | 167 | 3         |
| 168 | 100       | 169 | 109       | 170 | 198       | 171 | 116       | 172 | 213       | 173 | 180       | 174 | 234       | 175 | 9         |
| 176 | 118       | 177 | 25        | 178 | 254       | 179 | 64        | 180 | 18        | 181 | 224       | 182 | 189       | 183 | 5         |
| 184 | 250       | 185 | 1         | 186 | 240       | 187 | 42        | 188 | 94        | 189 | 169       | 190 | 86        | 191 | 67        |
| 192 | 133       | 193 | 20        | 194 | 137       | 195 | 155       | 196 | 176       | 197 | 229       | 198 | 72        | 199 | 121       |
| 200 | 151       | 201 | 252       | 202 | 30        | 203 | 130       | 204 | 33        | 205 | 140       | 206 | 27        | 207 | 95        |
| 208 | 119       | 209 | 84        | 210 | 178       | 211 | 29        | 212 | 37        | 213 | 79        | 214 | 0         | 215 | 70        |
| 216 | 237       | 217 | 88        | 218 | 82        | 219 | 235       | 220 | 126       | 221 | 218       | 222 | 201       | 223 | 253       |
| 224 | 48        | 225 | 149       | 226 | 101       | 227 | 60        | 228 | 182       | 229 | 228       | 230 | 187       | 231 | 124       |
| 232 | 14        | 233 | 80        | 234 | 57        | 235 | 38        | 236 | 50        | 237 | 132       | 238 | 105       | 239 | 147       |
| 240 | 55        | 241 | 231       | 242 | 36        | 243 | 164       | 244 | 203       | 245 | 83        | 246 | 10        | 247 | 135       |
| 248 | 217       | 249 | 76        | 250 | 131       | 251 | 143       | 252 | 206       | 253 | 59        | 254 | 74        | 255 | 183       |

표 2 > S<sub>2</sub> Box

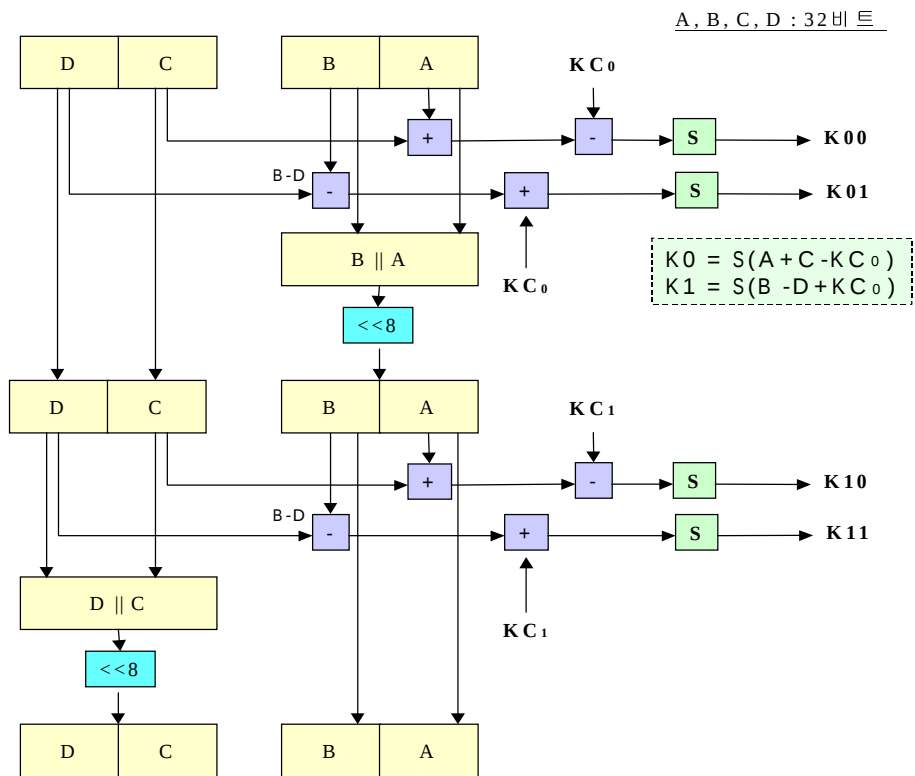
## 6. 키생성 알고리즘

각 라운드에 사용되는 키는 다음과 같은 방식으로 생성한다.

- ① 128비트 입력키를 32비트 4개의 조각으로 쪼갠 후(A, B, C, D),
- ②  $K0 = S(A+C-KC0)$   
 $K1 = S(B+KC0-D)$  (단, KC : 라운드상수)로 1라운드 키 및 2라운드 키를 생성하고,
- ③  $B||A=(B||A)<<8$
- ④  $K2 = S(A+C-KC1)$   
 $K3 = S(B+KC1-D)$  (단, KC : 라운드상수)로 3라운드 키 및 4라운드 키를 생성하고,
- ⑤  $D||C=(D||C)<<8$
- ⑥  $K4 = S(A+C-KC2)$   
 $K5 = S(B+KC2-D)$  (단, KC : 라운드상수)로 5라운드 키 및 6라운드 키를 생성하고,
- ⑦ 이후 16라운드 키 생성까지 반복한다.

| 상 수             |                  |
|-----------------|------------------|
| KC0 =0x9e3779b9 | KC8=0x3779b99e   |
| KC1 =0x3c6cf373 | KC9 =0x6cf3733c  |
| KC2=0x78dde6e6  | KC10 =0xdde6e678 |
| KC3 =0xf1bbcdcc | KC11 =0xbbcdccf1 |
| KC4 =0xc3779b99 | KC12 =0x779b3    |
| KC5 =0xc6ef3733 | KC13 =0xef3733c6 |
| KC6 =0x8dde6267 | KC14 =0xde6e678d |
| KC7 =0x1bbcdccf | KC15 =0xbcdccf1b |

표 3 > 키생성알고리즘 사용 상수



- 
- 
- 

그림 5 > 키생성알고리즘 구조도