128비트 블록 암호알고리즘(SEED) 표준

이인수 · 한국정보보호센터 기술개발부 기반기술팀

1. 배경

세계각국은 인터넷을 이용한 전자상거래를 21세기 국가경쟁력을 결정하는 중요요소로 간주하여, 국가 전략적으로 전자상거래의 활성화를 위해 많은 노력을 경주하고 있다. 우리나라도 1998년 5월 전자상거래 종합대책을 발표하는 등 새로운 세계경제 질서에 동참하여 정보사회로의 진입을 위해 적극적으로 대처하고 있다. 이의 일환으로 인터넷을 이용한 전자상거래가 활성화되기 위해 필수적으로 요구되는 안전성 · 신뢰성을 확보하기 위하여 한국정보보호센터에서는 국내 관련 전문가들과 공동으로 전자상거래에서 활용 가능한 128비트 블록 암호알고리즘(SEED) 초안을 개발하였고, 공개 검증과정을 거쳐 안전성과 성능이 개선된 최종 수정안을 개발('98. 12.) 완료하였다. 특히, 암호알고리즘(SEED) 활용과 관련한 산업체의 현실적 문제점 분석 및 해결방안을 모색하고, 국내 암호산업 육성을 꾀하고자 한국정보통신기술협회(TTA) 표준으로 제안하여 표준화를 추진하고 있다.

2. 설계기준

가. 전체구조

- ○ 데이터 처리단위 : 8, 16, 32비트 모두 가능
- ○ 암 · 복호화 방식 : 블록 암호방식
- ○ 입 · 출력문의 크기 : 128비트
- ○ 입력키의 크기 : 128비트
- ○ 안전성 : 차분공격/선형공격에 대하여 안전하도록 설계
- ○ 효율성 : 암 · 복호화 속도는 3중 DES이상

〈표 1〉 추진일정

일시	내용
'97. 9. 1. ~ '98. 9. 1.	128비트 블록 암호알고리즘(SEED) 초안 개발 완료
'98. 9. 2. ~ '98. 9. 30.	SEED 초안 1차 자체 평가 완료
'98. 10. 29. ~ '99. 2. 15.	공개검증을 위한 의견수렴 공고 및 알고리즘 공개
'98. 11. 6. ~ '98. 12. 31.	SEED 공개검증 위원회 구성 및 운영(4회)
'99. 2. 1.	SEED 수정안 및 분석보고서 공고
'99. 2. 26.	128비트 블록 암호알고리즘(SEED) 개발 결과 발표 및 활성화를 위한 공청회
	소스코드 1차 배포
'99. 3.	TTA 표준 제안
'99. 6. 29. ~ 현재	표준 최종안 공고 및 소스코드 재배포
'99. 9월 초	표준 제정(TTA)

○ 구조 : Feistel 구조
○ 내부함수 : SPN 구조이며, 비선형함수를 Look-up 테이블로 변형하여 사용
○ 라운드 수 : 안전성은 키전수 조사공격에 필요한 계산복잡도 및 평문·암호문 쌍(2^{128})이하가 되지 않아야 하며, 효율성 요구조건을 만족하여야 함
○ 키생성 알고리즘 : 알고리즘의 라운드 동작과 동시에 암·복호화 라운드 키가 생성될 수 있도록 설계

나. 안전성에 대한 설계조건

○ 안전성이 증명가능한 구조로 설계
○ 차분공격법(Differential Cryptanalysis, DC)에 대하여 안전하여야 한다.
○ 선형공격법(Linear Cryptanalysis, LC)에 대하여 안전하여야 한다.
○ 기타 공격방식(Higher Order DC, Related Key Attack 등)이 적용되기 어렵게 한다.
- Higher Order DC에 강하기 위하여 대수적 차수가 3이상인 부울함수를 사용한다.
- Related Key Attack에 강하기 위하여 Key Schedule에 비선형함수를 사용한다.

다. 효율성에 대한 설계조건

○ S/W로 구현시 3중 DES보다 고속이어야 한다.

라. SEED의 일반적 특징

○ 데이터 처리단위 : 8, 16, 32비트 모두 가능
○ 암·복호화 방식 : 블록 암호방식
○ 입·출력문의 크기 : 128비트
○ 입력키의 크기 : 128비트
○ 라운드 수 : 16라운드
○ 구조 : Feistel 구조
○ 내부함수
- 연산은 ⊞(모듈러 2^{32}에서의 덧셈), ⊕(비트별 배타적 논리합)만 사용
- 2개의 안전성이 입증된 S-Box 사용
- DC, LC에 대한 이론적 안전성 증명 가능
- 내부함수 F의 구조는 DES, MISTY등과 비교하여 우수함

3. 128비트 블록 암호알고리즘(SEED)

암호알고리즘은 암·복호화에 사용되는 키의 특성에 따라 암·복호화 키가 같은 대칭키 암호알고리즘과 암·복호화 키가 서로 다른 공개키 암호알고리즘으로 크게 구분할 수 있으며, 대칭키 암호알고리즘은 데이터 처리형식에 따라 스트림 암호알고리즘과 블록 암호알고리즘으로 나눌 수 있다. SEED는 대칭키 암호알고리즘으로, 블록단위로 메시지를 처리하는 블록 암호알고리즘이다.

대칭키 블록 암호알고리즘은 비밀성을 제공하는 암호시스템의 중요요소이다. n비트 블록 암호알고리즘이란 고정된 n비트 평문을 같은 길이의 n비트 암호문으로 바꾸는 함수를 말한다(n비트 : 블록크기). 이러한 변형과정에 암·복호키가 작용하여 암호화와 복호화를 수행한다.

블록 암호알고리즘은 대부분 Feistel 구조로 설계된다(예 : DES, FEAL, LOKI, MISTY, Blowfish, CAST, Twofish 등). Feistel 구조란 각각 t비트인 L_0, R_0 블록으로 이루어진 2t비트 평문 블록(L_0, R_0)이 r라운드($\gamma \geq 1$)를 거쳐 암호문 (L_γ, R_γ)으로 변환되는 반복구조를 말한다. 반복구조란 평문블록이 여러 라운드를 거쳐 암호화되는 과정을 말한다. 라운드 함수 $i(1 \leq i \leq r)$란 암호키 K로부터 유도된 각 서브키K_i(또는, 라운드 키라 불림)를 중요 입력으로 하여 $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$를 통해 $(L_{i-1}, R_{i-1}) \rightarrow (L_i^{K_i} R_i)$로 바꾸어 주는 함수를 말한다). 또한, 전체 알고리즘의 라운드 수는 요구되는 비도와 수행 효율성의 상호 절충적 관계에 의해

결정된다. 보통 Feistel 구조는 3라운드 이상이며, 짝수 라운드로 구성된다. 이러한 Feistel 구조는 ① 라운드 함수에 관계없이 역변환이 가능하며(즉, 암·복호화 과정이 같음), ② 두 번의 수행으로 블록간의 완전한 diffusion이 이루어지며, ③ 알고리즘의 수행속도가 빠르고, ④ H/W 및 S/W로 구현이 용이하고, 아직 구조상의 문제점이 발견되고 있지 않다는 장점을 지니고 있다.

〈표 2〉 SEED 기본사양 및 기능

기본사양	
전체구조	Feistel형
암호방식	블록암호방식
키길이	128비트
입·출력문 크기	128비트
라운드 수	16
기능	전자 데이터의 기밀성 기능 제공

가. 용어정의

(1) 평문 : 암호화되지 않은 원래의 정보
(2) 암호문 : 평문을 합당하게 푸는 방법을 모르는 사람에게는 알 수 없는 형태로 변환한 데이터
(3) 암호화 : 평문을 암호문으로 변환하는 과정
(4) 복호화 : 암호문을 평문으로 변환하는 과정
(5) 대칭키 암호알고리즘 : 암·복호화 키가 같은 암호알고리즘
(6) 블록 암호알고리즘 : 고정된 길이를 갖는 평문(암호문) 블록을 고정된 길이를 갖는 암호문(또는 평문) 블록으로 변환하는 함수
(7) 반복 블록 암호알고리즘 : 라운드 함수를 순차적으로 반복하여 암·복호화를 수행하는 블록 암호알고리즘
(8) Feistel 구조 : 각각 t비트인 L_0, R_0블록으로 이루어진 2t비트 평문 블록 (L_0, R_0)이 r라운드($\gamma \geq 1$)를 거쳐 암호문 (L_γ, R_γ)으로 변환되는 반복구조
(9) 라운드 함수 : 반복 블록 암호알고리즘의 각 라운드에서 사용되는 함수
(10) 라운드 키(서브키) : 라운드 함수에서 사용되는 키
(11) 암호키 : 평문 또는 암호문의 암·복호화에 사용되는 비밀정보

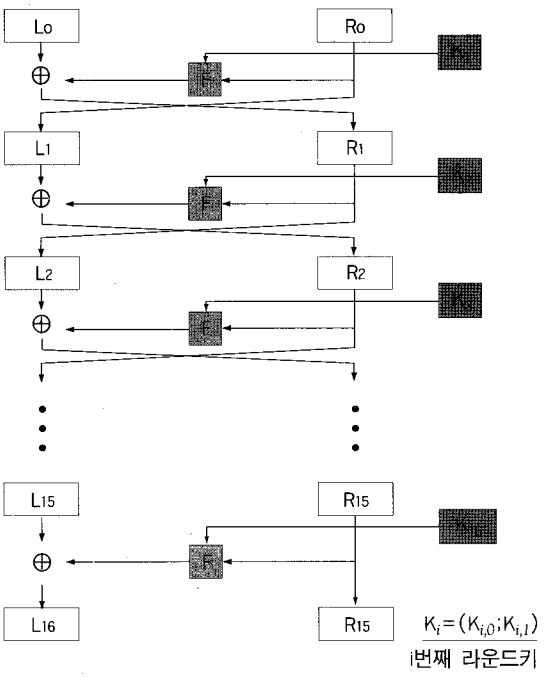
나. 기호와 표기

- a ⊕ b : 'a' bit-wise Exclusive-Or 'b'
- a ⊞ b : (a + b) mod 2^{32}
- a & b : 'a' bit-wise AND 'b'
- $X^{\ll s}$: X를 s비트 만큼 왼쪽으로 순환 이동하는 연산
- $X^{\gg s}$: X를 s비트 만큼 오른쪽으로 순환 이동하는 연산
- L_i : i 라운드에서 출력된 왼쪽 메시지 블록(64비트)
- R_i : i 라운드에서 출력된 오른쪽 메시지 블록(64비트)
- $K_i = (K_{i,0}, K_{i,1})$: i 라운드의 라운드 키(64비트)
- $K_{i,0}$: i 라운드 F 함수의 오른쪽 입력키(32비트)
- $K_{i,1}$: i 라운드 F 함수의 왼쪽 입력키(32비트)
- $X = (X_3 \| X_2 \| X_1 \| X_0)$: G함수의 입력값(32비트)
- $Y = (Y_3 \| Y_2 \| Y_1 \| Y_0)$: G함수에서 S-Box (S_1, S_2)의 출력값(32비트)
- $Z = (Z_3 \| Z_2 \| Z_1 \| Z_0)$: G함수의 출력값(32비트)
- m_i : 상수
- KC_i : 라운드 키 생성과정에서 사용되는 i+1 라운드 상수

다. 128비트 블록 암호알고리즘(SEED) 표준

1) 알고리즘 전체 구성도

본 알고리즘의 전체구조는 Feistel 구조로 이루어져 있으며, 128비트의 평문블록 단위당 128비트 키로부터 생성된 16개의 64비트 라운드 키를 입력으로 사용하여 총 16라운드를 거쳐 128비트 암호문 블록을 출력한다. 다음 (그림 1)은 SEED 알고리즘의 전체구조를 도식화한 것이다.



(그림 1) SEED 전체 구조도

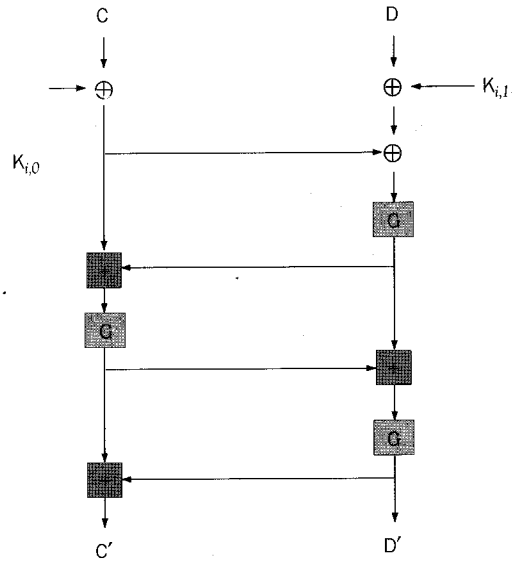
※ 128비트 입력 평문블록을 2개의 64비트 블록 ($L_0(64)$, $R_0(64)$)으로 나누어, 16개의 64비트 라운드 키를 이용하여 16라운드를 수행한 후, 최종 128비트 암호문 블록 ($L_{16}(64)$, $R_{16}(64)$)을 출력한다.

2) F 함수

Feistel 구조를 갖는 블록 암호알고리즘은 F 함수의 특성에 따라 구분될 수 있다. SEED의 F 함수는 수정된 64비트 Feistel 형태로 구성된다. F 함수는 각 32비트 블록 2개(C, D)를 입력받아, 32비트 블록 2개(C′, D′)를 출력한다. 즉, 암호화 과정에서 64비트 블록(C, D)와 64비트 라운드 키 $K_i=(K_{i,0};K_{i,1})$를 F 함수의 입력으로 처리하여 64비트 블록(C′, D′)을 출력한다.

(i : 라운드 수)

- $C' = G[G[G\{(C\oplus K_{i0})\oplus(D\oplus K_{i1})\}\boxplus(C\oplus K_{i0})]\boxplus G\{(C\oplus K_{i0})\oplus(D\oplus K_{i1})\}]\boxplus G[G\{(C\oplus K_{i0})\oplus(D\oplus K_{i1})\}\boxplus(C\oplus K_{i0})]$
- $D' = G[G[G\{(C\oplus K_{i0})\oplus(D\oplus K_{i1})\}\boxplus(C\oplus K_{i0})]\boxplus G\{(C\oplus K_{i0})\oplus(D\oplus K_{i1})\}]$



(그림 2) F-함수 구조도

3) G 함수

전체 G 함수는 다음과 같이 기술된다. :

$Y_3=S_2(X_3)$, $Y_2=S_1(X_2)$, $Y_1=S_2(X_1)$
$Y_0=S_1(X_0)$,

$Z_3 = (Y_0 \& m_3) \oplus (Y_1 \& m_0) \oplus (Y_2 \& m_1) \oplus (Y_3 \& m_2)$

$Z_2 = (Y_0 \& m_2) \oplus (Y_1 \& m_3) \oplus (Y_2 \& m_0) \oplus (Y_3 \& m_1)$

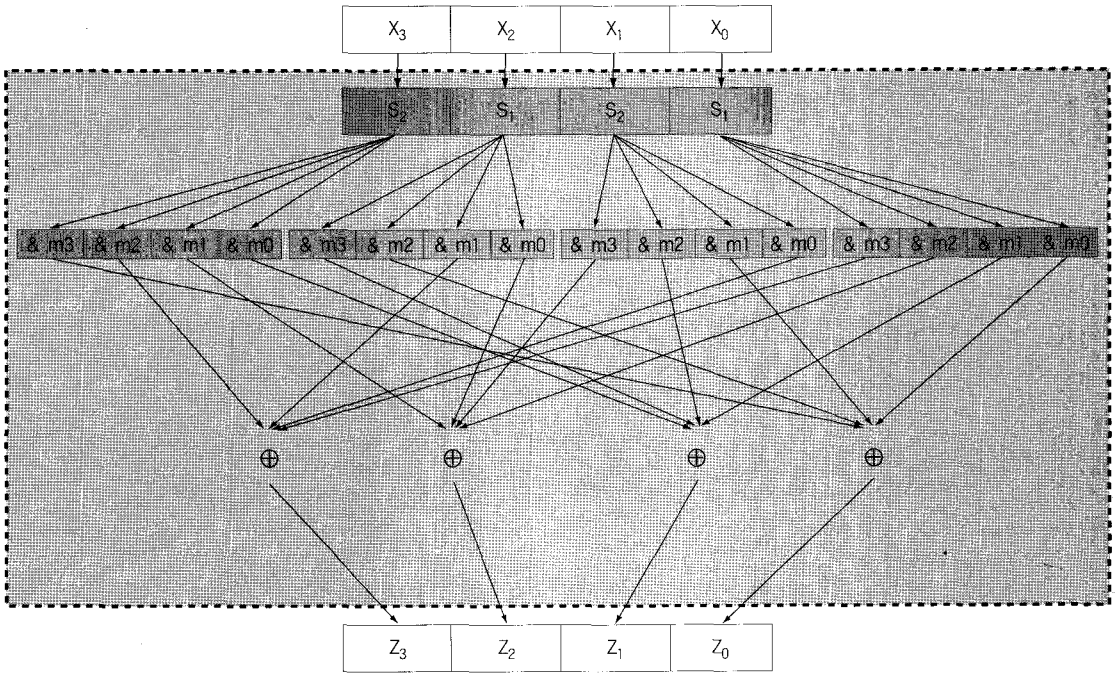
$Z_1 = (Y_0 \& m_1) \oplus (Y_1 \& m_2) \oplus (Y_2 \& m_3) \oplus (Y_3 \& m_3)$

$Z_0 = (Y_0 \& m_0) \oplus (Y_1 \& m_1) \oplus (Y_2 \& m_2) \oplus (Y_3 \& m_3)$

($m_3 = 0xfc$, $m_1 = 0xf3$, $m_2 = 0xcf$, $m_3 = 0x3f$)

4) S-Box

전단사함수 x^n, $0 \le n \le 255$에서 DC 및 LC 특성(DC 및 LC 확률이 2^{-6})이 가장 우수한 2개의 $n = 247, 251$을 선택하고, $GF(2^8)$상에서의 지수승을 구하기 위해 $GF(2^8)$상에서의 모든 원소를



(단, m0 = 0xfc, m1 = 0xf3, m2 = 0xcf, m3 = 0x3f 이고, &는 bit-wise AND 연산을 의미한다.)

(그림 3) G 함수

참고〉 위의 G 함수는 구현의 효율성을 위해 4개의 확장된 4바이트 SS-box들(4K bytes)의 exclusive-or로 구현할 수 있다. 이를 위해 다음과 같은 4개의 SS-box들을 저장해야 한다.

$SS_3 = S_2(X_3) \& m_2 \,||\, S_2(X_3) \& m_1 \,||\, S_2(X_3) \& m_0 \,||\, S_2(X_3) \& m_3$,
$SS_2 = S_1(X_2) \& m_1 \,||\, S_1(X_2) \& m_0 \,||\, S_1(X_2) \& m_3 \,||\, S_1(X_2) \& m_2$,
$SS_1 = S_2(X_1) \& m_0 \,||\, S_2(X_1) \& m_3 \,||\, S_2(X_1) \& m_2 \,||\, S_2(X_1) \& m_1$,
$SS_0 = S_1(X_0) \& m_3 \,||\, S_1(X_0) \& m_2 \,||\, S_1(X_0) \& m_1 || \, S_1(X_0) \& m_0$,

(여기서, || 는 concatenation).

이 확장 SS-box들을 이용하면 G 함수는 다음과 같이 구현될 수 있다. :

$Z = SS_3(X_3) \oplus SS_2(X_2) \oplus SS_1(X_1) \oplus SS_0(X_0)$

원시원소(primitive element) α의 멱승으로 표현한다.

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

지수함수의 입력 $x=0$이 출력 0, $x=1$이 출력 1으로 고정되는 것을 방지하기 위하여, 지수함수를 $S(x) = (A \cdot x^n) \oplus b$로 선형변환한다.

MSB LSB

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

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

($A^{(1)} = A$의 2행과 3행을 교환, 4행과 6행을 교환 / $A^{(2)} = A$의 1행과 5행을 교환, 6행과 7행을 교환)

A는 nonsingular matrix이므로, 서로 다른 2개의 입력 x, x'에 대하여 $Ax = Ax'$이다.

$b_1 = (1,0,1,0,1,0,0,1)^T = 169$, $b_2 = (0,0,1,1,1,0,0,0)^T = 56$이라 하고, 두 개의 S-box $S_1(x)$, $S_2(x)$는 각각

$$\begin{cases} (A^{(1)} \cdot x^{247}) \oplus b_1 = (P_7, P_6, P_5, P_4, P_3, P_2, P_1, P_0)^T \rightarrow \\ S_1(x) = P_7 \times 2^7 + P_6 \times 2^6 + P_5 \times 2^5 + P_4 \times 2^4 + P_3 \times 2^3 + P_2 \times 2^2 + P_1 \times 2^1 + P_0 \\ (A^{(2)} \cdot x^{251}) \oplus b_2 = (Q_7, Q_6, Q_5, Q_4, Q_3, Q_2, Q_1, Q_0)^T \rightarrow \\ S_2(x) = Q_7 \times 2^7 + Q_6 \times 2^6 + Q_5 \times 2^5 + Q_4 \times 2^4 + Q_3 \times 2^3 + Q_2 \times 2^2 + Q_1 \times 2^1 + Q_0 \end{cases}$$

으로 구성한다. (단, $x = (x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0)$ 이고, x_i는 2^i의 계수임)

○ S-box의 특성은 $\Delta_f = 4$, $\Delta_f = 16$, algebraic degree = 7이다.

부울함수를 $f: Z_2^8 \rightarrow Z_2^8$라 하면,

- $D_f(a,b) = \{x \in Z_2^8 | f(x \oplus a) \oplus f(x) = b\}$, $a \neq 0$이고, $\Delta_f(a,b) = \max_{a,b \neq 0} |D_f(a,b)|$일 때, $\Delta_f = 4$
- $L_f(a,b) = \{x \in Z_2^8 | (a \cdot x) \oplus (b \cdot f(x)) = 0\}$, $b \neq 0$이고, $\Delta_f(a,b) = \max_{a,b \neq 0} ||L_f(a,b)| - 2^{n-1}|$ 일 때, $\Delta_f = 16$
- algebraic degree는 7이다.

〈표 3〉 S_1-Box

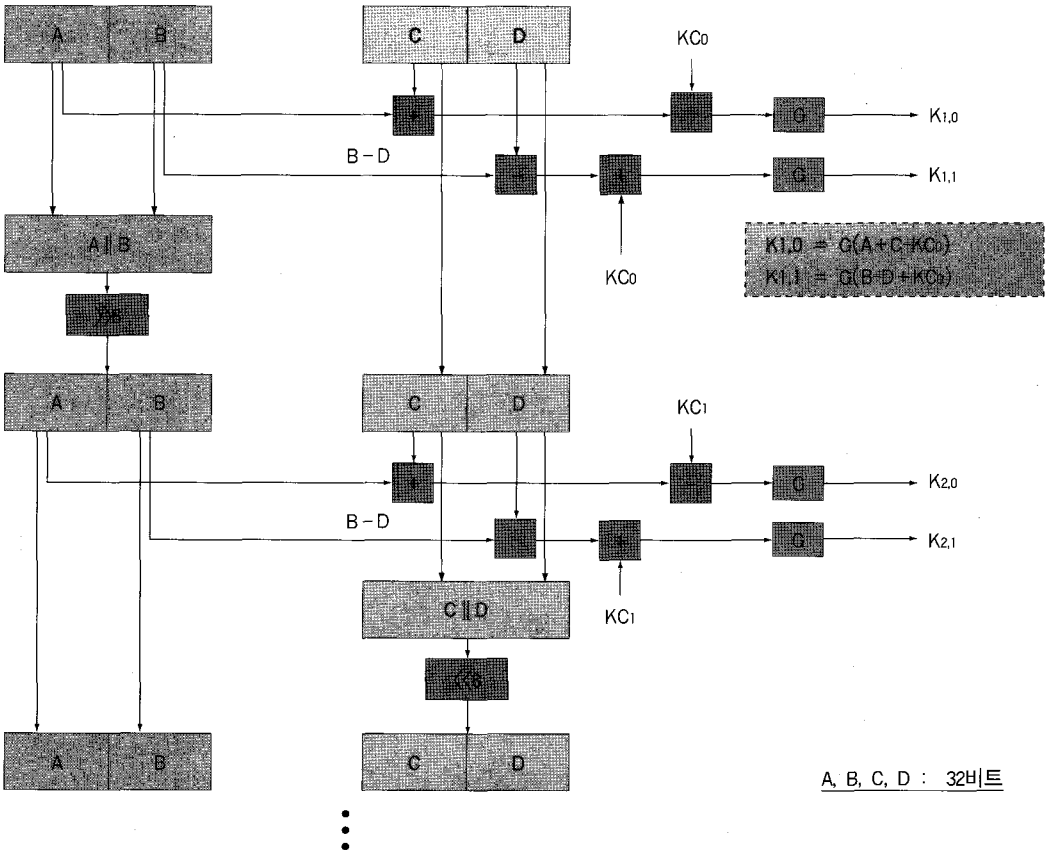
i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$
0	169	1	133	2	214	3	211	4	84	5	29	6	172	7	37
8	93	9	67	10	24	11	30	12	81	13	252	14	202	15	99
16	40	17	68	18	32	19	157	20	224	21	226	22	200	23	23
24	165	25	143	26	3	27	123	28	187	29	19	30	210	31	238
32	112	33	140	34	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

i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$	i	$S_1(i)$
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

〈표 4〉 S_2-Box

i	$S_2(i)$	i	$S_2(i)$	i	$S_2(i)$	i	$S_2(i)$	i	$S_2(i)$	i	$S_2(i)$	i	$S_2(i)$	i	$S_2(i)$
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	52	165	53	249	54	13	55	223
56	216	57	43	58	102	59	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	92	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

※ 본 알고리즘(SEED)의 S-Box는 8비트 입력(즉, 0~255)을 받아 8비트 출력(즉, 0~255)을 내는 함수로서, 예를 들면, S_1-box의 경우, 입력이 '21'이면 출력은 '226'이 된다.



(그림 4) 라운드 키 생성과정 구조도

5) 라운드 키 생성과정

SEED의 라운드 키 생성과정은 128비트 암호키를 64비트씩 좌우로 나누어 이들을 교대로 8비트씩 좌/우로 회전이동한 후, 결과의 4워드들에 대한 간단한 산술연산과 G 함수를 적용하여 라운드 키를 생성한다. 라운드 키 생성과정은 기본적으로 하드웨어나(모든 라운드 키를 저장할 수 없는) 제한된 자원을 갖는 스마트카드와 같은 응용에서의 효율성을 위하여, 암호화나 복호화시 암호키로부터 필요한 라운드 키를 간단히 계산할 수 있도록 설계하였다.

각 라운드에 사용되는 라운드 키는 다음과 같은 방식으로 생성한다.

① 128비트 입력키를 32비트씩 4개의 조각으로 쪼갠 후 (A, B, C, D),

② $K_{1,0}=G(A+C-KC_0)$; $K_{1,1}=G(B-D+KC_0)$ (단, KC_0 : 1 라운드 상수)로 1라운드 키를 생성하고,

③ $A||B=(A||B)^{\gg 8}$

④ $K_{2,0}=G(A+C-KC_1)$; $K_{2,1}=G(B-D+KC_1)$ (단, KC_1 : 2 라운드 상수)로 2라운드 키를 생성하고,

⑤ $C||D=(C||D)^{\ll 8}$

⑥ $K_{3,0}=G(A+C-KC_2)$; $K_{3,1}=G(B-D+KC_2)$ (단, KC_2 : 3 라운드 상수)로 3라운드 키를 생성하고,

⑦ 계속해서 16라운드 키를 생성할 때까지 반

복한다.

즉, 주어진 128비트 암호키 K=A||B||C||D를 32비트 레지스터 A, B, C, D로 나눈다. 각 라운드 i에 사용되는 라운드 키 $K_i=(K_{i,0}\ ;\ K_{i,1})$는 다음과 같은 방식으로 생성한다 :

```
for(i=1; i<=16; i++) {
    K_{i,0} ← G(A+C-KC_i);
    K_{i,1} ← G(B-D+KC_i);
    if(i%2==1) A||B ← (A||B)>>>8;
    else C||D ← (C||D)<<<8;
    }
```

〈표 5〉 라운드 키 생성과정에 사용된 상수

라운드 상수	
KC_0 = 0x9e3779b9	KC_8 = 0x3779b99e
KC_1 = 0x3c6ef373	KC_9 = 0x6ef3733c
KC_2 = 0x78dde6e6	KC_{10} = 0xdde6e678
KC_3 = 0xf1bbcdcc	KC_{11} = 0xbbcdccf1
KC_4 = 0xe3779b99	KC_{12} = 0x779b99e3
KC_5 = 0xc6ef3733	KC_{13} = 0xef3733c6
KC_6 = 0x8dde6e67	KC_{14} = 0xde6e678d
KC_7 = 0x1bbcdccf	KC_{15} = 0xbcdccf1b

4. 결론

인터넷을 통한 전자상거래 등에서 사용되고 있는 대부분의 암호알고리즘의 비도는 현재 40비트 안전도를 지원하고 있다. 56비트 DES (1998년까지 미국연방표준 알고리즘)가 작년 약 56시간만에 25만 달러의 비용으로 손쉽게 (키 전수검색 공격으로) 해독되었던 사실을 상기하면, 현재의 인터넷이 안전도 측면에서 매우 취약함을 미루어 짐작할 있다.

SEED는 128비트의 안전도를 제공하는 암호알고리즘으로써 현재 미국에서 추진하고 있는 차기 표준암호알고리즘(AES)의 안전도를 지원하고 있다. 따라서 SEED를 활용한 전자상거래 서비스의 확대는 국내 정보보호 안전도를 한층 더 높일 수 있으리라 생각된다. 참고로 현재 128비트 블록 암호알고리즘(SEED)의 소스코드는 약 47개의 업체 및 학계에 배포되어 있고, 특히 금융 분야를 중심으로 널리 배포되고 있다.