엑셀 매크로기능을 이용한 DES의 라운드 키 생성개발

김대학¹

¹대구가톨릭대학교 수학과

접수 2012년 10월 30일, 수정 2012년 11월 23일, 게재확정 2012년 11월 25일

요약

본 논문에서는 1977년 미국 국립기술표준원이 연방정보처리기준 46으로 공표한 암호화 표준인 현대 대칭키 블록 암호 DES (data encryption standard)의 라운드 키 생성기에 대한 엑셀 매크로 기능을 활용한 라운드 키 생성을 개발하였다. 평문과 암호문과의 관계를 숨기는 확산과 암호문과 암호 키 사이의 관계를 숨기는 혼돈을 반복하는 라운드의 반복으로 평문을 암호화 하는 DES의 설명과 라운드 키 생성 알고리즘을 소개하고 이를 엑셀 매크로기능을 이용하여 라운드 키를 구현하는 생성개발을 제안하고 개발된 매크로의 정확성과 활용성을 서술하였다.

주요용어: 대치암호, 라운드, 매크로, 암호화 표준, 축소 치환박스, 치환암호.

1. 서론

오늘날 컴퓨터와 인터넷은 하루가 다르게 계속 눈부시게 발전하고 있다. 인터넷을 통하여 전 세계 모든 곳의 정보를 원하는 대로 찾아볼 수도 있고 정보의 축적, 처리, 전송능력의 획기적 증대로 인하여 은행업무, 행정업무까지도 편리하게 처리할 수 있는 시대를 살아가고 있다. 그러나 인터넷을 통하여 우리의 삶의 많은 부분에서 좋은 변화를 초래하고 있지만 이에 못지않게 우리에게 엄청난 피해를 초래할 수 있는 역기능이 계속 생겨나고 있으며 그 유형 또한 다양하게 나타나고 있다. 따라서 이런 역기능으로 인한 피해를 줄이기 위해 다양한 기술들이 개발되어 사용되고 있다. 정보보호를 위한 대책 가운데 가장 경제적이고 효율적이면서도 계층적인 보안대책을 제공할 수 있는 방법이 암호방식을 이용하는 방법이다.

암호 (cryptography)란 평문 (plain text)을 해독 불가능한 형태로 변형 (암호화 과정; encryption) 하거나 또는 암호화된 통신문 (암호문; cipher text)을 해독 가능한 형태로 변환 (복호화 과정; decryption)하기 위한 원리, 수단, 방법 등을 취급하는 기술 또는 과학을 의미한다 (Hoffstein 등, 2008). 암호의 사용은 인류 역사와 함께 시작된 것으로 알려져 있다. 산업사회의 발달과 전기 통신 기술의 발전으로 유통되는 정보의 양이 급증하면서 정보보호를 위한 암호사용이 급격히 증대되었으며 20 세기의 무선통신 기술의 개발로 인하여 암호사용이 더욱 가속화 되었다. 특히 두 차례의 세계대전을 통하여 암호의 수요가 폭발적으로 증가하여 암호기술이 큰 발전을 맞이하였으며 암호장비의 개발도 활발해졌다.

평문 문자의 위치를 바꾸는 전치암호 (transposition cipher)나 문자를 다른 문자로 치환하는 대치 암호 (substitution cipher)등의 고대암호로부터 수학의 발전과 함께 20세기에 들어와서 고급암호가 발전하기 시작하였다. 대표적인 근대암호는 Vigenere 암호, Playfair 암호, Hill 암호 등이다 (Kahn,

¹ (712-702) 경상북도 경산시 하양읍 하양로 13-13, 대구가톨릭대학교 자연과학대학 수학과, 교수.
E-mail: dhkim@cu.ac.kr

1996). 이 시기에 Shannon (1949)은 확률론을 기초로 한 정보이론을 창시하였으며 원리적으로 해독 불가능한 암호방식을 제안하고 그 안전성을 평균 정보량을 이용하여 수리적으로 증명한 바 있다.

암호화가 적용되는 평문길이의 단위가 여러 개의 문자나 비트 (bit)를 사용하는 오늘날의 블록 암호 (block cipher)에서는 암호화 과정과 복호화 과정에서 적용되는 키 (key)가 동일한 가 또는 그렇지 않은가에 따라서 대칭키 암호 (symmetric key encipherment)와 공개키 암호 (public key encipherment)로 구분된다. 대칭키 암호방식은 암호화와 복호화에 동일한 키를 사용하기 때문에 키를 사전 분배하여 보관하고 있어야 한다. 반면 공개키 암호방식은 암호화 키와 복호화 키를 분리하여 암호화 키는 공개하고 복호화 키는 비밀리에 보관하도록 하고 있다. 이러한 공개키 암호방식은 Rivest 등 (1978)에 의한 RSA 암호방식 (그들의 이름 Rivest, Shamir, Adleman을 사용)을 비롯하여 수학적 문제에 기초한 여러 방식 등이 개발, 소개되었다.

한편, 1977년 1월, 미국 국립기술표준원 (NIST; national institute of standards technology)은 국가적으로 사용할 대칭 키 암호시스템을 공개모집하여 IBM이 제안한 DES (data encryption standard)를 FIPS (연방정보처리기준; federal information processing standard) 46이란 이름으로 발표하였으며 암호화의 표준으로 정의하였다. DES는 발표된 후 가장 널리 사용되는 대칭 키 블록 암호가 되었다 (Forouzan, 2008; Trappe와 Washington, 2006).

본 연구의 목적은 복잡한 암호화와 복호화의 논리를 C 언어나 C++ 언어로 구현하기 어려운 사람들이 암호화 과정이나 복호화 과정에서 쉽게 접할 수 있게 하기 위하여 마이크로소프트사의 엑셀 매크로를 이용하여 암호화와 복호화를 구현하는 과정에서 DES의 암호화중 가장 중요하면서도 절대적으로 필요한 라운드 키 (round key) 생성을 개발하고자 한다.

최근 들어 엑셀의 매크로 기능을 이용한 도구들이 계속 개발되고 있다. Choi와 Ha (2011a)는 엑셀 매크로기능을 이용하여 베이즈 (Bayes) 정리 교육도구를 개발하였으며 Choi와 Ha (2011b)는 엑셀 매크로를 이용한 절차 중심의 통계교육도구를 개발하였다. 또 Choi와 Kim (2010)은 엑셀의 함수를 이용한 표본추출에 관하여 연구한 바 있다. 이러한 추세를 감안하면 엑셀의 매크로 기능을 이용하는 다양한 도구들이 개발되고 있으며 앞으로도 계속 개발되어 많은 사용자들로 하여금 쉽게 활용할 수 있도록 할 것임을 짐작할 수 있다. 본 논문의 2절에서는 1977년, 미국표준 암호로 채택된 DES에 대하여 살펴보고 그 중 가장 중요한 역할을 하는 라운드 함수 (round function)에 대하여 설명하였다. 3절에서는 라운드 키 생성 알고리즘의 설명과 더불어 라운드 키를 생성하는 엑셀 매크로를 개발하는 내용을 기술하였고 4절에서는 개발된 매크로를 이용하여 입력 값인 암호 키를 이용한 라운드 키의 생성을 예를 들어 나타내었고 기존의 알려진 결과와 동일한지 확인하였으며 마지막으로 결론은 5절에 나타내었다.

2. DES와 라운드 함수

한 문자를 다른 문자로 대체하는 대치암호나 문자들의 위치를 바꾸는 전치암호 등의 고대암호는 동영상이나 음성 등의 형태로 데이터의 형태가 다양화됨에 따라서 컴퓨터의 발전과 함께 문자기반 (character-oriented)의 특성에서 비트기반 (bit-oriented)의 특성으로 변화되어 오늘날의 현대암호의 기본을 형성하게 되었다. 즉 오늘날의 암호관련분야의 연산의 기본단위가 문자가 아니라 비트로 수행됨을 의미한다.

현대 대칭 키 블록 암호는 n 비트 평문블록을 n 비트 암호문 블록으로 암호화한다. 이때 암호화나 복호화 과정에서는 k 비트 키를 사용한다. 현대 블록 암호는 입력 값을 이용하여 출력 값을 만드는 가능한 모든 경우 중에서 부분적 대응만을 허용하는 키가 있는 대치암호인 셈이다. 전치암호를 사용할 경우 전체 비트 속에 포함되어 있는 1과 0의 수가 동일하게 되어 부분적 정보를 제공하게 됨

으로 현대블록 암호는 대치암호로 설계된다. 현대 블록 암호는 암호문과 평문사이의 관계를 숨기는 의미의 확산 (dispersion)과 암호문과 키 사이의 관계를 숨기는 의미의 혼돈 (confusion)같은 성질을 만족시키기 위하여 전치와 대치 그리고 그 밖의 구성요소인 배타적 논리합 (exclusive or; XOR), 순환이동 그리고 라운드 (round)들을 결합하여 암호화된다. 이때 전치의 역할을 수행하는 요소를 P-박스 (permutation box), 대치의 역할을 수행하는 요소를 S-박스 (substitution box)라 부른다. P-박스는 n 비트를 입력받아 m 비트를 출력하는 치환함수로서 단순 (straight), 축소 (compression), 확장 (expansion)의 세 종류가 있으며 S-박스는 n 비트를 입력받아 m 비트를 출력하는 대치암호의 축소모형으로서 선형 S-박스와 비선형 S-박스의 두 종류가 있다. Table 2.1과 Table 2.2는 P-박스와 S-박스의 예를 보여주고 있다.

Table 2.1 7×7 Straight P-box

3	7	6	5	1	4	3
---	---	---	---	---	---	---

Table 2.1은 7×7 단순 P-박스를 나타내고 있다. 이 의미는 입력비트 중 3번째 비트를 출력비트의 1번째 비트로 치환하고 7번째 입력비트를 2번째 출력비트로 치환하는 등 입력비트 모두가 출력비트로 대응되는 일대일 대응관계를 유지함을 나타내고 있는 것이다. 즉 P-박스에 나타난 숫자와 그 위치 (순서)가 각각 입력비트와 출력비트에 해당된다. 축소나 확장 P-박스의 경우 일대일 대응이 보장되지 않는다.

Table 2.2 3×2 S-box

row \ column	00	01	10	11
0	00	10	01	11
1	10	00	11	01

Table 2.2는 선형 S-박스를 나타내고 있다. 입력 값 세 비트 중 왼쪽 최상위 비트는 행을 나타내고 나머지 오른쪽 두 비트는 열을 의미하며 출력비트는 선택된 행과 열의 교차되는 성분의 값이다. 예로서 입력비트가 010이면 출력비트는 01로 되어 대치의 역할이 수행되는 셈이다.

확산 (diffusion)과 혼돈 (confusion)은 각 반복이 S-박스, P-박스 그리고 기타 구성요소의 결합을 의미하는 반복적 합성암호를 사용하여 얻어진다. 이때 반복적으로 사용되는 합성암호를 라운드 (round)라고 칭한다. 블록 암호는 암호 키로부터 각 라운드에 사용될 서로 다른 키들을 생성하기 위하여 키 생성 알고리즘을 사용한다. N 라운드 암호에서 평문은 암호문을 생성하기 위하여 N 번 암호화 된다.

DES는 64비트 평문을 이용하여 64비트 암호문을 생성하는데 이때 실질적으로 56비트 암호 키를 이용하여 암호문을 생성한다. 암호화 과정은 두 개의 P-박스 (초기치환, 최종치환)와 16개의 라운드 함수로 구성된다. 각 라운드는 라운드 키 생성기에 의해 암호키로부터 생성된 48비트 라운드 키를 사용한다. 이 라운드 키의 생성을 엑셀 매크로를 이용하여 생성시키는 것이 본 연구의 주된 내용이다. Figure 2.1 (left)은 DES의 구조를 나타내고 있다. Figure 2.1을 살펴보면 초기치환을 거쳐 만들어진 64비트 입력 값을 이용하여 이를 32비트씩 두 부분으로 나누고 나누어진 L_0 와 R_0 를 다음단계의 입력으로 사용한다. L_0 는 그대로 L_1 으로 전달하고 R_0 는 라운드 키 생성기에 의하여 생성된 48비트 라운드 키 K_1 과 함께 Figure 2.1 (right)의 라운드 함수 (round function)에 전달하게 되고 32비트 R_0 를 32×48 확장 P-박스에 넣어 얻어진 48비트 출력 값과 라운드 키 K_1 과 배타적 논리합 연산을 통과하여 얻어진 새로운 출력 값 48비트를 여섯 개의 6×4 S-박스의 입력으로 전달한다. 이 후 이 여섯 개의 S-박스 출력 값 32비트를 32×32 단순 P-박스 치환을 통하여 새로운 32비트 R_1 을 생성하게

된다. 이제 얻어진 L_1 과 R_1 을 서로 바꾸어 (swap) 다음 라운드의 입력 값으로 사용한다. 이런 과정을 16번 반복하여 최종적으로 암호문을 얻는 방법이 DES이다.

Figure 2.1 DES structure (left) and round function (right)

3. 엑셀 매크로를 이용한 라운드 키 생성개발

본 절에서는 DES의 라운드 키 생성기 (round-key generator)에 대하여 살펴보고 엑셀 매크로를 이용하여 자동적으로 라운드 키를 생성하는 방법을 설명하고자 한다.

라운드 키 생성기의 알고리즘을 살펴보자. 암호 키는 보통 64비트로 주어지며 이 중 8비트는 패리티 비트 (parity bit)로 실제 키 생성 과정 전에 제거된다. 이는 패리티 비트 제거라고 불리는 Table 3.1의 64×56 축소 P-박스 치환에 해당된다.

Table 3.1 Parity bit delete compression P-box

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	52	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

축소 P-박스 치환을 거쳐 얻어진 56비트 키는 28비트 씩 두 부분으로 나누어지고 각 부분은 왼쪽으로 1비트 또는 2비트씩 순환이동 (circulation shift)시킨다. 라운드 번호에 따라 순환이동 시키는 비트의 양이 다른데 1, 2, 9, 16번째 라운드에서는 순환이동 비트 양이 1비트이고 나머지 라운드에서는

순환 이동 비트 량이 2비트이다. 이렇게 얻어진 두 부분을 결합하여 56비트 키로 작성한다. 이후 다시 56×48 축소 치환 P-박스 과정을 통하여 48비트 키를 얻게 된다. 이러한 과정을 각 라운드에 대하여 반복 수행함으로서 매 라운드마다 라운드 키를 얻게 된다. 이 과정은 Figure 3.1에 나타나 있다.

Figure 3.1 Round key generator

위의 라운드 키 생성기를 마이크로소프트사의 엑셀 프로그램을 이용하여 구현하기 위하여 매크로 기능을 활용하여 구성하여 보았다. 이런 엑셀 매크로를 사용함으로써 C 프로그래밍이나 C++ 프로그래밍 기법에 익숙하지 않은 사용자들은 쉽게 라운드 키를 생성할 수도 있게 되고 또한 암호화 과정에 대한 폭 넓은 이해에 도움이 될 수 있을 것이다. 실제로 사용되는 56×48 축소 P-박스 치환은 Table 3.2와 같다.

Table 3.2 Compression P-box

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Figure 3.2는 엑셀 매크로 기능을 이용하여 개발된 라운드 키 생성 초기화면을 나타낸다. 이 초기 화면은 암호 키 값의 입력 셀 B2, 세 개의 버튼 ‘preparation’, ‘round1’ 그리고 ‘all other rounds’ 으로 구성되어 있다. 이 화면에서 Figure 3.2와 같이 B2셀에 원하는 암호 키를 입력한 후 “preparation” 버튼을 누르면 Figure 3.3과 같은 화면이 나타난다. 이 화면에서는 입력된 암호 키에 대한 이진수 표현과 이 암호 키의 패리티 비트를 제거하고 축소 치환한 입력비트 값들이 D2와 D3셀에 각각 나타나게 설계되어 있다.

Figure 3.2 Initial stage for round key generation macro

Figure 3.3 After preparation button

이렇게 함으로서 라운드 키를 얻기 위한 사전 준비가 끝나게 된다. “preparation” 버튼을 통하여 얻어진 56비트 암호 키 (D3셀)를 좀 더 간단하게 나타내기 위하여 16진수로 표현한 결과를 N3셀에 나타내었다. 이제 라운드 키 생성을 위하여 “round 1” 버튼을 누르면 Figure 3.4와 같은 결과를 얻게 된다. 이 중 M13셀에 해당되는 값이 우리가 원하는 라운드 키 값이고 이를 16진수로 나타낸 값이 N13셀에 나타나있다.

Figure 3.4 After round1 button

이제 나머지 모든 라운드 (2~16 라운드)에 해당되는 라운드 키 값을 생성하기 위하여 “all other rounds” 버튼을 누르면 Figure 3.5와 같은 화면이 나타난다. 여기서 N13셀부터 N28셀까지의 16진수로 나타난 값들이 우리가 원하는 라운드 키 값을 알 수 있다. 물론 M13셀부터 M28셀까지의 2진수로 나타난 값들이 실제의 라운드 키 값이다.

Figure 3.5 After all other rounds button

4. 예제

개발된 라운드 키 생성 매크로의 정확성을 확인하기 위하여 다른 프로그램을 이용하여 이미 확인된 암호 키 값을 이용하여 매크로를 실행시켜 보았다. Table 4.1의 첫째 열에 있는 암호 키 값은 많은 사람들에게 의해 사용된 값으로 DES를 이용하여 암호화 할 때에 각 라운드 키 값은 모두 다 알려져 있다. 이 알려진 값에 대하여 제안된 엑셀 매크로 프로그램을 이용하여 얻은 16라운드 키 값들 모두가 이미 알려진 값들과 동일하게 나타났다. Table 4.1은 알려진 암호 키 값 외에도 2개의 서로 다른 암호 키 값을 이용하여 얻은 라운드 키들을 나타내고 있다.

Table 4.1 Obtained 16 round keys

round \ key	aabb09182736ccdd	c0b7a8d05f3a829c	123456abcd132536
1	194CD072DE8C	3DE3986A0EB6	7201A69E3355
2	4568581ABCCE	E7798C82F162	02BE21ED00E7
3	06EDA4ACF5B5	1AAFC1A4AF24	C93C4246EACF
4	DA2D032B6EE3	597C3BF80ED2	60E6C83695DD
5	69A629FEC913	E5A5CC5DC21B	50D5028B95E3
6	C1948E87475E	52CE87177448	6089534EEF21
7	708AD2DDB3C0	79B932A8B164	25E0077A4D5C
8	34F822F0C66D	A4A4EFA0EEA6	230592C9D19A
9	84BB4473DCCC	88B7D6037949	4252498DAFF8
0	02765708B5BF	745E6BA2B134	09D96039DE51
1	6D5560AF7CA5	E3F160E10FA6	8069CB5BC436
12	C2C1E96A4BF3	88CFD75C0A9B	3167018D6D8C
13	99C31397C91F	75731B57505D	411D81A872D5
14	251B8BC717D0	2795E103B1E8	51A0D5F3C2A7
15	3330C5D9A36D	DB48D7A0BD25	15C482960F8B
16	181C5D75C66D	0D4E7B3F5049	C42B08353596

5. 결론 및 토의

본 연구에서는 현대 대칭키 블록 암호의 표준으로 공표되고 사용되었던 DES의 라운드 키 생성과 관련하여 엑셀 매크로 기능을 이용하여 라운드 키 생성기를 구현하였다. 물론 막강한 C나 C++ 프로그래밍을 이용하여 DES나 라운드 키 생성 등은 당연히 가능하나 이런 프로그래밍에 익숙하지 않은 대다수의 사용자들에게 쉽고 간단히 접할 수 있는 엑셀을 이용한 라운드 키 생성 매크로를 제공함으로써 프로그래밍의 수고를 덜고 좀 더 암호학 (cryptology) 관련 분야에 흥미를 느끼게 할 수 있을 것이다. 학부에서 수학이나 통계학 혹은 정보, 전산관련 분야를 전공하는 많은 학생들이 쉽게 그리고 간단히 사용할 수 있는 엑셀 매크로 기능을 활용한 다양한 암호관련 결과물의 제공과 활용이 기대된다.

참고문헌

- Choi, H. S. and Ha, J. (2011a). Development of process-oriented education tool for Statistics with Excel Macro. *Journal of the Korean Data & Information Science Society*, **22**, 643-650.
- Choi, H. S. and Ha, J. (2011b). Development of Bayes' rule education tool with Excel Macro. *Journal of the Korean Data & Information Science Society*, **23**, 905-912.
- Choi, H. S. and Kim, T. Y. (2010). A study on sampling using the function of excel. *Journal of the Korean Data & Information Science Society*, **21**, 481-491.

- Forouzan, B. A. (2008). *Introduction to cryptography and network security*, The McGraw-Hill Companies, New York.
- Hoffstein, J., Pipher, J. and Silverman, J. H. (2008). *An introduction to mathematical cryptography*, Springer, New York.
- Kahn, D. (1996). *The codebreakers : The story of secret writing*, Scribner's, New York.
- Rivest, R. L., Shamir, A. and Adleman, L. (1978). A method of obtaining digital signature and public-key cryptosystem. *Communication of the Association for Computing Machinery*, **21**, 120-126.
- Shannon, C. E. (1949). Communication theory of secrecy system. *The Bell Laps Technical Journal*, **28**, 656-715.
- Trappe, W. and Washington, L. (2006). *Introduction to cryptography and coding theory*, Prentice Hall, Upper Saddle River.

On the development of DES round key generator based on Excel Macro

Daehak Kim¹

¹Department of Mathematics, Catholic University of Daegu

Received 30 October 2012, revised 23 November 2012, accepted 25 November 2012

Abstract

In this paper, we consider the development of round key generator of DES (data encryption standard) based on Microsoft Excel Macro, which was adopted as the FIPS (federal information processing standard) of USA in 1977. Simple introduction to DES is given. Algorithms for round key generator are adapted to excel macro. By repeating the 16 round which is consisted of diffusion (which hide the relation between plain text and cipher text) and the confusion (which hide the relation between cipher key and cipher text) with Microsoft Excel Macro, we can easily get the desired DES round keys.

Keywords: Compression P-box, data encryption standards, macro, permutation cipher, round, substitution cipher.

¹ Professor, Department of Mathematics, Catholic University of Daegu, Kyungsan 712-702, Korea.
E-mail: dhkim@cu.ac.kr