DES(Data Encryption Standard) 속성 진단과 강화된 대칭키 암호 알고리즘 적용방법

노시춘*

요 약

DES는 64비트 단위로 나뉘어 진 각각의 블록이 한번의 암호화 알고리즘을 거쳐 암호화 된다. 대칭알고리즘으로서 똑같은 키와 알고리즘이 암호화와 복호화에 쓰인다. 복호화 할 때 키를 반대로 적용하는 등의 약간의 차이는 있다. 키 길이는 64비트로 표현되는데 이 중에서 실제로는 56비트만이 키로서 사용되고 나머지 8비트는 패리티 체크 비트로 사용된다. 암호화는 64비트 블록과 56비트 키를 바탕으로 만든 16개의 보조키가 총 16번의 혼돈과 확산을 거쳐 완료된다. DES 알고리즘을 선택한 이유는 암호 강도에 대한 의문이 제기되고 있기는 하지만 상업적으로 가장 널리 보급되어 이용되고 있다. 또한 기본 알고리즘을 DES로 채택한 현장에서 앞으로도 상당한 기간 동안 이용이 계속될 것으로 예상되는 DES 알고리즘을 효과적으로 활용하는 방안이 현장에서 참고되기를 기대한다.

A Study of DES(Data Encryption Standard) Property, Diagnosis and How to Apply Enhanced Symmetric Key Encryption Algorithm

Si Choon Noh*

ABSTRACT

DES is a 64-bit binary, and each block is divided into units of time are encrypted through an encryption algorithm. The same key as the symmetric algorithm for encryption and decryption algorithms are used. Conversely, when decryption keys, and some differences may apply. The key length of 64 bits are represented by two ten thousand and two 56-bit is actually being used as the key remaining 8 bits are used as parity check bits. The 64-bit block and 56-bit encryption key that is based on a total of 16 times 16 modifier and spread through the chaos is completed. DES algorithm was chosen on the strength of the password is questionable because the most widely available commercially, but has been used. In addition to the basic DES algorithm adopted in the future in the field by a considerable period are expected to continue to take advantage of the DES algorithm effectively measures are expected to be in the field note

keywords : DES, Property, Diagnosis, Enhanced Symmetric Key, Encryption Algorithm

접수일(2012년 8월 31일), 수정일(1차: 2012년 9월 6일), 게재확정일(2012년 9월 7일)

* 남서울대학교 컴퓨터학과

1. 서 론

과거에 상상도 할 수 없을 만큼 엄청난 양의 정보들이 실시간으로 처리, 보관, 전송된다. 이로인해 타인의 정보를 가로채는 암호 해독으로 부터 자신의 정보를 보호하려는 암호 적용 에 관한 연구가 활발히 진행되고 있다. 일반적으로 공개키 방식의 암호 알고리즘 활용이 증가되는 환경에서도 대칭키(symmetric crypto system) 알고리즘은 피어 투 피어(peer to peer) 암호채널 구성에 필수적인 강력한 수단으로 인식되고 있다. 대칭키 방식의 대표적 알고리즘인 DES는 64비트 단위로 나뉘어 진 각각의 블록이 한번의 암호화 알고리즘을 거쳐 암호화 된다. DES는 원래 1972년 National Institute of Standard and Technology(NIST)의 전신인 National Bureau of Standards(NBS)가 몇 가지 기준을 제시 하였고 이를 만족시키는 알고리즘으로 IBM에서 Lucifer 시스템을 개선하여 만든 것이다. 본 연구는 DES 속성진단과 강화된 대칭키 암호 알고리즘 적용방법을 제안한다. 연구순서는 관련연구, 대칭키 알고리즘 속성 진단, 강화된 암호 알고리즘 적용방법, 결론의 순서 이다.

2. 관련연구

2.1. 암호화(encryption, ciphering)

원래의 메시지는 평문(plain text)이며 암호화된 메시지는 암호문(cipher text)이다. 평범한 사람 이 이해할 수 있는 내용을 특정한 사람을 제외 하고 이해할 수 없는 형태로의 변형과 특정한 사람을 제외하면 이해할 수 없는 형태를 이해할 수 있는 형태로 바꾸는 방법을 연구하는 원리, 기술 또는 과학을 암호학(cryptology)이라 한다. 암호화란 메시지의 내용이 해독되지 않도록 평문을 재구성하여 암호문을 만드는데, 이때 사용되는 메시지의 재구성 방법을 암호화 알고리즘이라 한다. 암호화 알고리즘에서는 암호화의 비밀성을 높이기 위해 키(key)를 사용하기도 한다. 복호화(decryption)란 암호화의 역 과정으로 암호화 된 메시지를 본래의 메시지를 환원하는 과정 이다.

2.2 암호계

암호화 기법을 적용하는 암호화 및 복호화 과정으로 구성된 시스템을 암호계(crypto system)라 한다. 암호계에는 키나 알고리즘이 포함되며 하나의 비밀키(private key, secret key)를 암호화와 복호화에 모두 사용하는 관용 암호계(conventional crypto system)와 비밀키와 공개키를 구분하는 공개키(public key system)시스템으로 나뉜다[1].

2.3 암호강도

암호강도(strength of cipher)는 암호화 알고리즘을 알고 있는 암호 공격자가 키 혹은 평문을 알아내고자 했을 때의 노력의 정도를 의미한다. 암호강도가 클수록 그 암호계는 안전한 암호계가 된다. 특별한 경우를 제외 하고는 비밀 키가 남에게 알려지지 않도록 잘 관리 되어야 한다. 알고리즘이 공개된 상태에서 키마저 알려진다면 누구나 쉽게 평문을 알아낼 수 있기 때문이다.

2.4 암호 알고리즘

암호 알고리즘은 암호화를 행할 때 사용하는 기본 요소에 따라 크게 환자(substitution)암호, 전치(transpostition) 암호, 혼합(product cipher) 암호, 공개키 암호 방식으로 분류될 수 있다.

2.4.1 환자암호(substitution cipher)

환자암호는 평문의 각 문자를 다른 문자나 심볼로 일대일로 대응시킴으로써, 평문의 문자가 어떤 암호문자로 변환되는지 알 수 없도록 하는 혼동(confusion)에 그 목적이 있다. 가장 기본적 인 환자암호 방식은 평문의 각 문자를 영문의 알파벳 순으로 정렬한 다음 일정한 거리만큼 앞 또는 뒤의 문자로 대치시키는 방법이다. 즉, 평문의 알파벳 A B C D E를 암호문의 알파벳 D E A B C로 바꾸는 것 이다. 이 방법은 역사적으로 줄리어스 시저가 사용한 기록이 있기 때문에 이 방법을 시저의 암호라 부른다 [2][3].

2.4.2 전치암호(transpostition cipher)

전치암호는 평문의 문자를 다시 재배열하는 방법이다. 따라서 전치암호의 목적은 확산, 즉 평문과 키가 가지고 있는 정보를 암호문 전체에 분산시키는데 있다. 영문에서 어떤 구나 단어의 형태를 바꾸고 암호 해독자가 암호를 해독하기 위해 더 많은 암호문을 필요로 하게 만드는 것이 목적이다. 간단한 전치암호의 예는 문장의 알파벳 순서를 뒤집어서 끝에서부터 적는 방법 인데, 평문 MY DREAM IS SUCCESS라는 문장은 암호문 EAMMY DRISS UCCESS로 바뀐다[3].

3. 대칭키(symetric crypto system) 알고리즘 속성 진단

3.1 DES 원리

대칭키 알고리즘의 대표적 속성은 하나의 키로 암호화와 복호화에 이용하는 관용 암호계 이다. 또한 혼합암호(product cipher)를 채용 하는데 혼합암호 환자와 전치 두 가지 방법을 모두 사용하는 방법이다. 혼합암호의 대표적인 예 는 DES가 있는데, DES에서는 환자와 전치를 문자단위가 아니라 비트단위로 적용 하면서 exclusive or 연산을 도입하였기 때문에 대단히 복잡해 졌다. DES 암호화 알고리즘은 표준화 되어 공개되어 있으므로 64(패리티 비트 제외 시 56비트)비트의 키에 비밀성을 의존한다. DES는 평문을 8글자 단위 로 나누어 8글자, 64비트의 키로 16번 반복 처리되어 암호화 되는데, 이용자가 제공한 64 비트 키는 16개의 다른 형태의 키로 변형되어 16회 반복처리 과정 에서 이용된다[4].

3.2 DES 알고리즘 진화 과정

DES 이전의 암호화 방법은 대체로 사람의 손이나 기계적 장치를 이용한 수동적 혹은 기계적 암호화 방법들로서 컴퓨터를 이용하여 쉽게 공격이 가능한 것이다. 이에 반해 DES는 처음부터 컴퓨터에서의 사용을 전제로 만들어 졌으므로 컴퓨터에 의한 공격에도 견딜 수 있는 알고리즘이 필요하였고, NIST(미국표준연구소) 공모에 의해 IBM이 제안해 표준으로 채택된 것 이다. DES알고리즘은 ANSI에서는 DEA(data encryption algorithm), ISO에서는 DEA-1으로 명명했고 지난 1998년 까지는 세계 표준으로 사용된 64비트 블록암호 알고리즘 이다. DES 진화과정을 보면 1977년 미국 표준으로 정해진 이래 1998년 NIST가 DES를 대신 할 새로운 128bit 블록 암호 알고리즘을 공모하여 5개 후보 중에서 Rijndael이 채택한 AES(advanced encryption standard)가 있다., DES를 대체하기 위해 스위스 연방기술 기관에서 개발한 128 비트 키를 사용하고 4비트 블록암호 방식으로 DES 보다 2배 정도 빠른 IDEA(international data encryption algorithm), 선형공격에 대응하고 DES 보다 3배 빠른 RC2, DES 보다 약 10배정도 빠른 속도의 RC4가 있다[4][5].

3.3 대칭키 블록 암호화 6개 기본원리 진단

블록 암호화는 크기가 고정된 블록을 위한 암호화 함수이다. 블록 암호화는 일정한 크기의 평문을 암호화해서 암호문을 만들어 내는데, 이 암호화 방법은 되돌리는 것이 가능한데, 일정한 암호문을 복호화하여 원래의 평문을 얻을 수 있다. 평문과 암호문은 항상 같은 크기를 가지며 이를 블록 암호화의 블록 크기라 한다. 대칭키 암호 알고리즘은 같은 키로 암호화, 복호화 하기 때문에, 대칭적 암호 알고리즘 이라 표현되므로서 키를 가진 서로에게 기밀성, 인증, 무결성을 제공한다. 대칭키 블록 암호 알고리즘 기본원리는 다음과 같이 6개 방향으로 진단 된다[5].

◉ Key Transformation

초기에 64비트인 DES 키는 56비트로 축소 된다. 이 때 나머지 8비트는 패리티 체크 비트 로 사용되거나 무시된다. 56비트로 축소된 DES 키는 16 ROUND의 연산에 쓰이는 16개의 48 비트 부속키로 만들어진다. 처음 56비트 키는 절반인 28비트씩 왼쪽, 오른쪽으로 나뉘어 지고 이 두개의 절반은 순환적으로 1혹은 2씩 왼쪽으로 SHIFT 된다. 이 과정은 ROUND에 따른 SHIFT 회수를 정해놓은 Table에 의해 결정된다. 키를 SHIFT 하는 이유는 16개의 ROUND 에서 사용할 부속키를 서로 다르게 하기 위해서다.

◉ Expansion Permutation

블록의 오른쪽 절반(32비트)을 48비트로 확장 한다. 이것은 두 가지 목적을 가지는데 첫 번째 는 32비트인 블록을 48비트인 부속키의 사이즈 에 맞추기 위해서이고, 두 번째는 이어서 실행 되는 S-Box Substitution에서 필요한 만큼의 길이를 맞추기 위해서 이다.

◉ S-Box Substitution

블록의 오른쪽 절반과 부속키 와의 XOR 후 얻은 48비트 결과 값을 6비트의 보조 블록 8개 로 나눈다. 이때 8개로 나뉘어 진 블록을 역시 8개로 분리된 S-Box에 넣어 4비트 결과 값을 얻게 된다. 연산순서는 첫 번째 블록이 첫 번째 S-Box에, 두 번째 블록은 두 번째 S-Box에 들어가는 식이다. S-Box는 4개의 행과 16개의 열로 이루어져 있는데 각각에는 4비트 정수의 값 (0~15)이 저장되어 있다. 이 값들은 6비트 보조블록에 의해 지정되는 행과 열에 의해 결정 된다. S-Box 연산은 DES에서 가장 중요한 과정이다. 다른 연산과 비교했을 때 S-Box는 비선형구조에다 분석하기 어렵기 때문이다.

◉ P-Box Permutation

S-Box Substitution의 결과 값인 32비트 블록 을 P-Box Permutation을 통해 동일한 크기의 결과 값(32비트)을 얻는다. 이번 연산 에서는 무시되거나 두 번 사용되는 비트가 없다. 모든 입력은 하나의 출력을 가진다. P-Box 결과 값은 초기에 나뉘어졌던 32비트 왼쪽 절반과 XOR되어 새로운 오른쪽 절반이 되고 기존의 오른쪽 절반은 새로운 왼쪽 절반이 되어 다음 ROUND를 준비한다.

◉ Final Permutation

모든 ROUND를 거친 32비트 왼쪽 절반과 오른쪽 절반은 64비트 하나의 블록이 된다. 그러나 마지막 ROUND에서는 오른쪽과 왼쪽의 절반은 서로 교환되지 않았다. 그 대신 최종 순열을 거치게 된다. 이 연산은 초기 순열의 역 연산이다. 복호화 알고리즘의 전체적인 흐름으로서 DES 알고리즘은 대칭 구조이기 때문에 복호화와 암호화를 같은 알고리즘으로 구현 할 수 있다. 단 복호화 알고리즘에서는 부속키를 암호화 역순으로 주어야 한다.

3.4 DES 알고리즘의 5개 단계 흐름 진단

DES 암호화 알고리즘의 전체적인 흐름을 진단 하면 다음과 같이 5개의 세부 단계로 진행된다. ① Initial Permutation(초기 순열)을 실행한다.② 64비트 블록을 왼쪽, 오른쪽 각각 32비트로 나눈다. ③ 데이터와 키를 조합하여 16round의 동일한 연산을 반복 실행 한다. ④ 왼쪽, 오른쪽으로 나누어진 블록을 하나로 합친다. ⑤ Final Permutation (최종 순열)을 실행한다. 하나의 Round 흐름을 진단하면 다음과 같이 8개 세부 단계로 진행된다. ① 56비트 키 중에서 48비트 선택(Compression Permutation)한다. ② 48비트 키를 왼쪽으로 정해진 만큼 SHIFT,실행 Round 순서에 의존한다. ③ 블록의 오른쪽 절반(32비트)을 48비트 로 확장 (Expansion Permutation)한다. ④ 48비트 키와 48비트 블록의 오른쪽 절반을 XOR 연산 한다. ⑤ S-Box Substitution 실행후 32비트 결과 값을 얻는다. ⑥ P-Box Permutation 을 실행하여 32 비트 결과 값을 얻는다. ⑦ P-Box를 통해 얻은 값과 블록 왼쪽 절반 32 비트를 XOR연산 한다. ⑧ 기존 오른쪽 절반을 새로운 왼쪽 절반에 넣고 위의 과정을 반복 한다.

4. 강화된 암호 알고리즘 적용방법

4.1 암호 강도지표 확보

암호강도의 정도를 나타내지 않기 위해 사용되는 평가지표(indicator)를 강도지표라 한다. 대표적 강도지표로 정보이론적인 지표인 암호문으로 부터 평문이나 키를 유추해 내기 어려운 정도인 불확정성(equivocation)과 이와 관련 되어 평문이나 키를 유추해 내기 위해 필요한 최소한의 암호문의 길이를 나타내는 판별거리 (utility distance)가 있다. 암호공격에 소요되는 계산횟수를 의미하는 워크 팩터(work factor) 등도 자주 이용된다.

4.2 워크 팩터의 증대

워크 팩터는 키를 알지 못한 공격자가 모든 가능한 키를 만들어 암호 알고리즘을 수행시킬 때 평문을 찾아낼 수 있는 평균적 횟수이다. 따라서 워크 팩터가 클수록 암호 알고리즘은 보다 강력하다. 좋은 암호는 평문의 정보를 암호문 전체에 고루 분산시켜야 하고 평문의 변경은 암호문의 여러 부분에 고루 영향을 미쳐야 한다. 평문의 각 문자 정보가 암호문 전체에 분산되는 특성을 확산(diffusion)이라 하며 암호 해독자는 해독을 위해 더 많은 양의 암호문을 필요로 하게 된다. 또한 암호 해독자는 평문의 어떤 문자가 암호문 에서 어떤 문자로 바뀌는지 알 수 없어야 한다.

4.3 연산모드 적용방법

DES 알고리즘 연산모드 적용을 위해서 연산 모드의 종류별로 적용방법을 진단해야 한다. 이때 검토되는 연산모드는 ECB 모드, CBC 모드, CFB 모드, OFB 모드가 있다.

4.3.1 ECB 모드(Electronic CodeBook mode)

ECB 모드는 DES알고리즘 연산모드 중 가장 간단한 방식이다. DES 암호 방식의 키 암호화 에 사용하며 평문을 64bit씩 나누어 암호화 하며 마지막 블록이 64bit 아니면 임의의 약속된 비트 모양을 padding하여 처리한다. ECB 모드는 동일한 평문블록 모양의 형식을 가지므로 동일 한 암호문을 출력하여 해독 가능성이 높다. 64bit 길이의 평문 암호화에 대표적 유용한 방법이다.

4.3.2 CBC 모드 (Cipher Block Chaining mode)

CBC 모드는 출력 암호문이 다음 평문 블록에 영향을 미친다. 각 암호문 블록이 전단의 암호문의 영향을 받으며 동일한 평문에 의한 동일한 암호문이 발생치 않는다.

암호화 Ci = EK(Mi⊕Ci-1)

복호화 Mi = DK(Ci)⊕Ci-1(단, C0 = IV0)

전송 중 암호문 블록 Ci에서의 한 비트의 오류

- 복호화된 평문 블록 Mi : 여러 비트의 영향
- 다음단의 평문블록 Mi+1 : 한 비트오류 유발
- 그 다음단의 평문블록 Mi+2 : 영향을 주지 않음

➜ 평문 블록 Mi에서의 한 비트의 오류

- 그 다음의 출력되는 모든 암호문에 영향을 미침

➜ 메시지 인증에 사용 -> 문서 인증 부호 MAC(Message Authentication Code)에 사용

4.3.3 CFB 모드 (Cipher FeedBack mode)

CBC 모드와 유사 -> 다른 점 : 암호문이 수신자의 암호기 입력으로 사용됨

암호화 Ci = EK(Ci-1)⊕Mi

복호화 Mi = EK(Ci-1)⊕Ci (단, C0 = IV0)

평문 블록내의 한 비트의 오류 -> 모든 암호문에 영향. 암호문 블록내의 한 비트의 오류 -> 복호화된 모든 평문 블록에 영향

4.3.4 OFB 모드(Output FeedBack mode)

OFB 모드는 ECB 모드의 단점과 CBC 모드와 CFB모드의 단점을 개선한 동작모드 이다. DES 암호키의 출력과 평문을 EX-OR하여 암호문 생성 -> 오류 전파가 없다. 암호문 송신자와 수신자 사이의 동기를 조절해야 한다. 전송 중인 암호문의 비트 손실이나 삽입에 유의해야 한다.

4.3.5 DES 알고리즘 적용

최근 DES 알고리즘을 암호-복호-암호의 과정으로 연달아 적용해서 보안성을 강화한 Triple-DES가 많이 사용된다. DES는 수차례의 기술진화로 안전성 측면에서 검증이 많이 이루어진 반면, 암복호에 시간소요가 부담이 된다. 그러나 시간소요 문제는 컴퓨팅 파워가 향상되면서 시간 단축이 가능해진 상태이다. 시간단축이 가능해진 상황에서는 “3.2 DES 알고리즘 진화 과정”에서 설명한 바와 같이 128 비트 알고리즘이 주로 권고되고 있다.

5. 결 론

암호화는 보안에 대처하는 가장 강력한 수단 이며

암호학은 암호작성과 암호해독 양쪽을 포함하는 학문으로서 정보화시대에 이용될 수 있는 중요한 연구 및 응용분야이다. DES는 64 비트 단위로 나뉘어 진 각각의 블록이 한번의 암호화 알고리즘을 거쳐 암호화 된다. 대칭키 알고리즘으로서 똑같은 키와 알고리즘이 암호화 와 복호화에 쓰인다. 키 길이는 64비트로 표현 되는데 이 중에서 실제로는 56비트만이 키로서 사용되고 나머지 8비트는 패리티 체크 비트로 사용된다. DES 알고리즘 선택 이유는 암호 강도에 대한 의문이 제기되고 있기는 하지만 상업적으로 가장 널리 보급되어 이용되고 있다. 또한 기본 알고리즘을 DES로 채택한 현장에서 앞으로도 상당한 기간 동안 이용이 계속될 것으로 예상되는 DES 알고리즘을 효과적으로 활용 하는 방안이 참고 되기를 기대 한다.

참고문헌

[1] Biham, Eli and Alex Biryukov: An Improvement of Davies' Attack on DES. J. Cryptology 10(3): 195 - 206 (1997)

[2] Biham, Eli, Orr Dunkelman, Nathan Keller: Enhancing Differential-Linear Cryptanalysis. ASIACRYPT 2002

[3] Campbell, Keith W., Michael J. Wiener: DES is not a Group. CRYPTO 1992: pp512 - 520

[4] Diffie, Whitfield and Martin Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard" IEEE Computer 10(6), June 1977

[5] Ehrsam and others., Product Block Cipher System for Data Security, U.S. Patent 3,962,539, Filed February 24, 1975

[6] Gilmore, John, "Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design", 1998, O'Reilly, ISBN 1-56592-520-3.

[7] Kaliski, Burton S., Matt Robshaw: Linear Cryptanalysis Using Multiple Approximations. CRYPTO 1994

[8] Knudsen, Lars, John Erik Mathiassen: A Chosen-Plaintext Linear Attack on DES. Fast Software Encryption - FSE 2000

[저자소개]

노 시 춘 (Si Choon Noh)

1987년 02월 : 고려대학교 경영정보학 석사
2005년 02월 : 경기대학교 정보보호기술 박사
2002년 11월 : KT 시스템보안부장
2004년 12월 : KT 충청전산국장
2005년 03월 ~ 현재 :남서울대학교 컴퓨터학과 교수
IT융합연구소연구위원

email : nsc321@nsu.ac.kr