(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년01월07일
(11) 등록번호 10-1583285
(24) 등록일자 2015년12월31일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 9/14* (2006.01)
(21) 출원번호 10-2014-0083716
(22) 출원일자 2014년07월04일
심사청구일자 2014년07월04일
(56) 선행기술조사문헌
KR1020120097729 A
KR1020100007327 A

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
최진영
서울특별시 노원구 동일로248길 16 506-1003(상계동, 수락파크빌아파트)
송유현
서울특별시 노원구 화랑로51가길 11-2 301호(공릉동)
(74) 대리인
특허법인충현

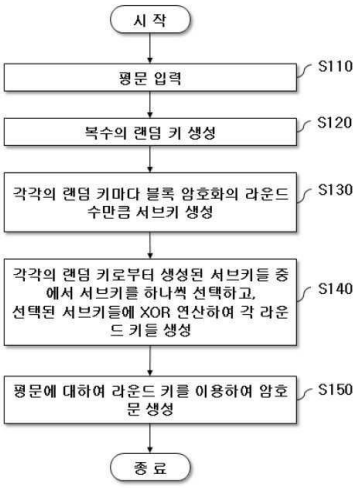
전체 청구항 수 : 총 12 항 심사관 : 문형섭

(54) 발명의 명칭 **확장 키를 이용한 블록 암호화 방법 및 그 방법에 따른 장치**

(57) 요 약

본 발명은 확장 키를 이용한 블록 암호화 방법 및 그 방법에 따른 장치에 관한 것으로서, 복수의 랜덤 키를 생성하고, 각각의 랜덤 키로부터 블록 암호화의 라운드 수만큼 서브키들을 생성하고, 각각의 랜덤 키로부터 생성된 서브키들 중에서 서로 상이한 랜덤 키로부터 생성된 것이고, 각각의 생성 순서가 상이한 것을 하나씩 선택하여 선택된 서브키들에 대하여 XOR 연산함으로써 각 라운드 키들을 생성하고 평문에 대하여 라운드 키들을 이용하여 암호문을 생성하는 블록 암호화 방법을 통해 블록 암호화 구조의 변경 없이 짧은 키를 확장하여 보안을 강화하고 동시에 고속의 암호화를 보장할 수 있다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

평문을 입력받는 단계;

복수의 랜덤 키를 생성하는 단계;

상기 각각의 랜덤 키마다 블록 암호화의 라운드 수만큼 서브키를 생성하는 단계;

상기 각각의 랜덤 키로부터 생성된 서브키들 중에서 서브키를 하나씩 선택하고, 상기 선택된 서브키들에 대하여 XOR 연산하여 각 라운드 키들을 생성하는 단계; 및

상기 평문에 대하여 상기 라운드 키들을 이용하여 암호문을 생성하는 단계;를 포함하되,

상기 선택된 서브키들은 서로 상이한 랜덤 키로부터 생성된 것이고, 각각의 생성 순서가 상이하며, 상기 선택된 서브키들의 생성 순서는 소정의 숫자만큼 차이가 나는 것을 특징으로 하는 블록 암호화 방법.

청구항 2

제 1 항에 있어서,

상기 소정의 숫자는 라운드 수보다 작은 정수인 것을 특징으로 하는 블록 암호화 방법.

청구항 3

제 1 항에 있어서,

상기 암호문을 생성하는 단계는,

상기 평문에 대하여 각 라운드마다 상기 라운드 키를 이용하여 XOR 연산하는 것을 특징으로 하는 블록 암호화 방법.

청구항 4

제 1 항에 있어서,

상기 암호문을 생성하는 단계는,

상기 생성된 암호문에 상기 암호문의 일부와 상기 랜덤 키들을 변수로 하는 해시 함수를 적용하는 OTP (One Time Pad) 변환 단계를 더 포함하는 블록 암호화 방법.

청구항 5

제 4 항에 있어서,

상기 해시 함수는 XOR 연산 및 MD5 연산을 이용하는 것을 특징으로 하는 블록 암호화 방법.

청구항 6

제 1 항에 있어서,

상기 블록 암호화는 DES 암호화인 것을 특징으로 하는 블록 암호화 방법.

청구항 7

제 6 항에 있어서,

상기 랜덤 키의 개수는 4개 이상인 것을 특징으로 하는 블록 암호화 방법.

청구항 8

제 1 항 내지 제 7 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 9

평문을 입력받는 입력부;

복수의 랜덤 키를 생성하고, 상기 생성된 각각의 랜덤 키마다 블록 암호화의 라운드 수만큼 서브키를 생성하는 키 생성부;

상기 각각의 랜덤 키로부터 생성된 서브키들 중에서 서브키를 하나씩 선택하고, 상기 선택된 서브키들에게 대하여 XOR 연산하여 라운드 키들을 생성하는 XOR 연산부; 및

상기 평문에 대하여 상기 라운드 키들을 이용하여 암호문을 생성하는 암호문 생성부;를 포함하되,

상기 XOR 연산부는 상기 선택된 서브키들이 서로 상이한 랜덤 키로부터 생성된 것이고, 각각의 생성 순서가 상이하며, 상기 선택된 서브키들의 생성 순서는 소정의 숫자만큼 차이가 나는 것을 특징으로 하는 블록 암호화 장치.

청구항 10

제 9 항에 있어서,

상기 소정의 숫자는 라운드 수보다 작은 정수인 것을 특징으로 하는 블록 암호화 장치.

청구항 11

제 9 항에 있어서,

상기 블록 암호화는 DES 암호화이고, 상기 랜덤 키의 개수는 4개 이상인 것을 특징으로 하는 블록 암호화 장치.

청구항 12

제 9 항에 있어서,

상기 생성된 암호문에 상기 암호문의 일부와 상기 랜덤 키들을 변수로 하는 해시 함수를 적용하는 OTP (One Time Pad) 변환부를 더 포함하되,

상기 해시 함수는 XOR 연산 및 MD5 연산을 이용하는 것을 특징으로 하는 블록 암호화 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록 암호화 방법 및 그 방법에 따른 장치에 관한 것으로서, 더욱 상세하게는 복수의 랜덤 키로부터 생성된 서브키들을 조합하여 XOR 연산함으로써 생성된 라운드 키를 이용한 블록 암호화 방법 및 그 방법에 따른 장치에 관한 것이다.

배 경 기 술

[0002] 블록 암호(Block cipher)란, 암호문을 만들기 위해 암호 키와 알고리즘이 데이터 블록 단위로 적용되는 암호화 방법을 말하고 대표적인 블록 암호 방법은 DES(Data Encyption Standard)이다. 미국의 국가 표준국(NIST ; National Institute of Standards and Technology)이 DES를 국가 표준으로 채택하였으며, 암호 알고리즘이 공개되어 있고, 로열티 없이 사용할 수 있도록 허가하였기 때문에 전 세계적으로 사용되었다.

[0003] DES는 대칭형 암호 방식으로 정보를 보내는 사람과 받는 사람이 동일한 비밀키를 가지고 사용하며, 암호화하고자 하는 평문을 일정 크기인 블록으로 분할하여 각 블록에 대하여 랜덤 키 및 서브 키를 이용하여 암호화를 적용한다. DES는 키의 비트 길이가 56비트로서 짧기 때문에 보안성이 취약하다는 단점이 있어 이를 극복하기 위하여 Triple-DES가 제안되었다. Triple-DES는 DES를 3번 반복하는 방식으로써 안전성은 매우 향상되었으나 속도가

느리다는 단점이 있다.

[0004] 현재 블록 암호에서 키의 길이가 충분하면서 고속의 암호화 방식인 AES-128비트/192비트/256비트 등이 개발되어 표준으로 사용되고 있으나 AES 이전 DES가 미국의 표준화로 채택되었던 점, 따라서 전 세계적으로 DES가 널리 활용되었으며 DES의 변형인 Triple-DES가 아직 사용되고 있는 점에 비추어 기존의 DES를 보완하여 약화된 암호 강도의 향상에 기여할 수 있는 기술적 수단이 요구된다.

선행기술문헌

비특허문헌

[0005] (비특허문헌 0001) H.X.MEL, "CRY PTO GRAPHYDECRY PTED", ADDISON WESLEY, 2001.

발명의 내용

해결하려는 과제

[0006] 본 발명이 해결하고자 하는 첫 번째 과제는 짧은 키를 확장하여 보안을 강화함과 동시에 기존 암호 방식이 갖는 처리 속도를 보장할 수 있는 블록 암호화 방법을 제공하는 것이다.

[0007] 본 발명이 해결하고자 하는 두 번째 과제는 블록 암호화 구조를 변경하지 않으면서 추가적인 보안성 향상을 보장할 수 있는 블록 암호화 방법을 제공하는 것이다.

[0008] 본 발명이 해결하고자 하는 세 번째 과제는 다수의 암호화 방식에 공통적으로 적용할 수 있으며, 짧은 키를 확장하여 보안을 강화한 블록 암호화 장치를 제공하는 것이다.

[0009] 또한, 상기된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공하는데 있다.

과제의 해결 수단

[0010] 본 발명은 상기 첫 번째 과제를 달성하기 위하여, 평문을 입력받는 단계; 복수의 랜덤 키를 생성하는 단계; 상기 각각의 랜덤 키마다 블록 암호화의 라운드 수만큼 서브키를 생성하는 단계; 상기 각각의 랜덤 키로부터 생성된 서브키들 중에서 서브키를 하나씩 선택하고, 상기 선택된 서브키들에 대하여 XOR 연산하여 각 라운드 키들을 생성하는 단계; 및 상기 평문에 대하여 상기 라운드 키들을 이용하여 암호문을 생성하는 단계;를 포함하되, 상기 선택된 서브키들은 서로 상이한 랜덤 키로부터 생성된 것이고, 각각의 생성 순서가 상이한 것을 특징으로 하는 블록 암호화 방법을 제공한다.

[0011] 본 발명의 일 실시예에 의하면, 상기 라운드 키들을 생성하는 단계는 상기 선택된 서브키들의 생성 순서가 소정의 숫자만큼 차이가 날 수 있다.

[0012] 본 발명의 다른 실시예에 의하면, 상기 암호문을 생성하는 단계는 상기 평문에 대하여 각 라운드마다 상기 라운드 키를 이용하여 XOR 연산할 수 있다.

[0013] 본 발명의 또 다른 실시예에 의하면, 상기 블록 암호화는 DES 암호화이고, 랜덤 키의 개수는 4개 이상일 수 있다.

[0014] 본 발명은 상기 두 번째 과제를 달성하기 위하여, 상기 생성된 암호문에 상기 암호문의 일부와 상기 라운드 키들을 변수로 하는 해시 함수를 적용하는 OTP (One Time Pad) 변환 단계를 더 포함하는 블록 암호화 방법을 제공한다.

[0015] 본 발명의 일 실시예에 의하면, 상기 해시 함수는 XOR 연산 및 MD5 연산을 이용할 수 있다.

[0016] 본 발명은 상기 세 번째 과제를 달성하기 위하여, 평문을 입력받는 입력부; 복수의 램덤 키를 생성하고, 상기 생성된 각각의 랜덤 키마다 블록 암호화의 라운드 수만큼 서브키를 생성하는 키 생성부; 상기 각각의 랜덤 키로부터 생성된 서브키들 중에서 서브키를 하나씩 선택하고, 상기 선택된 서브키들에게 대하여 XOR 연산하여 라운드 키들을 생성하는 XOR 연산부; 및 상기 평문에 대하여 상기 라운드 키들을 이용하여 암호문을 생성하는 암호문 생성부;를 포함하되, 상기 XOR 연산부는 상기 선택된 중간 서브키들이 서로 상이한 랜덤 키로부터 생성된 것

이고, 각각의 생성 순서가 상이한 것을 특징으로 하는 블록 암호화 장치를 제공한다.

[0017] 본 발명의 상기 실시예에 의하면, 상기 XOR 연산부는 상기 선택된 서브키들의 생성 순서가 소정의 숫자만큼 차이가 날 수 있다.

[0018] 본 발명의 상기 실시예에 의하면 상기 블록 암호화는 DES 암호화이고, 상기 랜덤 키의 개수는 4개 이상일 수 있다.

[0019] 본 발명의 일 실시예에 의하면 상기 생성된 암호문에 상기 암호문의 일부와 상기 라운드 키들을 변수로 하는 해시 함수를 적용하는 OTP (One Time Pad) 변환부를 더 포함하되, 상기 해시 함수는 XOR 연산 및 MD5 연산을 이용할 수 있다.

[0020] 본 발명은 상기 다른 기술적 과제를 해결하기 위하여, 상기 기재된 실시예들을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

발명의 효과

[0021] 본 발명에 따르면, 짧은 키를 확장하여 보안을 강화하고 동시에 기존 암호 방식이 갖는 처리 속도를 보장할 수 있는 블록 암호화 방법을 제공할 수 있다. 나아가, 블록 암호화 구조의 변경 없이 추가적인 OTP 단계를 통해 보안성을 향상시킬 수 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시예에 따른 확장 키를 이용한 블록 암호화 방법의 순서도이다.

도 2a는 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법의 순서도이다.

도 2b는 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법의 개념도이다.

도 3은 복수의 랜덤 키로부터 생성한 서브키들을 나타낸 표이다.

도 4a는 각각의 랜덤 키로부터 생성된 서브키 들 중에서 생성 순서가 1씩 차이나도록 서브키를 선택한 예시이다.

도 4b는 각각의 랜덤 키로부터 생성된 서브키 들 중에서 서브키를 선택한 예시이다.

도 5는 선택된 서브키들을 XOR 연산하여 생성한 라운드 키를 나타낸 표이다.

도 6은 64비트 평문에 본 발명의 일 실시예에 따른 확장 키를 이용한 블록 암호화 방법을 적용하여 64비트 암호문을 생성하는 것을 나타낸 개념도이다.

도 7a는 본 발명의 다른 실시예에 따른 OTP 변환 단계를 포함하는 블록 암호화 방법에 대한 암호화할 때의 OTP 변환 코드이다.

도 7b는 본 발명의 다른 실시예에 따른 OTP 변환 단계를 포함하는 블록 암호화 방법에 대한 복호화할 때의 OTP 변환 코드이다.

도 8은 본 발명의 또 다른 실시예에 따른 확장 키를 이용한 블록 암호화 장치의 구성도이다.

도 9는 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법을 실시하기 위한 라운드 키 생성 예이다.

도 10a는 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법에 의하여 텍스트 형식의 평문을 암호화하는 단계를 나타낸 표이다.

도 10b는 도 10a의 암호문을 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법에 의하여 복호화하는 단계를 나타낸 표이다.

도 11a는 그림 형식의 원본화면과 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법에 의하여 원본화면을 암호화한 암호화 화면을 나타낸 그림이다.

도 11b는 도 11a의 원본화면과 암호화 화면을 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법에 의하여 다시 복호화한 복호화 화면을 나타낸 그림이다.

발명을 실시하기 위한 구체적인 내용

[0023] 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요 혹은 기술적 사상의 핵심을 우선 제시한다.

[0024] 블록 암호화 방법 중에서 표준으로서 사용되었던 것은 DES 암호화 방법이다. DES는 미국에서 금융 업무용 표준으로 채택되었고, 그 알고리즘이 공개되어 있고 로열티 없이 사용할 수 있도록 허가되어 전 세계적으로 널리 사용될 수 있었다. 대칭형 암호 방식으로 정보를 보내는 사람과 받는 사람이 동일한 비밀 키를 가지고 사용하며 암호화되는 키가 작아 암호화가 빠르다. 우리 주변에서 DES를 이용한 것으로는 스마트 카드(smart card)를 들 수 있다. IBM에서 개발했고 미국 정부에서 1급 비밀 이하의 일반적인 데이터 전송에 사용할 수 있다는 인증을 받았다. DES는 암호화를 위해 메세지를 64비트 블록으로 나누고, 각각 복잡한 16 단계의 라운드를 거쳐 키와 혼합되어 암호문을 생성한다.

[0025] 다만, DES의 경우 키의 길이가 56비트로서 짧기 때문에 보안에 있어서 취약한 단점이 있다. 이를 해결하고자 키의 길이를 충분히 늘린 AES-128비트/192비트/256비트 암호화가 고안되었다. AES 암호화는 키의 길이가 충분히 길기 때문에 보안에 강하고 고속의 암호화를 보장하지만, DES가 활용되는 곳에 새로운 구조인 AES를 활용하여 암호화하기 위해서는 비용적인 문제가 있다. 이 때문에 DES를 그대로 활용하여 DES를 3번 반복한 Triple-DES도 고안되어 사용되고 있지만, Triple-DES는 안정성은 매우 향상되었으나 속도가 느리다는 단점을 가진다.

[0026] 따라서 본 발명은 DES 암호화 구조를 그대로 활용하면서 보안성을 향상시키고, 속도를 저하시키지 않기 위해 평문을 입력받는 단계; 복수의 랜덤 키를 생성하는 단계; 각각의 랜덤 키마다 블록 암호화의 라운드 수만큼 서브키를 생성하는 단계; 각각의 랜덤 키로부터 생성된 서브키들 중에서 서브키를 하나씩 선택하고, 선택된 서브키들에 대하여 XOR 연산하여 각 라운드 키들을 생성하는 단계; 및 평문에 대하여 라운드 키들을 이용하여 암호문을 생성하는 단계를 포함하되, 선택된 서브키들은 서로 상이한 랜덤 키로부터 생성된 것이고, 각각의 생성 순서가 상이한 것을 특징으로 하는 블록 암호화 방법을 제안한다.

[0027] 도 1은 본 발명의 일 실시예에 따른 확장 키를 이용한 블록 암호화 방법의 순서도이다.

[0028] S110 단계에서, 평문을 입력받는다. 평문은 암호화 하고자 하는 대상인 것으로 텍스트 파일, 그림 파일, 멀티미디어 파일 등 다양한 형태가 될 수 있다. 블록 암호화 방식에 따라서 정해진 블록 크기만큼씩 평문을 나누어 암호화하게 된다. 본 발명의 일 실시예에서는 64비트 블록으로 나누어 평문을 암호화하는 것을 예시하고 있다.

[0029] S120 단계에서, 복수의 랜덤 키를 생성한다. DES 암호화의 경우 하나의 랜덤 키를 이용하지만 본 발명에 따르면 확장 키를 생성하기 위하여 복수의 랜덤 키를 필요로 한다. 블록 암호화 방법이 DES 암호화인 경우, 랜덤 키의 개수는 키의 길이에 따라 결정되며 키의 길이가 64 비트인 경우 4개 이상일 수 있다. 이하에서 설명하게 될 도 9a, 도 9b, 도 10a, 도 10b의 실시예에도 4개의 랜덤 키를 생성하여 본 발명을 설명할 것이다. 랜덤 키의 길이는 64비트이며, 블록 암호화 방법에 따라서 달라질 수 있음은 자명할 것이다.

[0030] S130 단계에서, 각각의 랜덤 키마다 블록 암호화의 라운드 수만큼 서브키를 생성한다. DES의 경우는 서브키를 생성하기 위하여 64비트의 랜덤 키를 56비트로 축소 치환하며, 일반적인 DES 알고리즘으로 축소 치환할 수 있다. 서브키를 생성하는 방법은 DES 표준 키-생성기(key-generator)에 의한 것일 수 있다. 구체적으로 하나의 랜덤 키에 대하여 블록 암호화의 라운드 수만큼 서브키들을 생성하고, 이와 같이 복수의 랜덤 키 각각에 대하여 서브키들을 생성하게 되는 것이다. 따라서 랜덤 키의 개수가 n개 이고, 블록 암호화의 라운드 수가 m개라면 서브키는 n X m개만큼 생성되는 것이다. DES 의 경우 블록 암호화의 라운드는 16단계가 되고, 이하에서 설명하게 될 실시예의 경우 4개의 랜덤 키를 생성하기 때문에 서브키는 총 4 X 16 = 64 개가 생성된다. 이를 표로써 나타내면 도 3과 같다. 랜덤 키는 K1, K2, K3, K4이고, 서브키는 표의 세로방향으로 각각의 랜덤 키마다 라운드 수인 16개씩 생성된 것을 확인할 수 있다.

[0031] S140 단계에서, 각각의 랜덤 키로부터 생성된 서브키들 중에서 서브키를 하나씩 선택하고, 선택된 서브키들에 대하여 XOR 연산하여 각 라운드 키들을 생성한다. 선택된 서브키들은 서로 상이한 랜덤 키로부터 생성된 것이고, 각각의 생성 순서가 상이한 것을 특징으로 할 수 있다. 즉, 하나의 랜덤 키로부터 생성되어 생성 순서로 식별되는 서브키들 중에서 하나를 선택하고, 다른 랜덤 키로부터 생성된 서브키들 중에서 이미 선택된 서브키들과 생성 순서가 다른 것을 선택하게 되는 것이다. 예를 들어, 4개의 랜덤 키로부터 16 개의 라운드를 가지는 블록 암호화를 하기 위하여 16개의 서브키들이 생성하면, 동일한 랜덤 키로부터 생성된 서브키들은 16개이고, 4개의 랜덤 키마다 서브키를 하나씩 선택할 수 있다.

[0032] 본 발명의 일 실시예에 따르면 선택된 서브키들의 생성 순서가 소정의 숫자만큼 차이가 날 수 있다. 도 4a는 생성 순서가 1씩 증가하도록 서로 다른 서브키를 하나씩 선택한 것(K1_1, K2_2, K3_3, K4_4)을 나타낸다. 소정의 숫자는 라운드 수보다 작은 정수가 될 것이며 증가하거나 감소하도록 선택할 수 있으며, 통상의 기술자가 적절하게 결정하여 실시할 수 있음은 당연하다. 이때 선택된 서브키들의 생성 순서가 동일하면 안 된다.

[0033] 또한, 도 4b와 같이 서로 다른 서브키를 하나씩 선택할 수도 있다. 구체적으로 K1으로부터 생성된 서브키들 중에서 생성 순서가 2인 것(K1_2), K2로부터 생성된 서브키들 중에서 생성 순서가 10인 것(K2_10), K3으로부터 생성된 서브키들 중에서 생성 순서가 12인 것(K3_12), K4로부터 생성된 서브키들 중에서 생성 순서가 6인 것(K4_6)을 선택한 것을 나타낸다.

[0034] 본 발명의 일 실시예에 따르면 선택된 서브키들의 생성 순서가 소정의 숫자만큼 차이가 날 수 있다. 도 4a는 생성 순서가 1씩 증가하도록 서로 다른 서브키를 하나씩 선택한 것(K1_1, K2_2, K3_3, K4_4)을 나타낸다. 소정의 숫자는 라운드 수보다 작은 정수가 될 것이며 증가하거나 감소하도록 선택할 수 있다. 이때 선택된 서브키들의 생성 순서가 동일하면 안 된다. 이후 XOR 연산을 하게 되는 것과 관련하여 동일한 순서대로 XOR 연산할 경우 하나의 랜덤 키로부터 서브키를 생성한 효과만을 발생시키기 때문이다. 따라서 생성순서가 다른 것을 선택하여 XOR 연산해야만 랜덤 키들의 조합효과가 발생하여 이후 라운드 키가 확장된 효과를 가진다.

[0035] 선택된 서브키들은 XOR 연산에 의하여 라운드 키를 생성하게 된다. 도 5는 4개의 랜덤 키로부터 생성된 서브키들을 하나씩 선택하여 순차적으로 XOR 연산함으로써 총 16개의 라운드 키를 생성한 것을 표로 나타낸 것이다. 예를 들어, 1번째 라운드 키 R1은 K1_1 XOR K2_2 XOR K3_3 XOR K4_4 로 연산된 값이 된다.

[0036] 이 단계에 의하여 블록 암호화 방법은 키가 확장된 효과를 가지고, '확장된 키'라는 것은 라운드 키를 의미한다. 일반적인 블록 암호화 방법인 DES 암호화에서 하나의 랜덤 키로부터 각 라운드 수만큼 서브키를 생성하여 서브키를 각 라운드에 대응시켜 암호화하는 것과 비교하여, 본 발명에 따른 라운드 키는 복수의 랜덤 키로부터 다시 각각 라운드 수만큼 서브키들을 생성하고, 생성된 서브키들을 조합하여 XOR 연산함으로써 생성되는 것이기 때문에 원래의 방식에서의 라운드 키가 확장된 효과를 가진다. 이와 같이 확장된 라운드 키를 이용하는 것은 키의 수 조합을 증가시켜 키를 찾는 어려움을 더욱 가중시키게 되는 것을 의미한다.

[0037] S150 단계에서, 평문에 대하여 라운드 키들을 이용하여 암호문을 생성한다. 각 라운드마다 대응되는 라운드 키를 이용하여 XOR 연산함으로써 최종적으로 암호문을 생성할 수 있다. DES 암호화의 경우 공개된 알고리즘에 의하여, 각 라운드에서의 연산이 정의되어 있으며 첫 라운드 전에 초기 치환, 마지막 라운드 이후에 최종 치환이 추가될 수 있다. 물론 공개된 알고리즘이 아닌 다른 알고리즘에 의하여 연산하는 것도 가능하며 본 발명의 일 실시예에서는 XOR 연산을 이용하여 각 단계를 연산하는 것을 개시하고 있다. 도 6은 64비트 평문에 본 발명의 일 실시예에 따른 확장 키를 이용한 블록 암호화 방법을 적용하여 64비트 암호문을 생성하는 것을 나타낸 개념도이다.

[0038] 도 1에 의한 최종 암호문은 블록 단위로 암호화된 것으로 확장된 키에 의하여 보안성이 향상되어 키를 가지고 있지 않은 자가 복호화 시도하는 것이 이론적으로 불가능하다. 자세히 설명하면 S140 단계에서 서브키들을 XOR 하게 될 경우 원래의 값을 분리하는 것은 샤논(Shannon)의 정리에 의하여 불가능하기 때문에 확장된 키는 이론적으로 값을 알 수 없다. 암호화 속도 측면에서 라운드 키는 비트 수인 길이, 키의 개수가 변화 없이 블록 암호화 과정에 대입하게 되고 암호화를 거쳐 생성된 값도 비트의 변화가 없기 때문에 속도가 느려지는 문제는 발생하지 않는다. 따라서 짧은 키의 길이가 유지되어 DES의 장점인 속도가 빠르다는 점은 그대로 유지된다. 또한, 64비트의 랜덤 키 4개를 조합하여 사용하는 경우 56비트로 축소되고 결국 224비트의 키를 이용하게 된다. 224비트의 키가 모두 일치해야만 동일한 라운드 키들을 생성할 수 있고, 56비트 4개의 키를 모두 찾는 노력은 현실적으로 해결될 수 없는 비트 길이이다. 반면에 표준 DES는 라운드 키들이 56비트의 랜덤 키 하나에 종속되어 생성되기 때문에 하나의 키만 찾으면 라운드 키들을 모두 찾을 수 있어 보안에 취약한 것이다.

[0039] 블록 암호화 방법 중에서 파이스텔 암호(Feistel cipher) 들 중 대부분은 최종 치환 과정을 포함한다. 이 최종 치환이 보안성이 약하거나 최종치환 과정이 없는 경우 확장된 키를 이용하는 블록 암호화 방법의 보안성 효과를 증대시키기 위해서 OTP 변환 단계를 더 포함할 수 있다. 이에 도 2a는 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법의 순서도이고, 도 2b는 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법의 개념도이다.

[0040] 도 2a의 S210 단계 내지 S250 단계는 각각 도 1의 S110 단계 내지 S150 단계에 대응되어 중복되는 설명은 도 1의 상세한 설명으로 대체한다.

[0041] S260 단계에서, 암호문에 해시 함수를 적용하는 OTP(One Time Pad) 변환을 수행한다. 암호문은 이미 암호화된 것이지만 보안성을 향상시키기 위해 OTP 변환 단계를 추가할 수 있는 것이다. 이미 생성된 암호문을 입력받아 수행되기 때문에 기존의 블록 암호화의 구조를 변경시키지 않는 장점이 있어 어떠한 블록 암호화 방법이든 적용이 가능하다. 본 발명의 OTP 변환은 암호문의 일부, 랜덤 키, 카운터 변수를 연결하여 HASH 연산한 결과 값과 암호문의 일부를 XOR 연산한다. HASH는 MD5와 같은 일반적인 해시 함수가 될 수 있다. 본 발명의 다른 실시예는 도 7a의 코드로 OTP 변환하여 암호문을 변환하고, 도 7b의 코드로 OTP 변환 단계를 거친 암호문에 대하여 복호화할 수 있다.

[0042] 도 7a 및 7b의 변수 및 연산 설명은 다음과 같다. K1, K2, K3, K4는 64 비트의 램덤 키이고, '+'는 변수들을 연결하는 것을 의미한다. 따라서 K5는 K1 내지 K4를 연결하여 256 비트의 길이가 된다. RC는 암호문의 한 블록의 오른쪽 32비트이고, LC는 암호문의 한 블록의 왼쪽 32비트이다. I는 카운터 변수이고, xor은 XOR 연산을 의미한다. 반복 연산(For-Next 구문)에 의해 모든 암호문에 대하여 OTP 변환을 수행한다. 블록 암호화를 통해 평문을 암호화하는 경우 대부분 평문의 크기가 암호화 단위(예를 들어, 64비트, 128비트, 256비트 등)를 초과하기 때문에 추가적으로 블록 사이퍼 모드가 필요하다. OTP 변환은 일종의 블록 사이퍼 모드이며, 다른 것으로는 CBC, OFB, PCBC, CTR 등이 있다.

[0043] 본 발명에 따른 OPT 변환 단계를 거치면 추가적인 블록 사이퍼 모드를 포함할 필요가 없으며 전자 코드북(electronic codebook, ECB)의 단점인 영상 윤곽이 나타나는 등의 보안 취약성 문제를 극복할 수 있다.

[0044] 도 8은 본 발명의 또 다른 실시예에 따른 확장 키를 이용한 블록 암호화 장치(40)의 구성도이다.

[0045] 블록 암호화 장치(40)는 입력부(41), 키 생성부(42), XOR 연산부(43), 암호문 생성부(44)를 포함하고, 추가적으로 OTP 변환부(45)를 더 포함할 수 있다. 블록 암호화 장치(40)의 각 구성은 아래와 같이 도 1 및 도 2의 세부 단계와 대응되는 바, 구체적인 설명은 중복되어 기재하지 않고 대응관계를 기재한다.

[0046] 입력부(41)은 평문을 입력받는다. 블록 암호화 장치가 구현된 환경에 따라서 다양하게 입력부가 구현될 수 있으며 평문의 종류에 따라서 달라질 수 있음은 자명할 것이다. 도 1의 S110 단계와 대응되는 구성이다.

[0047] 키 생성부(42)는 복수의 랜덤 키를 생성하고, DES의 경우 64비트의 랜덤 키를 56비트로 축소하고 축소된 복수의 랜덤 키로부터 16 단계의 라운드 수만큼 서브키들을 생성한다. 키 생성부는 실시자에 의하여 변경가능할 것이며, DES-표준 키 제너레이터가 될 수도 있다. 도 1의 S120 및 S130 단계를 포함하는 구성이다.

[0048] XOR 연산부(43)는 키 생성부(42)로부터 서브키들을 입력받아 서로 다른 조합으로 선택하여 XOR 연산하여 라운드 키를 생성한다. DES의 경우 16개의 라운드 키를 생성하게 된다. 선택된 서브키들의 생성 순서가 소정의 숫자만큼 차이가 날 수 있다. 도 1의 S140 단계와 대응되는 구성이다.

[0049] 암호문 생성부(44)는 평문과 라운드 키들을 입력받아 각 라운드 단계를 거치면서 암호문을 생성한다. DES 암호화의 경우 각 라운드 단계는 공개 알고리즘에 의할 수 있으며, 본 발명의 일 실시예에 의하여 XOR 연산을 이용한 것일 수도 있다. 도 1의 S150 단계와 대응되는 구성이다.

[0050] OTP 변환부(45)는 추가적으로 포함될 수 있는 구성으로, 복수의 랜덤 키와 암호문을 입력 받아 해시 함수를 적용한다. 해시 함수는 XOR 연산 및 MD5 연산을 이용할 수 있다. 도 2의 S260 단계와 대응되는 구성이다.

[0051] 상기된 실시예의 블록 암호화 장치(40)를 이용하여 평문을 고속으로 암호문을 생성하고, 생성된 암호문은 이론적으로 공격이 불가능한 정도의 보안성을 보장한다. 기존 블록 암호화 방식의 구조 변화 없이 키를 안전한 길이만큼 확장하여 암호화 할 수 있는 장점이 있다. 특히, 블록 암호화의 대표적이고 가장 널리 활용되고 있는 DES 암호화의 구조를 변경시키지 않고 그대로 적용할 수 있기 때문에 앞으로 활용도가 높아 DES의 계속적 사용을 가져올 수 있다.

[0052] 도 9는 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법을 실시하기 위한 라운드 키 생성 예이다. 구체적으로 첫 번째 행은 라운드 키를 생성하기 위해 순차적으로 XOR하는 식이고, 두 번째 행은 64 비트의 K1, K2, K3, K4는 랜덤 키이며, 2 번째 행부터 18 번째 행은 두 번째 행의 랜덤 키로부터 생성된 각 16개의 서브키들에 대해서 첫 번째 행의 식을 계산한 결과 값이다. 따라서 최종적으로 가장 오른쪽 열이 라운드 키가 된다.

[0053] 도 9의 라운드 키를 적용하여 평문이 텍스트인 경우 적용 예를 도 10a, 도 10b에서 설명하고, 평문이 그림 파일인 경우의 적용 예를 도 11a, 도 11b에서 이하 설명한다.

[0054] 도 10a는 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법에 의하여 텍스트 형식의 평문을 암호화하는 단계를 나타낸 표이고, 도 10b는 도 10b의 암호문을 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법에 의하여 복호화하는 단계를 나타낸 표이다.

[0055] 평문은 블록 사이즈인 64비트로 나누어지고, 표의 각 행은 각 라운드를 의미하고, 열은 각 라운드마다 대응되는 라운드 키를 적용하여 암호화되는 구체적인 값을 나타낸다. 도 10a는 초기 치환과 최종 치환 과정을 포함하고, 최종 치환 후에 해시 함수인 HF 함수를 적용하여 OTP 변환 단계를 포함하고 있다. 도 10b는 도 10a의 결과인 암호문에 대하여 OTP 변환 단계인 HF 함수를 적용하고, 초기 치환을 거쳐 다시 각 라운드에 대응되도록 복호화를 한다. 라운드가 종료되면 암호문의 좌측 32비트와 우측 32비트를 SWAP하고, 최종 치환 단계를 거쳐 텍스트 형식으로 변환하면 평문이 된다. 도 10b의 복호화 단계는 암호화를 거꾸로 수행하는 것이기 때문에 도 10a의 각 단계와 거꾸로 대응된다.

[0056] 도 11a는 그림 형식의 원본화면과 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법에 의하여 원본화면을 암호화한 암호화 화면을 나타낸 그림이다. 원본 화면에서 붉은 색 3개의 원이 겹쳐진 모양은 암호화 화면에서 전혀 알 수 없게 변형되었다.

[0057] 도 11b는 도 11a의 원본화면과 암호화 화면을 본 발명의 다른 실시예에 따른 OTP 변환 단계를 더 포함하는 블록 암호화 방법에 의하여 다시 복호화한 복호화 화면을 나타낸 그림이다. 도 11a의 암호화 화면을 다시 복호화 과정을 거쳐 도 11b와 같이 원본 화면을 얻을 수 있다.

[0058] 나아가, 본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0059] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0060] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0061] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0062] 40: 블록 암호화 장치

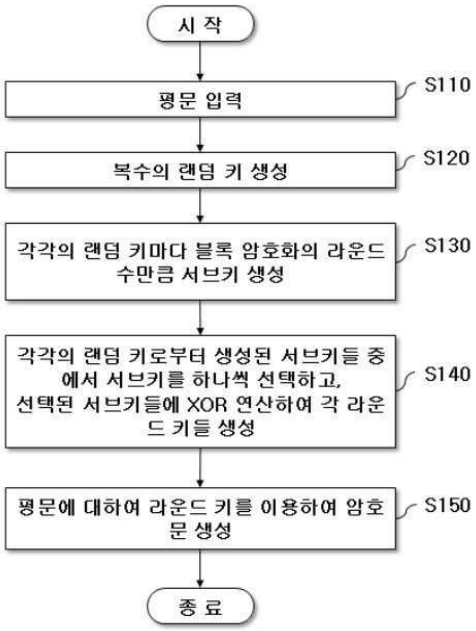
41: 입력부 42: 키 생성부

43: XOR 연산부 44: 암호문 생성부

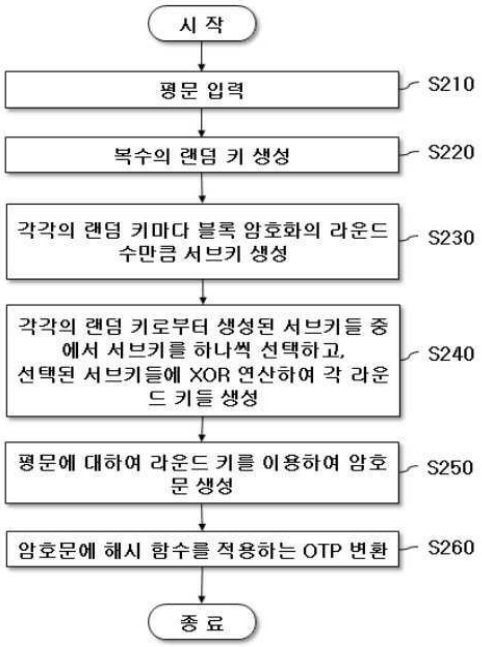
45: OTP 변환부

도면

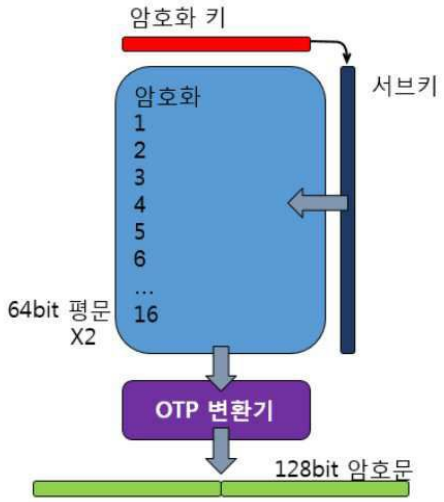
도면1


시 작
평문 입력
S110
복수의 랜덤 키 생성
S120
각각의 랜덤 키마다 블록 암호화의 라운드 수만큼 서브키 생성
S130
각각의 랜덤 키로부터 생성된 서브키들 중에서 서브키를 하나씩 선택하고, 선택된 서브키들에 XOR 연산하여 각 라운드 키들 생성
S140
평문에 대하여 라운드 키를 이용하여 암호문 생성
S150
종 료

도면2a


시 작
평문 입력
S210
복수의 랜덤 키 생성
S220
각각의 랜덤 키마다 블록 암호화의 라운드 수만큼 서브키 생성
S230
각각의 랜덤 키로부터 생성된 서브키들 중에서 서브키를 하나씩 선택하고, 선택된 서브키들에 XOR 연산하여 각 라운드 키들 생성
S240
평문에 대하여 라운드 키를 이용하여 암호문 생성
S250
암호문에 해시 함수를 적용하는 OTP 변환
S260
종 료

도면2b



도면3

랜덤 키	K1	K2	K3	K4
서브키	K1_1	K2_1	K3_1	K4_1
	K1_2	K2_2	K3_2	K4_2
	K1_3	K2_3	K3_3	K4_3
	K1_4	K2_4	K3_4	K4_4
	K1_5	K2_5	K3_5	K4_5
	K1_6	K2_6	K3_6	K4_6
	K1_7	K2_7	K3_7	K4_7
	K1_8	K2_8	K3_8	K4_8
	K1_9	K2_9	K3_9	K4_9
	K1_10	K2_10	K3_10	K4_10
	K1_11	K2_11	K3_11	K4_11
	K1_12	K2_12	K3_12	K4_12
	K1_13	K2_13	K3_13	K4_13
	K1_14	K2_14	K3_14	K4_14
	K1_15	K2_15	K3_15	K4_15
	K1_16	K2_16	K3_16	K4_16

도면4a

랜덤 키	K1	K2	K3	K4
서브키	K1_1	K2_1	K3_1	K4_1
	K1_2	K2_2	K3_2	K4_2
	K1_3	K2_3	K3_3	K4_3
	K1_4	K2_4	K3_4	K4_4
	K1_5	K2_5	K3_5	K4_5
	K1_6	K2_6	K3_6	K4_6
	K1_7	K2_7	K3_7	K4_7
	K1_8	K2_8	K3_8	K4_8
	K1_9	K2_9	K3_9	K4_9
	K1_10	K2_10	K3_10	K4_10
	K1_11	K2_11	K3_11	K4_11
	K1_12	K2_12	K3_12	K4_12
	K1_13	K2_13	K3_13	K4_13
	K1_14	K2_14	K3_14	K4_14
	K1_15	K2_15	K3_15	K4_15
	K1_16	K2_16	K3_16	K4_16

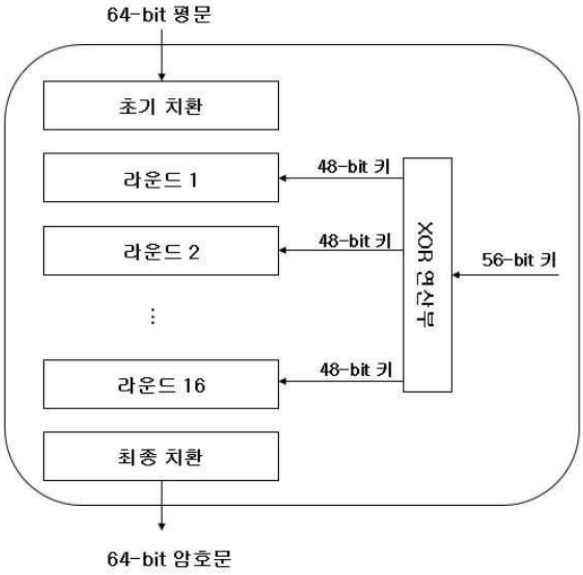
도면4b

랜덤 키	K1	K2	K3	K4
서브키	K1_1	K2_1	K3_1	K4_1
	K1_2	K2_2	K3_2	K4_2
	K1_3	K2_3	K3_3	K4_3
	K1_4	K2_4	K3_4	K4_4
	K1_5	K2_5	K3_5	K4_5
	K1_6	K2_6	K3_6	K4_6
	K1_7	K2_7	K3_7	K4_7
	K1_8	K2_8	K3_8	K4_8
	K1_9	K2_9	K3_9	K4_9
	K1_10	K2_10	K3_10	K4_10
	K1_11	K2_11	K3_11	K4_11
	K1_12	K2_12	K3_12	K4_12
	K1_13	K2_13	K3_13	K4_13
	K1_14	K2_14	K3_14	K4_14
	K1_15	K2_15	K3_15	K4_15
	K1_16	K2_16	K3_16	K4_16

도면5

K1으로부터 생성된 서브키	K2로부터 생성된 서브키	K3로부터 생성된 서브키	K4로부터 생성된 서브키	라운드 키
K1_1	K2_2	K3_3	K4_4	R1
K1_2	K2_3	K3_4	K4_5	R2
K1_3	K2_4	K3_5	K4_6	R3
K1_4	K2_5	K3_6	K4_7	R4
K1_5	K2_6	K3_7	K4_8	R5
K1_6	K2_7	K3_8	K4_9	R6
K1_7	K2_8	K3_9	K4_10	R7
K1_8	K2_9	K3_10	K4_11	R8
K1_9	K2_10	K3_11	K4_12	R9
K1_10	K2_11	K3_12	K4_13	R10
K1_11	K2_12	K3_13	K4_14	R11
K1_12	K2_13	K3_14	K4_15	R12
K1_13	K2_14	K3_15	K4_16	R13
K1_14	K2_15	K3_16	K4_1	R14
K1_15	K2_16	K3_1	K4_2	R15
K1_16	K2_1	K3_2	K4_3	R16

도면6



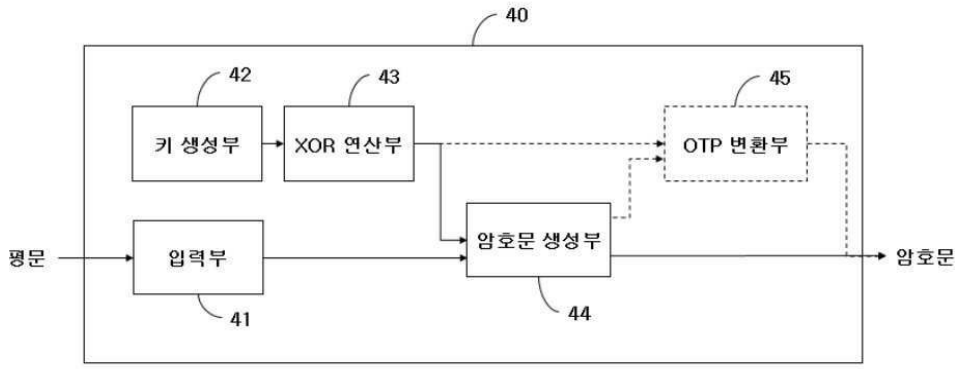
도면7a

1. K5 = K1+K2+K3+K4
2. For I=0 to 암호블럭수-1
3. LC2 =LC xor HASH (RC+K5+I.toString)
4. RC2 =RC xor HASH (LC2+K5+I.toString)
5. Next

도면7b

1. K5 = K1+K2+K3+K4
2. For I=0 to 암호블럭수-1
3. RC =RC2 xor HASH (LC2+K5+I.toString)
4. LC =LC2 xor HASH (RC+K5+I.toString)
5. Next

도면8



도면9

K1	K1 xor K2	K1 xor K2 xor K3	K1 xor K2 xor K3 xor K4
77B88C197A3E8D91	D144BA95E4B5529B	B3BC39AB68162A3C	3B7E79DCD6852B46
3DCC88FE5428	E795C72AC729	2DB8A1E62D12	6FFA599DD1B8
C539881BDCF6	ECD2E1C9DA9A	0434C8BEA4C2	98EDFC52D9F9
12AEE54DCDB1	93D34A157639	524460ACE743	D46F2B039D3D
D97C028B6C5D	2853D3BB1864	C8C9003EE642	E3BF25CB3DB0
60A7ECEBD394	35594D80EBB6	00A30FFCC542	C9BEC7694B3D
D0D4079147AF	0361D1352E95	2114038CE64A	6214F97DB196
618B72DE1A85	1D4DB5FB00D3	1B3FE0182F7F	A7F754C19DD0
A4F0A7D263FD	49CF971860AD	4692E7A05B36	D0B9ED56259B
8C9746E5EC87	4A29AF340F8B	844846435DBC	AE7E73796643
625A5B2E26DF	B9AC095E3057	226B000919BD	EF774CBEE00E
2DF160BFD1C7	412EAA67E1E8	083521C358B5	4AD7D9A477C6
824DDB06C7E3	F0BC9420BD4B	C10459430BBD	5DD97BBCA2E3
7D6311DEAD45	54AE42EE9436	45C28093199D	D24982449EF2
079D89EAC7D8	62F4364D4FEA	36DE6A7BB8C6	D4F5211E6F18
5B20D759F70B	55F73BDAB4C1	259A8FD4E89E	0FA8380A5756
194E3D2C9F7D	AEEBAC69B02F	A8178891ADCD	1503C4E95AB0

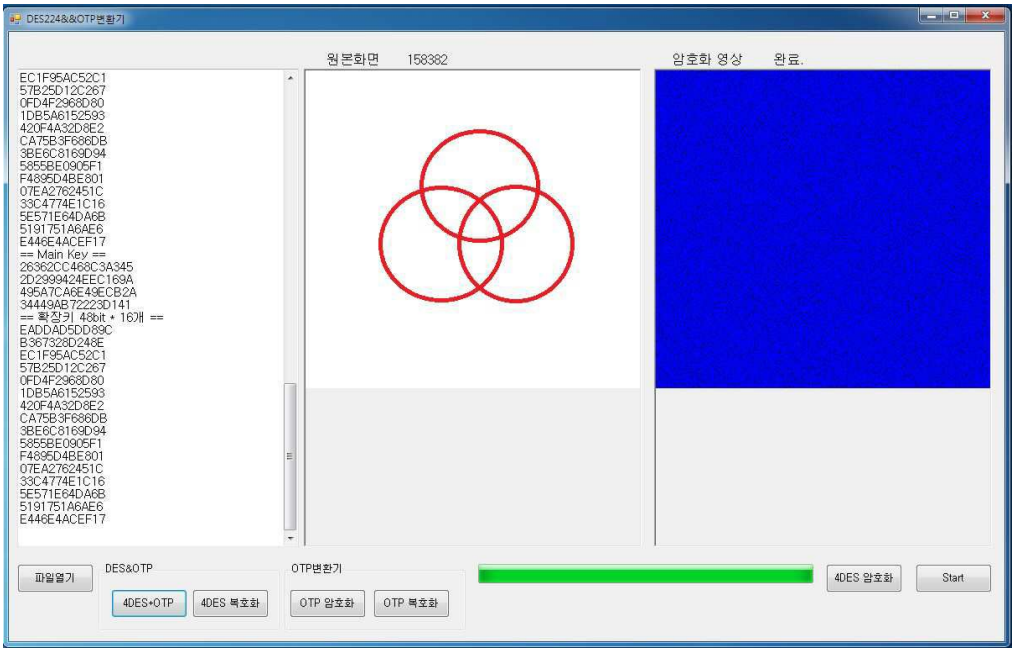
도면10a

"My frien"		"d is TOM"		평문
Hex : D7920667269656E		Hex : 420697320544F4D		아스키코드로 변환
FB12C96300FEA398		ED28E1CC001FC448		초기치환
Left	Right	Left	Right	Round key
00FEA398	1A3D2899	001FC448	F1250C43	6FFA599DD1B8
1A3D2899	D4884C1E	F1250C43	0A47311A	98EDFC52D9F9
D4884C1E	D069B7B2	0A47311A	88976CD4	D46F2B039D3D
D069B7B2	D4D73C74	88976CD4	9813A5CA	E3BF25CB3DB0
D4D73C74	E4B73FF8	9813A5CA	D74FA782	C9BEC7694B3D
E4B73FF8	8469809F	D74FA782	D93F0C7F	6214F97DB196
8469809F	7A1F2343	D93F0C7F	6FA3ACE6	A7F754C19DD0
7A1F2343	1C047C15	6FA3ACE6	11F9073F	D0B9ED56259B
1C047C15	DC6B5476	11F9073F	FE0C3B0A	AE7E73796643
DC6B5476	4A3CC4CC	FE0C3B0A	484B81D3	EF774CBEE00E
4A3CC4CC	C83DD991	484B81D3	887733FF	4AD7D9A477C6
C83DD991	F2C5DA6B	887733FF	54B7A4FB	5DD97BBCA2E3
F2C5DA6B	B5FA0BB6	54B7A4FB	177BA4B0	D24982449EF2
B5FA0BB6	8E25337B	177BA4B0	EB187A4B	D4F5211E6F18
8E25337B	4741EFBF	EB187A4B	3056ECAD	0FA8380A5756
4741EFBF	4F092B78	3056ECAD	C3ECBAB2	1503C4E95AB0
4F092B784741EFBF		C3ECBAB23056ECAD		SWAP
FECECA5F030FE90A		42653A1EA59F785F		최종치환
6971E9BEDA1372DB		E27E3D8EB6B6D975		HF함수 적용

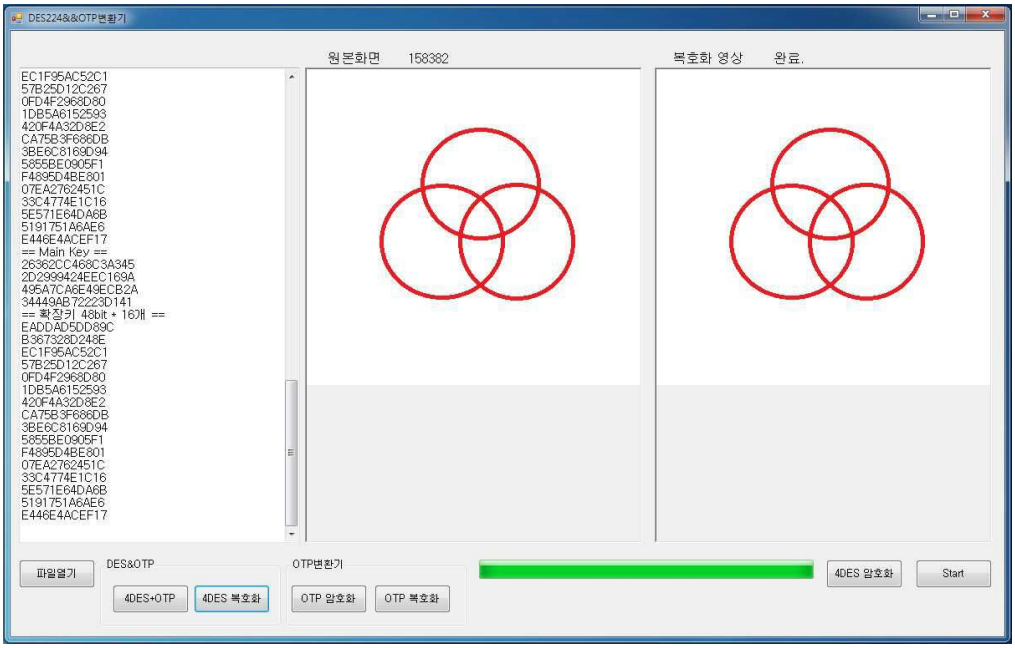
도면10b

6971E9BEDA1372DB		E27E3D8EB6B6D975		HF 함수 적용
FECECA5F030FE90A		42653A1EA59F785F		초기치환
Left	Right	Left	Right	Round key
4741EFBF	8E25337B	3056ECAD	EB187A4B	1503C4E95AB0
8E25337B	B5FA0BB6	EB187A4B	177BA4B0	0FA8380A5756
B5FA0BB6	F2C5DA6B	177BA4B0	54B7A4FB	D4F5211E6F18
F2C5DA6B	C83DD991	54B7A4FB	887733FF	D24982449EF2
C83DD991	4A3CC4CC	887733FF	484B81D3	5DD97BBCA2E3
4A3CC4CC	DC6B5476	484B81D3	FE0C3B0A	4AD7D9A477C6
DC6B5476	1C047C15	FE0C3B0A	11F9073F	EF774CBEE00E
1C047C15	7A1F2343	11F9073F	6FA3ACE6	AE7E73796643
7A1F2343	8469809F	6FA3ACE6	D93F0C7F	D0B9ED56259B
8469809F	E4B73FF8	D93F0C7F	D74FA782	A7F754C19DD0
E4B73FF8	D4D73C74	D74FA782	9813A5CA	6214F97DB196
D4D73C74	D069B7B2	9813A5CA	88976CD4	C9BEC7694B3D
D069B7B2	D4884C1E	88976CD4	0A47311A	E3BF25CB3DB0
D4884C1E	1A3D2899	0A47311A	F1250C43	D46F2B039D3D
1A3D2899	00FEA398	F1250C43	001FC448	98EDFC52D9F9
00FEA398	FB12C963	001FC448	ED28E1CC	6FFA599DD1B8
FB12C96300FEA398		ED28E1CC001FC448		SWAP
4D7920667269656E		6420697320544F4D		최종치환
"My frien"		"d is TOM"		텍스트로 변환

도면11a



도면11b


DES224&&OTP변환기
원본화면 158382
복호화 영상 완료.
EC1F95AC52C1
57B25D12C267
0FD4F2968D80
1DB5A6152593
420F4A32D8E2
CA75B3F686DB
3BE6C8169D94
5855BE0905F1
F4895D4BE801
07EA2762451C
33C4774E1C16
5E571E64DA6B
5191751A6AE6
E446E4ACEF17
== Main Key ==
26362CC468C3A345
2D2999424EEC169A
495A7CA6E49ECB2A
34449AB72223D141
== 확장키 48bit * 16개 ==
EADDAD5DD89C
B367328D248E
EC1F95AC52C1
57B25D12C267
0FD4F2968D80
1DB5A6152593
420F4A32D8E2
CA75B3F686DB
3BE6C8169D94
5855BE0905F1
F4895D4BE801
07EA2762451C
33C4774E1C16
5E571E64DA6B
5191751A6AE6
E446E4ACEF17
파일열기
DES&OTP
4DES+OTP
4DES 복호화
OTP변환기
OTP 암호화
OTP 복호화
4DES 암호화
Start