



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0097729
(43) 공개일자 2012년09월05일

(51) 국제특허분류(Int. Cl.)

H04L 9/14 (2006.01) H04L 9/28 (2006.01)

(21) 출원번호 10-2011-0017119

(22) 출원일자 2011년02월25일

심사청구일자 2011년02월25일

(71) 출원인

창원대학교 산학협력단

경상남도 창원시 의창구 사림동 9 창원대학교

(72) 발명자

이수현

경상남도 창원시 의창구 퇴촌로 92, 55호관
55419 (용동, 창원대학교)

김승현

경상남도 창원시 의창구 동산로175번길 13-1 (신
월동)

(74) 대리인

김대현

전체 청구항 수 : 총 2 항

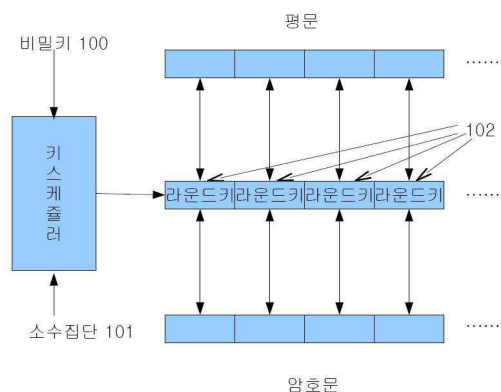
(54) 발명의 명칭 소수의 원시근을 이용한 암호화 방법

(57) 요약

본 발명은 정보의 암호화 방법에 관한 것으로, 특히 통신망 상에서 암호문의 일부가 우연히 해독되어도 해독된 일부의 암호문과 평문의 대조를 통해 비밀키 및 전체 평문 내용의 해독을 어렵게 하는 암호화, 복호화 방법 및 키 스케줄러의 구성에 관한 것이다.

본 발명에 따른 소수의 원시근을 이용한 암호화 방법은, 소수 집단과 비밀키를 입력받는 제1 단계; 비밀키를 소수 집단의 소수의 개수만큼 나누며, 소수 집단의 각 소수에 대한 원시근을 산출하는 제2 단계; 각 원시근과 나누어진 비밀키를 부분별로 대응시켜 배타적 논리합(XOR) 연산을 수행하여 제1 라운드키를 생성하는 제3 단계; 제1 라운드키와 원시근의 누승으로 발생하는 기약잉여계를 배타적 논리합 연산을 수행하여 제2 라운드키를 생성하는 제4 단계; 제3 라운드키부터 제n 라운드키까지를 제4 단계의 연산 방법으로 생성하는 제5 단계; 및 제2 라운드키 생성시부터 제n 라운드키까지는 각 라운드의 부분별로 소수의 개수의 보수 라운드 마다 나누어진 비밀키를 추가하여 배타적 논리합 연산을 수행하는 제6 단계;를 포함하여 키 스케줄러를 구성하는 것을 특징으로 한다.

대표도 - 도1



특허청구의 범위

청구항 1

소수 집단과 비밀키를 입력받는 제1 단계;

상기 비밀키를 상기 소수 집단의 소수의 개수만큼 나누며, 상기 소수 집단의 각 소수에 대한 원시근을 산출하는 제2 단계;

상기 각 원시근과 상기 나누어진 비밀키를 부분별로 대응시켜 배타적 논리합(XOR) 연산을 수행하여 제1 라운드를 생성하는 제3 단계;

상기 제1 라운드키와 상기 원시근의 누승으로 발생하는 기약잉여계를 배타적 논리합 연산을 수행하여 제2 라운드를 생성하는 제4 단계;

제3 라운드키부터 제n 라운드키까지를 상기 제4 단계의 연산 방법으로 생성하는 제5 단계; 및

상기 제2 라운드키 생성시부터 상기 제n 라운드키까지는 각 라운드의 부분별로 상기 소수의 개수의 보수 라운드마다 상기 나누어진 비밀키를 추가하여 배타적 논리합 연산을 수행하는 제6 단계;

를 포함하여 키 스케줄러를 구성하는 것을 특징으로 하는 소수의 원시근을 이용한 암호화 방법.

청구항 2

제1항에 있어서,

평문블록 부분별로 상기 생성된 라운드키와 반복 배타적 논리합 연산을 수행하여 암호문을 생성하되, 각 라운드의 부분별로 상기 소수의 개수의 보수의 역수 라운드마다 비트 반전 연산을 실시하는 것을 특징으로 하는 소수의 원시근을 이용한 암호화 방법.

명세서

기술 분야

[0001] 본 발명은 정보의 암호화 방법에 관한 것으로, 특히 통신망 상에서 암호문의 일부가 우연히 해독되어도 해독된 일부의 암호문과 평문의 대조를 통해 비밀키 및 전체 평문 내용의 해독을 어렵게 하는 암호화, 복호화 방법 및 키 스케줄러의 구성에 관한 것이다.

배경 기술

[0002] 일반적으로, 암호화 알고리즘은 기본적으로 약속된 둘 또는 특정 그룹의 인원들에게만 정보를 제공하기 위한 기술이다. 현재 다양한 암호화 알고리즘이 상용되고 있고 키 분배 방식에 따라 공개키 암호화 알고리즘과 비밀키 암호화 알고리즘으로 구분할 수 있다.

[0003] 공개키 암호화 알고리즘으로는 대표적으로 RSA알고리즘이 있으며 기본적인 개념은 키를 평문의 암호화에 사용되는 공개키와 암호문의 복호화에 사용되는 비밀키를 가지고 공개키를 공개하여 암호화에 사용하는 방법이다. 이때 비밀키를 모르면 암호문을 복호화 시킬 수가 없으며 비밀키를 가진 개인 또는 집단만이 암호문을 해독함으로써 그 목적을 달성한다.

[0004] 비밀키 암호화 알고리즘은 하나의 비밀키를 공유한 개인 또는 집단간에 정보를 공유하는 방법으로 비밀키인 비밀키 하나만을 가지고 암호화 및 복호화를 수행한다는 것이 공개키 암호화 방식과의 차이점이다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 상기한 암호화 알고리즘의 유형중 비밀키 암호화 알고리즘에 관한 것으로, 비밀키 암호화 알고리즘으로 암호화된 문서의 일부를 우연히 해독하였을 때 해독된 내용과 암호문의 대조를 통해 비밀키와 나머지 전체 암호문이 해독될 수 있는 종래 비밀키 암호화 알고리즘의 문제점을 해결하여 소수의 원시근을 이용한 암호

화 방법을 제공하는데 그 목적이 있다.

[0006] 본 발명이 해결하려는 과제들은 이상에서 언급한 과제로 제한되지 않으며, 여기에 언급되지 않은 본 발명이 해결하려는 또 다른 과제들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0007] 본 발명에 따른 소수의 원시근을 이용한 암호화 방법은, 소수 집단과 비밀키를 입력받는 제1 단계; 비밀키를 소수 집단의 소수의 개수만큼 나누며, 소수 집단의 각 소수에 대한 원시근을 산출하는 제2 단계; 각 원시근과 나누어진 비밀키를 부분별로 대응시켜 배타적 논리합(XOR) 연산을 수행하여 제1 라운드키를 생성하는 제3 단계; 제1 라운드키와 원시근의 누승으로 발생하는 기약잉여계를 배타적 논리합 연산을 수행하여 제2 라운드키를 생성하는 제4 단계; 제3 라운드키부터 제 n 라운드키까지를 제4 단계의 연산 방법으로 생성하는 제5 단계; 및 제2 라운드키 생성시부터 제 n 라운드키까지는 각 라운드의 부분별로 소수의 개수의 보수 라운드 마다 나누어진 비밀키를 추가하여 배타적 논리합 연산을 수행하는 제6 단계;를 포함하여 키 스케줄러를 구성하는 것을 특징으로 한다.

[0008] 또한, 본 발명의 소수의 원시근을 이용한 암호화 방법은, 평문블록 부분별로 생성된 라운드키와 반복 배타적 논리합 연산을 수행하여 암호문을 생성하되, 각 라운드의 부분별로 소수의 개수의 보수의 역수 라운드 마다 비트 반전 연산을 실시하는 것을 특징으로 한다.

발명의 효과

[0009] 상기 과제의 해결 수단에 의해, 본 발명의 소수의 원시근을 이용한 암호화 방법은, 사용되는 키의 길이, 각 라운드키의 길이를 임의로 적용할 뿐만 아니라 문서의 길이에 따라 각 평문 블록에 적용되는 라운드키를 모두 다르게 하여 전수 대조법으로 해독된 일부의 암호문을 통해 전체 평문의 정보를 해독할 수 없게 함으로써 종래의 비밀키 암호화 알고리즘 보다 암호화 강도가 커지는 효과가 있다.

도면의 간단한 설명

[0010] 도 1은 본 발명의 일실시예에 따른 소수의 원시근을 이용한 암호화 방법의 전체적인 개요를 도시한 도면이다.
 도 2는 본 발명의 일실시예에 따른 소수의 원시근을 이용한 암호화 방법의 키 스케줄러를 구성하는 과정을 도시한 도면이다.
 도 3은 본 발명의 일실시예에 따른 소수의 원시근을 이용한 암호화 방법의 암호화 과정을 도시한 도면이다.
 도 4는 본 발명의 일실시예에 따른 소수의 원시근을 이용한 암호화 방법의 복호화 과정을 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0011] 이상과 같은 본 발명에 대한 해결하려는 과제, 과제의 해결 수단, 발명의 효과를 포함한 구체적인 사항들은 다음에 기재할 실시예 및 도면들에 포함되어 있다. 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다.

[0012] 이하, 첨부된 도면을 참조하여 본 발명을 보다 상세히 설명하기로 한다.

[0013] 도 1은 본 발명의 일실시예에 따른 소수의 원시근을 이용한 암호화 방법의 전체적인 개요를 도시한 도면이다.

[0014] 먼저, 도 1을 참조하여 본 발명의 일실시예에 따른 전체적인 구성을 살펴보면, 미리 선택한 임의의 개수의 소수 집단(101)과 비밀키(100)를 키 스케줄러에 입력하여 라운드키(102)를 발생시키고 각 블록에 일정한 횟수만큼 배타적 논리합(XOR, 이하 'XOR' 이라 함) 연산과 비트 반전 연산을 수행하여 암호화 및 복호화를 수행한다.

[0015] 도 2는 본 발명의 일실시예에 따른 소수의 원시근을 이용한 암호화 방법의 키 스케줄러를 구성하는 과정을 도시한 도면이다.

[0016] 도 2를 참조하여 키 스케줄러의 구성에 대해 살펴보면, 키 스케줄러는 일정한 길이의 비밀키(100)를 입력받아 선택한 소수 집단(101)의 수와 같은 수의 조각으로 나누고 선택한 각 소수에 대한 원시근을 모두 찾는다.

[0017] 제1 라운드키(102)는 각 원시근과 입력받은 비밀키(100)의 각 부분과 XOR을 하여 내림차순으로 정렬하여 각

부분의 라운드키(102)로 사용한다. 제2 라운드키부터는 그 이전 라운드의 키(102)와 원시근의 해당 누승의 소수와의 나머지, 즉 원시근의 누승으로 발생하는 기약잉여계 수와 XOR 연산을 수행한다.

[0018] 이때, 각 부분별로 사용한 소수의 개수의 보수 라운드 마다(0번째 부분은 n라운드마다, 1번째 부분은 n-1라운드마다, ... n-1번째 부분은 매 라운드마다) 입력받은 비밀키(100)의 각 부분과 추가로 XOR 연산을 수행한다. 각 부분별로 기약잉여계 수가 모두 사용되면 다음 원시근의 기약잉여계 수를 사용하여 키 스케줄링을 진행한다. 각 부분별로 소수로부터 파생된 원시근이 모두 사용되고 나면 다시 처음 사용된 원시근부터 순서대로 키 스케줄링을 진행한다.

[0019] 예를 들어, 128비트의 비밀키를 입력받으면, 이 비밀키를 32비트 단위로 끊어 4조각으로 나눈다. 시드(seed) 값으로 사용할 32비트 소수 4개를 선택하고 각 소수에 대한 원시근을 모두 찾는다. 제1 라운드키는 각 원시근과 입력받은 128비트의 비밀키의 각 부분과 XOR 연산을 수행하여 내림차순으로 각 부분의 제1 라운드키로 사용한다. 제2 라운드부터는 그 이전 라운드의 키와 원시근의 누승의 나머지, 즉 기약잉여계와 XOR 연산하되, 각 부분별로 4의 보수 라운드마다(0번째 부분은 4라운드마다, 1번째 부분은 3라운드마다, 2번째 부분은 2라운드마다, 3번째 부분은 매 라운드마다) 입력받은 비밀키의 각 부분과 추가로 XOR 연산한다. 각 부분별로 기약잉여계 수가 모두 사용되면 다음 원시근의 기약잉여계 수가 사용된다. 소수로부터 발생한 원시근을 모두 사용하면 다시 처음 사용했던 원시근부터 차례로 사용한다.

[0020] 도 3은 본 발명의 일실시예에 따른 소수의 원시근을 이용한 암호화 방법의 암호화 과정을 도시한 도면이다.

[0021] 도 3을 참조하여 생성된 라운드키로 암호문을 생성하는 과정을 살펴보면, 암호화는 평문블록 부분별로 생성된 라운드키와 반복 XOR 연산함으로써 이루어진다. 여기에 추가적으로 라운드키와 XOR 연산 후 각 라운드의 부분별로 소수의 개수의 보수의 역수 라운드 마다, 즉 각 부분의 순서 라운드 마다(0번째 부분은 매 라운드마다, 1번째 부분은 2라운드마다, 2번째 부분은 3라운드마다, 3번째 부분은 4라운드마다, ...) 비트 반전 연산을 실시한다.

[0022] 전체 부분 수의 공배수의 라운드를 진행하면(ex. 4부분이면 24라운드, 5부분이면 120라운드, 6부분도 역시 120라운드 ...) 한 블록의 암호화가 끝나고 다음 블록의 암호화를 실시하며 이렇게 평문의 끝까지 암호화를 실시한다.

[0023] 암호화가 끝나고 맨 마지막 부분에 각 소수별로 몇 번째 원시근 몇 번째 누승의 나머지 값에서 암호화가 종료했는지 기록하고 암호문을 전달한다.

[0024] 예를 들어, 암호화는 평문 각 32비트 부분별로 생성된 라운드키와 XOR 연산함으로써 이루어진다. 여기에 추가적으로 각 라운드의 4의 보수의 역수 라운드 마다(0번째 부분은 매 라운드마다, 1번째 부분은 2라운드마다, 2번째 부분은 3라운드마다, 3번째 부분은 4라운드 마다) 비트 반전을 실시한다. 총 24라운드를 진행하면 한 블록의 암호화가 끝나고 다음 128비트 블록의 암호화를 실시하며 이렇게 평문의 끝까지 암호화를 실시한다. 암호화가 끝나고 맨 마지막 부분에 각 시드 소수별로 몇 번째 원시근 몇 번째 누승의 나머지 값에서 암호화가 종료했는지 기록하고 암호문을 전달한다.

[0025] 도 4는 본 발명의 일실시예에 따른 소수의 원시근을 이용한 암호화 방법의 복호화 과정을 도시한 도면이다.

[0026] 도 4를 참조하여 암호문에서 평문을 복원하는 과정을 살펴보면, 복호화는 암호문의 마지막에 추가된 암호화 종료시의 정보를 바탕으로 암호화에 사용된 전체 라운드키를 우선 생성하여 라운드키 스택(301)에 저장한다.

[0027] 이후, 암호문의 마지막 블록에서부터 역순으로 라운드키 스택(301)에서 라운드키를 꺼내 XOR 연산해 나가면서 암호문을 복호화한다.

[0028] 이때, 암호화시 블록의 각 부분별로 비트 반전 연산이 있었기 때문에 블록의 처음 라운드키와 XOR 연산을 수행하기 전 우선 비트 반전 연산을 실시하고 이후 각 부분에 맞게 (0번째 부분은 매 라운드마다, 1번째 부분은 2라운드마다, 2번째 부분은 3라운드마다, 3번째 부분은 4라운드 마다, ...) 라운드키와 XOR 연산 전에 비트 반전을 실시한다.

[0029] 예를 들어, 복호화는 암호문의 맨 마지막 암호화 종료시의 정보와 정보를 제외한 암호문의 길이를 통해 전체 라운드 키를 복호화 이전에 계산하여 암호화의 역순으로 복호화를 실시한다.

[0030] 이와 같이, 본 발명의 일실시예에 따른 소수의 원시근을 이용한 암호화 방법은, 사용되는 키의 길이, 각 라운드키의 길이를 임의로 적용할 뿐만 아니라 문서의 길이에 따라 각 평문 블록에 적용되는 라운드키를 모두 다르게 하여 전수 대조법으로 해독된 일부의 암호문을 통해 전체 평문의 정보를 해독할 수 없게 함으로써 종래

의 비밀키 암호화 알고리즘 보다 암호화 강도가 커질 수 있다.

[0031] 이와 같이, 상술한 본 발명의 기술적 구성은 본 발명이 속하는 기술분야의 당업자가 본 발명의 그 기술적 사상이나 필수적 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다.

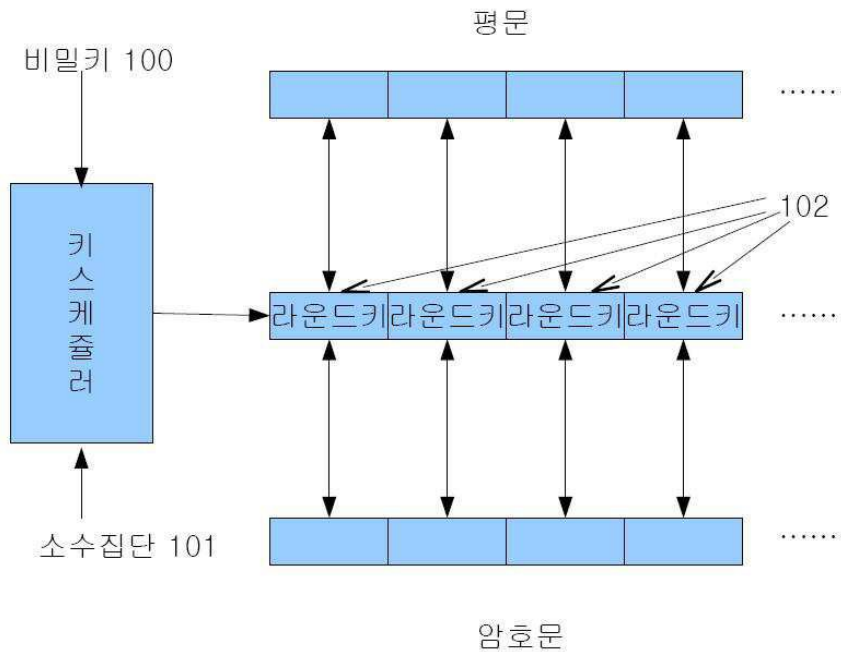
[0032] 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적인 것이 아닌 것으로서 이해되어야 하고, 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타나며, 특허청구범위의 의미 및 범위 그리고 그 등가 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

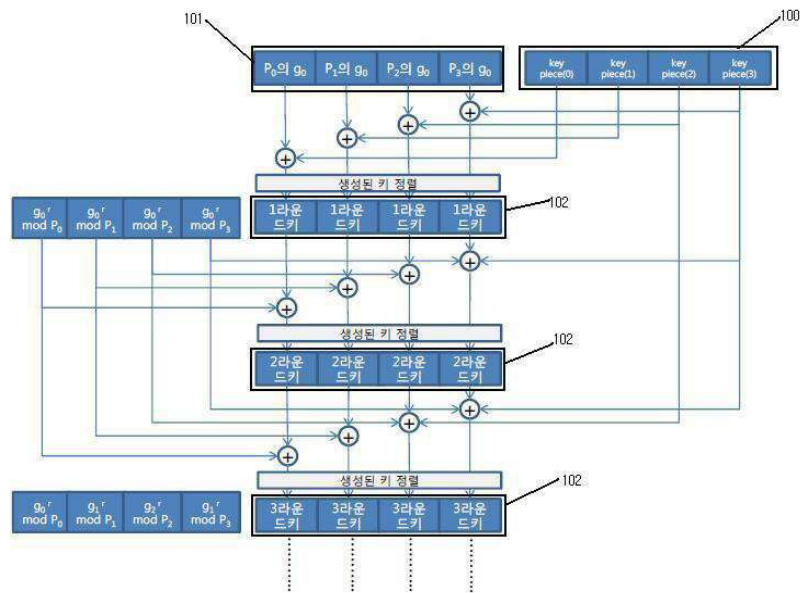
[0033] 100 : 비밀키
101 : 소수 집단
102 : 라운드키
301 : 라운드키 스택

도면

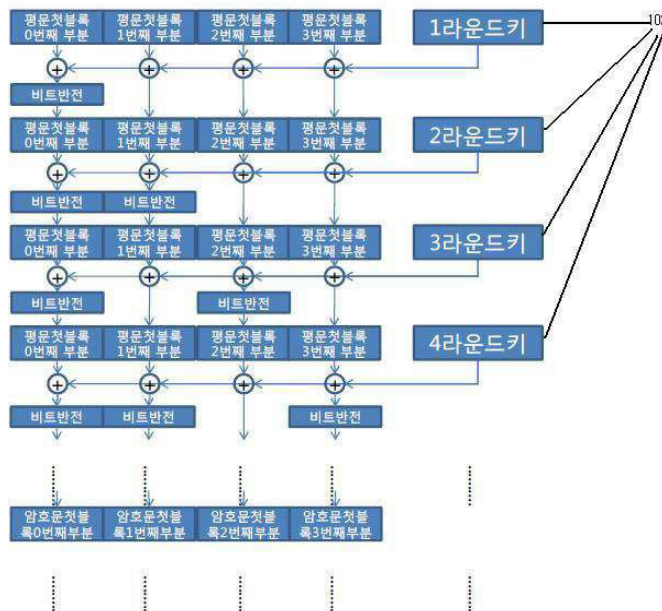
도면1



도면2



도면3



도면4

