(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) Int. Cl.[6]
H04K 1/04

(45) 공고일자 2003년04월11일
(11) 등록번호 10-0363457
(24) 등록일자 2002년11월21일

(21) 출원번호 10-1995-0704765
(22) 출원일자 1995년10월30일
번역문제출일자 1995년10월30일
(86) 국제출원번호 PCT/US1994/02960
(86) 국제출원일자 1994년03월16일
(81) 지정국 국내특허 : 오스트레일리아 바베이도스 불가리아 브라질 캐나다 체코 헝가리 일본 북한 대한민국 스리랑카 마다가스카르 몽고 노르웨이 뉴질랜드 폴란드 루마니아 슬로바키아 우크라이나 미국 베트남 AP ARIPO특허 : 말라위 수단
EA 유라시아특허 : 벨라루스 카자흐스탄 러시아
EP 유럽특허 : 오스트리아 스위스 리히텐슈타인 독일 덴마크 스페인 핀랜드 영국 룩셈부르크 네덜란드 포르투칼 스웨덴
OA OAPI특허 : 부르키나파소 베넹 중앙아프리카 콩고 코트디브와르 카메룬 가봉 기네 말리 모리타니 니제르 세네갈 차드 토고

(65) 공개번호 특1996-0702232
(43) 공개일자 1996년03월28일
(87) 국제공개번호 WO 1994/26045
(87) 국제공개일자 1994년11월10일

(30) 우선권주장 93107314.2 1993년05월05일 EP(EP)
08/061205 1993년05월13일 미국(US)

(73) 특허권자 리우,준쿠안
미합중국,캘리포니아94536,프리몬트,펜실베니아애비뉴3500,아파트107
(72) 발명자 리우,준쿠안
미합중국,캘리포니아94536,프리몬트,펜실베니아애비뉴3500,아파트107
(74) 대리인 박경재

심사관 : 정용주

(54) 암호체계용매핑레퍼토리

명세서

기술분야

<1> 본 발명은 일반적으로 암호화에 관한 것이며, 보다 구체적으로는 비밀 키이(secret key)에 의해 제어되는 데이타 암호 및 해독용 장치 및 방법에 관한 것이다.

배경기술

<2> 현 "전자" 시대에서, 나날의 상업, 사무 및 개인의 거래는 공공의 원격 통신 채널을 통해 교환되는 데이타에 의해 점차 이루어지고 있다. 극히 신중을 요하는 데이타는 불안한 기억장치에 종종 저장된다. 공공의 원격통신 채널을 통해 교환되거나 불안한 기억장치에 저장되는 데이타는 다른 사람에 의한 접근 용이하게 승인되어 비밀성 및 프라이버시가 보장될 수 없다.

<3> 기억장치에 있거나 공공의 원격통신채널을 통해 전송되는 경우 승인되지 않은 데이타 접근을 방지함에 있어서의 한가지 해결책이 데이타의 암호이다. 암호는 플레인텍스트를(plaintext) 난해한 사이퍼텍스트(ciphertext)로 변형시키는 계산형태이다. 해독은 난해한 사이퍼 텍스트로부터 플레인 텍스트를 회복시키는 암호의 역계산이다.

<4> 실제로, 데이타는 우선 공공채널을 통해 전송되거나 기억장치로 보내지기 전에 암호자에 의해 플레인텍스트로부터 사이퍼텍스트로 암호화된다. 데이타의 수신 또는 검색의 경우, 해독기는 본래의 데이타를 얻기 위하여 사이퍼텍스트를 도로 플레인텍스트로 해독시켜야 한다.

<5> 비밀키이의 암호법에 있어서 , 비밀키이는, 승인된 해독자가 해독을 효과적으로 이행하는 것과는 역으로 구성할 수 있도록 암호자가 승인된 해독기에 대한 암호를 어떠한 방식으로 이행하였는지에 관한 정보를 통과시키는데 사용된다. 그 반면에, 그러한 키이를 갖지 않은 승인되지 않은 다른 해독자는, 사이퍼텍스트를 해독하는것이 가능한 경우가 난해 하다는 것을 알 것이다.

<6> 종래에는, 비밀키이의 암호체계에 있어서, 암호 및 해독에 대한 단계 또는 알고리즘의 확립된 계산 시퀀스가 있다. 비밀키이의 암호체계는 대개는 알고리즘이 공공연히 공지되어 있다라는 가정으로 설계된다. 비밀로 유지될 필요성이 있는 것만이 전송자와 승인된 수신자 사이에서만 고유되는 비밀키이이다.

<7> 전형적으로 비밀키이는, 암호 및 해독을 달성하도록 입력으로서 플래인텍스트와 함께 취해지는 사용자 선택값을 알고리즘에 제공한다. 대개는, 알고리즘은 어떤 모듈로 연산만큼 키이값을 플레인텍스트

에 부가함으로써 플레인텍스트를 수정한다.

<8> 실제로, 비밀키이는 전송자로부터 안전채널을 통해 승인된 수신자 에게 비밀리에 통신된다. 이러한 방식으로, 승인된 수신자는 비밀키이의 도움과 연관된 공공연히 공지된 알고리즘을 사용하여 사이퍼텍스트를 효과적으로 해독할 수 있다. 그 반면에, 비밀키이의 당사자 및 기타 사이퍼 참략법의 공거래자가 아닌 다른사람은, 알기 쉬운 해독을 제공하는것처럼 보이도록 하나씩 키이스페이스에서의 가능한 키이를 엄밀히 시험해야 한다. 키이 스페이스가 극히 큰 경우, 암호체계는 높은 암호 강도를 지닌다고 언급되며 그의 해독은 계산적으로 실행불가능하다고 언급된다.

<9> 계산태스크는, 상당한 자원에 의해 상당한 시간내에 실제로 달성될 수 없는 경우 계산적으로 실행될 수 없다. 예를들면, 가장 신속한 사용가능 컴퓨터상에서의 1백년은 비합리적인 것으로 간주될 수 있다. 마찬가지로, 1백조 달러의 비용이 드는 특수구조의 컴퓨터를 사용하는 것은 불합리한 것으로 간주될 수 있다.

<10> 비밀키이 체계의 일례는 플레인 텍스트가 우선 2진 비트 스트링으로 코딩되고 비밀키이에 모듈로 2가 가산됨으로써 사이퍼 텍스트로 변형되는 "1회용 패드(one time pad)" 또는 버남(Vernam)스킴이다. 비밀키이는 플레인텍스트만큼 긴 임의 비트(random bit)의 스트링이며 단지 1회만 사용된다. 이러한 스킴은 완벽한 비밀성을 지니는 것으로 입증될 수 있으나, 또한 플레인텍스트의 각 비트에 대한 비밀키이의 한 비트의 바람직스럽지 않은 요건을 지닌다. 메세지만큼 길어야 하는 키이 비트에 대한 필요성 및 키이비트가 재사용될 수 없는 것은 현시대의 데이타 거래의 문맥에서 상기 스킴을 비실용적이게 한다.

<11> 의사임의 생성기로 대량의 임의 키이비트를 생성시키려는 시도가 행해졌다. 의사임의 생성기는 전형적으로 피드백 시프트 레지스터에 의해 실현된다. 생성되는 의사임의 시퀀스는 피드백 시프트 레지스터에서의 초기값에 의해 완전히 결정된다. 그러한 초기값은 키이로서 사용될 수 있음으로써, 소수의 키이비트가 긴 시퀀스의 "임의" 비트를 생성시키는 것을 허용한다.

<12> 그러나, 의사임의 생성기를 사용하는 1회용 패드 암호체계는, 이를태면 사이퍼텍스트의 일부 및 그의 해당 플레인텍스트가 공지되는 경우, "공지된 플레인텍스트" 침범에 영향을 받기 쉽다.

<13> 다른 스킴은 보다 짧은 키이스트링을 사용하는 비밀키이 암호 체계를 제공하는 것으로 간주되었다. 이들 스킴중에서 주목할 점은 Unted States National Bureau of Standards의 1977년 1월 Federal Information Processing Standard (FIPS) 공보 No.46에 의해 공표된 "Data Encryption Standard(DES)" 이다. 그 후로, DES는 표준공중암호 스킴으로서 확립되었다. DES에 의하면, 암호 및 해독은 한 블록씩(block-by-block)이행되며, 각각의 블록은 64비트의 길이이다. 알고리즘은 주로 각 64비트 블록내의 부속 블록중 일련의 미리 한정된 순열, 키이가산, 및 미리 한정된 치환 동작의 16번 반복으로 이루어져 있다. 56비트 키이는 반복에 대해 16개의 값을 생성하도록 시프트레지스터를 통해 사이클링된다.

<14> DES가 지난 10년간 표준으로서 공식 채택되었지만, DES가 신규하고 개선된 표준으로 대체될 때가 된것으로 생각되고 있다. 한가지 이유는 56-비트 키이가 매우 짧을 수 있기 때문이다. 이는 대략 10^{17} 가지의 키이의 키이 스페이스를 형성한다. 현대의 고속 및 멀티 프로세서 컴퓨터의 관점에서 보아, 이러한 사이즈의 키이 스페이스의 소모적 연구(즉, 알기 쉬운 해독을 제공하는지의 여부를 알아보도록 모든 가능한 키이를 엄밀히 시험하려는 키이 스페이스의 소모적 연구)는 계산적으로 실행가능하다. 또 다른 단점은 여러가지의 순열 및 치환 변형 및 필요한 반복의 횟수의 선택과 같은 기초 설계 원리가 분명히 발표되지 않는 다는 점이다. 그러한 체계로 형성되는 트랩도어(trapdoor)의 가능성에 대한 논쟁이 있었다. 따라서, 이는 사용자가 그러한 체계의 실제 비밀성을 용이하고 정확히 평가할 수 없는 경우 진정한 공공의 암호체계일 수 없다. 또한, 사용자는 그러한 체계를 보다 안전하게 하거나 암호강도를 증대시키도록 알고리즘 이나 변형을 수정하려는 어떠한 체계적 방법도 지니지 않는다. 어쨌든, 암호강도가 계산 오버헤드(overhead)의 지수적인 증가를 초래시키지 않고서는 증가 될 수 없는 것처럼 보인다. 이는 다른 짧은 키이스킴과 유사한 DES가 암호를 이루기 위한 계산적인 강도 알고리즘의 원리에 의존하기 때문이다. 그와 같은 짧은 키이는 보다 더 긴 플레인 텍스트를 암호화하는데 여러번이지만 서로다른 상태로 사용된다.

<15> 또 다른 스킴은 RSA(Rivest, Shamir, 및 Adleman) 공중키이체계이다. 이는 암호를 이루기 위한 계산적으로 복잡한 알고리즘의 원리에 의존한다. 그러한 스킴은 한쌍의 비유사한 암호 및 해독키이를 생성시키도록 사용자로 하여금 2개의 매우 큰 솟수(prime number), 바람직하게는 수백개의 숫자각각을 고르게 한다. 암호는 암호키이에 의한 모듈로 연산제어하에서의 지수상태로서 이행된다. 암호키이는 어느누구라도 사용자용으로 의도된 메세지를 암호화하도록 공공연하게 될 수 있지만, 해독키이를 추론함에 있어서는 쓸모가 없다. 따라서, 암호화된 메세지는 단지 해독키이를 소유한 사용자에 의해서만 판독될 수 있다.

<16> 바람직스럽지 않은 특징은 체계의 비밀성을 얻기에 용이하지 않은 매우 큰 솟수의 사용에 기초를 둔다는 점이다. 또한, 그러한 체계는 2개의 큰 솟수의 곱을 인수분해하는 신속한 방법이 발견되는 경우 용이하게 파기될 수 있다.

<17> 따라서, 여전히 개선된 데이타 암호체계에 대한 필요성이 존재한다.

발명의 상세한 설명

<18> 그러므로, 본 발명의 일반적인 목적은 상기에 언급된 단점에 직면하지 않는 개선된 데이타 암호 및 해독 방법 및 장치를 제공하는 것이다.

<19> 본 발명의 한 목적은 기초원리가 명확히 이해될 수 있으며 그의 비밀성을 손상시키지 않고서도 공공연하게 될수 있는 데이타 암호 및 해독 방법 및 장치를 제공하는 것이다. 이러한 방식으로, 본 발명은 표준으로서 확립될 수 있는 진정한 공중 암호 체계를 제공한다.

<20> 본 발명의 다른 목적은 극히 안전한 데이타 암호 및 해독방법 및 장치를 제공하는 것이다.

<21> 본 발명의 다른 목적은 암호 강도가 사용자에 의해 선택될 수 있는 데이타 암호 및 해독 방법 및

장치를 제공하는 것이다.

<22> 본 발명의 또 다른 목적은 적은 계산 오버헤드를 지니며 구현하는데 단순한 데이타 암호 및 해독 방법 및 장치를 제공하는 것이다.

<23> 이들 및 추가적인 목적은 매핑(mapping)의 광대한 레퍼토리(repeltoire)중에서 사용자에 의해 선택될수 있는 매핑을 생성시킴으로써 달성된다. 그러한 매핑은 한 블록씩 분할되어진 플레인텍스트상에 작용한다. 블록 사이즈(N)는 사용자에 의해 선택될 수 있으며 각각의 플레인 텍스트 블록은 N차원의 플레인 텍스트 벡터(X)와 등가이다. 한 세트의 사용자에 의해 선택될 수 있는 매핑 파라메타에 의해 특정화되는 매핑은 플레인텍스트 벡터(X)를 N차원의 사이퍼텍스트 벡터(Y)로 매핑시킨다. 관련된 역 매핑은 또한 사이퍼텍스트 벡터(Y)를 도로 플레인텍스트 벡터(X)로 역 매핑시키기 위해 존재한다. 레퍼토리에서의 매핑의 일반적인 원리 및 형태는 상기 방법 및 장치의 비밀성을 손상시키지 않고서도 공공연하게 될 수 있다. 그러한 매핑은 상기 레퍼토리가 각 매핑 파라메타의 범위 및 블록 사이즈의 지수함수인 사이즈를 지니는 특징을 갖는다.

<24> 본 발명의 한 실시태양에 의하면, 각 매핑 파라메타의 범위 및 블록사이즈는 또한 은밀히 유지되며 단지 비밀키이에 의해 사용자간에만 은밀히 공유된다. 따라서, 비밀키이에 은밀히 관여하지 않는 다른 사람들은 상기 레퍼토리내의 매 매핑마다 철저히 시험을 해보는 보통의 사이퍼 침범 방법으로는 좌절된다. 이는 그들이 확정불가능한 사이즈의 레포토리중에서의 소모적 연구의 계산적으로 실행불가능한 태스크에 직면하기 때문이다.

<25> 본 발명의 다른 실시태양에 의하면, 각 매핑 파라메타의 범위 , 및 블록사이즈(N)는 은밀히 유지될 필요성이 없다. 일단 그들의 충분히 큰 값이 극히 큰 것으로 간주되는 미리 결정된 사이즈를 갖는 레퍼토리를 생성하도록 선택되는 경우, 상기 블록 사이즈(N) 및 상기 범위는 표준으로서 확립되며 공공연하게 될 수 있다.

<26> 사이퍼 침범에 있어서 다른 사람들은 극히 큰 사이즈의 레퍼토리중 에서의 소모적 연구의 계산적으로 실행불가능한 데스크에 여전히 직면하다.

<27> 바람직한 실시예에서, 매핑은

<28> $Y_t = AX_t + Z_t$

<29> 와 같은 형태를 이루고 관련된 역 매핑은

<30> $X_t = A^{-1}[Y_t + Z_t]$

<31> 이며 , 이 경우에

<32> X_t 및 Y_t는 각각 t번째 블록에 해당하는 N 차원의 플레인텍스트 및 사이퍼텍스트 백터이고,

<33> A 및 A^{-1}은 각각 Nx N 매핑 및 해당 역 매핑 매트릭스이며,

<34> Z_t는 t번째 블록에 해당하는 N차원의 제2성분 벡터이다.

<35> A 및 Z_t는 비밀키이의 일부인 매핑 파라메타를 구성한다. 본질적으로, Nx N매핑 매트릭스(A)는 매핑 스페이스를 한정한다. 각 매트릭스 요소가 범위(L)를 따라 변하게 허용되는 경우, 매핑의 레퍼토리는 모든 매트릭스 요소, 즉 L^{NXN}을 순열 배치하므로써 제공되는 사이즈를 지닌다. 이는 지수함수이며 레퍼토리 사이즈는 비록 N및 L의 적절한 값에 대해서 조차 거대해진다. 예를들면 , N=3이며 L=100인 경우, 레퍼토리는 10^{18}의 매핑 모집단을 지닌다.

<36> 바람직한 실시예에서 , 제2성분(Z_t)은 보다 더 스킴의 비밀성을 강화시키도록 각 사이퍼텍스트 벡터를 구성하기 위해 부가된다. 이는 특히 공지된 플레인텍스트 침범 및 작은 블록사이즈상에서의 통계적 침범의 잠재적인 취약성에 대하여 효과적이다. 한 구현예에 있어서 , 제2성분은 블록에서 블록으로 변화하는 의사임의 벡터이다. 다른 구현예에 있어서, 제 2성분은 비선형 함수 또는 비선형 함수 및 의사임의 벡터의 혼합이다.

<37> 본 발명은 플레인텍스트 스트링에 의사임의 숫자의 스트링을 부가함으로써 플레인텍스트 스트링을 암호화하는 종래의 방법과 같은 취약성을 지니지 않는다. 이는 본 발명의 매핑이 N차원 스페이서에서 발생하며, 각 의사임의 숫자가 일반적으로는 단일의 플레인텍스트 캐릭터를 사이퍼텍스트 캐릭터로 변화시키도록 종래의 경우에서와 같이 단일의 플레인텍스트 캐릭터에 직접 부가되는 것이 아니라, 플레인텍스트 캐릭터의 선형 컴비네이션에 부가된다. 이러한 스킴에서 의사임의 숫자를 다른 사람들에 의해 분석하는 문제는 비결정적 다항식(NP)에 의한 문제로서 수학적으로 공지되어 있는 것이다.

<38> 본 발명의 한가지 중요한 실시태양은 일반적으로 사이즈, 특정하게는 특정 매핑 특성이 비밀키이로써 사용자에 의해 선택될 수 있는 매핑의 체제(framework)의 제공이다. 비밀키이가 없는 경우, 다른 사람들은 매핑의 확정불가능한 레퍼토리에서의 소모적 연구를 시도하는 계산적으로 실행불가능한 태스크에 직면한다.

<39> 본 발명의 또한가지 중요한 실시태양은 계산 오버헤드가 블록사이즈의 제곱으로서만 증가하며, 그 반면에 암호강도가 지수적으로 증가한다는 것이다. 따라서 , 계산 오버헤드가 거의 없으면서 극히 높은 암호 강도를 이루는 것이 가능하다. 이와는 대조적으로, 종래의 암호체계의 계산오버헤드는 암호강도가 증가됨에 따라 지수적으로 증가하려는 경향이 있다. 이는 NP에 의한 문제의 또 다른 징후이다.

<40> 본 발명의 추가적인 목적, 특징 및 이점은, 첨부된 도면과 연관지어 설명되는 이하의 바람직한 실시예에 대한 설명으로부터 이해될 것이다.

도면의 간단한 설명

<41> 제 1도는 본 발명에 사용될 수 있는 일반적인 비밀키이의 암호체계를 개략적으로 예시한 것이다.

<42> 제 2A도는 종래의 암호체계에 대한 계산 오버헤드 대 암호강도를 예시한 것이다.

<43> 제 2B도는 본 발명에 대한 계산 오버헤드대 암호강도를 예시한 것이다.

<44> 제 3도는 각 매핑 매트릭스 요소(L)의 범위 및 블록 사이즈(N)와 같은 매핑 파라메타의 지수함수로서 증가하는 본 발명의 암호강도를 예시한 것이다.

<45> 제 4도는 본 발명의 바람직한 실시예에 따른 암호 장치의 기능블록 다이어그램이다.

<46> 제 5도는 본 발명의 바람직한 실시예에 따른 암호장치의 기능 블록 다이어그램이다.

<47> 제 6A도는 사이즈(N=9)의 블록에 대한 기초 플레인텍스트 벡터요소의 여러가지 순열 또는 있을 수 있는 선택을 목록으로 나타낸 것이다.

<48> 제 6B도는 3X3 이미지로 배열되어 있는 요소를 갖는 블록으로부터 다수의 요소를 선택하는 실제의 순열 구성을 예시한 것이다.

실시예

<49> 제 1도는 본 발명에 사용될 수 있는 일반적인 비밀키이의 암호체계를 개략적으로 예시한 것이다. 플레인텍스트(X;10)는 암호장치 또는 프로세스(30)에 의해 사이퍼텍스트(Y;20)로 암호화되고 있다. 사용자에 의해 선택될 수 있는 비밀키이(K;40)는 암호(30)를 제어하는 암호자에 의해 사용된다. 그러한 비밀키이(11)는 해독자와 은밀히 공유되며, 상기 해독자는 다시금 상기 비밀키이를 사용하여 수신된 사이퍼텍스트(Y)를 도로 플레인텍스트(X)로 해독하기 위한 해독장치 또는 프로세스(50)를 제어한다.

<50> 본 발명의 한가지 중요한 실시태양은 매핑의 레퍼토리를 생성시키기 위한 매핑 체제의 제공이다. 일반적으로 그의 사이즈, 특정하게는 특정 매핑특성은 비밀키이로써 사용자에 의해 선택될 수 있다. 그러한 비밀키이를 지니고 있지 않은 경우, 다른 사람들은 매핑의 확정 불가능한 레퍼토리에서의 소모적 연구를 시도하는 계산적을 실행불가능한 태스크에 직면한다.

<51> 매핑은 플레인텍스트를 사이퍼텍스트로 매핑 또는 암호화시킨다. 각각의 매핑은, 비밀키이(K)로부터 추론될 수 있으므로 본질적으로 사용자에 의해 선택될 수 있는 한세트의 매핑 파라메타에 의해 특정화 될 수 있다.

<52> 본 발명은 한 블록씩 플레인텍스트 벡터로 분할되는 각 플레인텍스트 스트림을 지닌다. 블록 사이즈가 N인 경우, 매핑은 N차원의 플레인텍스트 벡터를 해당 N차원의 사이퍼텍스트 벡터로 매핑시킨다.

<53> 매핑은 그의 레퍼토리가 각 매핑 파라메타의 범위뿐만 아니라 블록 사이즈에 따른 사이즈를 지닌다. 사용자는 이들 파라메타를 조정함으로써 바람직한 레벨의 암호강도를 선택할 수 있다. 각각의 매핑 파라메타가 L로 제공되는 범위를 지니는 경우, 이후에 보여주겠지만, 매핑의 레퍼토리는 L^{NXN}으로 제공되는 사이즈를 지닌다. 따라서, 키이 스페이스는 N에 따라 지수적으로 성장한다. 예를들면, L=100이고 N=3인경우, $\{K\} \fallingdotseq 10^{18}$ 이며 이는 DES의 경우보다 대략 10배 더 크다. N이 9까지 확장되는 경우, $\{K\} \fallingdotseq 10^{162}$ 이다. 이는 소모적 연구를 하는 침범자가 비록 N을 안다고 할지라도 10^{162}의 키이를 철저히 시험해야 할 것이다. 바람직한 실시예에서, N 및 L은 또한 은밀하게 유지되며, 침범자는 확정불가능한 큰키이 스페이스에 직면한다.

<54> 본 발명의 또 한가지 중요한 실시태양은 대응적으로 높은 계산 오버헤드를 지니지 않고서도 암호강도가 실제로 증가될 수 있다는 것이다. 그와 대조적으로, 종래의 암호체계의 계산 오버헤드는 암호강도가 증가됨에 따라 지수적으로 증가하려는 경향이 있다. 이는 NP에 의한 문제의 또 다른 징후이다.

<55> 제 2A도는 종래의 암호체계에 대한 계산 오버헤드 대 암호강도를 예시한 것이다. 제 2B도는 본 발명에 대한 계산 오버헤드 대 암호강도를 예시한 것이다. 상기 두 도면의 비교는, 종래의 체계에 대한 계산 오버헤드가 지수적으로 증가하는 반면에, 본 발명의 계산 오비헤드가 대수적으로 증가하는 것을 예시한다. 이는 본 발명의 계산 오버헤드가 블록 사이즈의 제곱으로서 증가하는 반면에, 암호 강도가 지수적으로 증가하기 때문이다.

<56> 제3도는 각 매핑 매트릭스 요소(L)의 범위 및 블록사이즈(N)와 같은 매핑 파라메타의 지수 함수로서 증가하는 본 발명의 암호강도를 예시한 것이다. L에 관한 2개의 값의 관계가 도시되어 있다. L=2는, 각 매핑 매트릭스요소가 2개의 값, 예컨대 "0" 및 "1" 중 하나를 갖도록 허용되는 경우에 해당한다. L=100은, 각 매핑 매트릭스 요소가 1백개의 가능한 값, 예컨대 0 내지 99 또는 -49 내지 50을 갖는 범위에 걸쳐 변하도록 허용되는 경우에 해당한다. 본 발명은 계산 오버헤드에서의 증가가 거의 없으면서 극히 높은 암호강도를 이루는 것이 가능하다.

<57> **암호 및 해독 방법.**

<58> 본 발명의 바람직한 방법은 다음과 같은 단계를 포함한다.

<59> 단계 I. 블록 사이즈(N)의 선택

<60> 각각의 플레인텍스트 블록은 N차원의 플레인텍스트 벡터에 해당한다. 각각의 N차원의 플레인텍스트 벡터는 N차원의 사이퍼텍스트 벡터로 암호가능하다. 따라서,

<61> 플레인텍스트 $X= X_i = [X_1, X_2 - X_N]$

<62> 사이퍼텍스트 $Y= Y_i = [Y_1, Y_2 - Y_N]$ (1)

<63> $i = 1,2\cdot\cdot, N$

<64> 본래의 플레인텍스트는 대개 캐릭터 스트림의 형태를 이룬다. 이러한 캐릭터 표시는 미리 한정된 캐릭터 코드 테이블에 의해 수치적인 표시로 변환된다. X_i 및 Y_i들은 수치적인 표시로 코딩된다.

<65> 일반적으로, X_1. $X_2\cdots\cdot$, X_N 은 플레인텍스트 캐릭터내의 요소들이 들어있는 동일한 순서에 반드시 해당하지 않는다. 매핑이전의 초기 블록순열은 블록 요소의 개시순서를 재편성하는데 사용될 수 있다. 초기블록순열은 비밀키이에 의해 한 사용자로부터 다른 사용자로 전달될 암호정보의 일부로서 특정화 될 수 있다. 이러한 방식으로 나머지 사용자는 플레인텍스트가 사이퍼텍스트로부터 해독되어진 후에 플레인텍스트를 도로 그의 본래의 순서로 재배열시키도록 역단계를 이행할 수 있다.

<66> 단계 II. t번째 블록에 대한 매핑의 생성

<67> $Y_t = AX_t + Z_t$ (2)

<68> 와 같이 사용자에 의해 한세트의 파라메타 (A, Z_t)-

<69> 이 경우,

<70> t는 t번째 블록 또는 벡터에 대한 레이블(lable)이고,

<71> A는 일반적으로 역전가능한 Nx N 매핑 매트릭스

$$A=a_{ij}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ . & . & & \\ . & . & & \\ . & . & & \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{bmatrix} \quad (3)$$

<73> i, j= 1,2 -, N 이며,

<74> $Z_t = [Z_1, Z_2 - , Z_N]_t$ (4)

<75> 이다 - 를 특정화시키는 것은 여러 실시예에 따른 서로 다른 형태를 가정할 수 있는 제 2 백터 성분이다. 이하에서 보다 상세하게 기술되겠지만, 한 실시예에서 한 블록씩 변하는 것이 바로임의 백터이다. 예를들면,

<76> $(Z_i) = b_i\ (t, C_i)$ (5)

<77> 이 경우,

<78> $R(t, C_i)$는 t에서의 의사임의 함수이며,

<79> b_i는 예컨대 $b =[b_1 ,b_2 - b_N]$ 와 같은 상수 벡터이고,

<80> C_i 는 R의 초기값이다. 또 다른 실시예에서, $(Z_i)_t$는 또한 X_i의 비선형 함수일 수 있다.

<81> 단계III. 해독을 위한 한 사용자로 부터 암호정보를 다른 사용자로 보내도록 사용자간에 은밀히 비밀키이를 공유하는것, 예를 들면,

<82> K = [블록 사이즈 ; 매핑 파라메타, 임의 함수 특정화; 초기 블록순열, · · · ·]

<83> =[N ; A; Z_t, - ; -] (6)

<84> 일반적으로 비밀키이(K)는 한세트의 암호 또는 해독 파라메타가 암호 및 해독을 각각 제어하기 위해 추론되는 것을 허용한다. 키이 스페이스 {K}는 범위내에 있는 각 키이 파라메타의 모든 가능한 값에 의해 생성되는 그러한 세트의 모든 가능한 키이를 포함한다. 예를들면, 각각의 매핑 매트릭스 요소가 {L} = {0,1,2- , L-1}와 같은 L의 가능한 값을 지니는 범위를 갖는 경우, a_{ij} ε {L}가 된다. 이때, N이 주어지면, 키이 스페이스에 상주하는 가능한 키이의 세트는

<85> $\{K\} \fallingdotseq L^{NXN}$ (7)

<86> 이 된다.

<87> 단계IV. t번째 블록에 대한 역 매핑의 생성

<88> 식 (2)으로부터

<89> $X_t = A^{-1}(Y_t - Z_t)$ (8)

<90> 이 생성된다. 역 매핑 파라메타 (A^{-1}, Z_t , -)는 식(6)에서의 비밀 키이로부터 추론될 수 있다. 특히, 역 매핑 매트릭스 (A^{-1})는 매핑 매트릭스(A)를 역으로 함으로써 추론될 수 있다.

<91> 매핑 또는 역 매핑은 절단 문제를 방지하도록 징수로 이행되는 것이 바람직스럽다. 따라서, 플레인텍스트 표시뿐만 아니라 모든 매핑 파라메타는 정수로 제공되며 계산은 정확하다. 사이퍼텍스트가 도로 플레인텍스트로 해독되어진 후에 , 수치 표시로 된 플레인텍스트는 해독에서 사용되는 동일한 캐릭터 코드 테이블에 의해 캐릭터표시로 된 본래의 플레인텍스트로 도로 디코딩(decoding) 될 수 있다.

<92> 바람직한 실시예에서, 제2 벡터 성분(Z_t)은 비제로(non-zero)이다. 이는 특히 작은 블록 사이즈 상에서의 통계적 침범의 잠재적인 취약성 및 공지된 플레인텍스트 침범에 대하여 비밀성을 부가적으로 강화시키기 위하여 각 사이퍼텍스트 벡터를 편성하도록 부가된다.

<93> 한 바람직한 구현예에서, 제2백터 성분은 블록에서 블록으로 변화는 의사임의 벡터이다. t번째 블록에 대하여, 식(2)에 의해, 각각의 사이퍼텍스트 백터 요소는,

$$\begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + ,\cdots, a_{1n}x_N + b_1R(t, c_1) \\ y_2 &= a_{21}x_1 + a_{22}x_2 + ,\cdots, a_{2n}x_N + b_2R(t, c_2) \\ &\cdot \\ &\cdot \\ &\cdot \\ y_N &= a_{N1}x_1 + a_{N2}x_2 + ,\cdots, a_{NN}x_N + b_NR(t, c_N) \end{aligned} \qquad (9)$$

<95> 로 제공된다.

<96> 비밀키이는 파라메타

$$k = [\ N;\ a_{ij}\ ;\ b_i\ ;\ c_i\ ;\ \cdots\ ] \qquad (10)$$

<98> 를 지닌다. 해독은 식(8)으로 제공되며 , 플레인텍스트는

<99> $X_t = A^{-1}(Y_t - Z_t\ )$ 로 회복될 수 있다.

<100> 또 다른 바람직한 구현예에서, 속도 계산은 Nx N 매핑 매트릭스(A)를 역으로 할 필요성없이 사이퍼텍스트로 부터 플레인텍스트를 신속하게 복귀하는데 사용된다. 이러한 예에서 제 2성분 ($(Z_i)_t$)은 비선형 함수 또는 의사 임의 함수 중 하나인 것이 바람직스럽다. 전과 같이, 사이퍼텍스트 벡티요소는 대체로 식(2)에 의해 제공된다.

<101> $Y_i = a_{ij}X_i + Z_i$

<102> $i, j = 1,2\cdots, N$

<103> 상기 방법은 $\{X_i\} = \{X_s\} \cup \{Xr\}$ $r = r_1. r_2\cdots, Y_{N-M}$

<104> $1< M\leq N$

<105> 이도록 각 플레인텍스트 벡터

<106> $X_s \in \{X_i\}$ $S = S_1. S_2 \cdots, S_M$

<107> 중에서 기초 플레인텍스트 벡터 요소의 임의 부분집합을 선택하는 것을 필요로 한다.

$$Yi = a_{is}X_s + Z_i \qquad (12)$$

<109> 와 같이 X_s의 함수로서 사이퍼텍스트 매핑을 한정하면,

<110> (a) i = S 인 경우,

$$Ys = a_{ss}X_s + Zs \qquad (13)$$

<112> 이며 , Zs 는 식(5) Zs = bsR (t, C_s) 에서와 같이 임의값이고,

<113> (b) i = r 인 경우

$$Yr = a_{rs}Xs + Zr \qquad (14)$$

<115> 이며 , 이 경우,

$$Zr = brG(X_r) \qquad (15)$$

<117> 이때 , $G(X_r)$ 는 예컨대,

$$G(X_r) = X_r^3 \qquad (16)$$

<119> 과 같이 비선형 함수라는 특성을 지닌다. 식 (13)으로 부터

<120> $X_s = [Y_s - b_sR(t, C_s)] / a_{ss}$

<121> 가 된다. 식(14) 및 식(15)으로 부터

$$\begin{aligned} x_r &= G^{-1}[z_r/b_r] \\ &= G^{-1}[(y_r - a_{rs}x_s)/b_r] \\ &= G^{-1}[y_r - ((y_s - b_sR(t, c_s))a_{rs}/a_{ss})/b_r \end{aligned}$$

<123> 가 된다. 예를들면,

<124> N=9

<125> S=1,5,8

<126> 이고 이 때,

<127> i = 1,2····, 9

<128> r = 2,3,4,6,7,9

<129> 이며 키이는

$$\begin{aligned} k = [\ & N=9\ ;\ S_1=1,\ S_2=5,\ S_3=8\ ; \\ & a_{11},\ a_{55},\ a_{88}\ ; \\ & a_{21},\ a_{25},\ a_{28},\ a_{31},\ a_{35},\ a_{38}\ ,\cdots\ a_{98}\ ; \\ & b_1,\ b_2,\ \cdots\ b_9\ ; \\ & c_1,\ c_5,\ c_8\ ;\ \cdots \end{aligned} \qquad] \quad (17)$$

<131> t번째 블록을 암호화하기 위하여, 식(13)으로 부터

$$\begin{aligned} Y_1 &= a_{11}x_1 + b_1R(t, c_1) \\ Y_5 &= a_{55}x_5 + b_5R(t, c_5) \\ Y_8 &= a_{88}x_8 + b_8R(t, c_8) \end{aligned}$$

<133> 가 된다. 식(14)으로 부터

$$y_2 = a_{21}x_1 + a_{25}x_5 + a_{28}x_8 + b_2G(x_2)$$
$$y_3 = a_{31}x_1 + a_{35}x_5 + a_{38}x_8 + b_3G(x_3)$$
$$y_4 = a_{41}x_1 + a_{45}x_5 + a_{48}x_8 + b_4G(x_4)$$
$$y_6 = a_{61}x_1 + a_{65}x_5 + a_{68}x_8 + b_6G(x_6)$$
$$y_7 = a_{71}x_1 + a_{75}x_5 + a_{78}x_8 + b_7G(x_7)$$
$$y_9 = a_{91}x_1 + a_{95}x_5 + a_{98}x_8 + b_9G(x_9)$$

<135> 가 된다. t번째 블록을 해독하기 위하여, 식(13)으로부터, 기초 플레인텍스트 벡터요소는,

$$x_1 = [\ y_1 - b_1R(t,\ c_1)\ ]/a_{11}$$
$$x_5 = [\ y_5 - b_5R(t,\ c_5)\ ]/a_{55}$$
$$x_8 = [\ y_8 - b_8R(t,\ c_8)\ ]/a_{88}$$

<137> 로서 용이하게 얻어지고, 식(14) 및 식(15)으로부터 , 비-기초 플레인텍스트 벡터 요소는

$$x_2 = G^{-1}[(y_2 - (a_{21}x_1 + a_{25}x_5 + a_{28}x_8))/b_2]$$
$$x_3 = G^{-1}[(y_3 - (a_{31}x_1 + a_{35}x_5 + a_{38}x_8))/b_3]$$
$$x_4 = G^{-1}[(y_4 - (a_{41}x_1 + a_{45}x_5 + a_{48}x_8))/b_4]$$
$$x_6 = G^{-1}[(y_6 - (a_{61}x_1 + a_{65}x_5 + a_{68}x_8))/b_6]$$
$$x_7 = G^{-1}[(y_7 - (a_{71}x_1 + a_{75}x_5 + a_{78}x_8))/b_7]$$
$$x_9 = G^{-1}[(y_9 - (a_{91}x_1 + a_{95}x_5 + a_{98}x_8))/b_9]$$

<139> 이며 식 (16)으로부터

<140> $G^{-1}[\ \ ]=[\ \ ]$ 의 세제곱근을 취함

<141> 이 되고 이러한 방식으로 플레인텍스트[X_1, X_2····, X_9]는 NX N 매트릭스를 역으로 하지 않고서도 신속하게 회복될 수 있다.

<142> **암호 및 해독장치**

<143> 제 4도는 본 발명의 바람직한 실시예에 따른 암호장치의 기능블록 다이어그램이다. 암호장치(30)는 본질적으로 입력 플레인텍스트를 수신하는 플레인텍스트 입력버퍼(200), 기억장치(220), 프로세서(240), 캐릭터 코드 테이블(260), 및 사이퍼텍스트 출력 버퍼(280)을 포함한다.

<144> 기억장치(220)는 그중에서도 특히 암호를 제어하기 위한 제어 파라메타를 저장하는데 사용된다. 그러한 제어 파라메타의 예들은 N,A,Z_t,···· 이다. 상기에 기술된 바와같이, N은 블록사이즈이며, A는 Nx N 매핑 매트릭스이고, Z_t는 사이퍼텍스트 벡터(Y_t)의 제 2성분을 형성하는 벡터이다. b가 N차원의 상수벡터이고 C가 의사임의 생성기로의 입력용 초기값 벡터인 경우에 $Z_t = Z_t(b,c)$와 같은 Z_t를 제어하기 위한 다른 파라메타가 존재할 수 있다.

<145> 프로세서(240)는 플레인텍스트 프리 프로세서(241), 암호 프로세서(243), 블록 계수기(245), 의사임의 생성기(247), 및 키이 프로세서(249)와 같은 기능 블록으로서 예시되어 있는 여러기능부를 포함한다.

<146> 동작에 있어서, 비밀키이(K)는 우선 키이 프로세서(249)에 의해 프로세싱되어 N,A,Z_t(b,c)와 같은 제어 파라메타를 얻으며 이러한 제어 파라메타는 그후 기억장치(220)에 저장된다. 바람직스럽게는, 키이 프로세서는 또한 입력키이가 저장된 한세트의 키이 타당성 검사 규칙에 대하여 타당한지의 여부를 검사한다. 입력키이가 무효인 것으로 인지되는 경우, 메시지는 상기 장치로 부터 통신되어 문제가 무엇인지에 대해 사용자에 통지한다. 한구현예에서 , 비밀키이(11)는 제어 파라메타의 연결을 포함하며 키이 프로세서(249)는 제어 파라메타가 기억장치(220)에 저장되기 전에 제어 파라메타를 분해(parse) 한다. 또 다른 구현예에서 , 비밀 키이(K)는 제어 파라메타의 세트에 필요한 것에 비해 감소될 입력 세트를 포함한다. 키이 프로세서(249)는 또한 키이 생성기로서 사용되며 , 이러한 키이 생성기는 결국 저장장치(220)에 저장되는 완전한 제어 파라메타 세트로 상기 감소된 입력 세트를 확장시킨다. 예를 들면, 2^{256}의 키이 스페이스가 요구되는 경우, 키이는 256 비트 길이이며 완전 제어 파라메타 세트상에 매핑하는 미리 결정된 키이에 의해 매핑될 수 있다. 일단 제어 파라메타가 적소에 있는 경우, 제어 파라메타는 프로세서(240)에 의해 액세스될 수 있다.

<147> 암호장치(30)에 들어가는 캐릭터 스트림의 형태를 이루는 입력 플레인텍스트는 플레인텍스트 프

리 프로세서(241)에 의해 프로세싱되기 전에 플레인텍스트에 의해 버퍼링된다.

<148> 플레인텍스트 프리 프로세서(241)는 저장장치(220)로 부터의 블록 사이즈 파라메터에 따라 사이즈(N)의 한 블록씩 입력 플레인텍스트 캐릭터 스트림을 분해한다. 한 구현예에서, 플레인텍스트 프리 프로세서는 또는 저장장치(220)내의 파라메타에 응답하여 초기 블록 순열을 이행한다. 캐릭터 코드 테이블(260)은, 각 블록이 플레인텍스트 벡터(X)와 등가이도록 각 캐릭터를 수치값으로 변환시키는데 사용된다. 캐릭터 코드 테이블은 선택적으로는 암호장치(30)의 외측에 위치될 수 있다.

<149> 블록 계수기(247)는 프로세싱되고 있는 블록의 트랙을 유지한다. 따라서, t번째 블록은 플레인텍스프 벡터(X_t)를 형성한다.

<150> 플레인텍스트 벡터(X_t)는 그후, 해당 사이퍼텍스트 벡터(Y_t)가 계산되는 암호 프로세서(243)내에 입력된다. 사이퍼텍스트 벡터(Y_t)는, X_t에 관해 Nx N 매트릭스(A)를 연산하고 이에 제 2성분(Z_t)을 가산함으로써 얻어진다. 매트릭스(A) 및 제 2성분은 저장장치(220)로 부터 얻어질 수 있다.

<151> 바람직한 실시예에서, 제 2성분은 한 블록씩 변하는 임의화 성분이다. 의사임의 생성기(R_t(C);247)는 각 블록에 대하여 하나씩 의사임의 벡터의 시리즈를 제공한다. 각각의 시리즈는 초기값 벡터(C)에 의존한다. t번째 블록에 대해, Z_t는 시리즈로 t번째 의사임의 벡터를 취한다.

<152> 이러한 방식으로, 사이퍼텍스트 벡터는 암호 프로세서(243)에 의해 계산되고 이때 암호장치(30)로 부터 사이퍼텍스트 출력 버퍼(280)를 거쳐 출력된다.

<153> 제 5도는 본 발명의 바람직한 실시예에 따른 해독 장치의 기능블록 다이어그램이다. 해독장치(50)는 암호장치(20)와 구조상 유사하며, 암호장치의 역동작을 본질적으로 이행한다. 이는 입력 사이퍼프로세서(340), 캐릭터 코드 테이블(360), 및 사이퍼텍스트 출력 버퍼(380)를 포함한다.

<154> 기억장치(320)는 그중에서도 특히 해독을 제어하기 위한 제어 파라메타를 저장하는데 사용된다. 그러한 제어 파라메타의 예들은, 암호의 경우와 동일한 것이며 또한 입력비밀 키이로 부터 추론될 수 있는 N,A,Z_t(b,c) 이다. 그러나, 해독장치에 있어서, 매핑 매트릭스(A)가 계산에 직접 사용되지 않는 대신에, 추론된 역 매핑 매트릭스(A^{-1})가 사용된다.

<155> 프로세서(340)는 사이퍼텍스트 프리프로세서(341), 해독 프로세서(343), 블록계수기(345), 의사 임의 생성기(347), 및 키이프로세서(349)와 같은 기능 블록으로서 예시되어 있는 여러 기능부를 포함한다. 이들 기능 블록은 암호장치(30)의 경우의 대응부이다. 그 이외에도, 프로세서(340)는 또한 역 프로세서(344)를 포함한다. 역 프로세서(344)는 매핑 매트릭스(A)가 주어지면 역 매핑 매트릭스(A^{-1})를 계산한다.

<156> 동작에 있어서, 비밀키이(K)는 우선 암호장치(30)와 유사한 키이 프로세서(349)에 의해 프로세싱된다 N,A,Z_t(b,c),···· 와 같은 제어 파라메타가 적소에 있는 경우에, 제어 파라메타는 프로세서(340)에 의해 액세스될 수 있다.

<157> 해독장치(50)에 들어가는 변형된 수치 스트링의 스트림의 형태를 이루는 입력 사이퍼텍스트는 사이퍼 텍스트 프리 프로세서(341)에 의해 프로세싱되기 전에 사이퍼텍스트 입력버퍼(320)에 의해 버피링된다.

<158> 사이퍼텍스트 프리프로세서(341)는 저장장치(320)로 부터의 블록 사이즈 파라메타에 따라 사이즈(N)의 한 블록씩 입력 사이퍼텍스트 스트림을 분해한다. 이러한 방식으로, 각각의 블록은 사이퍼텍스트 벡터(Y)와 등가이다.

<159> 블록계수기(347)는 프로세싱되고 있는 블록의 트랙를 유지한다. 따라서, t번째 블록은 사이퍼텍스트 벡터(Y_t)를 형성한다.

<160> 사이퍼텍스트 벡터(Y_t)는 그후, 해당 플레인텍스트 벡터(X_t)가 계산되는 해독 프로세서(343)내로 입력된다. 플레인텍스트 벡터(X_t)는, 사이퍼 텍스트 벡터(Y_t)에 대해 Nx N역 매핑 매트릭스 (A^{-1})를 연산하기 전에 Y_t 로 부터 우선 제2성분 (Z_t)을 감산함으로써 얻어진다. 역 매핑 매트릭스 (A^{-1})및 제 2성분은 기억장치(320)로 부터 얻어질 수 있다. 제 2성분은 해독장치(30)에서의 제2성분과 동일하다.

<161> 바람직한 실시예에 있어서, 제 2성분은 한 블록씩 변하는 임의화 성분이다. 암호장치(30)에서의 의사임의 생성기와 동일한 의사 임의 생성기(R_t(C) ; 347)는 암호장치(30)에서의 각각 블록을 임의화하는데 사용되었던 동일한 의사임의 벡터의 시리즈를 제공한다.

<162> 본래의 플레인텍스트가 초기블록순열에 직면하였던 경우에 있어서, 해독 프로세서(343)는 또한 기억장치(320)의 파라메타에 응답하여 역 블록 순열을 이행한다.

<163> 일단 플레인텍스트 벡터(X_t)가 해독되는 경우, 플레인텍스트 벡터(X_t)는 암호장치에 사용된 것과 유사한 캐릭터 코드 테이블(360)에 의해 데코팅된다. 그러한 캐릭터 코드 테이블은 선택적으로는 해독장치(50)의 위측에 위치될 수 있다. 플레인텍스트 벡터를 이루는 코딩된 수치값은 그 본래의 캐릭터로 다시 디코딩된다.

<164> 이러한 방식으로, 본래의 플레인텍스트는 회복된 다음에 해독장치(50)로부터 사이퍼텍스트 출력 버퍼(380)를 거쳐 출력된다.

<165> 제 4도 및 제 5도는 각각 제1도에 도시된 암호체계의 일부인 암호장치 및 해독장치의 바람직한 하드웨어 실시예를 예시한 것이다. 본 발명은 또한 암호장치(30) 및 해독장치(50)에 의해 이행되는 여러

기능부를 구현하기 위한 소프트웨어 제어하의 컴퓨터를 예상한다. 예를들면, 프로세서(240,340)는 범용컴퓨터의 마이크로 프로세서로 가정될수 있다. 기억 장치(220,320) 및 버퍼(200,300)는 컴퓨터에 있는 기억장치의 여러형태로 가정될 수 있다. 소프트웨어는 상기에 기술된 방법에 따라 암호 및 해독동작을 제어하기 위해 컴퓨터의 기억장치중 하나에 상주 할 수 있다.

<166> **임의 이미지 스킴 - 매핑 파라메타의 체계적 선택**

<167> 상기에 기술된바와 같이, 본 발명은 사용자에게 레퍼토리로 부터 매핑을 선택하는 것을 필요로 한다. 그러한 선택은 비밀키이에 의해 표기되며 상기 키이로부터 한 세트의 매핑 파라메타가 추론될 수 있다.

<168> 매핑의 러퍼토리는 본질적으로, 지정된 범위내에서 Nx N 매핑 매트릭스의 요소를 순열시킴으로써 생성된다. 상기에 지적된바와 같이 , 레퍼토리는 비록 N 및 L의 적정한 값에 대해서도 실제로 극히 크게 되는 사이즈를 지닌다.

<169> 바람직한 실시예에서, 체계적 방법은, 용이하게 구별 및 인식 될수 있도록 매핑을 여러 그룹으로 분류하는데 사용된다. 이러한 방식으로, 사용자는 분류된 매핑중에서 체계적으로 선택할 수 있다. 이는, 비밀 키이가 정규적으로 변경될 필요가 있는 경우, 또는 한 세트의 키이가 한 그룹의 사람들에게 부여될 필요성이 있는 경우에 특히 편리하다.

<170> 그러한 스킴은 블록이나 플레인텍스트 요소를 순열시킴으로써 매핑의 카테고리를 형성하는 것이다. 이는 상기 속도 계산 구현예에서 기술된 플레인텍스트 중에서의 기초 플레인텍스트 벡터의 부분 집합의 선택과 유사하다. 사용자는 임의로 기초 플레인텍스트 벡터 요소의 부분 집합을 선택한다. 가장 단순한 실시예에 있어서 , 나머지 선택되지 않은 플레인텍스트 벡터요소는 단지 선택된 기초 플레인텍스트 벡터 요소만의 선형 컴비네이션으로부터 생긴다. 다시말하면, 사이퍼텍스트 벡터는 본질적으로 상기 선택된 기초 플레인텍스트 벡터요소애 의해 신장되는 부속 스페이스로 매핑된다.

<171> 일반적으로, 각각의 요소가 2개의 값 중 하나를 취할 수 있는 경우 N개의 요소를 순열시키는 방법이 2^N 가지가 있다. 이항(binomial) 이론에 의해, 2^N 가지의 선택은 N개 요소중에서의 M개 기초벡터 요소의 모든 가능한 순열의 합으로서 그룹을 이룰 수 있다.

$$\sum_{o}^{M} C(N,M) = \sum_{o}^{M} \frac{N!}{M!(N-M)!} = 2^N$$

<173> 제 6A도는 사이즈(N=9)의 블록에 대한 기초 플레인텍스트 벡터 요소의 여러가지 순열 또는 가능한 선택을 목록으로 나타낸 것이다. 순열된 구성의 총 갯수는 결과적으로 2^9=512이다.

<174> 제 6B도는 3×3 이미지에서 좌에서 우로 그리고 위에서 아래로 순서적으로 배열된 요소를 지니는 블록으로부터 다수의 요소를 선택하는 실제의 순열 구성을 예시한 것이다. 그러한 구성은 M이 증가하는 배열되어 있으며 #1에서 #511까지의 구성번호를 갖는다(도시되지 않은 평범한 경우에 해당한다). 예를 들면, 제6B도를 참조하면, 사용자는 구성번호(#54)를 선택할 수 있는데, 이는 기초 플레인텍스트 벡터 $X=[X_1,0,X_3, X_5,0,0,0,0]$인 것을 명시한다. 비밀키이가 주기적으로 변경될 수 있다는 점을 사용자가 이해하는 경우, 사용자는 비밀키이의 해당 시퀀스를 제공하도록 본 발명의 스킴에 의한 미리 결정된 구성 시퀀스를 용이하게 선택할 수 있다.

<175> 또다른 실시예에 있어서, 체계적 매핑 파라메타를 생성시키는 스킴은 앞서 언급된 초기 블록 순열에 의해 달성될 수 있다. 일반적으로, 플레인텍스트 벡터 요소(X_1, X_2 - , X_N)는 들어오는 플레인텍스트 캐릭터 스트림의 요소와 동일한 순서에 반드시 해당할 필요성이 없다. 예를들면, 캐릭터 스트림의 블록에서 X_1은 7번째 캐릭터에 해당할 수 있으며 X_2는 1번째 캐릭터에 해당할 수 있다. N개의 슬롯에 N개의 요소를 채우는 방법이 N의 계승(N!)가지가 있다. 초기 블록순열은 선택적으로 사용자 및 비밀키이내에 합체되는 사양에 의해 선택될 수 있다. 상이한 순서는 한 규정순서에 따라 블록요소를 여러구성(또는 이미지)상에 펼친 다음에, 그들을 타 규정 순서에 따라 판독함으로써 생성될 수 있다. 예를들면, 블록사이즈(N)=9인 경우, 한 이미지는 3×3 매트릭스이다. 블록요소([X_1. X_2, X_3, X_4, X_5, X_6, X_7, X_8. X_9])는 좌에서 우로 초안 39페이지에서 삽입 매트릭스로부터 요소를 판독함으로써 얻어진다. 일반적으로, 서로 다른 순열들은 사용되는 이미지 및 요소가 배열되어 상기 이미지로 부터 판독되는 방식의 변화에 의해 얻어진다.

<176> 지금까지 기술된 본 발명의 여러 실시태양의 실시예가 바람직한 구현이지만, 당업자라면 그의 변형도 가능하다는 점을 이해할 것이다. 그러므로, 본 발명은 첨부된 전체 청구범위내에서 보호받을 권리가 있다.

(57) 청구의 범위

청구항 1

사용자가 플레인텍스트를 사이퍼텍스트로 암호화하고 다시 사이퍼텍스트를 플레인 텍스트로 해독하는 암호 체계에 있어서,

사용자간에 공유되는 비밀 키이(secret key);

상기 비밀 키이를 통해 사용자에 의해 선택 가능한 일 부분을 포함하는 상기 비밀 키이로부터 추론하는 일 세트의 암호 파라메타;

플레인텍스트를 사이퍼텍스트로 매핑시키기 위해 상기 암호 파라메타에 의해 결정되며, 상기 비밀 키이를 통해 사용자에 의해 선택 기능한 사이즈(size)를 갖는 레퍼토리를 구비한 타입의 매핑(mapping);

상기 비밀 키이로부터 추론할 수 있는 한 세트의 해독 파라메타; 및

상기 사이퍼텍스트를 플레인텍스트로 역으로 매핑하기 위하여 상기 세트의 암호해독 파라메타에 의해 결정되는 역 매핑(inverse mapping) ; 을 포함하며

사용자가 암호화 강도를 소정의 정도로 달성하도록 상기 비밀 키이를 통하여 매핑의 레파토리의 사이즈를 조절할수 있는 것을 특징으로 하는 암호체계.

청구항 2

제 1 항에 있어서, 상기 블록 사이즈 파라메타에 따라 사이즈를 각각 지니는 플레인텍스트 블록 또는 벡터로 한 블록씩 플레인 텍스트를 분할하도록 블록 사이즈 파라메타에 응답하는 수단을 더 포함하며,

상기 매핑은 플레인텍스트 벡터를 해당 사이퍼 텍스트 벡터로 메핑시키고, 그리고 상기 사용자에 의해 선택 가능한 암호 파라메타의 일부분이 상기 블록 사이즈 파라메타를 포함하는 것을 특징으로 하는 암호체계.

청구항 3

제 1 항에 있어서,

미리 한정된 길이를 갖는 입력으로 부터 상기 비밀키이를 생성하는 비밀 키이 생성기를 더 포함하는 암호체계.

청구항 4

사용자가 플레인 텍스트를 사이퍼텍스트로 암호화하고 사이퍼텍스트를 다시 플레인 텍스트로 해독하는 암호체계에 있어서,

암호및 해독을 각각 제어하는 한 세트의 암호 파라메타 및 한 세트의 해독 파라메타;

사용자간에 공유되는 비밀키이;

상기 비밀 키이로부터 상기 한 세트의 암호 파라메타의 사용자에 의해 선택 가능한 부분을 추론하는 수단;

플레인 텍스트를 사이퍼텍스트로 매핑하기 위한 그의 레퍼토리에서, 상기 비밀 키이를 통해 사용자에 의해 선택가능한 사이즈를 갖는 레퍼토리를 구비하는 형식으로, 매핑을 생성하도록 상기 한 세트의 암호 파라메타에 응답하는 수단;

상기 비밀 키이로부터 상기 세트의 해독 파라메타의 사용자에 의해 선택 가능한 부분을 추로하는 수단; 및

상기 매핑과 연관된 역 매핑을 생성하여 사이퍼텍스트를 다시 플레인텍스트로 역 매핑하도록 상기 한 세트의 해독 파라메타에 응답하는 수단을 포함하는 암호체계.

청구항 5

플레인텍스트를 사이퍼텍스트로 한 블록씩 암호화하는 데이타 암호장치에 있어서,

사용자에 의해 선택가능한 부분을 포함하는 일 세트의 암호 파라메타를 저장하기 위한 저장수단;

사용자가 선택할 수 있는 가능한 값의 범위를 각각 지니는, 플레인텍스트를 사이퍼텍스트로 매핑하는 것을 제어하기 위한 매핑 파라메타들 및 블록 사이즈 파라메타를 포함하는 상기 사용자가 선택가능한 암호 파라메타의 부분;

입력 플레인 텍스트를 한 블록씩 분할하여 각각의 블록에 해당하는 플레인텍스트 벡터를 얻도록 상기 블록 사이즈 파라메타에 응답하는 플레인텍스트 프로세싱 수단;

플레인텍스트를 사이퍼텍스트로 매핑하기 위해 상기 세트의 암호 파라메타에 의해 결정되며 사용자에 의해 선택될 수 있는 사이즈를 갖는 레퍼토리를 구비한 형식인 매핑; 을 포함하며, 사용자가 소정의 정도로 암호화 강도를 수행하도록 상기 비밀 키이를 통하여 매핑의 레퍼토리의 크기를 조정할 수 있으며 또한 상기 데이타 암호화 장치로부터 사이퍼 텍스트를 출력하기 위한 사이퍼텍스트 출력 수단을 조절할 수 있는 데이타 암호장치.

청구항 6

제 5 항에 있어서, 상기 암호 파라메타의 사용자에 의해 선택가능한 부분을 입력 비밀 키이로 부터 추론하는 키이 프로세싱 수단을 더 포함하는 데이타 암호장치.

청구항 7

제 6 항에 있어서, 미리 한정된 길이를 갖는 입력으로부터 상기 비밀 키이를 생성하는 비밀 키이 생성기를 더 포함하는 데이타 암호장치.

청구항 8

제 5 항에 있어서, 캐릭터 표시를 이루는 플레인텍스트를 수치 표시로 변환시키는 캐릭터 코딩 수단을 더 포함하는 데이타 암호장치.

청구항 9

관련 암호 장치로부터의 사이퍼텍스트를 플레인텍스트로 한 블록씩 해독하는 데이타 해독 장치에 있어서,

사용자에 의해 선택가능한 부분을 포함하는 일 세트의 해독 파라메타를 저장하기 위한 저장수단;

사용자가 선택할 수 있는 가능한 값의 범위를 각각 지니는, 사이 퍼텍스트를 플레인텍스트로 역매핑하는 것을 제어하기 위한 역매핑 파라메타들 및 블록 사이즈 파라메타를 포함하는 상기 사용자가 선택가능한 해독 파라메타의 부분;

사이퍼텍스트를 플레인텍스트로 역매핑하기 위해 상기 세트의 해독 파라메타에 의해 결정되며 그리고 사용자에 의해 선택될 수 있는 사이즈를 갖는 레퍼토리를 구비한 형식인 매핑의 역인 역매핑;을 포함하며, 사용자가 소정의 정도로 암호화 강도를 수행하도록 상기 비밀 키이를 통하여 매핑의 레퍼토리의 크기를 조정할 수 있으며 또한 상기 데이타 해독 장치로부터 플레인텍스트를 출력하기 위한 사이퍼텍스트 출력 수단을 조절할 수 있는 데이타 해독 장치.

청구항 10

제 9 항에 있어서, 상기 해독 파라메타의 사용자에 의해 선택 가능한 부분을 입력 비밀키이로 부터 추론하는 키이 프로세싱 수단을 더 포함하는 데이타 해독장치.

청구항 11

제 10 항에 있어서, 미리 한정된 길이를 갖는 입력으로부터 상기 비밀 키이를 생성하는 비밀키이 생성기를 더 포함하는 데이타 해독장치.

청구항 12

제 9 항에 있어서, 코딩된 수치 표시를 이루는 플레인텍스트를 다시 캐릭터 표시로 변환하는 캐릭터 디코딩 수단을 더 포함하는 데이타 해독장치.

청구항 13

사용자가 플레인텍스트를 사이퍼텍스트로 암호화하고 사이퍼텍스트를 다시 플레인텍스트로 해독하는 암호화방법에 있어서,

사용자간에 비밀키이를 공유하는 단계;

상기 비밀 키이를 통해 사용자가 선택가능한 부분을 포함하는 상기 비밀 키이로부터 한 세트의 암호 파라메타를 추론하는 단계;

상기 세트의 암호 파라메타에 의해 한정되며 상기 비밀 키이를 통해 사용자에 의해 선택될 수 있는 사이즈를 구비한 레퍼토리를 갖는 타입인 매핑을 생성하는 단계;

상기 비밀키이로부터 한 세트의 해독 파라메타를 추론하는 단계; 및

사이퍼텍스트를 다시 플레인텍스트로 역 매핑하도록 상기 세트의 해독 파라메타에 의해 한정된 역매핑을 생성하는 단계;를 포함하며, 사용자가 소정의 정도로 암호화 강도를 이루도록 상기 비밀 키이를 통해서 매핑의 레퍼토리의 크기를 조절할 수 있는 암호화방법.

청구항 14

제 13 항에 있어서, 블록 사이즈 파라메타에 따라 사이즈를 각각 지니는 플레인텍스트 블록 또는 벡터로 블록 사이즈 파라메타에 응답하여 한 블록씩 플레인텍스트를 분할하는 단계를 더 포함하며,

상기 매핑은 플레인텍스트 벡터를 해당 사이퍼텍스트 벡터로 매핑하고,

상기 사용자에 의해 선택 가능한 암호 파라메타의 일부분이 상기 블록 사이즈 파라메타를 포함하는 암호방법.

청구항 15

제 13 항에 있어서, 미리 한정된 길이를 갖는 입력으로부터 상기 비밀키이를 생성하는 단계를 더 포함하는 암호방법.

요약

암호장치 및 방법은 플레인텍스트 및 사이퍼텍스트 벡터 간의 매핑 및 관련 역 매핑의 레퍼토리를 제공한다. 플레인 텍스트(200)는 한 블록씩 분할되고, 블록 사이는 N개의 캐릭터와 같이 사용자에 의해 선택될 수 있다. 각각의 매칭은 한쌍의 N차원의 플레인텍스트(200) 및 사이퍼텍스트 벡터(280)사이로 매핑한다. 매핑 또는 관련 역 매핑은 Nx N 매트릭스요소를 갖는 매트릭스에 의해 구현되는데, 이경우 각각의 요소는 L값의 범위를 취하도록 허용된다. 그러한 범위내에서 매트릭스 요소를 순열시킴으로써, 레퍼

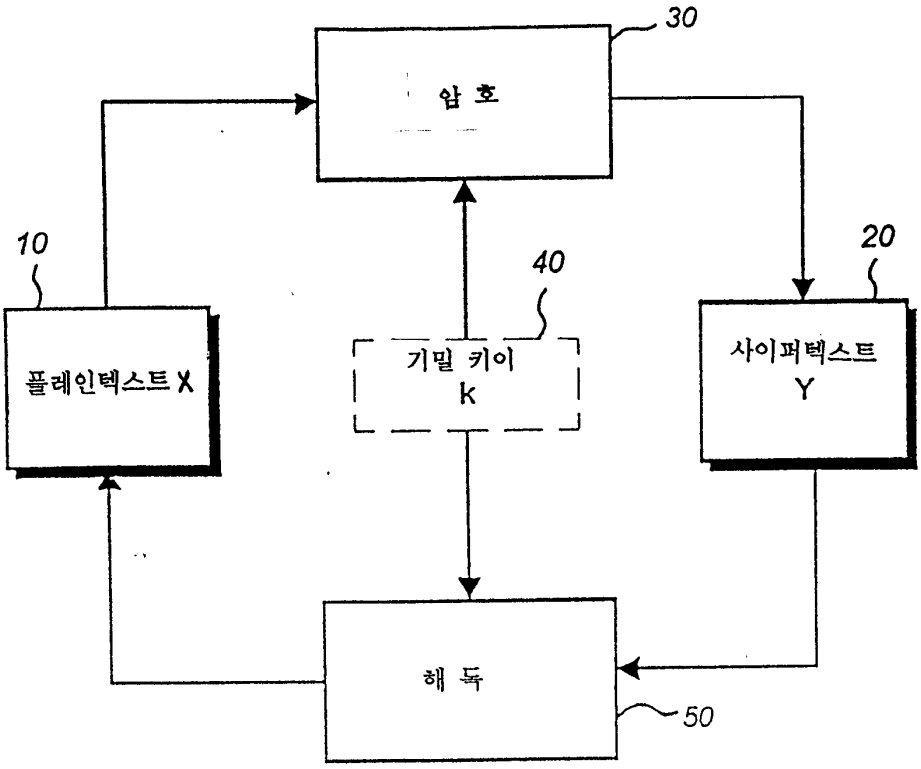
토리는 사이즈 = Lexp(Nx N)를 지닌다. 사용자간에 공유된 비밀키이는 선택된 매핑 또는 관련 역 매핑에 관한 정보를 포함하며 값(N,L)을 포함할 수 있다. 바람직한 실시예에서, 한 블록씩 변하는 의사임의 벡터(247)는 또다른 성분으로서 사이퍼텍스트 벡터(280)에 가산된다.

대표도

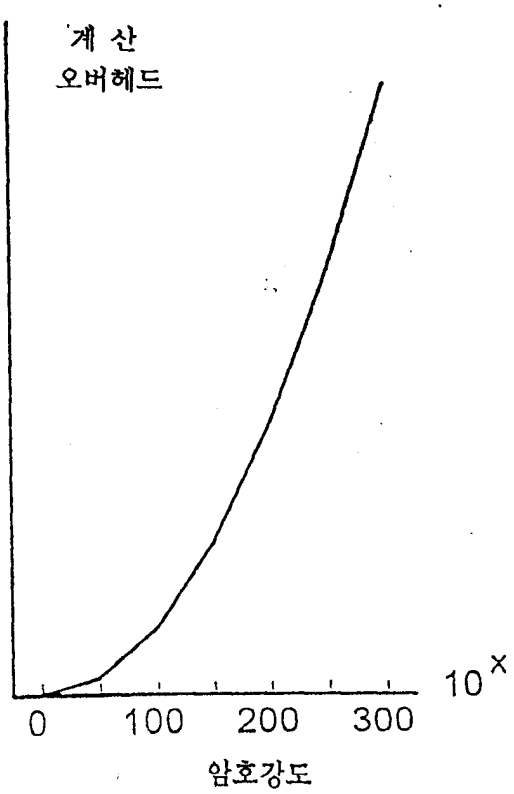
도1

도면

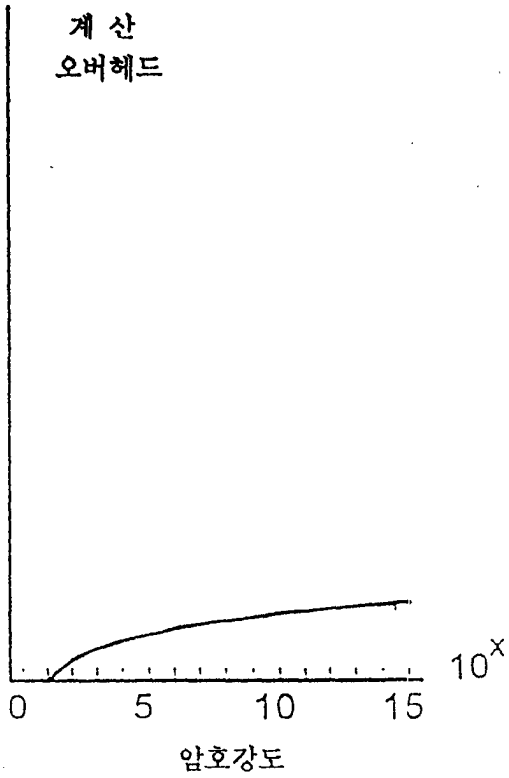
도면1



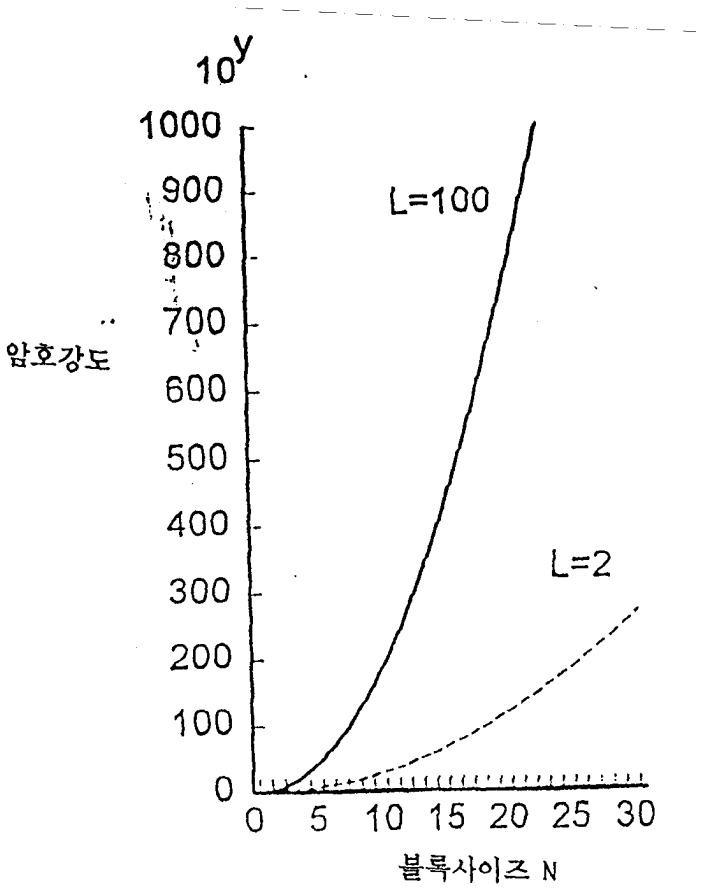
도면2a



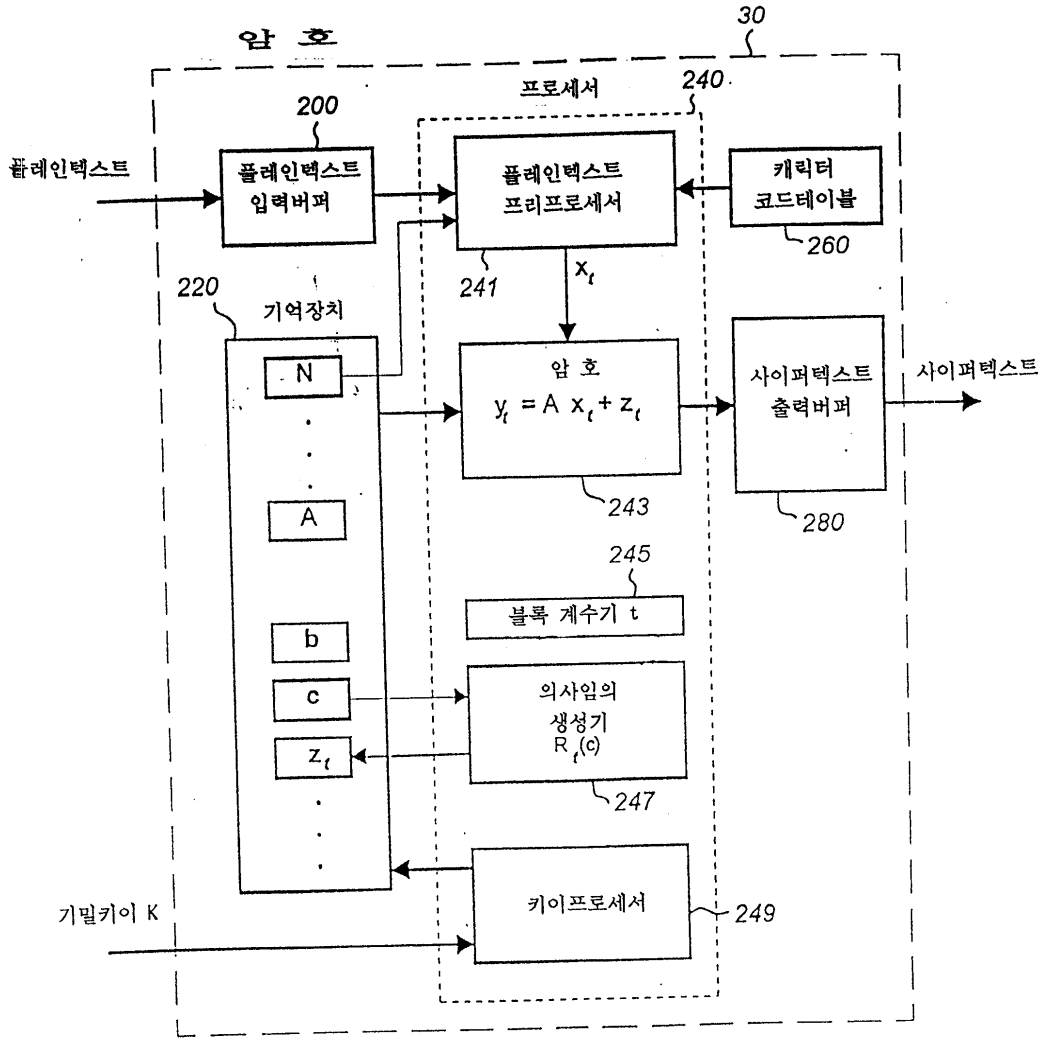
도면2b



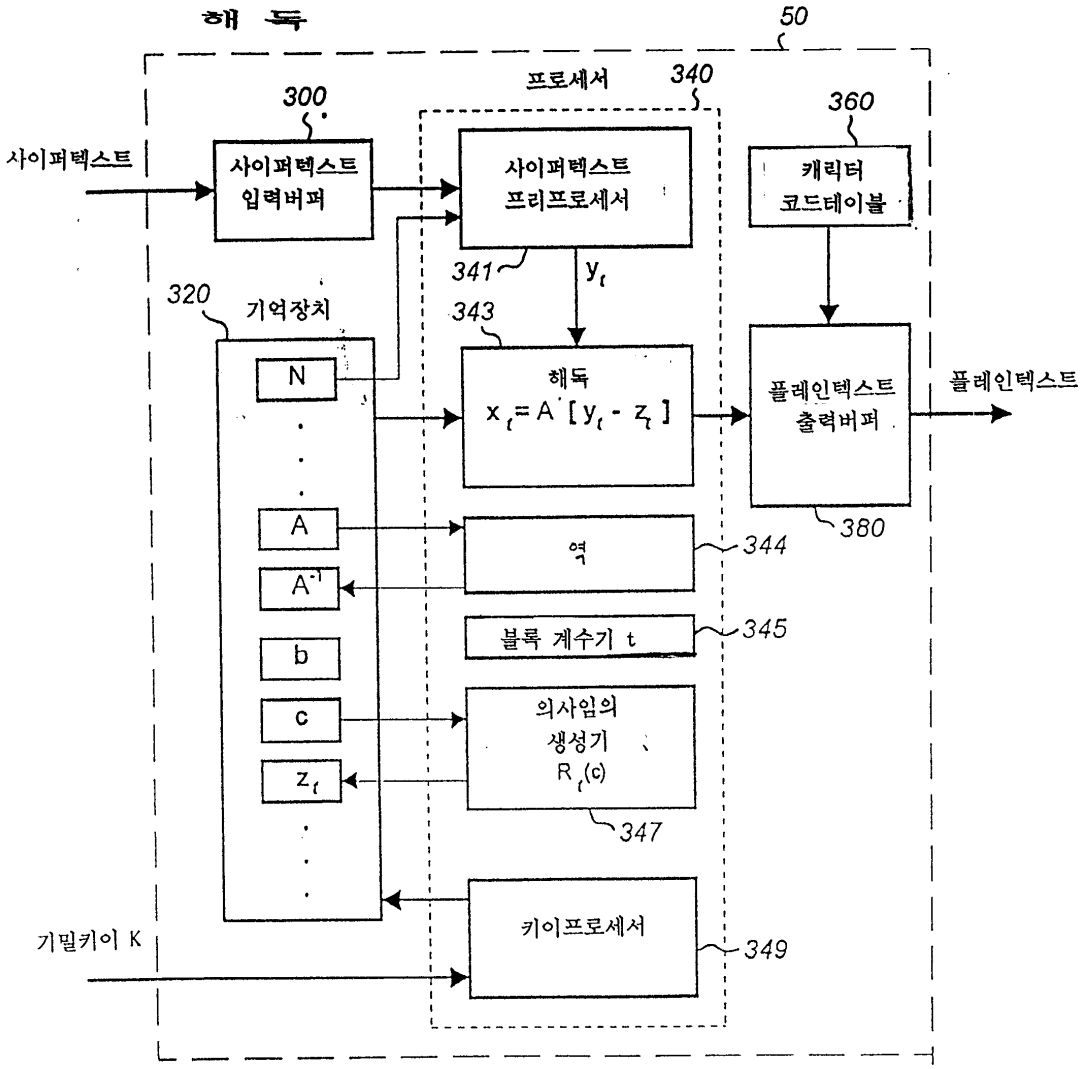
도면3


10^y
1000
900
800
700
600
500
400
300
200
100
0
암호강도
L=100
L=2
0 5 10 15 20 25 30
블록사이즈 N

도면4


암 호
30
프로세서
240
200
플레인텍스트
플레인텍스트 입력버퍼
플레인텍스트 프리프로세서
캐릭터 코드테이블
260
241
x_t
220
기억장치
N
A
b
c
z_t
암 호
$y_t = A\,x_t + z_t$
243
사이퍼텍스트 출력버퍼
사이퍼텍스트
280
245
블록 계수기 t
의사임의 생성기 $R_t(c)$
247
키이프로세서
249
기밀키이 K

도면5


해 독
50
프로세서
340
300
360
사이퍼텍스트
사이퍼텍스트 입력버퍼
사이퍼텍스트 프리프로세서
캐릭터 코드테이블
341
y_t
320
기억장치
343
N
해독
$x_t = A^{-1}[y_t - z_t]$
플레인텍스트 출력버퍼
플레인텍스트
380
A
역
344
A^{-1}
블록 계수기 t
345
b
c
의사임의 생성기 $R_t(c)$
z_t
347
키이프로세서
349
기밀키이 K

도면6a

N = 9, M = 0 - 9	2^9 = 512	
이항계수 C(N,M)	각 그룹의 번호	구성번호 (Fig. 6B 참조)
C(9,0)	1	not shown
C(9,1)	9	1-9
C(9,2)	36	10-45
C(9,3)	84	46-129
C(9,4)	126	130-255 (도시되지않음)
C(9,5)	126	256-381 (도시되지않음)
C(9,6)	84	382-465 (도시되지않음)
C(9,7)	36	466-501 (도시되지않음)
C(9,8)	9	502-510
C(9,9)	1	511