(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
H04L 9/00

(11) 공개번호 특2002-0041807
(43) 공개일자 2002년06월03일

(21) 출원번호 10-2002-7002394
(22) 출원일자 2002년02월25일
번역문 제출일자 2002년02월25일
(86) 국제출원번호 PCT/IB2000/01157
(86) 국제출원출원일자 2000년08월24일
(87) 국제공개번호 WO 2001/17159
(87) 국제공개일자 2001년03월08일

(81) 지정국 국내특허 : 아랍에미리트, 안티구아바부다, 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아-헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 코스타리카, 쿠바, 체코, 독일, 덴마크, 도미니카연방, 알제리, 에스토니아, 스페인, 핀랜드, 영국, 그루지야, 헝가리, 이스라엘, 아이슬란드, 일본, 케냐, 키르기즈, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 라이베리아, 레소토, 리투아니아, 룩셈부르크, 라트비아, 모로코, 몰도바, 마다가스카르, 마케도니아, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 슬로베니아, 슬로바키아, 타지키스탄, 투르크메니스탄, 터어키, 트리니다드토바고, 탄자니아, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 남아프리카,
AP ARIPO특허: 케냐, 레소토, 말라위, 수단, 스와질랜드, 우간다, 시에라리온, 가나, 감비아, 짐바브웨,
EA 유라시아특허: 아르메니아, 아제르바이잔, 벨라루스, 키르기즈, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크메니스탄,
EP 유럽특허: 오스트리아, 벨기에, 스위스, 사이프러스, 독일, 덴마크, 스페인, 핀랜드, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴,
OA OAPI특허: 부르키나파소, 베넹, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기네, 말리, 모리타니, 니제르, 세네갈, 차드, 토고, 기네비쏘, 적도기네,

(30) 우선권주장 1573/99 1999년08월30일 스위스(CH)
60/194,171 2000년04월03일 미국(US)

(71) 출원인 나그라카드 에스.에이.
듀보진 잔-자끄
스위스, 체하-1033 체세욱스-슈어-라우사네, 라우트 드 제네바 22

(72) 발명자 사셀리,마르코
스위스,체하-1803샤르동,체민데로체20
니콜라스,크리스토프
스위스,체하-1028프레베렌지,루드로잔29
힐,마이클존
스위스,체하-1296코페,루트드꼬뮤니10

(74) 대리인 강명구

심사청구 : 없음

(54) 다중-모듈 암호화 방법

요약

암호화/해역 모듈을 이용할 때, 모듈에 입력되거나 모듈로부터 출력되는 데이터를 분석함으로서 모듈에 의해 이용되는 키이를 결정하기 위한 방법이 존재한다. 이 결함을 덜기 위해, 제안된 다중-모듈 방법은 업스트림 모듈로부터의 결과 일부가 가용해지자마자 다운스트림 모듈이 그 암호화/해역 연산을 개시하는 과정으로 이루어진다.

대표도

도 1

명세서

기술분야

본 발명은 데이터의 암호화 및 해역 분야에 관한 것이고, 특히, 유료TV 시스템의 틀 내에서 승인되지 않은 사람이 접근하지 못하게 하는 데이터의 암호화 및 해역 분야에 관한 것이다.

배경기술

이러한 시스템에서, 데이터는 암호화 서브시스템이라 불리는 상당한 연산력을 필요로하는 보안 환경에서 암호화된다. 그후 데이터는 IRD(일체형 수신기 디코더)와 칩 카드의 도움으로, 분산된 한 개 이상의 서브시스템에 전달된다. 비승인자도 이 칩카드와, 이 칩카드와 상호작용하는 분산된 서브시스템에 제한없는 접근을 할 수 있다.

암호화/해역 시스템에서 여러 암호화/해역 수단을 함께 묶는 것(체인형성)이 공지된 방식이다. 다음에 설명되는 것들 중에, 암호화/해역이라는 표현은 더 큰 암호화/해역 시스템에 사용되는 특정 암호화 수단을 의미하는 데 사용될 것이다.

속도, 차지하는 메모리 공간, 보안성의 세가지 측면에서 이 시스템들의 동작을 최적화시키는 것이 오랫동안 연구되어왔다. 속도는 수신한 데이터를 해역하는 데 필요한 시간을 의미하는 것으로 이해하면 된다.

대칭 키이를 가진 암호화/해역 시스템이 공지되어 있다. 그 내재적 보안성은 여러 기준의 함수로 측정될 수 있다.

제 1 기준은 일부 성분을 추출하고 다른 성분으로 이를 대체함에 의한 조사 방법의 용이성이나 난이성에 관한 물리적 보안성의 기준이다. 암호화/해역 시스템의 동작 특성 및 방식에 관해 비승인자에게 알리고자 의도된 이 대체 성분은 감지되지 않는 방식으로 비승인자에 의해 선택되고, 나머지 시스템에 의해 감지불가능한 것으로 선택된다.

제 2 기준은 물리적 관점에서는 침입적이지 않으나 수학적 종류의 분석을 요청하는 공격의 범위 내의 시스템 보안성의 기준이다. 일반적으로, 이 공격들은 알고리즘 및 암호화 코드를 해독하려 시도하는 고출력 컴퓨터에 의해 실행될 것이다.

대칭 키이를 가지는 암호화/해역 수단은 예를 들자면, DES(데이터 암호화 표준)로 불리는 시스템이다. 이 상대적으로 구형인 수단들은 현재, 전체적으로 상대적인 물리적 보안성과 시스템 보안성을 제공하기만 한다. 시스템 보안성의 조건을 만족시키기에 DES 키이의 길이가 너무 작은, 그러한 DES가 암호화/해역의 새 수단이나 더 큰 키이를 가진 새 수단에 의해 점점 더 대체되고 있는 것이 바로 이러한 이유에 있다. 일반적으로, 대칭 키이를 가지는 이 수단들은 암호화 라운드를 포함하는 알고리즘을 요청한다.

또다른 공격 기법은 단일 전력 분석 및 타이밍 분석(Simple Power Analysis and Timing Analysis)이다. 단일 전력 분석에서, 데이터 암호화나 해역에 관련된 임무를 가진 마이크로프로세서가 전원(일반적으로 5V)에 연결된다는 사실을 이용한다. 아이들 상태일 때, 고정된 양의 전류 i가 마이크로프로세서에 흐른다. 액티브 상태일 때, 순간 전류 i는 유입 데이터에만 좌우되는 것이 아니라, 암호화 알고리즘에도 좌우된다. 단일 전력 분석은 시간의 함수로 전류 i를 측정한다. 마이크로프로세서가 실행하고 있는 알고리즘의 종류는 이로부터 추정될 수 있다.

마찬가지 방식으로, 타이밍 분석 방법은 해역 모듈에 제시된 샘플의 함수로 연산 시간(duration)을 계산하는 과정으로 이루어진다. 따라서, 제시된 샘플과 결과 연산용 시간 사이의 관계는 키이같은 해역 모듈 비밀 매개변수를 검색하는 것을 가능하게 한다. 이러한 시스템은 미국 캘리포니아주, 샌프란시스코, Suite 1088, Market St. 870 소재, Cryptography Research 사의 Paul Kocher에 의해 출판된 " Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other Systems" 에 설명되어 있다.

암호화 시스템의 보안성을 향상시키기 위하여, 대칭 키이를 가진 알고리즘이 제안되었다. 그 예로는 소위 RSA(Rivest, Shamir, and Adleman) 시스템이라 불리는 시스템이 있다. 이 시스템들은 한쌍의 정합 키이의 발생을 포함하고, 그 한 쌍은 암호화에 기여하는 퍼블릭 키이와, 해역에 기여하는 프라이비트 키이로 이루어진다. 이 알고리즘들은 시스템 보안성 및 물리적 보안성의 양면에서 높은 수준의 보안성을 나타낸다. 이 알고리즘들은 다른 한편으로, 특히 암호화 단계에서, 기존 시스템보다 느리다.

가장 최근의 공격 기술은 차등 전력 분석(Differential Power Analysis)을 나타내는, 소위 DPA 개념을 요청한다. 이 방법들은 암호화 키이의 주어진 위치에서 0이나 1의 존재에 관하여, 다수의 시도 후 확인가능하다는 가정을 바탕으로 한다. 이 방법들은 거의 비-파괴적으로서, 감지불가능하게 하며, 물리적 침입 성분과 수학적 분석 성분을 모두 요청한다. 그 동작 방식은 오일 필드(oil field)를 조사하기 위한 기술을 연상시킨다. 즉, 표면에서 공지된 전력의 폭발이 발생하고, 폭파 위치로부터 어떤 거리로 떨어진 이어폰과 프로브는 너무 큰 채굴을 할 필요없이 서브표면의 층위 조성에 관한 가정을 이루어지게 한다. 이때 본 서브표면에서 침전 베드의 경계에 의한 쇼크 웨이브의 반사를 이용한다. DPA 공격은 미국, 뉴욕주, Yorktown Heights, IBM T.J.Watson Research Center의 Suresh Chari, Charanjit Jutla, Josyula R. Rao, Pankaj Rohatgi에 의해 1999년 2월 1일에 출판된 문서 " A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards" 의 섹션 2.1에 기술되어 있다.

DPA 공격에 저항해야 한다는 당위성은 암호화/해역 알고리즘의 출력에서, 또는 입력 정보 내에서, 소위 " 화이트닝(whitening)" 전파방해 시스템을 이용하게 한다. 화이트닝 기술은 앞서 언급한 동일 문서의 섹션 3.5에 설명된다.

더우기, 유료TV 시스템의 분산된 서브시스템에서 연산 전력이 제한된다는 사실은 한번도 만족할만하게 해결된 적이 없는 한가지 문제점을 야기시킨다. 즉, 앞서 기술한 체인형성(함께 묶음)을 충분한 정도로 실행하는데 있어 문제점이 생긴다.

발명의 상세한 설명

본 발명의 목적은 앞서 기술한 것처럼 현대의 조사 방법에 대항할 수 있는 암호화/해역 방법을 가용하게 하는 것이다.

본 발명에 의해 의도되는 목적은 청구범위 제 1 항의 특징부에 의해 설명되는 방법에 의해 이루어진다.

이 방법의 특징은 이전(업스트림) 모듈로부터의 결과가 종료되었을 때 중간 모듈이 시작되지 않으나, 정보의 일부가 이미 가용해지자마자 중간 모듈이 시작된다는 사실에 있다. 따라서, 외부 관찰자의 경우에, 이 모듈에 대한 입력 조건이나 출력조건을 성립시키는 것이 불가능하다.

해역은 칩 카드와 상호작용하는 분산된 서브시스템에서 발생하고, 이 칩 카드는 암호화 서브시스템에 비해 매우 제한된 연산 전력만을 수용하기 때문에, 해역의 최종 단계동안 상대적으로 빠르게 동작하는 퍼블릭 비대칭 키이를 이용하는 것이 바람직하다. 이는, 한편으로, 과정을 빠져나갈 때 시스템의 강인한 지속 특성을 보존하게 할 수 있고, 다른 한편으로, 암호화 서브시스템에서 프라이비트 키이의 도움으로 암호화에 관련된 연산 전력을 집중시킬 수 있다.

차례를 따라 순차적으로 이어지는 암호화/해역의 두 수단을 부분적으로 삽입하거나, 연관시킬 가능성에 의해 추가적인 보안성이 제공된다는 것이 발견되었다. 연관된다거나 부분적으로 삽입된다는 것은 첫 번째 암호화/해역 수단이 데이터에 대해 그 작업을 아직 종료하지 않았을 때 동일 데이터에 대한 두 번째 암호화/해역 수단의 동작을 개시하는 과정으로 이루어지는 처리를 의미한다. 이는 제 2 모듈의 동작에 들어가기 전에 제 1 모듈의 작업으로부터 발생하는 것처럼 데이터를 마스킹하는 것을 가능하게 한다.

체인형성(함께묶음)은 제 1 모듈의 출력에서 연산되는 데이터가 제 2 모듈에 의한 처리를 위해 부분적으로 가용해지자마자 시작된다.

발명은 암호화/해역 시스템에서 여러 암호화/해역 수단을 조합함으로서, 그리고 이 수단들이 차례로 이어지는 순서로 연관시키거나 부분적으로 삽입시킴으로서, 앞서 언급한 공격에 대해 보호하는 것을 가능하게 한다.

발명의 특정 실시예에서, 암호화/해역 시스템은 세 개의 알고리즘이 순차적으로 사용되는 암호화 서브시스템을 포함한다.

a) 프라이비트 키이 d1을 가진 비대칭 알고리즘 A1: 이 알고리즘 A1은 메시지 m으로 표시되는 평데이터(plain data)에 서명을 실행한다. 이 연산은 공식 c1 = m exponent d1, 모듈로 n1에 의해 표시되는 수학 연산을 이용하여 제 1 암호문을 운반한다. 이 공식에서, n1은 비대칭 알고리즘 A1의 퍼블릭 키이의 일부를 형성하고, 모듈로는 상대 정수 세트 내 적합성의 공지된 수학적 오퍼레이터를 나타내며, d1은 알고리즘 A의 프라이비트 키이이다.

b) 비밀 키이 K를 이용한 대칭 알고리즘 S: 이 알고리즘은 암호문 c1을 암호문 c2로 변환한다.

c) 프라이비트 키이 d2를 가진 비대칭 알고리즘 A2: 이 알고리즘 A2는 앞서와 같이 c3 = c2 exponent d2 mod n2로 표시되는 수학 연산을 이용하여 암호문 c2를 암호문 c3로 변환한다. 이 공식에서, n2는 비대칭 알고리즘 A2의 퍼블릭 키이 일부를 형성하고, d2는 알고리즘 A2의 프라이비트 키이이다.

암호문 c3는 공지된 수단에 의해 암호화 서브시스템을 떠나고 분산된 서브시스템에 도달한다. 유료TV 시스템의 경우에 이는 비디오 데이터나 메시지에도 동등하게 적용할 수 있다.

분산된 서브시스템은 앞서와는 역으로, 세 개의 알고리즘 A1', S', A2'을 이용한다. 이 세 알고리즘은 암호화/해역 시스템을 나타내면서 암호화 서브시스템과 분산된 서브시스템간에 분포되는 세 개의 암호화/해역 수단 A1-A1', S-S', A2-A2'의 일부를 형성한다.

d) 알고리즘 A2'은 c2 = c3 exponent e2 mod n2로 표시되면서 c2를 복구하는 c3에 대한 수학 연산을 실행한다. 이 공식에서, e2와 n2로 구성되는 세트는 비대칭 알고리즘 A2-A2'의 퍼블릭 키이이다.

e) 비밀 키이 K를 이용한 대칭 알고리즘은 암호문 c1을 복구한다.

f) 퍼블릭 키이 e1, n1을 가진 비대칭 알고리즘 A1'은 m = c1 exponent e1 mod n1으로 표시되는 수학 연산을 실행함으로서 m을 검색한다.

분산된 서브시스템에서 연관 상태는 해독 이전 단계 d)에서 c2가 아직 완전히 복구되지 않았을 때 해독 단계 e)를 시작하고, 단계 3에 의해 c1이 완전히 복구되지 않았을 때 해독 단계 f)를 시작하는 과정으로 이루어진다. 그 장점은 단계 e의 종료시 암호문 c1을 분산된 서브시스템 내에서 추출하는 것을 목표로 하는 공격을 방해한다는 것이며, 그래서 이를 평데이터 m과 비교하여 c1과 m을 이용하여 알고리즘 A1'을 공격하고, 그리고나서 점차적으로 코딩 체인을 물러서는 점이다.

집중은 안전한 물리적 환경에 설치되는 암호화 서브시스템에 필요하지 않다. 다른 한편으로, 분산된 서브시스템에 필요하다. 유료TV의 경우에, IRD는 실제로 가입자의 구역에 설치되며, 앞서 설명한 종류의 공격 대상일 수 있다.

세 개의 연계된 해역 알고리즘 A1', S', A2'의 조합의 공격은 암호문 c1과 c2가 각 단계 d), e), f) 사이에서 완전하게 재구축될 경우보다 계속될 기회가 적다. 더욱이, 알고리즘 A1'과 A2'이 퍼블릭 키이 e1, n2 및 e2, n2와 함께 사용된다는 사실은, 분산된 서브시스템에 필요한 연산 수단이 암호화 서브시스템에 필요한 연산수단에 비해 훨씬 줄어든다는 것을 의미한다.

한 예로, 프라이비트 키이를 가진 암호화 단계들인 단계 a)와 c)는 퍼블릭 키이를 가진 해역 단계 d)와 f)보다 20배 더 길다.

앞서의 실시예로부터 도출된 발명의 특정 실시예에서, 알고리즘 A1, A2는 그 대응하는 A1', A2'과 동일하다.

앞선 실시예로부터 역시 도출된 발명의 특정 실시예에서, 단계 d)에서 암호문 c3가 비대칭 알고리즘 A2의 프라이비트 키이 d2와 함께 해역될 때 단계 c)에서 비대칭 알고리즘 A2의 퍼블릭 키이 e2, n2가 사용된다. 본 실시예는 연산 전력 측면에서 분산된 서브시스템의 자원을 얻기 어려울 때 가능한 대안을 구성한다.

칩카드가 데이터 해역에 주로 사용되지만, 암호화 연산을 실행하기 위해 필요한 용량을 가지는 칩카드도 있다. 이 경우에, 앞서 설명한 공격들은 관리센터같은 보호 위치로부터 떨어져서 동작하는 이런 암호화 카드에 또한 관계할 것이다. 이는, 발명에 따른 방법이 일련의 암호화 동작에 적용되기 때문이다. 즉, 업스트림 모듈에 의해 운반되는 정보의 일부가 가용해지자마자 다운스트림 모듈이 그 암호화 연산을 시작하기 때문이다. 이 과정은 여러 암호화 모듈을 삽입하는 장점을 가지며, 그 결과 업스트림 모듈로부터의 결과가 주어진 시간에 완전히 가용하지 못하다. 더욱이, 다운스트림 모듈은 완전한 결과와 함께 그 연산을 시작하는 것이 아니라 부분적일 때 시작하므로, 공지된 입력 상태나 출력 상태에 대해 모듈의 동작 방식을 해역하는 것을 실제적으로 불가능하게 한다.

도면의 간단한 설명

도 1은 암호화 연산의 도면.

도 2는 해역 연산의 도면.

도 3은 암호화 방법에 대한 대안의 도면.

도 4는 해역 방법에 대한 대안의 도면.

실시예

도 1에서, 데이터 세트 m이 암호화 체인에 삽입된다. 제 1 요소 A1은 익스포넌트(exponent) d1과 모듈로(modulo) n1으로 구성되는 소위 프라이비트 키이를 이용하여 암호화 연산을 실행한다. 이 연산의 결과는 C1으로 표시된다. 발명

의 연산 모드에 따라, 결과 C1의 일부가 가용해지자마자 다음 모듈이 그 연산을 실행한다. 그 다음 모듈 S는 비밀 키이와 함께 그 암호화 연산을 실행한다. 암호화 연산이 n분적으로 가용해지자마자, 익스포넌트 d2와 모듈로 n2로 구성되는 프라이비트 키이를 이용하여 제 3 암호화 연산에 대해 결과 C2가 모듈 A2에 전송된다. C3로 표시되는 최종 결과는 방송전파나 케이블같은 공지된 경로에 의해 기꺼이 전송된다.

도 2는 암호화를 위해 작용한 경우와 유사하지만 역순으로 진행되는 세 해역 모듈 A1', S', A2'으로 구성되는 해역 시스템을 나타낸다. 따라서, 익스포넌트 e2와 모듈로 n2로 구성되는 소위 퍼블릭 키이를 바탕으로 해역 연산을 실행하는 모듈 A2'과 함께 먼저 시작된다. 암호화의 경우와 마찬가지 방식으로, 모듈 A2'으로부터의 결과 C2 일부가 가용해지자마자, 제 2 해역 연산을 위해 모듈 S'으로 전송된다. 해역 종료를 위해, 모듈 A1'은 익스포넌트 e1과 모듈로 n1으로 구성되는 소위 퍼블릭 키이를 바탕으로 그 연산을 실행한다.

발명의 특정 실시예에서, 두 모듈 A1, A2의 키이는 동일하다. 즉, 암호화 측에서, d1=d2, n1=n2이다. 마찬가지로, 해역 중에, e1=e2, n1=n2이다. 이 경우에, 프라이비트 키이를 d, n으로, 퍼블릭 키이를 e, n으로 말할 수 있다.

발명의 또다른 실시예에서, 도 3과 4에 도시되는 바와 같이, 모듈 A2는 소위 프라이비트 키이 대신에 소위 퍼블릭 키이를 이용한다. 암호화 순간에, 퍼블릭 키이 e2, n2는 모듈 A2에 의해 이용되고(도 3), 해역 중에, 모듈 A2'은 프라이비트 키이 d2, n2를 이용하여 연산한다. 이 구조가 해역 세트에 대한 총 작업을 나타내지만, 프라이비트 키이의 이용이 모듈 A2에 의해 제공되는 보안성을 강화시킨다.

도 3과 4에 도시되는 예가 다른 조합에 대해 제한적인 것이 아니다. 예를 들어, 퍼블릭 키이를 가진 암호화 연산과 프라이비트 키이를 가진 해역 연산을 실행하도록 모듈 A1을 구성하는 것이 가능하다.

비밀 키이 S를 가진 암호화/해역 모듈을 모듈 A1 및 A2와 동일한 종류의 비대칭 키이를 가진 종류의 모듈로 대체하는 것이 또한 가능하다.

(57) 청구의 범위

청구항 1.

여러 암호화/해역 모듈을 순서대로 이용하는 암호화 및 해역 방법으로서,

업스트림 암호화/해역 모듈로부터의 결과 일부가 가용해지자마자 다운스트림 암호화/해역 모듈이 그 연산을 개시하는 것을 특징으로 하는 방법.

청구항 2.

제 1 항에 있어서, 업스트림 해역 모듈로부터의 결과 일부가 가용해지자마자 다운스트림 해역 모듈이 그 해역 연산을 개시하는 것을 특징으로 하는 방법.

청구항 3.

제 1 항에 있어서, 업스트림 암호화 모듈로부터의 결과 일부가 가용해지자마자 다운스트림 암호화 모듈이 그 암호화 연산을 개시하는 것을 특징으로 하는 방법.

청구항 4.

제 1 항에서 3 항까지 중 어느 한 항에 있어서, 상기 방법은 세 개의 모듈(A1, S, A2)로 구현되고, 이중 중앙 모듈(S)은 비밀 대칭 키이(k)를 가진 종류인 것을 특징으로 하는 방법.

청구항 5.

상기 항들 중 어느 한 항에 있어서, 암호화에 대한 제 1 모듈(A1) 및 최종 모듈(A2)과, 해역에 대한 제 1 모듈(A2) 및 최종 모듈(A1)은 비대칭 키이를 가진, 즉, 프라이비트 키이와 퍼블릭 키이를 가진 RSA 형인 것을 특징으로 하는 방법.

청구항 6.

상기 항들 중 어느 한 항에 있어서, 두 모듈(A1, A2)은 암호화를 위해 프라이비트 키이(d,n; d1,n1; d2,n2)를, 그리고, 해역을 위해 퍼블릭 키이(e,n; e1,n1; e2,n2)를 이용하는 것을 특징으로 하는 방법.

청구항 7.

상기 항들 중 어느 한 항에 있어서, 두 모듈(A1, A2)은 동일한 프라이비트 키이(d,n)와 퍼블릭 키이(e,n) 세트를 이용하는 것을 특징으로 하는 방법.

청구항 8.

제 6 항에 있어서, 두 모듈(A1, A2)은 서로 다른 세트의 프라이비트 키이(d1,n1; d2,n2)와 퍼블릭 키이(e1,n1; e2, n2)를 이용하는 것을 특징으로 하는 방법.

청구항 9.

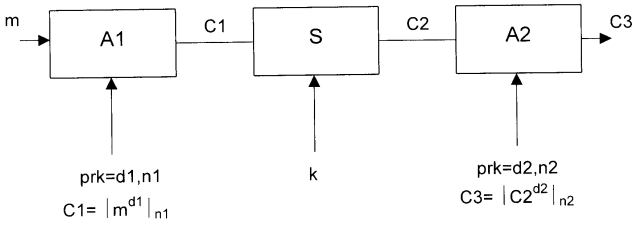
제 5 항에 있어서, 암호화 중, 최종 모듈(A2)은 퍼블릭 키이(e2,n2)를 이용하고, 해역 중, 제 1 모듈(A2)은 프라이비트 키이(d2,n2)를 이용하는 것을 특징으로 하는 방법.

청구항 10.

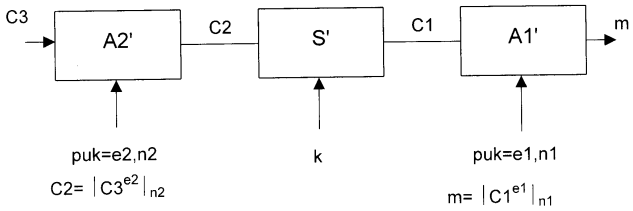
제 1 항에서 3 항까지 중 어느 한 항에 있어서, 상기 방법은 비대칭 키이를 가진 세 개의 암호화/해역 모듈(A1, A, A2)로 구현되는 것을 특징으로 하는 방법.

도면

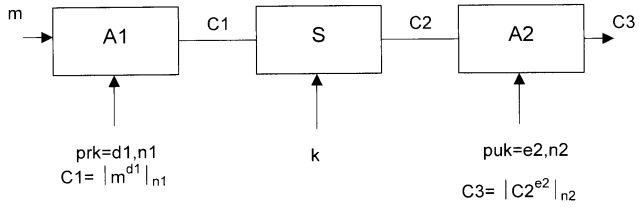
도면 1



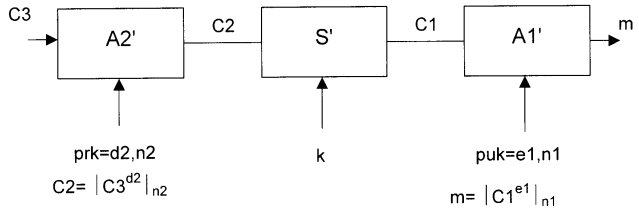
도면 2


C3
A2'
C2
S'
C1
A1'
m
puk=e2,n2
C2= |C3^e2|n2
k
puk=e1,n1
m= |C1^e1|n1

도면 3


m
A1
C1
S
C2
A2
C3
prk=d1,n1
C1= |m^d1|n1
k
puk=e2,n2
C3= |C2^e2|n2

도면 4


C3
A2'
C2
S'
C1
A1'
m
prk=d2,n2
C2= |C3^d2|n2
k
puk=e1,n1
m= |C1^e1|n1