(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년03월20일
(11) 등록번호 10-1126024
(24) 등록일자 2012년03월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/06* (2006.01)
(21) 출원번호 10-2007-7018259
(22) 출원일자(국제) 2006년02월21일
심사청구일자 2010년05월24일
(85) 번역문제출일자 2007년08월09일
(65) 공개번호 10-2007-0106515
(43) 공개일자 2007년11월01일
(86) 국제출원번호 PCT/US2006/005942
(87) 국제공개번호 WO 2006/091528
국제공개일자 2006년08월31일
(30) 우선권주장
11/064,912 2005년02월24일 미국(US)
(56) 선행기술조사문헌
"An OAEP Variant with a Tight 1-32 Security Proof- Draft 1.0," RSA LABORATORIES, http://eprint.iacr.org/2002/034.pdf (2002-03-18)
US6578150 A
US6996233 A
US4870681 A
전체 청구항 수 : 총 35 항

(73) 특허권자
액세스 비지니스 그룹 인터내셔날 엘엘씨
미국, 미시간주 49355, 아다, 풀톤 스트리트 이스트 7575
(72) 발명자
베이세, 니마
미국, 미시간 49417, 그랜드 해븐, 13568 레드버드 레인
바르만, 데이비드 더블유.
미국, 미시간 49408, 펜빌, 6414 127쓰 에비뉴
레피엔, 토마스 제이
미국, 미시간 49417, 그랜드 해븐, 11861 주니퍼 힐스 코트
(74) 대리인
강명구

심사관 : 이형일

(54) 발명의 명칭 **3 단계 데이터 암호화 시스템 및 방법**

(57) 요 약

본 발명은 3 단계 암호화 방법 및 3 단계 해역 방법, 그리고 3 단계 암호화 방법 및 3 단계 해역 방법을 구현하는 장치에 관한 것이다. 메시지를 3 단계 암호화 방법에 따라 암호화하기 위해, 메시지의 내용을 제 1 폼(M)에서 제 2 폼(M')으로 변환하고, 메시지의 내용을 스페이스 패턴에 따라 분리하며, 그리고 메시지의 내용을 스크램블 패턴에 따라 스크램블 한다. 3 단계 암호화 방법을 이용하여 암호화된 메시지를 해역하기 위해, 스크램블 및 스페이스 패턴이 역으로 되고, 메시지의 내이 제 2 폼(M')에서 제 1 폼(M)으로 변환된다.

특허청구의 범위

청구항 1

공개 암호 키(E)와 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)의 함수로, 메시지의 내용을 제 1 폼(M)에서 제 2 폼(M')으로 변환하는 단계(104)와;

상기 메시지의 내용을 제 2 폼(M')으로 변환한 후, 상기 메시지의 내용을 추가로 암호화하기 위해, 제 3 소수(R)를 기초로 하는 스페이스 패턴에 따라 상기 변환된 메시지의 내용을 분리하는 단계(106)와;

상기 메시지의 내용을 제 2 폼(M')으로 변환한 후, 제 4 소수(S)를 기초로 하는 스크램블 패턴(108)에 따라 상기 변환된 메시지의 내용을 스크램블하여, 상기 메시지의 내용을 추가로 암호화하는 단계(108)

를 포함하는 것을 특징으로 하는 메시지 암호화 방법.

청구항 2

제 1 항에 있어서,

메시지의 내용을 제 1 폼(M)에서 제 2 폼(M')으로 변환하기 전에, 상기 메시지의 내용을 알파벳 구문에서 숫자 표현(202)으로 변환하는 단계를 더 포함하는 것을 특징으로 하는 메시지 암호화 방법.

청구항 3

제 2 항에 있어서,

상기 메시지의 내용이 알파벳 구문에서 숫자 표현(202)으로, 해시(hash) 함수를 이용하여 변환되는 것을 특징으로 하는 메시지 암호화 방법.

청구항 4

제 1 항에 있어서,

상기 공개 암호 키가 상기 제 1 비밀 소수와 상기 제 2 비밀 소수에 대해 소수인 것을 특징으로 하는 메시지 암호화 방법.

청구항 5

제 4 항에 있어서,

상기 메시지의 내용이 제 1 폼(M)에서 제 2 폼(M')으로, 다음의 식,

$$M' = M^{E} \bmod (P * Q)$$

에 따라 변환되는 것을 특징으로 하는 메시지 암호화 방법.

청구항 6

제 1 항에 있어서,

상기 메시지의 내용을 분리하기 위한 상기 스페이스 패턴이 다음의 식,

$$F(R) = R * \bmod (K)$$

에 따른 제 3 비밀 소수(R)와 계수(K)의 함수인 것을 특징으로 하는 메시지 암호화 방법.

청구항 7

제 6 항에 있어서,

스페이스 패턴에 따라 상기 메시지의 내용을 분리하는 단계는

상기 메시지의 내용을 복수의 구분된 패킷으로 분리하는 단계를 포함하는 것을 특징으로 하는 메시지 암호화 방

법.

청구항 8

제 6 항에 있어서,

스페이스 패턴에 따라 상기 메시지의 내용을 분리하는 단계는

상기 메시지의 내용을 복수의 그룹으로 분배하도록 메시지의 내용에 초과 캐릭터(characters)들을 삽입하는 단계를 포함하는 것을 특징으로 하는 메시지 암호화 방법.

청구항 9

제 8 항에 있어서,

상기 초과 캐릭터가 스페이스인 것을 특징으로 하는 메시지 암호화 방법.

청구항 10

제 1 항에 있어서,

상기 스크램블 패턴이 다음의 식,

$$G(S) = S * \mathrm{mod}(J)$$

에 따른 비밀 계수(J)와 제 4 비밀 소수(S)의 함수인 것을 특징으로 하는 메시지 암호화 방법.

청구항 11

제 1 항에 있어서,

상기 메시지의 내용을 변환하는 단계(104)와 상기 메시지의 내용을 분리하는 단계(106)와 상기 메시지의 내용을 스크램블 하는 단계(108) 후에, 암호화된 메시지를 수신 장치로 송신하는 단계(110)를 더 포함하는 것을 특징으로 하는 메시지 암호화 방법.

청구항 12

공개 암호 키(E)와 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)의 함수로, 제 1 폼(M)에서 제 2 폼(M')으로 메시지의 내용을 변환하는 단계(104)와;

상기 메시지의 내용을 제 2 폼(M')으로 변환한 후, 스페이스 패턴에 따라 상기 메시지의 내용을 추가로 암호화(106)하기 위해, 상기 변환된 메시지의 내용을 분리하는 단계로서, 상기 스페이스 패턴은 제 3 비밀 소수 (R)와 제 2 공개 암호 키(K)의 함수인 상기 분리 단계(302)와;

상기 메시지의 내용을 제 2 폼(M')으로 변환한 후, 스크램블 패턴에 따라 상기 메시지의 내용을 추가로 암호화(108)하기 위해, 상기 변환된 메시지의 내용을 스크램블하는 단계로서, 상기 스크램블 패턴은 제 4 비밀 소수(S)와 비밀 계수(J)의 함수인 상기 스크램블 단계(308)와;

암호화된 메시지를 암호화 장치에서 수신 장치로 전송하는 단계(110)와;

상기 스크램블 패턴을 역으로 하도록(114), 상기 스크램블 패턴을 계산하고(504) 상기 암호화된 메시지 전체를 파싱(parsing)하는 단계와;

상기 메시지의 내용을 단일한 메시지에 배치하도록(116), 상기 스페이스 패턴을 계산하고(506) 상기 암호화된 메시지 전체를 파싱하는 단계와;

해역 키(D)와 제 2 비밀 소수(Q)의 함수로서 상기 메시지의 내용을 상기 제 2 폼(M')에서 상기 제 1 폼(M)으로 변환하는 단계(118)

를 포함하는 것을 특징으로 하는 암호화 및 해역 방법.

청구항 13

제 12 항에 있어서,

상기 제 1 비밀 소수(P)와 상기 제 2 비밀 소수(Q)의 곱이 상기 제 1 폼(M)의 메시지의 내용의 숫자 표현의 값보다 큰 것을 특징으로 하는 암호화 및 해역 방법.

청구항 14

제 13 항에 있어서,

상기 공개 키(E)가 상기 제 1 비밀 소수(P)와 상기 제 2 비밀 소수(Q)에 대한 소수인 것을 특징으로 하는 암호화 및 해역 방법.

청구항 15

제 14 항에 있어서,

상기 메시지의 내용이 상기 제 1 폼(M)에서 상기 제 2 폼(M')으로, 다음의 식

$$M' = M^{E} * \mathrm{mod}(P * Q)$$

에 따라 변환되는 것을 특징으로 하는 암호화 및 해역 방법.

청구항 16

제 12 항에 있어서,

상기 스페이스 패턴이 다음의 식,

$$F(R) = R * \mathrm{mod}(K)$$

에 따라 계산되는 것을 특징으로 하는 암호화 및 해역 방법.

청구항 17

제 12 항에 있어서,

상기 스크램블 패턴이 다음의 식,

$$G(S) = S * \mathrm{mod}(J)$$

에 따라 계산되는 것을 특징으로 하는 암호화 및 해역 방법.

청구항 18

제 12 항에 있어서,

해역 키가 다음의 식,

$$D * E = 1 * \mathrm{mod}((P-1) * (Q-1))$$

에 따라 계산되는 것을 특징으로 하는 암호화 및 해역 방법.

청구항 19

제 18 항에 있어서,

상기 메시지의 내용이 상기 제 2 폼(M')에서 상기 제 1 폼(M)으로, 다음의 식

$$M = (M')^{D} * \mathrm{mod}(P * Q)$$

에 변환되는 것을 특징으로 하는 암호화 및 해역 방법.

청구항 20

제 1 프로세서(706)와, 상기 제 1 프로세서(706)와 연결된 제 1 메모리(708)와, 통신 네트워크(712)와 상기 제 1 프로세서(706) 및 상기 제 1 메모리(708)와 연결된 제 1 네트워크 인터페이스를 포함하는 암호화 모듈(702)과;

제 1 폼(M)에서 제 2 폼(M')으로, 공개된 암호 키(E)와 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)의 함수로서 메시지의 내용을 변환하도록, 상기 제 1 메모리 내에 저장되며 상기 제 1 프로세서에 의해 수행가능한 변환 로직과;

메시지의 내용이 제 2 폼(M')으로 변환된 후, 상기 메시지의 내용을 추가로 암호화하기 위해, 제 3 비밀 소수(R)를 기초로 하는 스페이스 패턴에 따라 상기 메시지의 내용을 분리하도록, 상기 제 1 메모리에 저장되며 상기 제 1 프로세서에 의해 수행되는 분리 로직과;

메시지의 내용이 제 2 폼(M')으로 변환된 후, 상기 메시지의 내용을 추가로 암호화하기 위해, 제 4 비밀 소수(S)를 기초로 하는 스크램블 패턴에 따라 상기 메시지의 내용을 스크램블하도록, 상기 제 1 메모리에 저장되며 상기 제 1 프로세서에 의해 수행되는 스크램블 로직과;

상기 통신 네트워크(712)를 통해 암호화된 메시지를 송신하도록, 상기 제 1 메모리에 저장되며 상기 제 1 프로세서에 의해 수행되는 통신 로직

을 포함하는 것을 특징으로 하는 메시지 암호화 시스템.

청구항 21

제 20 항에 있어서,

상기 메시지의 내용이 상기 제 1 폼(M)에서 제 2 폼(M')으로, 다음의 식,

$$M' = M^{E} \bmod (P * Q)$$

에 따라 변환되는 것을 특징으로 하는 메시지 암호화 시스템.

청구항 22

제 20 항에 있어서,

상기 메시지의 내용을 분리하기 위한 스페이스 패턴이 다음의 식,

$$F(R) = R * \bmod (K)$$

에 따른 제 3 비밀 소수(R)와 계수(K)의 함수인 것을 특징으로 하는 메시지 암호화 시스템.

청구항 23

제 22 항에 있어서,

스페이스 패턴에 따라 상기 메시지의 내용을 분리하는 구문이

상기 메시지의 내용을 복수의 구분된 패킷으로 전달하는 것을 특징으로 하는 메시지 암호화 시스템.

청구항 24

제 22 항에 있어서,

스페이스 패턴에 따라 상기 메시지의 내용을 분리하는 구문이

상기 메시지의 내용을 복수의 그룹으로 분배하도록, 상기 메시지의 내용에 복수의 초과 캐릭터를 삽입하는 단계를 포함하는 것을 특징으로 하는 메시지 암호화 시스템.

청구항 25

제 20 항에 있어서,

상기 스크램블 패턴이 다음의 식,

$$G(S) = S * \mathrm{mod}(J)$$

에 따른 비밀 계수(J)와 제 4 비밀 소수(S)의 함수인 것을 특징으로 하는 메시지 암호화 시스템.

청구항 26

공개된 암호 키(E)와 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)의 함수로 제 1 폼(M)에서 제 2 폼(M')으로 메시지의 내용을 변환하는 수단과;

상기 메시지의 내용이 제 2 폼(M')으로 변환된 후, 상기 메시지의 내용을 추가로 암호화하기 위해, 스페이스 패턴에 따라 상기 메시지의 내용을 분리하는 수단으로서, 이때 상기 스페이스 패턴은 제 3 비밀 소수(R)와 제 2 공개 암호 키(K)의 함수인 상기 분리 수단과;

상기 메시지의 내용이 제 2 폼(M')으로 변환된 후, 상기 메시지의 내용을 추가로 암호화하기 위해, 스크램블 패턴에 따라 상기 메시지의 내용을 스크램블 하는 수단으로서, 상기 스크램블 패턴은 제 4 비밀 소수(S)와 비밀 계수(J)의 함수인 상기 스크램블 수단과;

상기 스크램블 패턴을 역으로 하도록, 상기 스크램블 패턴을 계산하고 상기 암호화된 메시지 전체를 파싱하는 디스크램블 수단과;

상기 메시지의 내용을 일체화된 메시지에 배치하도록, 상기 스페이스 패턴을 계산하고 상기 암호화된 메시지 전체를 파싱하는 일체화 수단과;

해역 키(D)와 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)의 함수로서, 상기 제 2 폼(M')에서 상기 제 1 폼(M)으로 상기 메시지의 내용을 변환하는 제 2 변환 수단

을 포함하는 것을 특징으로 하는 메시지 암호화 및 해역 시스템.

청구항 27

제 26 항에 있어서,

상기 제 2 변환 수단은, 공개 암호화 키(E)와 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)의 함수로서, 비밀 해역 키(D)를 다음의 식

$$D * E = 1 * \mathrm{mod}((P-1)*(Q-1))$$

에 따라 계산하며,

상기 계산된 비밀 해역 키(D)를 사용하여, 상기 메시지의 내용을 상기 제 2 폼(M')에서 다시 상기 제 1 폼(M)으로, 다음의 식

$$M = (M')^{D} * \mathrm{mod}(P * Q)$$

에 따라 계산하는 것을 특징으로 하는 메시지 암호화 및 해역 시스템.

청구항 28

암호화된 메시지를 수신하는 단계(111)와;

제 4 비밀 소수(S)를 기초로 하는 스크램블 패턴을 바탕으로 암호화된 메시지의 내용을, 상기 스크램블 패턴을 이용하여, 디스크램블하는 단계(114)와;

제 3 비밀 소수(R)를 기초로 하는 스페이스 패턴을 바탕으로 암호화된 메시지의 분리된 내용을, 상기 스페이스 패턴을 이용하여, 하나의 단일화된 메시지로 배치하는 단계(116)와;

메시지의 내용을 디스크램블하고 메시지의 내용을 하나의 단일화된 메시지로 배치한 후, 공개 암호 키(E)와 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)를 바탕으로 상기 메시지의 내용을 제 2 폼(M')에서 다시 제 1 폼(M)으로 변환하는 단계

를 포함하는 것을 특징으로 하는 메시지 해역 방법.

청구항 29

제 28 항에 있어서, 상기 메시지의 내용을 디스크램블하는 단계는

제 4 비밀 소수(S)와 비밀 계수(J)를 이용하여 메시지의 내용에 대한 스크램블 패턴을 계산하는 단계(504)와;

암호화된 메시지 전체를 파싱하고 스크램블 패턴을 반전하는 단계

를 포함하며, 이때, 상기 스크램블 패턴은 공식

$$G(S) = S * \mathrm{mod}(J)$$

에 따라 계산되는 것을 특징으로 하는 메시지 해역 방법.

청구항 30

제 28 항에 있어서, 상기 메시지의 분리된 내용을 하나의 단일화된 메시지로 배치하는 단계는,

제 3 비밀 소수(R)와 제 2 공개 암호화 키(K)를 이용하여 메시지의 내용에 대한 스페이스 패턴을 계산하는 단계(506)와;

상기 분리된 메시지 전체를 파싱하여 스페이스 패턴을 반전하는 단계

를 포함하며, 이때,

상기 스페이스 패턴은 식

$$F(R) = R * \mathrm{mod}(K).$$

에 따라 계산되는 것을 특징으로 하는 메시지 해역 방법.

청구항 31

제 28 항에 있어서, 상기 메시지의 내용을 제 2 폼(M')에서 다시 제 1 폼(M)으로 변환하는 단계는

공개 암호화 키(E)와 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)의 함수로, 비밀 해역 키(D)를 계산하는 단계와;

계산된 비밀 해역 키(D)를 이용하여, 식 $M = (M')^{D} * \mathrm{mod}(P * Q)$ 에 따라, 메시지의 내용을 제 2 폼(M')에서 다시 제 1 폼(M)으로 변환하는 단계

를 포함하며, 이때, 상기 비밀 해역 키(D)는 식

$$D * E = 1 * \mathrm{mod}((P-1) * (Q-1))$$

에 따라 계산되는 것을 특징으로 하는 메시지 해역 방법.

청구항 32

프로세서(714)와, 상기 프로세서(714)로 연결되는 메모리(716)와, 통신 네트워크(712)와, 상기 통신 네트워크(712), 상기 프로세서(714) 및 상기 메모리(716)와 연결되는 네트워크 인터페이스(716)를 포함하는 해역 모듈(704)과;

통신 네트워크(712)를 통해 암호화된 메시지를 수신하도록 메모리(716)에 저장되며 프로세서(714)에 의해 실행되는 통신 로직과;

제 4 비밀 소수(S)를 기초로 하는 스크램블 패턴을 바탕으로 암호화된 메시지의 내용을, 상기 스크램블 패턴을 이용하여, 디스크램블하도록 메모리(716)에 저장되며 프로세서(714)에 의해 실행되는 디스크램블 로직과;

제 3 비밀 소수(R)를 기초로 하는 스페이스 패턴을 바탕으로 암호화된 메시지의 분리된 내용을, 상기 스페이스 패턴을 이용하여, 하나의 단일화된 메시지로 배치하도록 메모리(716)에 저장되고 프로세서(714)에 의해 실행되는 단일화 로직과;

메시지의 내용이 디스크램블되고 메시지의 내용이 하나의 단일화된 메시지로 배치된 후, 공개 암호화 키(E)와 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)를 바탕으로, 메시지의 내용을 제 2 폼(M')에서 다시 제 1 폼(M)으로 변환하도록 메모리(716)에 저장되며 프로세서(714)에 의해 실행되는 변환 로직

을 포함하는 것을 특징으로 하는 메시지 해역 시스템.

청구항 33

제 32 항에 있어서, 프로세서에 의해 상기 디스크램블 로직은,

제 4 비밀 소수(S)와 비밀 계수(J)를 이용하여 메시지의 내용에 대한 스크램블 패턴을 계산하고,

암호화된 메시지 전체를 파싱하여 스크램블 패턴을 반전하도록

실행되며, 이때, 상기 디스크램블 로직은, 프로세서에 의해, 식

$$G(S) = S^{*}\mathrm{mod}(J)$$

에 따라 스크램블 패턴을 계산하도록 실행되는 것을 특징으로 하는 메시지 해역 시스템.

청구항 34

제 32 항에 있어서, 프로세서에 의해 상기 단일화 로직은

제 3 비밀 소수(R)와 제 2 공개 암호화 키(K)를 이용하여 메시지의 내용에 대한 스페이스 패턴을 계산하고,

분리된 메시지를 파싱하여 스페이스 패턴을 반전하도록

실행되며, 이때, 상기 단일화 로직은, 프로세서에 의해, 식

$$F(R) = R^{*}\mathrm{mod}(K)$$

에 따라 스페이스 패턴을 계산하도록 실행되는 것을 특징으로 하는 메시지 해역 시스템.

청구항 35

제 32 항에 있어서, 프로세서에 의해 상기 변환 로직은

공개 암호화 키(E)와 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)의 함수로 비밀 해역 키(D)를 계산하고,

계산된 비밀 해역 키(D)를 이용하여, 식 $M = (M')^{D}\ ^{*}\mathrm{mod}(P*Q)$ 에 따라 메시지의 내용을 제 2 폼(M')에서 제 1 폼(M)으로 변환하도록

실행되며, 이때, 상기 변환 로직은, 프로세서에 의해, 식

$$D*E = 1^{*}\mathrm{mod}((P-1)*(Q-1))$$

에 의해, 비밀 해역 키(D)를 계산하도록 실행되는 것을 특징으로 하는 메시지 해역 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 통신 네트워크, 구체적으로, 무선 매체 전체나 일부에 제공된 통신 네트워크에서 데이터 보안을 위한 데이터 암호화 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 통신 네트워크, 구체적으로, 무선 매체 전체나 일부에 제공된 통신 네트워크의 확산에 따라, 데이터 보안이 중요한 문제가 되고 있다. 무선 네트워크 기술이 유선 네트워크 기술에 비해 상대적으로 신규하다. 이와 같은 무선 네트워크를 보호하는 현재의 기술이 유선 네트워크를 위해 개발되었거나 이에 사용되는 기술로부터 유래된다. 예를 들면, 네트워크(무선 또는 유선)를 보호하는 기술 중 하나가 통신을 암호화하는 것이다. 이는

승인되지 않은 파티(party)에 의해 통신 해석되어 네트워크가 위태롭게 되는 것을 방지한다. 중간에 무선 부분을 포함하지 않는 직접적인 유선 네트워크 경로에 대하여는 현재 만족스러운 결과를 나타낸다. 암호화된 전송을 위협하기 위해서는, 공격자(attacker)들이 일반적으로 암호화 알고리즘을 깨트리도록 하는 다중 트랜잭션(transaction)에 대해 주의를 기울일 필요가 있다. 예를 들어, 외부 파티가 직접적인 케이블 연결에 대한 트랜잭션(transaction)에의 접속을 다시 획득하도록, 외부 파티가 유선 네트워크나 이에 연결된 서버에 대한 접속을 다시 획득할 수 있으며, 하나의 트랜잭션이 서버에 의해 수신되거나 전송될 시점을 외부 파티가 결정할 수 있을 때까지, 데이터 스트림을 밀접하게 모니터할 수 있다. 다르게는, 외부 파티가 서버에 저장된 어떤 보안 데이터베이스와 같은, 서버에 포함된 데이터에 접속을 시도할 수 있다. 일단 접속되고, 충분한 데이터가 모아지면, 공격자(attacker)가 데이터를 해역할 수 있다. 서버에 저장된 데이터를 보호하기 위한 기술이 알려져 있으며, 이는 유선 매체의 관련 비-접속성이 무선 통신에 접속하거나 끼어드는 것을 원천적으로 어렵게 한다. 그러나, 통신을 무선으로 전송할 때, 통신을 전달하는 무선 신호는 종종 전 방향성 방송 신호이며, 이로써 가청 범위에 있는 누구든지 접속할 수 있게 한다. 이에 따라, 서버에서 또는 통신 매체에 대하여 공격으로부터 트랜잭션을 보호하도록 구현되는 기술이 부분적으로라도 무선 네트워크(데이터가 서버에 의해 보호될 수 없고 무선 신호를 안전하게 가둬둘 수 없음)를 통해 전송되는 트랜잭션을 보호하기는 조금 부족하다. 트랜잭션이 부분적으로라도 무선 네트워크를 통해 전송되는 경우에, 누구든지 데이터 스트림을 가로채려는 시도를 할 수 있다. 이는 지정된 암호화 알고리즘이 공격자에 의해 위협을 받을 수 있다는 가능성을 증가시킨다.

[0003] 무선 네트워크를 사용하는 트랜잭션에서, 주요한 관심사 중 하나는, 신용 카드 번호, 은행 계좌 번호 및 사회 안전 번호와 같은 개인 및/또는 안전 정보를 얻기 위해, 보호를 위해 암호화된 트랜잭션을 가로채고 이를 해역하는 외부 파티의 능력이다. 따라서, 외부 파티가 트랜잭션을 가로채 해역하는 것을 방지하도록 무선 트랜잭션을 보호할 필요성이 있다.

발명의 상세한 설명

[0004] 본 발명은 3 단계 암호화 방법 및 3 단계 해역 방법, 그리고 3 단계 암호화 방법 및 3 단계 해역 방법을 구현하는 장치에 관한 것이다. 메시지를 3 단계 암호화 방법에 따라 암호화하기 위해, 메시지의 내용을 제 1 폼(M)에서 제 2 폼(M')으로 변환하고, 메시지의 내용을 스페이스 패턴에 따라 분리하며, 그리고 메시지의 내용을 스크램블 패턴에 따라 스크램블 한다. 3 단계 암호화 방법을 이용하여 암호화된 메시지를 해역하기 위해, 스크램블 및 스페이스 패턴이 역으로 되고, 메시지의 내이 제 2 폼(M')에서 제 1 폼(M)으로 변환된다.

실 시 예

[0017] 도 1은 본 발명의 일 실시예에 따른 3 단계 암호화 및 3 단계 해역 기술을 나타내는 흐름도이다. 어떤 하나의 장치가 3 단계 암호화 기술이나, 3 단계 해역 기술이나 이들의 조합을 구현할 수 있음은 당연하다.

[0018] 일반적으로, 게시된 3 단계 암호화 및 해역 기술이 무선 네트워크에 적어도 부분적으로 참여하는 통신을 보호하는데 사용될 수 있다. 그러나, 게시된 3 단계 암호화 및 해역 기술이 하드웨어 매체나 다른 유형의 통신 매체에 대한 통신을 위해 사용될 수 있음은 본 발명의 속하는 분야의 평균적 지식을 가는 자에게 자명하다.

[0019] 전송 장치가 수신 장치로 메시지를 전송하기 전에, 일반적으로 3 단계 암호화 기술이 전송 장치에 의해 메시지를 암호화하는 데 사용된다. 전송 장치는 외부 파티가 메시지를 쉽게 가로채지 못하도록 막는다. 이 경우에, 메시지는 통신 매체를 통해 수신 장치로 전달되고, 에 대한 접속을 획득하도록 한다.

[0020] 일반적으로 수신 장치가 전송 장치로부터 메시지를 수신한 후에, 메시지를 해역하기 위해 수신 장치에 의해 3 단계 해역 기술이 사용된다. 수신 장치는, 3 단계 암호화 기술이 보호하는, 신용카드 번호, 은행 계좌, 및 사회 보장 번호와 같은 개인 및/또는 보안 정보에 대한 접속을 획득하도록 하는 메시지를 해역한다.

[0021] 일 실시예에서, 송신/전송 장치(암호화 능력을 가짐)가 게시된 3 단계 암호화 기술(102)을 사용하여 메시지를 암호화하고, 이 메시지를 수신 장치(110)로 전송한다. 이러한 통신이 양 방향일 수 있으며, 다양한 장치들이 송신 및 수신을 모두 할 수 있음이 분명하다. 그리하여, 여기에 사용된 송신 장치나 수신 장치의 명칭이 문맥에 따라 적용될 수 있으며, 하나의 통신을 위한 송신 장치가 다른 통신에 대한 수신 장치일 수 있다. 송신 장치가 퍼스널 컴퓨터, 퍼스널 디지털 보조기기(assistant), 서버, 워크스테이션, 기구(예를 들면, 네트워크상에서 데이터를 송수신하는 세탁/건조기, 냉장고, 물 처리 시스템 또는 스토브와 같은 스마트 기기) 도는 종래 기술에 따른 다른 유형의 네트워크 가용 장치 또는 이들의 조합을 포함한다. 또한, 개량되거나 네트워크를 활성화하도록 구성된 네트워크 비 가용 장치를 포함한다. 수신 장치가 메시지(11)를 수신하고, 게시된 3 단계 해역 기술

(112)을 이용하여 암호화된 메시지를 해역한다. 암호화 장치와 같이, 수신 장치가 퍼스널 컴퓨터, 퍼스널 디지털 보조기기(assistant), 서버, 워크스테이션, 기구(예를 들면, 네트워크상에서 데이터를 송수신하는 세탁/건조기, 냉장고, 물 처리 시스템 또는 스토브와 같은 스마트 기기) 도는 종래 기술에 따른 다른 유형의 네트워크 가용 장치 또는 이들의 조합을 포함한다. 또한, 개량되거나 네트워크를 활성화하도록 구성된 네트워크 비 가용 장치를 포함한다.

[0022] 암호화 메시지(110)를 암호화 장치로부터 수신 장치로 전송하는데 사용되는 무선 프로토콜이 무선 피델리티("Wi-Fi")를 포함할 수 있다. 무선 피델리티는 802.11(a), 802.11(b) 또는 802.11(9)와 같은 IEEE 802.11 표준 설정; 일반적인 패킷 라디오 서비("GPRS"); 블루투스, 위성이나 셀룰러 전송; 울트라 와이드밴드; WiMax; 또는 RF, 빛이나 다른 전송 매체를 사용하는 다른 유형의 무선 프로토콜에 적합다. 또한, 무선 프로토콜이 네트워크의 다양한 부분에 대해 서로 다른 무선 기술의 조합을 추가로 포함할 수 있다.

[0023] 네트워크로 전송될 메시지에 대한 3 단계 암호화 기술(102)의 동작시에, 소인수 분해를 이용하여, 전송 중에 메시지의 원래 내용을 감추도록, 메시지의 내용이 제 1 폼(M)으로부터 제 2 폼(M', 104)로 변환된다.

[0024] 메시지의 내용이 이후에, 이하에 설명된 바와 같이 복수의 구분된 패킷이나 복수의 그룹핑으로 분리되어(106), 메시지가 전송되는 구간을 비 균질화(de-homogenize) 한다. 이로써, 제 3 파티가 전송을 엿듣거나 메시지 내용을 해역하는 것을 더욱 어렵게 한다.

[0025] 일 실시예에서, 메시지의 내용을 분리하기 위해, 전송시에 지정된 시간 구간으로 분리된 복수의 구분된 패킷을 통해 메시지의 내용의 일부가 분산(spread)되도록, 메시지의 내용이 쪼개진다. 다른 실시예에서, 메시지의 내용을 분리하기 위해, 초과 캐릭터(가령, 공백(spaces))들이, 메시지의 내용 사이에 삽입되어, 메시지의 내용을 다수의 그룹으로 분배하게 된다.

[0026] 마지막으로, 메시지의 내용을 포함하는, 복수의 구분된 패킷이나 복수의 그룹핑이 사용자 정의된 패턴(108)에 따라 뒤섞인다. 이의 실시예가 이하에서 상세히 설명된다.

[0027] 상기 언급한 3 단계 암호화 기술(102)을 사용하여 암호화된 메시지를 해역하기 위해, 3 상 암호화 기술(102)이 간단히 역으로 된다(112). 일반적으로, 보안성 증가를 위해, 게시된 3 상 암호화 기술(102)을 사용하여 암호화된 메시지를 해역하기 위한 필수 알고리즘과 변수를 수신 장치가 알고 있다. 그러나, 다른 실시예에서, 메시지를 해역하기 위한 필수 알고리즘과 변수가 보안성을 감소시키는 댓가로 수신 장치에 전달될 수도 있다.

[0028] 초기에, 사용자 정의 패턴을 역으로 함으로써, 여러 구분된 펄스 또는 여러 그룹핑 내에 메시지의 내용이 디스크램블 된다(discrambled, 114). 다음으로, 메시지의 내용을 포함하는 복수의 패킷이 하나의 메시지로 다시 형성되거나, 원래 메시지를 깨뜨리는데 사용되는 방법에 따라 복수의 그룹핑 사이의 초과 캐릭터가 제거된다(116). 일반적으로, 원래 메시지를 깨트리는데 사용되는 방법이 하나 또는 두 개의 디지트 숫자의 형태로 메시지의 헤드에 표시된다. 마지막으로, 메시지의 내용이 제 2 폼(M')으로부터 제 1 폼(M, 118)으로 변환된다.

[0029] 도 2는 3 단계 암호화 기술의 변환 단계(200)의 일 실시예를 나타내는 흐름도이다. 일반적으로, 메시지의 내용이 암호화되기 전에, 메시지 내용의 알파벳 구문이 숫자 표면(202)으로 변환된다. 예를 들어, 문자 "a"가 01과 같이 숫자 형태로 표현되도록 변환될 수 있으며, 문자 "b"가 02 등과 같은 숫자 형태로 변환된다. 알파벳 변환은 정보 교환에 대한 미국 표준 코드(American Standard code For Information Interchange("ASCII")나 확장된 이진 코드 십진 교환 코드(Extended Binary Code Decimal Interchange Code("EBCDIC") 표준에 부합하거나, 또는 임의 변환일 수도 있다. 알파벳 구문을 숫자 표면으로 변환하기 위한 함수가 공지되어 있으며, 대부분의 프로그램 언어가 이러한 형태의 동작을 수행하는 표준 함수를 포함한다.

[0030] 제 1 폼(M)에서 제 2 폼(M')으로, 메시지 내용을 변화하기 위해, 송신 장치 및/또는 수신 장치의 암호화 컴포넌트와 해역 컴포넌트가 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)와 공지된 암호 키(E)와 비밀 암호 키(D)를 이용하여 프로그램된다. 추가로, 제 1 및 제 2 비밀 소수의 곱이 N이 되도록 정의된다.

[0031] 보안성 개선을 위해, 공지된 암호 키가 제 1 및 제 2 비밀 소수(P, Q)에 대 다음과 같이 서로 소(relatively prime, 206) 이어야 한다.

[0032] $$GCD(E,(P-1)*(Q-1))=1$$

[0033] 여기서, GCD는 최대공약수이다. 잘 알려진 바와 같이, 둘 이상의 정수가 1을 제외한 양의 공약수를 공유하는 경우에, 둘 이상의 정수가 서로 소인 것으로 정의된다.

[0034] 비밀 해역 키(D)가 수신 장에의 의해 수신된 메시지를 디코드하는데 사용된다. 제 1 암호 소수(P), 제 2 암호 소수(Q), 그리고 공지된 암호 키(E)를 선택한 후에, 비밀 암호 키(D)가 다음 식을 사용하여 계산된다:

[0035] $$D * E = 1 * \mathrm{mod}((P-1)*(Q-1)).$$

[0036] 제 1 비밀 소수(P)와 제 2 비밀 소수(Q)의 곱(N)과 공개 암호 키(E)를 이용하여, 메시지의 내용이 제 1 폼(M)에서 제 2 폼(M')으로 다음 식에 따라 변환된다(208).

[0037] $$M' = M^{E} \bmod N.$$

[0038] 제 1 폼(M)으로부터 제 2 폼(M')으로의 변환이 정확히 동작하도록 하기 위해, N의 숫자 값이 제 1 폼(M)의 메시지의 내용의 숫자 값보다 커야한다.

[0039] 도 3a 및 4a가 3 상 암호화 기술의 분리 단계를 나타내는 흐름도이다. 일반적으로, 메시지의 내용이 변환 단계 후에 분리되나, 다른 실시예에서는, 메시지의 내용이 변환 단계 전에 분리될 수 있다.

[0040] 도 3a에 도시된 실시예에서, 메시지의 내용을 분리하기 위해, 메시지의 내용이 쪼개진다(300). 이에 따라 메시지의 내용이 복수의 구분된 패킷(304)을 통해 펼쳐진다. 일반적으로, 복수의 구분된 패킷에 대한 스페이스(spacing) 패턴을 결정하기 위해, 제 3 비밀 소수(R) 및 공개된 제 2 암호 키(K)가 선택된다. 공개된 암호 키(K)의 값이 10과 같은 계수(modulus), 비밀 암호 키(D) 또는 다른 추천 값일 수 있다

[0041] 일 실시예에서, 스페이스 패턴이 복수의 구분된 패킷 사이에서 암호화 장치가 대기하는 캐릭터의 수일 수 있다. 그러나, 다른 실시예에서, 복수의 구분된 패킷 사이의 스페이스에 대한 다른 수단에 대응하는 스페이스 패턴의 값을 가지도록 사용자가 선택할 수 있다. 스페이스 패턴이 일반적으로 다음 식에 따라 계산된다(302).

[0042] $$F(R) = R * \mathrm{mod}(K)$$

[0043] 일부 실시예에서, 스페이스 패턴이 "R 모드 K"와 "K-R 모드 K" 사이에서 변경될 수 있다. 또는 사용자에 의해 선택된 다른 식에 따라 계산될 수 있다.

[0044] 도 4a에 도시된 또 다른 실시예에서, 메시지(400)의 내용을 복수의 그룹핑(grouping)으로 분리하기 위해, 초과 캐릭터가 메시지(404)의 내용 전체에 삽입된다. 초과 캐릭터는 스페이스이거나 사용자가 원하는 다른 유형의 캐릭터일 수 있다. 도 3a의 실시예 내의 스페이스 패턴을 결정하기 위한 위에 언급한 것과 동일한 프로세스에 따라 초과 캐릭터의 개수에 대한 스페이스 패턴이 결정된다. 일반적으로, 제 3 비밀 소수(R)와 제 2 공지된 암호 키(K)가 선택된다. 제 2 공개 암호 키(K)의 값이 10과 같은 계수일 수 있으며, 비밀 암호 키(D)의 값이나 다른 추천 값일 수 있다. 스페이스 패턴이 다음 식에 따른 계산된다(402).

[0045] $$F(R) = R * \mathrm{mod}(K).$$

[0046] 일부 실시예에서, 스페이스 패턴이 "R 모드 K" 및 "K-R 모드 K"나 사용자에 의해 선택된 다른 식 사이에서 변경될 수 있다.

[0047] 일반적으로, 스페이스 단계(300, 400) 후에, 남아 있는 메시지 내용의 섹션이 섞인다(scarmbled)(306, 406). 그러나, 다른 실시예에서, 3 단계 암호화 기술의 순서가 변경되어, 스페이스 단계(300)나 변환 단계(200) 이전에, 메시지의 내용이 뒤섞일 수 있다(306, 406).

[0048] 도 3b는 3a에 도시된 실시예에 따른 3 단계 암호화 방법의 스크램블(scrambiling) 단계(306)를 나타내는 흐름도이다. 일반적으로, 제 4 소수(S) 및 비밀 계수(J)가 선택된다. 비밀 계수(J)의 값이 10과 같은 정수이거나 비밀 암호 키 중 하나 또는 한 세트의 전체 비밀 수(number)일 수 있다. 제 4 소수(S)와 비밀 계수(J)가 다음 식에 따라 스크램블 패턴을 계산(308)하는 사용된다.

[0049] $$G(S) = S * \mathrm{mod}(J)$$

[0050] 일 실시예에서, 스크램블 패턴이 복수의 구분된 패킷 중 어느 것이 지정된 발명에 따라 스크램블 될 것인지를 나타낸다. 예를 들어, 스크램블 패턴이 숫자 2와 동일한 경우, 이는 모든 다른 구분된 패킷 상에 스크램블 동작이 가해진다는 것을 의미한다. 스크램블 동작이 두 개의 숫자 캐릭터를 역으로 하거나, 상수를 숫자 메시지 값에 더하거나 또는 사용자가 원하는 다른 함수 (310)를 포함할 수 있다.

[0051] 도 4b는 도 4a에 도시된 실시예에 따른 스크램블 단계(406)를 나타내는 흐름도이다. 도 3a 및 3b에 도시된 실시예에 대해 위에 언급한 바와 같이, 제 4 소수(S)와 비밀 계수(J)가 다음의 식에 따라 스크램블 패턴을 계산(408)하는 데 사용된다.

[0052] $$G(S) = S * \mathrm{mod}(J)$$

[0053] 도 5는 도 3a 및 3b에 도시된 실시예에 따라 생성된 암화화 메시지의 해역를 나타내는 흐름도이다. 암호화 장치가 3 단계 암호화 기술을 통해 메시지를 처리한 후에, 암호화된 메시지가 수신 장치(502)로 전달될 수 있다. 일단 수신되면, 수신 장치가 3 단계 암호화 기술을 역으로 하여 암호화된 메시지를 해역한다.

[0054] 일반적으로, 도 3b에 기술된 프로세스를 간단히 역으로 동작시킴으로써 복수의 구분된 패킷 내의 메시지의 내용이 디스크램블 된다(discrambled, 504). 일반적으로, 스크램블 패턴을 계산하고, 스크램블(504)을 역으로 하여 암호화된 메시지의 내용을 통해 파싱(parse) 동작을 할 수 있도록, 수신 장치는 비밀 계수(J)와 제 4 소수(S)를 알고 있을 것이다.

[0055] 디스크램블 단계(504) 후에, 메시지를 포함하는 복수의 구분된 패킷이 단일 메시지(506)로 다시 형성된다. 일반적으로, 수신 장치가 제 3 비밀 소수(R)와 제 2 공개 암호 키(K)를 알고 있다. 따라서, 수신 장치가 스페이스 패턴을 계산하고 도 3a에 506으로 나타낸 프로세스를 역으로 하도록 메시지를 파싱한다.

[0056] 복수의 구분된 패킷이 하나의 메시지(506)로 재형성된 후에, 메시지의 내용이 제 2 폼(M')으로부터 제 1 폼(M)으로 변환된다(M510). 일반적으로, 수신 장치가 공개 암호 키(E)와 제 1 및 제 2 비밀 소수(P, Q)를 알고 있다. E, P 및 Q를 사용하여, 수신 장치가 다음 식에 따라 비밀 암호 키(D)를 계산한다(508).

[0057] $$D * E = 1 * \mathrm{mod}((P-1)*(Q-1))$$

[0058] 수신 장치가 이후에, 다음 식에 따라 제 2 폼(M')으로부터 제 1 폼(M)으로 메시지의 내용을 변환한다(510).

[0059] $$M = (M')^{D} * \mathrm{mod}(P*Q)$$

[0060] 도 6은 도 4a 및 4b에 도시된 실시예에 따라 암호화 장치(602)로부터 수신된암복화된 메시지의 해역(600)를 나타내는 흐름도이다. 일반적으로, 도 4b에 도시된 상술한 프로세스를 간단히 역으로 함으로서 초과 캐릭터가 나뉜 메시지의 내용이 뒤섞인다(604). 일반적으로, 스크램블 패턴을 계산하고 스크램블 프로세스를 역하기 위해 메시지 전체를 파싱하도록, 수신 장치가 비밀 계수(J)와 제 4 소수(S)를 알고 있다.

[0061] 디스크램블 단계(604) 후에, 메시지를 포함하는 복수의 구분된 패킷이 단일 메시지로 재형성된다(606). 일반적으로, 수신 장치가 소수(R)와 제 2 암호화 키(K)를 알고 있으므로, 스페이스 패턴을 계산하고 도 4a 도시된 분리 프로세스를 역으로 동작하도록 하기 위해 메시지 전체를 파싱할 수 있다.

[0062] 복수의 분리된 패킷이 하나의 메시지로 재구성(606)된 후에, 메시지의 내용이 제 2 폼(M')으로부터 제 1 폼(M)으로 변환된다(610). 일반적으로, 수신 장치가 공개 암호 키(E)와 제 1 비밀 소수(P)와, 제 2 비밀 소수(Q)를 알고 있다. E, P, Q를 이용하여, 수신 장치가 다음과 같은 식에 따라 비밀 암호 키(D)를 계산한다(608).

[0063] $$D * E = 1 * \mathrm{mod}((P-1)*(Q-1))$$

[0064] 수신 장치가 이후에 제 2 폼(M')에서 제 1 폼(M)으로, 다음 식에 따라 메시지의 내용을 변환한다(610).

[0065] $$M = (M')^{D} * \mathrm{mod}(P*Q)$$

[0066] 다른 실시예에서, 암호화 프로세스 내의 각 단계의 순서에 따라, 해역 프로세스 내의 단계의 순서가 역으로 될 수 있다.

[0067] 도 7은 3 단계 암호화 기술을 이용하여 메시지를 암호화하기 위한 암호화 모듈(702)의 일 실시예와, 3 단계 해역 기술을 사용하여 메시지를 해역하는 해역 모듈(704)의 일 실시예를 나타내는 블럭도이다. 암호화 및 해역 모듈들(702, 704)가 3 단계 암호화 및 복화 기술을 수행할 있는 하드웨어나 소프트웨어 형태일 수 있다. 단일 장치가 암호화 및 해역 모듈(702, 704) 양쪽을 포함할 수 있어, 하나의 장치가 양 방향 통신을 수행할 수 있다. 단일 장치가 암호화 및 해역 모듈(702, 704) 중 어느 하나를 포함하여 하나의 장치가 일 방향만으로의 통신을 수행할 수 있다.

[0068] 암호화 모듈(702)이 일반적으로 암호화 프로세서(706)를 포함하며, 암호화 프로세서(706)에 연결된 암호화 메모리(708), 그리고 암호화 프로세서(706)와 암호화 메모리(708) 및 통신 네트워크(712)에 연결된 암호화 네트워크 인터페이스(710)를 포함한다. 이 명세서에서, "~와 연결된" 이라는 구문은 직접적으로 연결되거나 하나 이상의 중간 컴포넌트를 통해 간접적으로 연결된다는 것을 의미한다. 이러한 중간 컴포넌트가 하드웨어나 소프트웨어 기반 컴포넌트를 모두를 포함할 수 있다.

[0069] 암호화 프로세서(706)가 표준 펜티엄 프로세서, 인텔 확장 프로세서, 통상적인 프로세서나 다른 형태의 프로세서 하드웨어일 수 있다. 또는 암호화 프로세서가 제 1 폼(M)에서 제 2 폼(M')으로 메시지의 내용을 변환하고, 스페이스 패턴에 따라 메시지의 내용을 분리하고, 스크램블 패턴에 따라 메시지의 내용을 뒤섞는 위에 설명한 기능들을 수행하도록 소프트웨어 프로그램을 작동시킬 수 있다. 일반적으로, 이러한 함수가 소프트웨어 프로그램 내의 로직으로 구현되고, 암호화 메모리(708) 내에 저장되며 암호화 프로세서(706)에 의해 수행될 수 있다.

[0070] 암호화 메모리(708)가 롬(ROM)이나 플래시 메모리와 같은 유형의 메모리 중 하나일 수 있으며, 영구 또는 삭제 가능한 디스크 또는 드라이브의 형태일 수 있다. 암호화 네트워크 인터페이스(710)가 무선 네트워크, 하드웨어 통신 네트워크나 따른 형태의 통신 매체에 대해 통신을 할 수 있는 네트워크 인터페이스의 형태일 수 있다.

[0071] 유사하게, 해역 모듈(704)이 해역 프로세서(714), 해역 프로세서(714)에 연결된 해역 메모리(716), 해역 프로세서(714)와 해역 메모리(716)와 통신 네트워크(712)에 연결된 해역 네트워크 인터페이스(718)를 포함한다.

[0072] 암호화 프로세서(714)가 표준 펜티엄 프로세서, 인텔 확장 프로세서, 통상적인 프로세서나 다른 형태의 프로세서 하드웨어일 수 있다. 또는 암호화 프로세서가 스크램블 패턴에 따라 메시지의 내용을 디스크램블하고(descrambling), 스페이스 패턴에 따라 메시지의 분리된 내용을 일체화하고, 제 2 폼(M')에서 제 1 폼(M)으로 메시지의 내용을 변환하는 위에 설명한 기능들을 수행하도록 소프트웨어 프로그램을 작동시킬 수 있다. 일반적으로, 이러한 함수가 소프트웨어 프로그램 내의 로직으로 구현되고, 해역 메모리(716) 내에 저장되며 해역 프로세서(714)에 의해 수행될 수 있다. 해역 메모리(716)가 롬이나 플래시 메모리와 같은 형식의 메모리일 수 있으며, 또는 영구적이거나 제거가능한 디스크 또는 드라이브 중 어느 하나 일 수 있다.

[0073] 해역 네트워크 인터페이스(718)가 무선 네트워크나 회로 접속된 통신 네트워크 또는 통신 매체의 다른 형식일 수 있다.

[0074] 도 8a 및 8b는 메시지 암호화(도 8a)의 일 예를 나타내며, 이후에 3 단계 데이터 암호화 방법의 일 실시예를 이용하여 해역(8b)된다. 도 8a에 도시된 바와 같이, 제 1 폼(M)의 메시지가 23의 값을 가지도록 정의된다(802). 나아가, 제 1 비밀 소수가 5의 값을 가지도록 정의되고, 제 2 비밀 소수가 7의 값을 가지도록 정의되며, 공개된 암호화 키(E)가 29의 값을 가지도록 정의된다. 상술한 바와 같이, 제 1 및 제 2 비밀 소수의 값이 소수(prime number)이며 공개 암호 키(E)가 제 1 및 제 2 비밀 소수에 대해 소수이다. 나아가, 제 1 및 제 2 소수의 곱이 35가 되도록 계산되고, 이는 제 1 폼(M)의 메시지의 값보다 제 1 및 제 2 소수의 곱이 크다는 조건을 만족한다.

[0075] 상술한 바와 같이 다음의 식에 따라 메시지가 제 1 폼(M)에서 제 2 폼(M')으로 변환된다(804).

$$M' = M^{E} * \mathrm{mod}(P * Q)$$

[0076]
$$M' = (23)^{29} * \mathrm{mod}(35).$$

[0077] 변환 단계(804)가 수행될 때, 제 1 폼(M)의 메시지 값이 제 2 폼(M')의 18의 값을 가지도록 계산된다.

[0078] 변환 단계(804) 후에, 스페이스 단계(806)가 수행된다. 일 예에서, 제 3 비밀 소수가 31로 정의되고, 제 2 공개 암호 키가 10으로 정의된다. 다음의 식에 따라 상술한 바와 같이, 스페이스 패턴이 계산되며(806), 결과적으로 1의 값을 가진다.

$$F(R) = R * \mathrm{mod}(K)$$

[0079]
$$F(31) = 31 * \mathrm{mod}(10)$$

[0080] 일 예에서, 1의 값이 하나의 스페이스(간격), "00"이 되도록 정의된다.

[0081] 메시지가 구분된 패킷(808)으로 분리되는 실시예에서, "18"에서 1의 값이 구분된 패킷 사이에 하나의 스페이스를 가지는 "1_8"의 값으로 분리된 패킷이 된다.

[0082] 다르게는, 메시지(810)를 나누도록 초과 스페이스가 복수의 그룹 사이에 배치되는 실시예에서, "18"에서 복수의 그룹핑 사이에 두 개의 초과 캐릭터를 가지는 "1008"로 메시지가 분리되고, 초과 캐릭터는 스페이스를 정의한다.

[0083] 스페이스 단계(806) 후에, 스크램블 패턴이 계산된다(812). 일 실시예에서, 제 4 소수가 17이 되도록 정의되며, 비밀 계수가 15가 되도록 정의된다. 스크램블 패턴이 다음의 식에 따라 산출된다.

$$G(S) = S * \mathrm{mod}(J)$$

[0084] $$G(17) = 17 * \mathrm{mod}(15),$$

[0085] 결과적으로 2의 값이 된다. 일 예에서, 2의 값이 모든 다른 패킷이나 그룹핑이 스크램블되는 것을 의미한다.

[0086] 일 예에서, 그룹핑이나 패킷이 스크램블될 때, 10의 상수가 숫자 값에 더해지고 두 개의 숫자 캐릭터가 뒤집히고 되는 것을 의미하도록 정의된다. 메시지가 구분된 패킷(808)으로 분리되는 실시예에서, "1__8"의 메시지가 먼저 "1__18"으로 변환되고 이후에 "1__81"로 변환된다. 따라서, 23의 메시지 값이 "1___81"의 암호화된 값을 가진다.

[0087] 초과 스페이스가 메시지(810)를 나누는 그룹 사이에 배치되는 실시예에서, "1008"의 메시지가 먼저 "10018"이 되고, "10081"이 된다. 따라서, 23의 메시지 값이 10081의 암호화 값을 가진다.

[0088] 암호화 장치가 이후에 10081의 암호화된 값을 수신 장치(814)로 전송한다. 도 8b를 참조하면, 수신 장치가 이러한 암호화된 메시지(818)를 수신하고, 메시지의 내용을 먼저 디스크램블 할 수 있다(820). 수신 장치가 스크램블 된 각 그룹핑이나 패킷이 역으로 된 두 개의 숫자 캐릭터와 원래 메시지에 부가된 10의 값을 포함하고 있어야 한다는 것을 알고 있어야 한다. 추가로, 수신 장치가 제 4 소수가 17로 정의되며 비밀 계수가 15로 정의된다는 것을 인지하고 있어야 하며, 이에 따라 상술한 바와 같이, 스크램블 패턴의 값이 2가 되는 것을 수신 장치가 정확히 산출할 수 있다.

[0089] 메시지가 구분된 패킷(822)으로 나뉘는 실시예에서, "1__81"의 메시지가 먼저 "1__18"로 변경된 후, "1__8"로 변경된다(820). 초과 스페이스가, 메시지를 나누는 복수의 그룹 사이에 배치되는(824) 실시예에서, "10081"의 메시지가 "10018"로 먼저 변경되고, 이후에 "1008"로 변경된다(820).

[0090] 디스크램블 단계(820) 후에, 수신 장치가 메시지를 다시 일체화된 메시지로 배치한다(826). 수신 장치가 1의 스페이스 패턴을 정확히 계산하도록 수신 장치는 제 3 소수가 31로 정의되고 공개 계수가 10으로 정의된다는 사실을 인지하며, 하나의 스페이스 또는 "00"이 메시지 내용의 그룹핑이나 패킷 사이에 삽입된다는 것을 인지한다.

[0091] 메시지가 구분된 패킷으로 분리되는(822) 실시예에서, "1__8"의 메시지가 "18"로 변경된다. 나아가, 메시지(824)를 분리하도록 초과 스페이스가 복수의 그룹 사이에 배치되는 실시예에서, "1008"의 메시지가 "18"로 변경된다.

[0092] 마지막으로, 수신 장치가 메시지의 내용을 제 2 폼(M')에서 제 1 폼(M)으로 변경하도록 변환 단계(830)를 수행한다. 제 1 비밀 소수가 5의 값을 가지도록 정의되고, 제 2 비밀 소수가 7의 값을 가지도록 정의되며, 공개 암호 키(E)가 29의 값을 가지도록 정의된다는 것을 수신 장치가 인식하여야 한다. 이러한 값을 사용하여, 수신 장치가 비밀 해역 키(D)를 다음의 식에 따라 상술한 바와 같이 계산한다(828).

$$D * E = 1 * \mathrm{mod}((P-1)*(Q-1))$$

[0093] $$D * 29 = 1 * \mathrm{mod}(4*6),$$

[0094] 결과적으로 5의 값이 된다. 비밀 해역 키(D)를 이용하여, 다음 식에 따라, 수신 장치가 제 2 폼(M')에서 제 1 폼(M)으로 메시지를 변환한다(830).

$$M = (M')^{D} * \mathrm{mod}(P*Q)$$

[0095] $$M = (18)^{5} * \mathrm{mod}(7*5).$$

[0096] 3 단계 암호화 프로세스가 수행되기 전의 제 1 폼의 메시지의 값과 동일한, 23의 제 1 폼(M)을 가지는 메시지

값에서 위 식의 결과가 830이 된다.

[0097] 3 단계 암호화 기술이나 3 단계 해역 기술을 구현하는 장치가 추가 구문을 3 단계 암호화 기술이나 3 단계 해역 기술에 포함할 수도 있다. 예를 들어, 도 9에 도시된 바와 같이, 일 실시예에서, 도 8a의 3 단계 해역 기술을 구현하는 장치가 복수의 패킷이나 복수의 그룹의 순서를 스크램블 하는 제 4 구문(916)을 수행할 수 있다. 따라서, 새로운 구문이 정확히 역으로 될 수 없을 정도로, 새로운 구문이 데이터를 왜곡하지 않는 한, 추가 단계가 3 단계 암호화 기술이나 3단계 해역 기술에 부가된다.

[0098] 첨부된 실시예들에 대해 다양한 변경을 할 수 있음은 당업자에게 자명하며, 여기에 정의된 일반적인 개념들이 본 발명의 사상 및 범위를 벗어나지 않는 한, 다른 실시예들 및 응용 예들에 적용될 수 있다. 따라서, 본 발명은 이하의 실시예들에 한정되는 것이 아니며, 본 발명의 범위는 첨부된 청구항 및 이의 등가물에 의해서 정의된다.

도면의 간단한 설명

[0005] 도 1은 본 발명의 일 실시예에 따른 3 단계 암호화 및 해역 기술을 나타내는 흐름도이다.

[0006] 도 2는 3 단계 암호화 기술의 변환 단계에 대한 하나의 실시예를 나타내는 흐름도이다.

[0007] 도 3a는 3 단계 암호화 기술의 분리 단계에 대한 하나의 실시예를 나타내는 흐름도이다.

[0008] 도 3b는 도 3a에 도시된 3 단계 암호화 기술의 일 실시예의 스크램블(scrambilization) 단계를 나타내는 흐름도이다.

[0009] 도 4a는 3 단계 암호화 기술의 분리 단계에 대한 다른 실시예를 나타내는 흐름도이다.

[0010] 도 4b는 도 4a에 도시된 3 단계 암호화기술의 일 실시예 스크램블 단계를 나타내는 흐름도이다.

[0011] 도 5는 도 3a 및 3b에 도시된 3 단계 암호화 기술의 일 실시예의 3 단계 해역 기술을 나타내는 흐름도이다.

[0012] 도 6은 도 4a 및 4b에 도시된 3 단계 암호화 기술의 일 실시예에 대한 3 단계 해역 기술을 나타내는 흐름도이다.

[0013] 도 7은 암호화 모듈의 일 실시예와 해역 모듈의 일 실시예를 나타내는 블럭도이다.

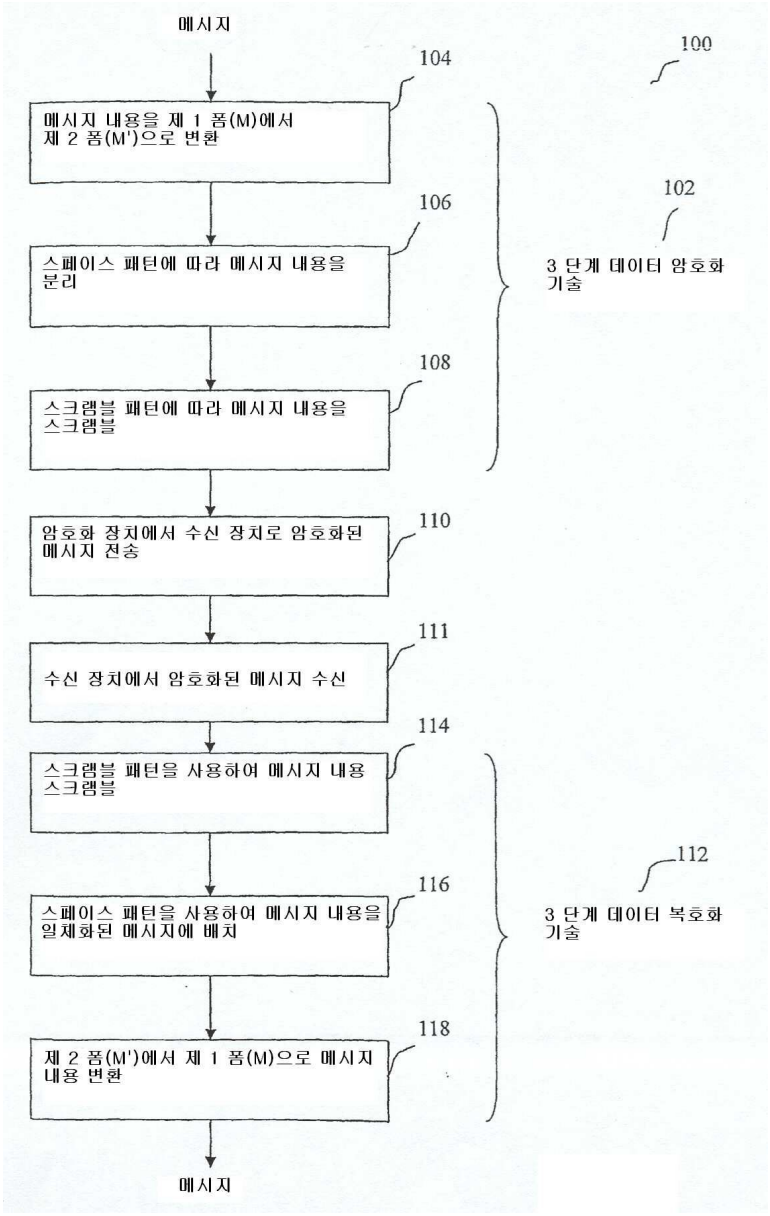
[0014] 도 8a은 3 단계 암호화 기술의 일 실시예를 나타내는 흐름도이다.

[0015] 도 8b는 도 8a에 도시된 3 단계 해역 기술의 일 실시예를 나타내는 흐름도이다.

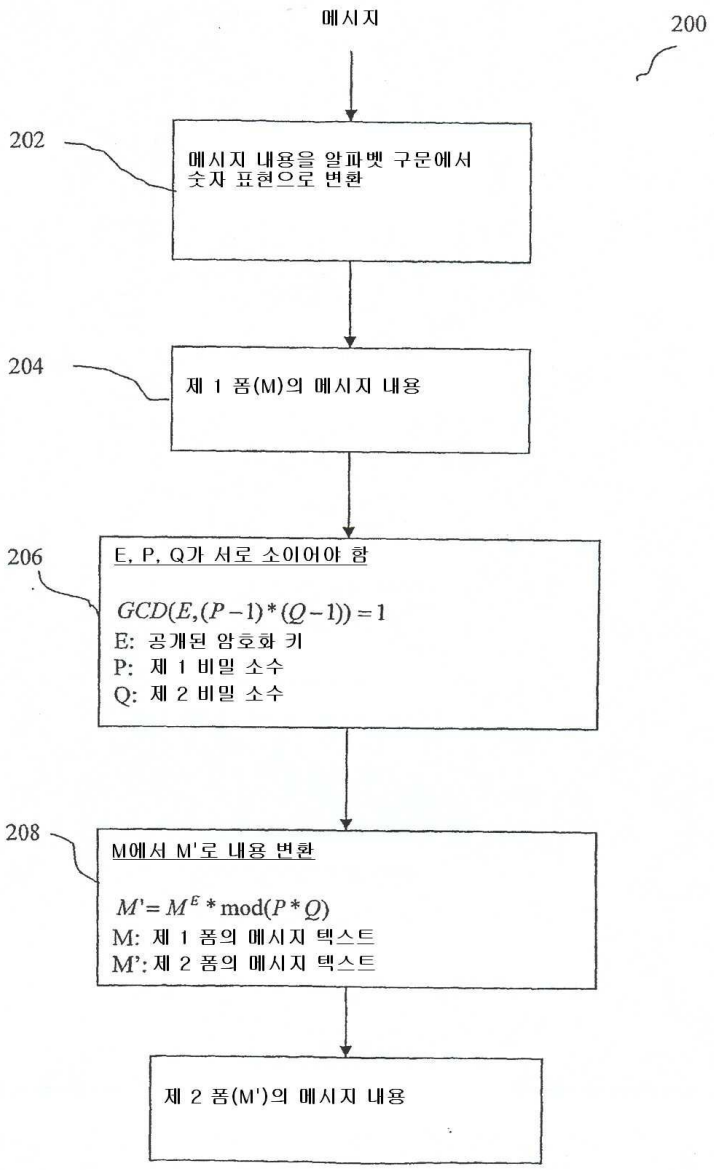
[0016] 도 9는 추가적인 제 4 단계를 가지는 3 단계 암호화 기술의 일 실시예를 나타내는 흐름도이다.

도면

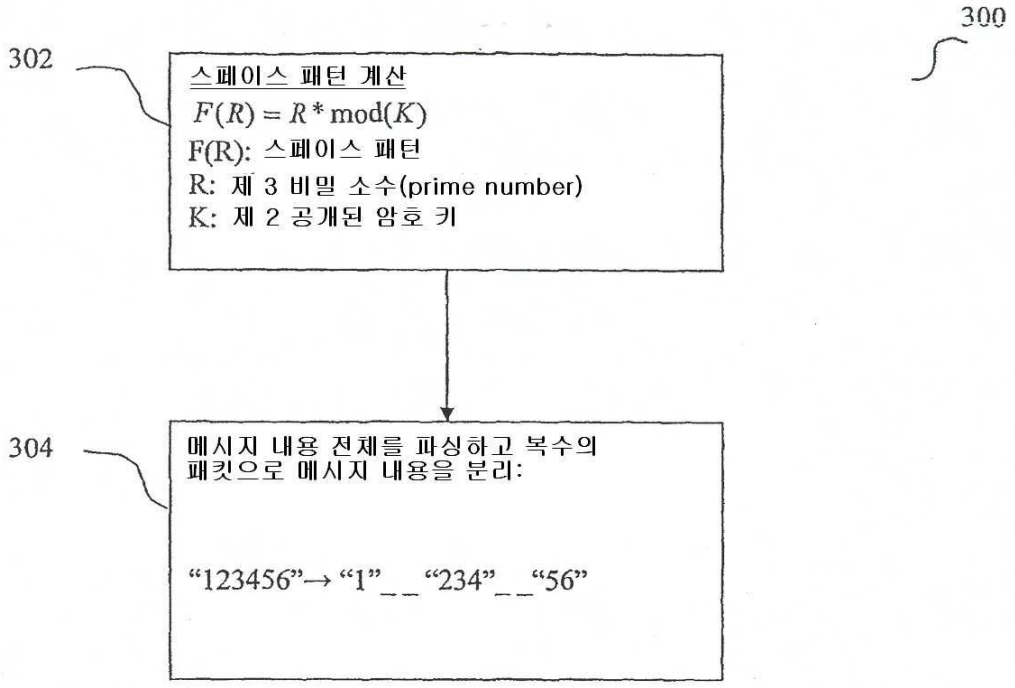
도면1


메시지
104
메시지 내용을 제 1 폼(M)에서 제 2 폼(M')으로 변환
106
스페이스 패턴에 따라 메시지 내용을 분리
108
스크램블 패턴에 따라 메시지 내용을 스크램블
110
암호화 장치에서 수신 장치로 암호화된 메시지 전송
111
수신 장치에서 암호화된 메시지 수신
114
스크램블 패턴을 사용하여 메시지 내용 스크램블
116
스페이스 패턴을 사용하여 메시지 내용을 일체화된 메시지에 배치
118
제 2 폼(M')에서 제 1 폼(M)으로 메시지 내용 변환
메시지
100
102
3 단계 데이터 암호화 기술
112
3 단계 데이터 복호화 기술

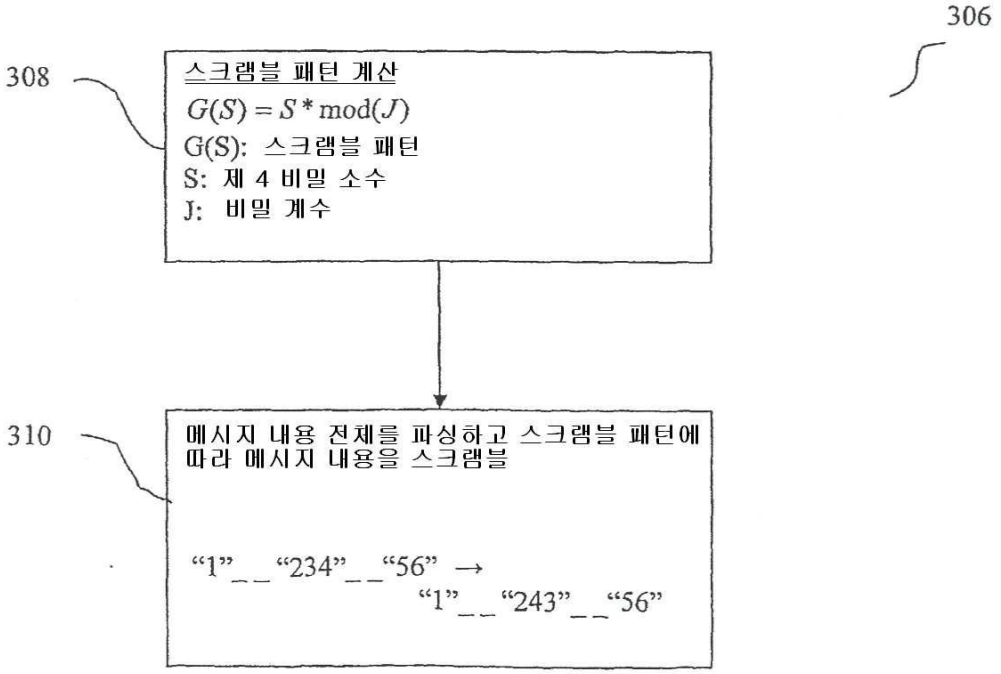
도면2


메시지
200
202
메시지 내용을 알파벳 구문에서
숫자 표현으로 변환
204
제 1 폼(M)의 메시지 내용
206
E, P, Q가 서로 소이어야 함
$GCD(E,(P-1)*(Q-1))=1$
E: 공개된 암호화 키
P: 제 1 비밀 소수
Q: 제 2 비밀 소수
208
M에서 M'로 내용 변환
$M'=M^E * \mathrm{mod}(P*Q)$
M: 제 1 폼의 메시지 텍스트
M': 제 2 폼의 메시지 텍스트
제 2 폼(M')의 메시지 내용

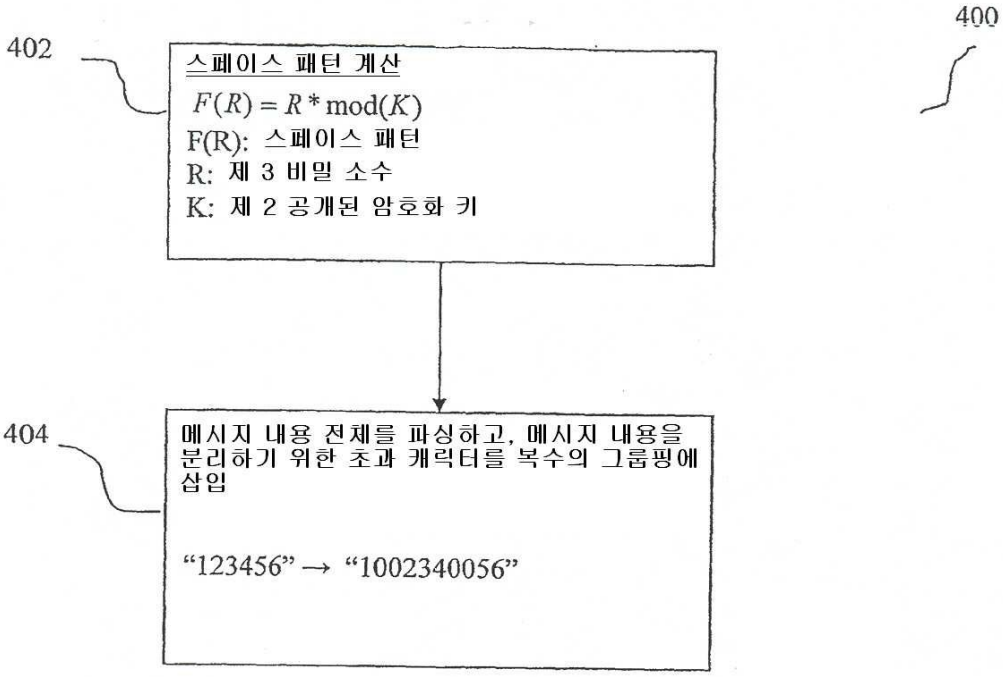
도면3a


300
302
스페이스 패턴 계산
$F(R) = R * \mathrm{mod}(K)$
F(R): 스페이스 패턴
R: 제 3 비밀 소수(prime number)
K: 제 2 공개된 암호 키
304
메시지 내용 전체를 파싱하고 복수의 패킷으로 메시지 내용을 분리:
"123456"→ "1"__"234"__"56"

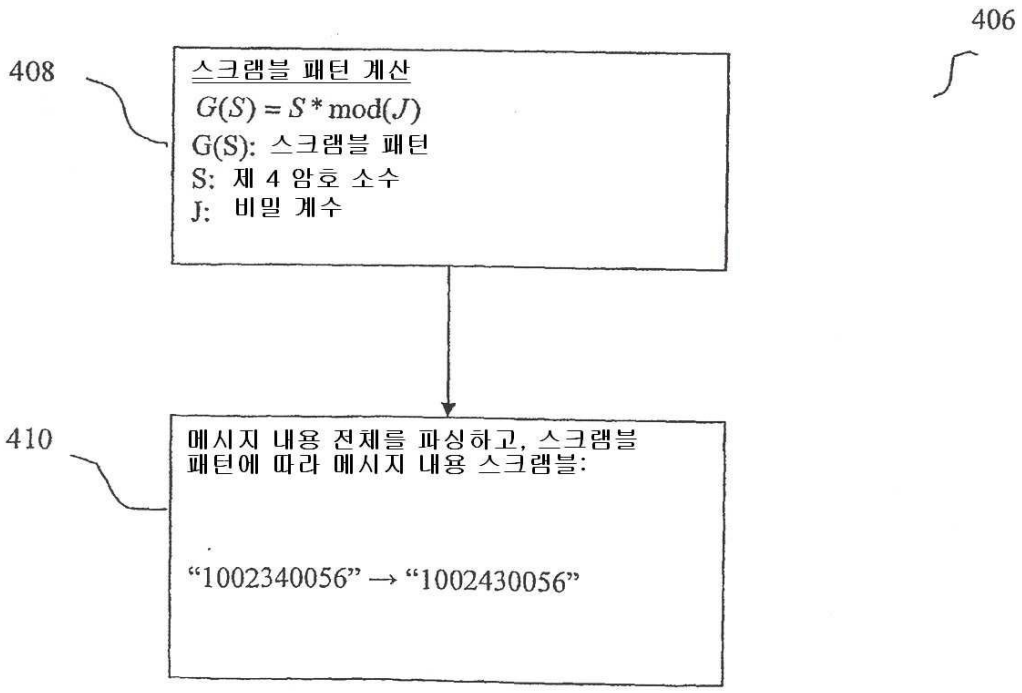
도면3b


306
308
스크램블 패턴 계산
$G(S) = S * \mathrm{mod}(J)$
G(S): 스크램블 패턴
S: 제 4 비밀 소수
J: 비밀 계수
310
메시지 내용 전체를 파싱하고 스크램블 패턴에 따라 메시지 내용을 스크램블
"1"__"234"__"56" →
"1"__"243"__"56"

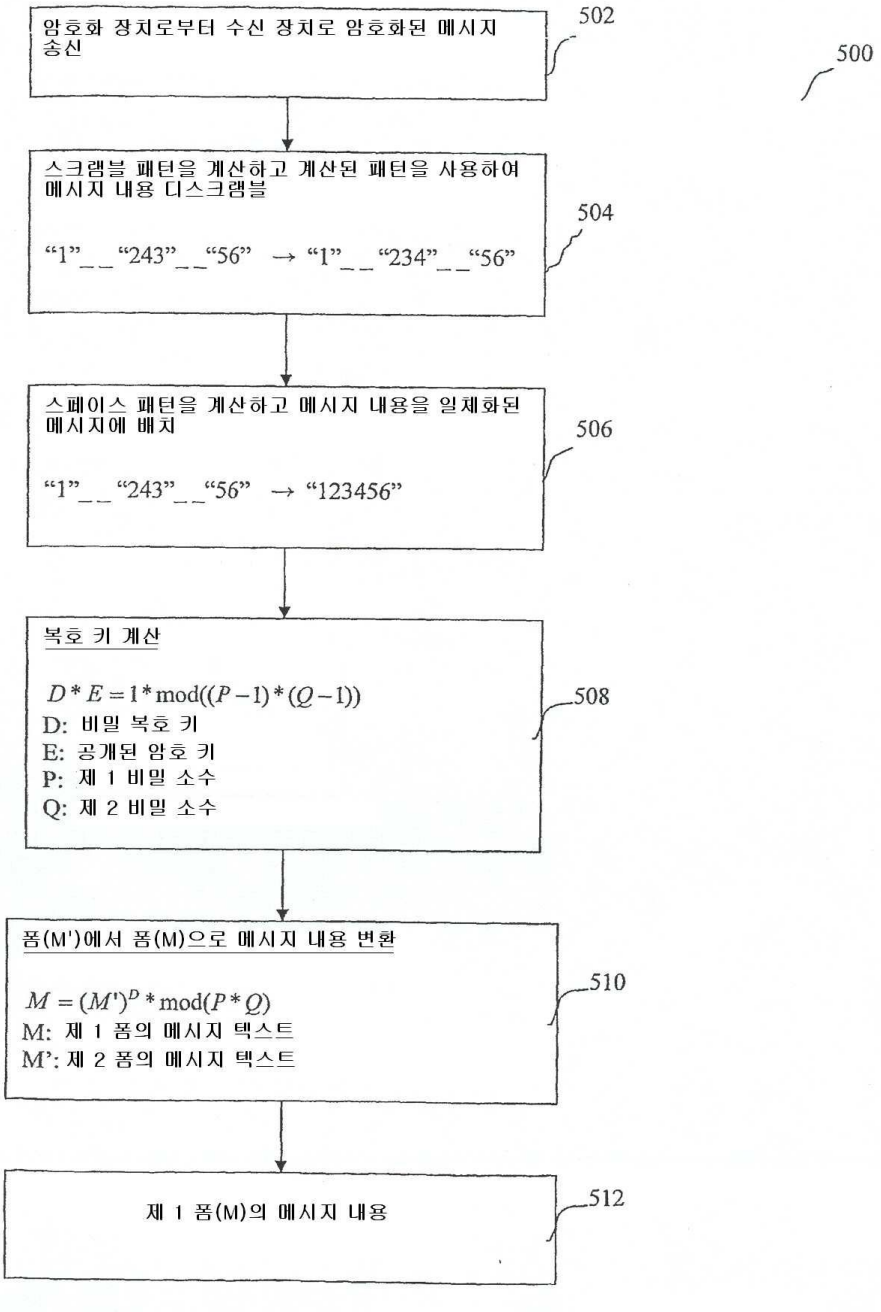
도면4a


400
402
스페이스 패턴 계산
$F(R) = R * \mathrm{mod}(K)$
F(R): 스페이스 패턴
R: 제 3 비밀 소수
K: 제 2 공개된 암호화 키
404
메시지 내용 전체를 파싱하고, 메시지 내용을 분리하기 위한 초과 캐릭터를 복수의 그룹핑에 삽입
"123456" → "1002340056"

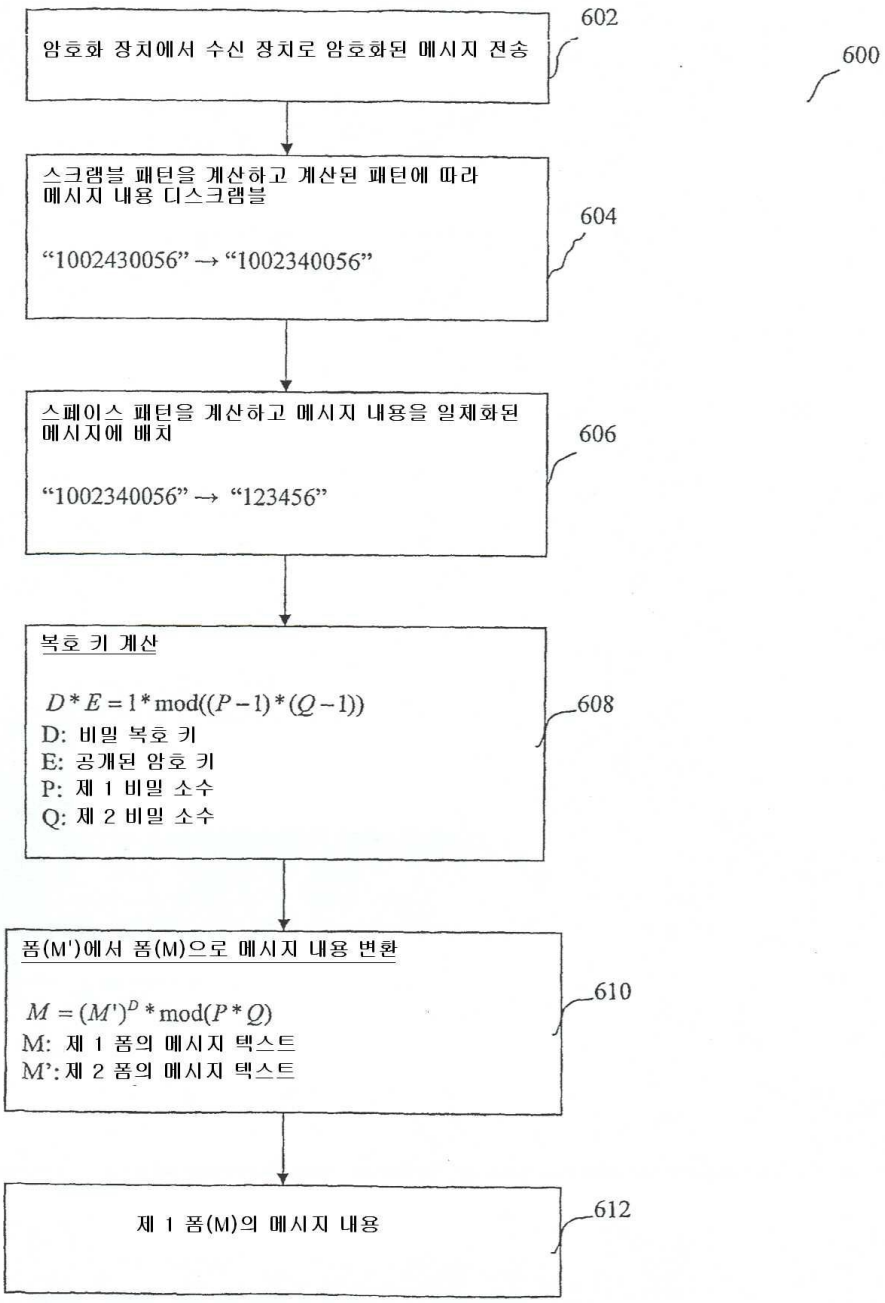
도면4b


406
408
스크램블 패턴 계산
$G(S) = S * \mathrm{mod}(J)$
G(S): 스크램블 패턴
S: 제 4 암호 소수
J: 비밀 계수
410
메시지 내용 전체를 파싱하고, 스크램블 패턴에 따라 메시지 내용 스크램블:
"1002340056" → "1002430056"

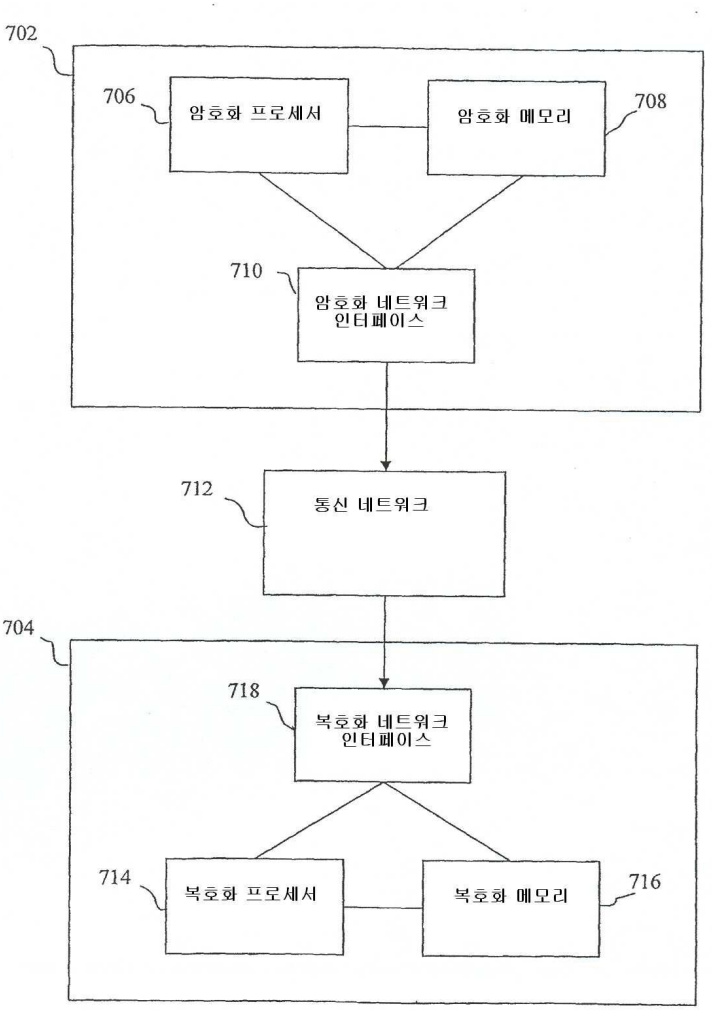
도면5


암호화 장치로부터 수신 장치로 암호화된 메시지 송신
502
500
스크램블 패턴을 계산하고 계산된 패턴을 사용하여 메시지 내용 디스크램블
"1"__"243"__"56" → "1"__"234"__"56"
504
스페이스 패턴을 계산하고 메시지 내용을 일체화된 메시지에 배치
"1"__"243"__"56" → "123456"
506
복호 키 계산
$D * E = 1 * \mathrm{mod}((P-1)*(Q-1))$
D: 비밀 복호 키
E: 공개된 암호 키
P: 제 1 비밀 소수
Q: 제 2 비밀 소수
508
폼(M')에서 폼(M)으로 메시지 내용 변환
$M = (M')^{D} * \mathrm{mod}(P * Q)$
M: 제 1 폼의 메시지 텍스트
M': 제 2 폼의 메시지 텍스트
510
제 1 폼(M)의 메시지 내용
512

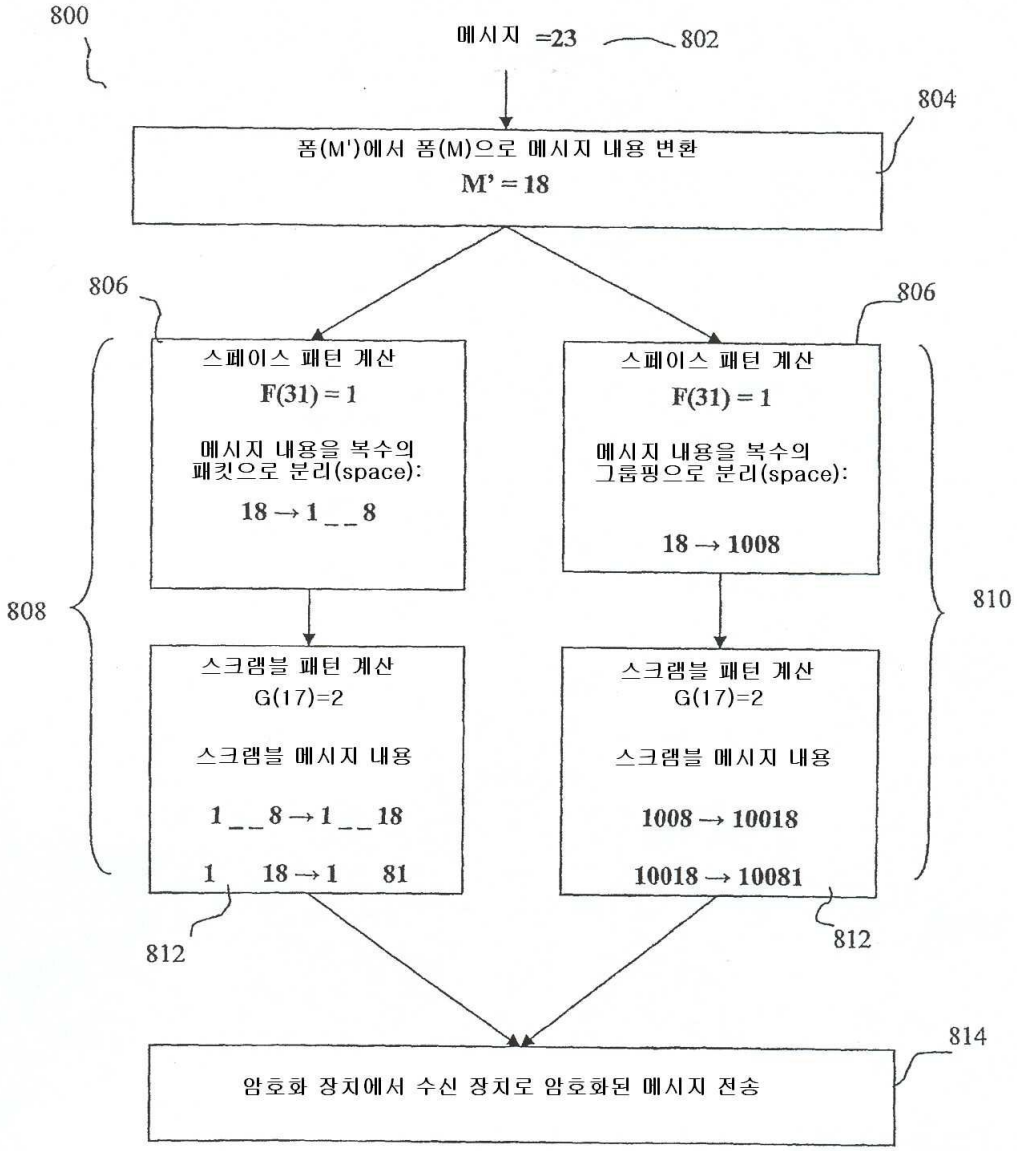
도면6


600
602
암호화 장치에서 수신 장치로 암호화된 메시지 전송
604
스크램블 패턴을 계산하고 계산된 패턴에 따라 메시지 내용 디스크램블
"1002430056" → "1002340056"
606
스페이스 패턴을 계산하고 메시지 내용을 일체화된 메시지에 배치
"1002340056" → "123456"
608
복호 키 계산
$D*E=1*\mathrm{mod}((P-1)*(Q-1))$
D: 비밀 복호 키
E: 공개된 암호 키
P: 제 1 비밀 소수
Q: 제 2 비밀 소수
610
폼(M')에서 폼(M)으로 메시지 내용 변환
$M=(M')^{D}*\mathrm{mod}(P*Q)$
M: 제 1 폼의 메시지 텍스트
M': 제 2 폼의 메시지 텍스트
612
제 1 폼(M)의 메시지 내용

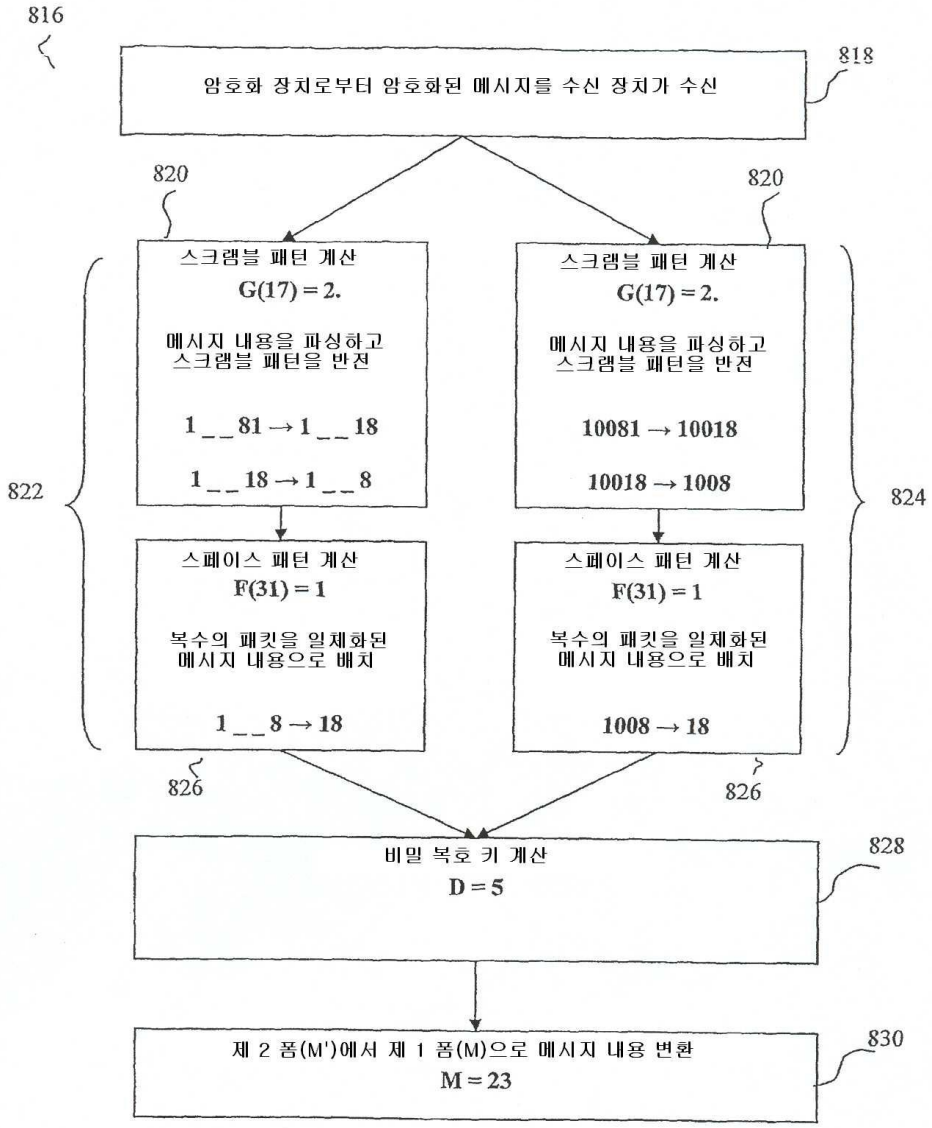
도면7


702
706
암호화 프로세서
암호화 메모리
708
710
암호화 네트워크 인터페이스
712
통신 네트워크
704
718
복호화 네트워크 인터페이스
714
복호화 프로세서
복호화 메모리
716

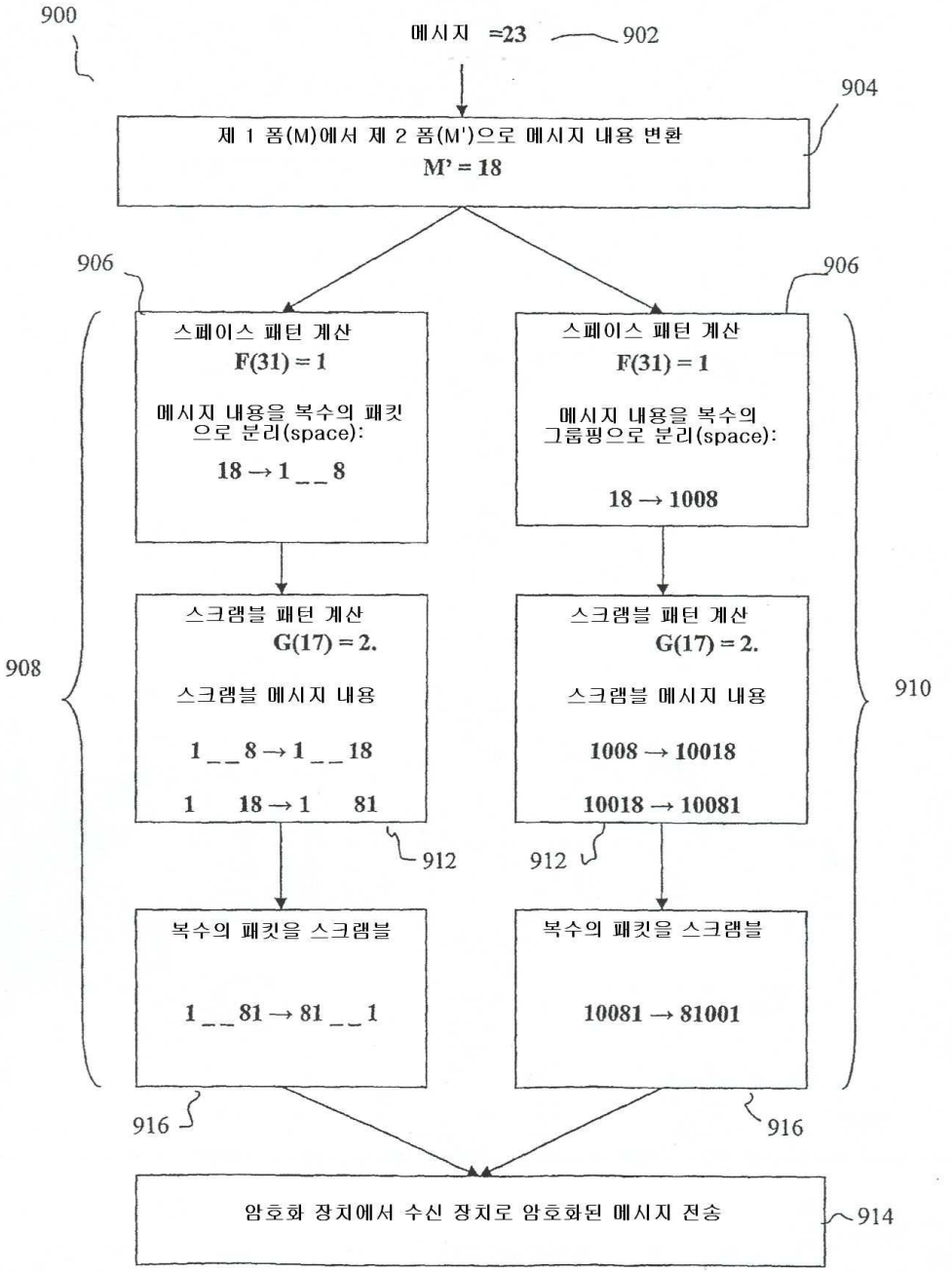
도면8a


800
메시지 =23
802
804
폼(M')에서 폼(M)으로 메시지 내용 변환
M' = 18
806
806
스페이스 패턴 계산
F(31) = 1
메시지 내용을 복수의 패킷으로 분리(space):
18 → 1 _ _ 8
스페이스 패턴 계산
F(31) = 1
메시지 내용을 복수의 그룹핑으로 분리(space):
18 → 1008
808
810
스크램블 패턴 계산
G(17)=2
스크램블 메시지 내용
1 _ _ 8 → 1 _ _ 18
1 18 → 1 81
스크램블 패턴 계산
G(17)=2
스크램블 메시지 내용
1008 → 10018
10018 → 10081
812
812
814
암호화 장치에서 수신 장치로 암호화된 메시지 전송

도면8b


816
암호화 장치로부터 암호화된 메시지를 수신 장치가 수신
818
820
820
스크램블 패턴 계산
G(17) = 2.
메시지 내용을 파싱하고
스크램블 패턴을 반전
1 _ _ 81 → 1 _ _ 18
1 _ _ 18 → 1 _ _ 8
스크램블 패턴 계산
G(17) = 2.
메시지 내용을 파싱하고
스크램블 패턴을 반전
10081 → 10018
10018 → 1008
822
824
스페이스 패턴 계산
F(31) = 1
복수의 패킷을 일체화된
메시지 내용으로 배치
1 _ _ 8 → 18
스페이스 패턴 계산
F(31) = 1
복수의 패킷을 일체화된
메시지 내용으로 배치
1008 → 18
826
826
비밀 복호 키 계산
D = 5
828
제 2 폼(M')에서 제 1 폼(M)으로 메시지 내용 변환
M = 23
830

도면9


900
메시지 =23
902
904
제 1 폼(M)에서 제 2 폼(M')으로 메시지 내용 변환
M' = 18
906
906
스페이스 패턴 계산
F(31) = 1
메시지 내용을 복수의 패킷으로 분리(space):
18 → 1 _ _ 8
스페이스 패턴 계산
F(31) = 1
메시지 내용을 복수의 그룹핑으로 분리(space):
18 → 1008
908
910
스크램블 패턴 계산
G(17) = 2.
스크램블 메시지 내용
1 _ _ 8 → 1 _ _ 18
1 18 → 1 81
스크램블 패턴 계산
G(17) = 2.
스크램블 메시지 내용
1008 → 10018
10018 → 10081
912
912
복수의 패킷을 스크램블
1 _ _ 81 → 81 _ _ 1
복수의 패킷을 스크램블
10081 → 81001
916
916
암호화 장치에서 수신 장치로 암호화된 메시지 전송
914