(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년01월02일
(11) 등록번호 10-0790511
(24) 등록일자 2007년12월24일

(51) Int. Cl.
H04L 12/22 (2006.01) *H04L 9/32* (2006.01)
H04L 12/28 (2006.01)
(21) 출원번호 10-2006-0108584
(22) 출원일자 2006년11월03일
심사청구일자 2006년11월03일
(56) 선행기술조사문헌
KR100200531 B1
(뒷면에 계속)
전체 청구항 수 : 총 14 항

(73) 특허권자
김경원
서울 노원구 월계1동 447-14
(72) 발명자
김경원
서울 노원구 월계1동 447-14
(74) 대리인
서동헌, 윤창일, 이동욱, 허성원

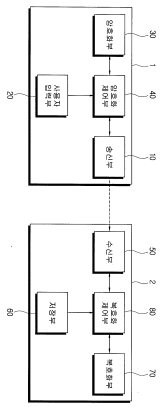
심사관 : 양찬호

(54) 암호화 및 복호화 시스템과 암호화 및 복호화 방법

(57) 요 약

본 발명은 암호화 및 복호화 방법에 있어서, 복수의 변수 및 상기 각 변수의 사칙연산에 의한 함수를 복수 개 설정하는 단계와; 상기 설정된 변수의 초기값 및 연산의 반복값을 설정하는 단계와; 상기 초기값 및 상기 반복값에 기초한 상기 함수의 결과값을 설정하여 암호화 하는 단계와; 정보 송신자가 상기 암호화된 암호정보를 정보 수신자에게 송신하는 단계와; 상기 정보 수신자는 수신된 암호정보를 상기 초기값, 상기 반복값에 기초한 상기 연속방정식에 따라 복호화 하는 단계를 더 포함하는 것을 특징으로 한다. 이에 의하여, 암호화를 해제하기 위한 공격으로부터 시스템을 안전하게 보호할 수 있다.

대표도 - 도1



(56) 선행기술조사문헌
KR1020040083794 A
KR1019980033368 A
KR1020030000720 A
KR1020030028747 A
KR1020030067934 A
KR1020020075472 A

특허청구의 범위

청구항 1

암호화 및 복호화 시스템에 있어서,

정보 송신자로부터 입력된 입력정보에 따라 초기값 및 연산의 반복값을 설정하고, 복수 개 변수의 사칙연산에 의해 이루어지는 복수 개의 기설정된 함수에 따라 상기 초기값 및 상기 반복값과, 상기 함수에 포함된 계수와 상기 초기값 및 상기 반복값 중 적어도 어느 하나가 변형된 헤더에 기초한 암호정보를 생성하여 정보 수신자에게 송신하는 암호화 장치와,

상기 수신된 암호정보를 상기 함수에 대응하는 복호정보에 기초하여 복호화를 수행하고, 상기 복호화에 의한 상기 입력정보를 추출하는 복호화 장치를 포함하는 것을 특징으로 하는 암호화 및 복호화 시스템.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 복호화 장치는 상기 수신된 암호정보가 상기 복호정보에 의한 결과값의 소정범위에 속하는지 판단하여 복호화 하는 것을 특징으로 하는 암호화 및 복호화 시스템.

청구항 4

제1항에 있어서,

상기 암호화 장치는 상기 반복값에 의한 반복과정에서 임의의 결과값을 추출하여, 상기 추출된 결과값에 기초하여 암호정보를 생성하는 것을 특징으로 하는 암호화 및 복호화 시스템.

청구항 5

암호화 장치에 있어서,

사용자입력부와;

소정의 암호정보를 송신하는 송신부와;

상기 사용자입력부로부터 입력된 입력정보에 따라 암호화를 수행하는 암호화부와;

정보 송신자로부터 상기 사용자입력부를 통해 입력된 정보에 따라 초기값 및 연산의 반복값을 설정하고, 복수의 변수 및 상기 각 변수의 사칙연산에 의해 기설정된 복수 개의 함수에 대한 상기 초기값 및 상기 반복값과, 상기 함수에 포함된 계수와 상기 초기값 및 상기 반복값 중 적어도 어느 하나가 변형된 헤더에 기초하여에 기초하여 암호정보를 생성하도록 상기 암호화부를 제어하고, 상기 암호화된 암호정보를 상기 송신부를 통해 정보 수신자에게 송신하는 제어부를 포함하는 것을 특징으로 하는 암호화 장치.

청구항 6

삭제

청구항 7

제5항에 있어서,

상기 제어부는 상기 반복값에 의한 반복과정에서 임의의 결과값을 추출하여, 상기 추출된 결과값에 기초하여 암호정보를 생성하도록 상기 암호화부를 제어하는 것을 특징으로 하는 암호화 장치.

청구항 8

복호화 장치에 있어서,

소정의 암호정보를 수신하는 수신부와;

복수의 변수 및 상기 각 변수의 사칙연산에 의해 기설정된 복수 개의 함수와, 상기 초기값 및 상기 반복값과, 상기 함수에 포함된 계수와 상기 초기값 및 상기 반복값 중 적어도 어느 하나가 변형된 헤더에 기초하여 생성된 암호정보에 대응하는 복호정보를 저장하는 저장부와,

상기 수신된 암호정보에 대해 복호화를 수행하는 복호화부와;

상기 수신된 암호정보를 상기 복호정보에 기초하여 복호화를 수행하도록 상기 복호화부를 제어하고, 상기 복호화에 의해 상기 입력정보를 추출하는 제어부를 포함하는 것을 특징으로 하는 복호화 장치.

청구항 9

제8항에 있어서,

상기 제어부는 상기 수신된 암호정보가 상기 복호정보에 의한 결과값의 소정범위에 속하는지 판단하여 복호화하는 것을 특징으로 하는 복호화 장치.

청구항 10

암호화 및 복호화 방법에 있어서,

복수의 변수 및 상기 각 변수의 사칙연산에 의한 함수를 복수 개 설정하는 단계와;

상기 설정된 변수의 초기값 및 연산의 반복값을 설정하는 단계와;

상기 초기값 및 상기 반복값과, 상기 함수에 포함된 계수와 상기 초기값 및 상기 반복값 중 적어도 어느 하나가 변형된 헤더에 기초하여 암호화 하는 단계와;

정보 송신자가 상기 암호화된 암호정보를 정보 수신자에게 송신하는 단계와;

상기 정보 수신자는 수신된 암호정보를 상기 초기값 및 상기 반복값과, 상기 헤더에 기초한 상기 연속방정식에 따라 복호화 하는 단계를 더 포함하는 것을 특징으로 하는 암호화 및 복호화 방법.

청구항 11

삭제

청구항 12

제10항에 있어서,

상기 암호화 하는 단계는 상기 반복값에 의한 반복과정에서 임의의 결과값을 추출하여, 상기 추출된 결과값에 기초하여 암호화 하는 것을 특징으로 하는 암호화 및 복호화 방법.

청구항 13

제10항에 있어서,

상기 복호화 하는 단계는, 상기 수신된 암호정보가 상기 복호정보에 의한 결과값의 소정범위에 속하는지 판단하여 복호화하는 것을 특징으로 하는 암호화 및 복호화 방법.

청구항 14

암호화 및 복호화 시스템에 있어서,

정보 송신자로부터 입력된 입력정보에 따라 초기값 및 연산의 반복값을 설정하고, 복수 개 변수의 사칙연산에 의해 이루어지는 복수 개의 기설정된 함수에 따라 상기 초기값 및 상기 반복값과, 상기 반복값에 의한 반복과정에서 추출된 임의의 결과값에 기초하여 암호정보를 생성하여 정보 수신자에게 송신하는 암호화 장치와,

상기 수신된 암호정보를 상기 함수에 대응하는 복호정보에 기초하여 복호화를 수행하고, 상기 복호화에 의한 상기 입력정보를 추출하는 복호화 장치를 포함하는 것을 특징으로 하는 암호화 및 복호화 시스템.

청구항 15

암호화 장치에 있어서,

사용자입력부와;

소정의 암호정보를 송신하는 송신부와;

상기 사용자입력부로부터 입력된 입력정보에 따라 암호화를 수행하는 암호화부와;

정보 송신자로부터 상기 사용자입력부를 통해 입력된 정보에 따라 초기값 및 연산의 반복값을 설정하고, 복수의 변수 및 상기 각 변수의 사칙연산에 의해 기설정된 복수 개의 함수에 대한 상기 초기값 및 상기 반복값과, 상기 반복값에 의한 반복과정에서 추출된 임의의 결과값에 기초하여 암호정보를 생성하도록 상기 암호화부를 제어하고, 상기 암호화된 암호정보를 상기 송신부를 통해 정보 수신자에게 송신하는 제어부를 포함하는 것을 특징으로 하는 암호화 장치.

청구항 16

복호화 장치에 있어서,

소정의 암호정보를 수신하는 수신부와;

복수의 변수 및 상기 각 변수의 사칙연산에 의해 기설정된 복수 개의 함수와, 상기 초기값 및 상기 반복값과, 상기 반복값에 의한 반복과정에서 추출된 임의의 결과값에 기초하여 생성된 암호정보에 대응하는 복호정보를 저장하는 저장부와;

상기 수신된 암호정보에 대해 복호화를 수행하는 복호화부와;

상기 수신된 암호정보를 상기 복호정보에 기초하여 복호화를 수행하도록 상기 복호화부를 제어하고, 상기 복호화에 의해 상기 입력정보를 추출하는 제어부를 포함하는 것을 특징으로 하는 복호화 장치.

청구항 17

암호화 및 복호화 방법에 있어서,

복수의 변수 및 상기 각 변수의 사칙연산에 의한 함수를 복수 개 설정하는 단계와;

상기 설정된 변수의 초기값 및 연산의 반복값을 설정하는 단계와;

상기 초기값 및 상기 반복값과, 상기 반복값에 의한 반복과정에서 추출된 임의의 결과값에 기초하여 암호화 하는 단계와;

정보 송신자가 상기 암호화된 암호정보를 정보 수신자에게 송신하는 단계와;

상기 정보 수신자는 수신된 암호정보를 상기 초기값 및 상기 반복값과, 상기 반복값에 의한 반복과정에서 추출된 임의의 결과값에 기초한 상기 연속방정식에 따라 복호화 하는 단계를 더 포함하는 것을 특징으로 하는 암호화 및 복호화 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<8> 본 발명은 암호화 및 복호화 방법과 암호화 및 복호화 시스템에 관한 것이다. 보다 상세하게는 함수를 이용한 암호화 및 복호화 방법과 암호화 및 복호화 시스템에 관한 것이다.

<9> 소정의 정보를 원거리에서 송수신하는 네트워크 시스템에서는 일정한 권한을 가진 자 이외에는 송수신되는 정보를 확인할 수 없도록 하기 위해 암호화 및 복호화 방법을 이용한다. 네트워크 시스템이 발달되고 보편화되면서 이러한 암호화 및 복호화 방법은 그 중요성이 날로 부각되고 있다.

<10> 그런데, 정보의 수집을 위해 암호화된 네트워크 시스템을 공격하는 공격자는 암호화 장치에서 복호화 장치로 전송되는 패킷을 가로채고 가로챈 패킷을 분석함으로써, 암호화 알고리즘을 파악하기 위해 노력한다. 그리하여 암호화 및 복호화 방법을 사용하는 정보 송수신자는 공격자가 전송되는 패킷에 포함된 정보를 손쉽게 확인할 수 없도록 여러 가지 복잡한 알고리즘을 연구하고 이용하게 된다.

<11> 암호화 및 복호화를 위한 알고리즘 중에서, 방정식을 설정하고 정보 송신자가 입력한 정보를 방정식에 대입한 결과값을 정보 수신자에게 전송하여, 정보 수신자가 가지는 함수를 통해 복호화를 수행하는 암호화 및 복호화 방법이 있다. 함수를 이용한 알고리즘은 초기값에 따른 결과값이 명확히 존재하므로 보편화 되었다.

<12> 그런데, 이러한 알고리즘은 단순히 함수를 구성하는 방정식의 차수를 높게 설정한다고 하여도 공격자는 단순한 연산을 여러 번 반복 수행함으로써 알고리즘을 용이하게 파악할 수 있다. 예를 들어, 함수를 구성하는 방정식의 차수와 연립방정식에서의 변수의 개수가 유한한 이상 방정식은 연산의 반복에 의해 쉽게 해가 구해지는 문제가 있다.

발명이 이루고자 하는 기술적 과제

<13> 따라서, 본 발명의 목적은, 함수에 의한 알고리즘을 이용하면서 암호화를 해제하기 위한 공격으로부터 시스템을 안전하게 보호할 수 있는 암호화 및 복호화 시스템과 암호화 및 복호화 방법을 제공하는 것이다.

발명의 구성 및 작용

<14> 상기 목적은, 암호화 및 복호화 시스템에 있어서, 정보 송신자로부터 입력된 입력정보에 따라 초기값 및 연산의 반복값을 설정하고, 복수 개 변수의 사칙연산에 의해 이루어지는 복수 개의 기설정된 함수에 따라 상기 초기값 및 상기 반복값에 기초한 암호정보를 생성하여 정보 수신자에게 송신하는 암호화 장치와, 상기 수신된 암호정보를 상기 함수에 대응하는 복호정보에 기초하여 복호화를 수행하고, 상기 복호화에 의한 상기 입력정보를 추출하는 복호화 장치를 포함하는 것을 특징으로 하는 암호화 및 복호화 시스템에 의해서도 상기 목적은 달성된다.

<15> 그리고, 상기 암호정보는, 상기 상기 함수에 포함된 계수와, 상기 초기값, 상기 반복값 중 적어도 어느 하나가 변형된 헤더를 포함하는 것이 바람직하다.

<16> 또한, 상기 암호화 장치는 상기 반복값에 의한 반복과정에서 임의의 결과값을 추출하여, 상기 추출된 결과값에 기초하여 암호정보를 생성하는 것이 바람직하다.

<17> 그리고, 상기 복호화 장치는 상기 수신된 암호정보가 상기 복호정보에 의한 결과값의 소정범위에 속하는지 판단하여 복호화 하는 것이 바람직하다.

<18> 한편, 암호화 장치에 있어서, 사용자입력부와; 소정의 암호정보를 송신하는 송신부와; 상기 사용자입력부로부터 입력된 입력정보에 따라 암호화를 수행하는 암호화부와; 정보 송신자로부터 상기 사용자입력부를 통해 입력된 정보에 따라 초기값 및 연산의 반복값을 설정하고, 복수의 변수 및 상기 각 변수의 사칙연산에 의해 기설정된 복수 개의 함수에 대한 상기 초기값 및 상기 반복값에 기초하여 암호정보를 생성하도록 상기 암호화부를 제어하고, 상기 암호화된 암호정보를 상기 송신부를 통해 정보 수신자에게 송신하는 제어부를 포함하는 것을 특징으로 하는 암호화 장치에 의해서도 상기 목적은 달성된다.

<19> 여기서, 상기 암호정보는, 상기 함수에 포함된 계수와, 상기 초기값, 상기 반복값 중 적어도 어느 하나가 변형된 헤더를 포함하는 것이 바람직하다.

<20> 그리고, 상기 제어부는 상기 반복값에 의한 반복과정에서 임의의 결과값을 추출하여, 상기 추출된 결과값에 기초하여 암호정보를 생성하도록 상기 암호화부를 제어하는 것이 바람직하다.

<21> 한편, 복호화 장치에 있어서, 소정의 암호정보를 수신하는 수신부와; 복수의 변수 및 상기 각 변수의 사칙연산에 의해 기설정된 복수 개의 함수에 대응하는 복호정보를 저장하는 저장부와, 상기 수신된 암호정보에 따라 복호화를 수행하는 복호화부와; 상기 수신된 암호정보를 상기 복호정보에 기초하여 복호화를 수행하도록 상기 복호화부를 제어하고, 상기 복호화에 의해 상기 입력정보를 추출하는 제어부를 포함하는 것을 특징으로 하는 복호화 시스템에 의해서도 상기 목적은 달성된다.

<22> 여기서, 상기 제어부는 상기 수신된 암호정보가 상기 복호정보에 의한 결과값의 소정범위에 속하는지 판단하여 복호화 하는 것이 바람직하다.

<23> 한편, 암호화 및 복호화 방법에 있어서, 복수의 변수 및 상기 각 변수의 사칙연산에 의한 함수를 복수 개 설정

하는 단계와; 상기 설정된 변수의 초기값 및 연산의 반복값을 설정하는 단계와; 상기 초기값 및 상기 반복값에 기초한 상기 함수의 결과값을 설정하여 암호화 하는 단계와; 정보 송신자가 상기 암호화된 암호정보를 정보 수신자에게 송신하는 단계와; 상기 정보 수신자는 수신된 암호정보를 상기 초기값, 상기 반복값에 기초한 상기 연속방정식에 따라 복호화 하는 단계를 더 포함하는 것을 특징으로 하는 암호화 및 복호화 방법에 의해 달성된다.

<24> 여기서, 상기 암호정보는, 상기 함수에 포함된 계수와, 상기 초기값, 상기 반복값 중 적어도 어느 하나가 변형된 헤더를 포함하는 것이 바람직하다.

<25> 그리고, 상기 암호화 하는 단계는 상기 반복값에 의한 반복과정에서 임의의 결과값을 추출하여, 상기 추출된 결과값에 기초하여 암호화 하는 것이 바람직하다.

<26> 또한, 상기 복호화 하는 단계는, 상기 수신된 암호정보가 상기 복호정보에 의한 결과값의 소정범위에 속하는지 판단하여 복호화 하는 것이 바람직하다.

<27> 이하, 첨부된 도면을 참조하여 본 발명에 따른 암호화 및 복호화 시스템에 대해 상세히 설명한다.

<28> 도 1 본 발명에 따른 암호화 및 복호화 시스템의 구성을 도시한 도면이다. 도 1에 도시된 바와 같이, 본 발명에 따른 암호화 및 복호화 시스템은 암호화 장치(1)와, 복호화 장치(2)를 포함한다.

<29> 그리고, 암호화 장치(1)는 송신부(10)와, 사용자 입력부(20)와, 암호화부(30)와, 암호화 제어부(40)를 포함한다.

<30> 송신부(10)는 소정의 암호정보를 송신하며, 본 발명에 따른 송신부(10)는 유무선 프로토콜에 의해 암호정보를 송신할 수 있으며, 암호화 장치(1)와 복호화 장치(2)가 원거리에 있는 경우 ADSL, VDSL 등의 유선 통신망에 의하고, 근거리에 있는 경우 무선랜 (Wireless LAN), 블루투스 (Bluetooth) 등의 무선 통신망에 의하는 것이 바람직하다.

<31> 사용자입력부(20)는 암호화될 정보를 사용자로부터 입력받는다. 사용자입력부(20)를 통해 입력되는 정보는 사용자의 계좌번호, 비밀번호 등과 같이 타인에게 공개가 금지되어야 할 정보를 포함하는 것이 바람직하다. 본 발명에 따른 사용자입력부(20)는 암호화 장치(1)가 컴퓨터 시스템인 경우, 마우스 키보드 등으로 구현되며, 암호화 장치(1)가 휴대전화인 경우 휴대전화에 마련된 버튼 등으로 구현되는 것이 바람직하다.

<32> 암호화부(30)는 사용자입력부(20)로부터 입력된 입력정보에 따라 암호화를 수행한다. 본 발명에 따른 암호화부(30)는 사용자입력부(20)로부터 입력된 정보에 따라 암호정보를 생성하기 위한 소프트웨어로 구현되는 것이 바람직하다.

<33> 암호화 제어부(40)는 정보 송신자로부터 사용자입력부(20)를 통해 입력된 정보에 따라 초기값 및 연산의 반복값을 설정하고, 복수의 변수 및 각 변수의 사칙연산에 의해 기설정된 복수 개의 함수에 대한 상기 초기값 및 상기 반복값에 기초하여 암호정보를 생성하도록 암호화부(30)를 제어한다.

<34> 그리고, 암호화 제어부(40)는 암호화된 암호정보를 송신부(10)를 통해 정보 수신자에게 송신한다.

<35> 암호화 제어부(40)는 함수가 연속방정식으로 구현되는 경우, 아래의 수학식 1과 같이 복수의 변수 및 각 변수의 사칙연산에 의해 복수 개의 연속방정식을 설정한다.

<36> [수학식 1]

<37>
$$x(i+1)=x(i)+0.1(3(y(i)-x(i))$$
$$y(i+1)=y(i)+0.1(2x(i)-y(i)-x(i)z(i))$$
$$z(i+1)=z(i)+0.1(x(i)y(i)-5z(i))$$

<38> 암호화 제어부(40)는 정보 송신자로부터 사용자입력부(20)를 통해 입력된 입력정보에 따라 설정된 복수 개의 함수에 대해, 초기값 및 연산의 반복값을 설정한다. 그리하여, 암호화 제어부(40)는 설정된 초기값을 복수 개의 함수에 각각 대입하고, 대입한 결과값을 다시 복수 개의 함수에 대입하는 과정을 설정된 연산의 반복값만큼 수행한다. 암호화 제어부(40)는 이렇게 산출된 결과값에 따라 암호정보를 생성하여 송신부(10)를 통해 복호화 장치(2)로 송신한다.

<39> 한편, 암호화 제어부(40)는 연산의 반복값에 의한 반복과정에서 임의의 결과값을 추출하여, 추출된 결과값에 기초하여 암호정보를 생성하는 것도 가능하다. 예를 들어, 연산의 최종 반복값이 1,000,000인 경우에 대해 설명하면, 암호화 제어부(40)는 연산을 500,000번 반복한 후, 이에 대한 결과값과 반복한 회수에 대응하는 암호정보를

생성하여 송신부(10)를 통해 복호화 장치(2)로 송신한다. 이로써, 복호화 장치(2)는 수신된 암호정보에 기초하여 복호화를 수행함으로써, 하나의 함수에 의하는 경우에도 확장된 암호화 과정을 제공하는 것이 가능하다.

<40> 여기서, 정보 송신자가 송신한 암호정보는, 연속방정식의 계수와, 초기값과, 반복값 중 적어도 어느 하나가 변형된 헤더를 포함하는 것이 바람직하다. 즉, 일정한 규칙에 의해 정보 송신자와 정보 수신자가 연속방정식의 계수와, 초기값과, 반복값 등을 변경하고 이를 헤더에 포함시켜 암호정보를 송신함으로써, 공격자가 연속방정식을 통한 알고리즘을 파악한 경우에도 암호화를 해제하기 위한 공격으로부터 암호화 및 복호화 시스템을 보호하는 것이 가능하다.

<41> 이하, 본 발명에 따른 복호화 장치(2)에 대해 상세히 설명한다.

<42> 도 1에 도시된 바와 같이, 본 발명에 따른 복호화 장치(2)는 수신부(50)와, 저장부(60)와, 복호화부(70)와, 복호화 제어부(80)를 포함한다.

<43> 수신부(50)는 소정의 암호정보를 수신한다. 본 발명에 따른 수신부(50)는 암호화 장치(1)의 송신부(10)와 마찬가지로 유무선 프로토콜에 의해 암호정보를 송신할 수 있으며, 암호화 장치(1)와 복호화 장치(2)가 원거리에 있는 경우 ADSL, VDSL 등의 유선 통신망에 의하고, 근거리에 있는 경우 무선랜 (Wireless LAN), 블루투스(Bluetooth) 등의 무선 통신망에 의하는 것이 바람직하다.

<44> 저장부(60)는 복수의 변수 및 각 변수의 사칙연산에 의해 기설정된 복수 개의 연속방정식에 대응하는 복호정보를 저장한다. 저장부(60)는 다양한 형태의 메모리로 구현될 수 있으며, 후술할 복호화부(70) 내에 구비되는 것도 가능하다.

<45> 복호화부(70)는 수신부(50)를 통해 수신된 암호정보에 대해 복호화를 수행한다. 본 발명에 따른 복호화부(70)는 암호화부(30)가 가지는 알고리즘과 동일한 알고리즘에 의한 복호정보에 의해 복호화를 수행한다. 복호화부(70)는 소프트웨어로 구현되는 것이 바람직하다.

<46> 복호화 제어부(80)는 수신부(50)를 통해 수신된 암호정보에 대해 복호정보에 기초하여 복호화를 수행하도록 복호화부(70)를 제어하고, 복호화에 의해 사용자입력부(20)로부터 입력된 입력정보를 추출한다.

<47> 복호화 제어부(80)는 암호화 제어부(40)에 의해 설정된 복수 개의 연립방정식을 행렬에서의 역행렬 연산 등을 통해 사용자가 입력한 입력정보에 대응하는 초기값 및 연산의 반복값을 구하는 과정을 수행하도록 복호화부(70)를 제어한다. 그리하여, 암호화 장치(1)에서 사용자가 입력한 입력정보를 암호정보로부터 추출할 수 있다.

<48> 여기서, 복호화 제어부(80)는 수신된 암호정보가 복호정보에 의한 결과값의 소정범위에 속하는지 판단하여 복호화하는 것도 가능하다. 즉, 복호화 제어부(80)는 저장부(60)에 저장된 복호정보에 의한 연속방정식의 결과값과 수신부(50)에 의해 수신된 암호정보에 포함된 결과값이 다르다고 하더라도, 결과값의 소정범위에 속하는 경우 이를 결과값과 일치하는 암호정보로 인식하게 된다. 여기서, 소정범위란 최소 단위보다는 작아야 하며, 최소 단위는 일반적으로 정수인 것이 바람직하다. 이로써, 본 발명에 따른 암호화 및 복호화 방법을 보다 다양한 식에 적용할 수 있다.

<49> 이하, 도 2를 통해 본 발명에 따른 암호화 및 복호화 시스템에 대해 상세히 설명한다.

<50> 먼저, 암호화 장치(1)의 암호화 제어부(40)는 복수 개의 변수 및 상기 각 변수의 사칙연산에 의한 연속방정식을 복수 개 설정한다(S10). 그리고, 암호화 제어부(40)는 사용자입력부(20)를 통해 입력된 정보에 따라 복수 개의 연속방정식의 초기값 및 연산의 반복값을 설정한다(S20). 다음으로, 암호화 제어부(40)는 설정된 초기값 및 반복값에 기초한 연속방정식의 결과값을 설정하여 암호화한다(S30).

<51> 그리하여, 정보 송신자가 암호화된 암호정보를 정보 수신자에게 송신하면(S40), 복호화 장치(2)의 복호화 제어부(80)는 수신부(50)를 통해 수신된 암호정보를 복호정보에 의해 복호화하도록 복호화부(70)를 제어한다(S50).

<52> 여기서, 정보 송신자가 송신한 암호정보는, 연속방정식의 계수와, 초기값과, 반복값 중 적어도 어느 하나가 변형된 헤더를 포함하는 것이 바람직하다.

<53> 그리고, 암호화 제어부(40)는 단계 S30에서, 반복값에 의한 반복과정에서 임의의 결과값을 추출하여, 추출된 결과값에 기초하여 암호화 하도록 하는 것도 가능하다.

<54> 한편, 복호화 제어부(80)는 단계 S50에서, 수신된 암호정보가 복호정보에 의한 결과값의 소정범위에 속하는지 판단하여 복호화하도록 하는 것도 가능하다.

<55> 이상, 바람직한 실시예를 통하여 본 발명에 관하여 상세히 설명하였으나, 본 발명은 이에 한정되는 것은 아니며 특허청구범위 내에서 다양하게 실시될 수 있다.

발명의 효과

<56> 상기한 바와 같이, 본 발명에 따르면, 함수에 의한 알고리즘을 이용하면서 암호화를 해제하기 위한 공격으로부터 시스템을 안전하게 보호할 수 있다.

도면의 간단한 설명

<1> 도 1은 본 발명에 따른 암호화 및 복호화 시스템의 구성을 도시한 블록도이며,

<2> 도 2는 본 발명에 따른 암호화 및 복호화 방법을 도시한 흐름도이다.

<3> * 도면의 주요 부분에 대한 부호의 설명 *

<4> 10 : 송신부 20 : 사용자입력부

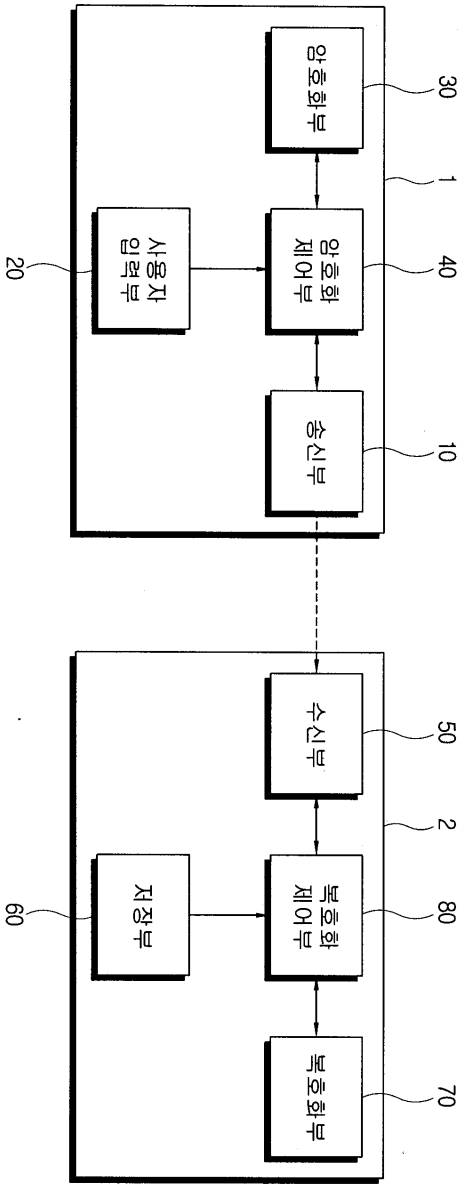
<5> 30 : 암호화부 40 : 암호화제어부

<6> 50 : 수신부 60 : 저장부

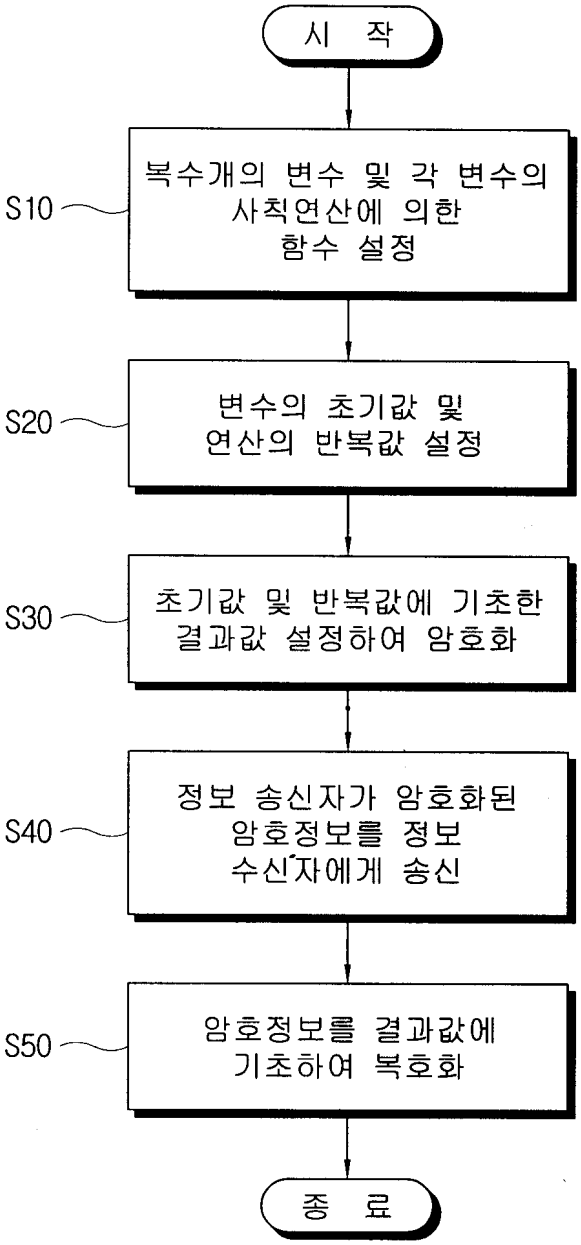
<7> 70 : 복호화부 80 : 복호화제어부

도면

도면1


암호화부
30
1
사용자 입력부
20
암호화 제어부
40
송신부
10
수신부
50
2
저장부
60
복호화 제어부
80
복호화부
70

도면2


시 작
S10
복수개의 변수 및 각 변수의 사칙연산에 의한 함수 설정
S20
변수의 초기값 및 연산의 반복값 설정
S30
초기값 및 반복값에 기초한 결과값 설정하여 암호화
S40
정보 송신자가 암호화된 암호정보를 정보 수신자에게 송신
S50
암호정보를 결과값에 기초하여 복호화
종 료