(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0010571
(43) 공개일자 2015년01월28일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01)
(21) 출원번호 10-2014-0059781
(22) 출원일자 2014년05월19일
심사청구일자 2014년05월19일
(30) 우선권주장
1020130085442 2013년07월19일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
윤지원
서울특별시 동작구 사당로20길 119, 101동 309호 (사당동, 르메이에르)
노희경
인천광역시 연수구 아트센터대로97번길 75, 1306동 1302호 (송도동, 송도더샵하버뷰13단지)
(74) 대리인
특허법인엠에이피에스

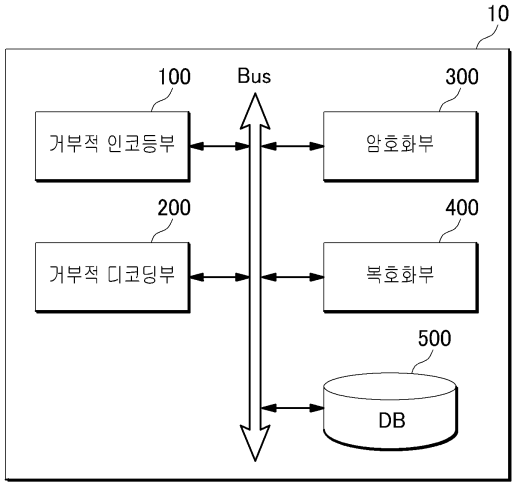
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **거부적 암호화 시스템 및 방법**

(57) 요 약

본 발명은 확률적 언어 모델(probabilistic language model)에 기반한 매핑 정보를 저장하는 데이터베이스; 주어진 제 1 평문을 상기 매핑 정보를 사용하여 제 1 이진 데이터(binary data)로 변환하는 거부적 인코딩부; 상기 제 1 이진 데이터를 암호화하여 제 1 암호문을 생성하는 암호화부; 주어진 제 2 암호문을 복호화하여 제 2 이진 데이터를 생성하는 복호화부; 및 상기 제 2 이진 데이터를 상기 확률적 언어 모델에 기초하여 제 2 평문으로 변환하는 거부적 디코딩부;를 포함하되, 상기 제 2 암호문이 상기 제 1 암호문과 동일할 경우, 진짜 복호화 암호키를 사용하여 복호화한 경우에는 상기 제 2 평문은 상기 제 1 평문과 동일하며, 가짜 복호화 암호키를 사용하여 복호화한 경우에는 상기 제 2 평문은 상기 제 1 평문과 상이한 거부적 암호화 장치를 제공한다.

대 표 도 - 도2



특허청구의 범위

청구항 1

거부적 암호화 장치에 있어서,

확률적 언어 모델(probabilistic language model)에 기반한 매핑 정보를 저장하는 데이터베이스;

주어진 제 1 평문을 상기 매핑 정보를 사용하여 제 1 이진 데이터(binary data)로 변환하는 거부적 인코딩부;

상기 제 1 이진 데이터를 암호화하여 제 1 암호문을 생성하는 암호화부;

주어진 제 2 암호문을 복호화하여 제 2 이진 데이터를 생성하는 복호화부; 및

상기 제 2 이진 데이터를 상기 확률적 언어 모델에 기초하여 제 2 평문으로 변환하는 거부적 디코딩부;를 포함하되,

상기 제 2 암호문이 상기 제 1 암호문과 동일할 경우,

진짜 복호화 암호키를 사용하여 복호화한 경우에는 상기 제 2 평문은 상기 제 1 평문과 동일하며,

가짜 복호화 암호키를 사용하여 복호화한 경우에는 상기 제 2 평문은 상기 제 1 평문과 상이한 거부적 암호화 장치.

청구항 2

제 1 항에 있어서,

상기 매핑 정보는 주어진 데이터 집합에서의 각 문자의 누적 빈도 분포 및 대응되는 이진 코드 정보이며,

누적 분포 훈련(training)을 통해, 상기 주어진 데이터 집합으로부터 추출되는 거부적 암호화 장치.

청구항 3

거부적 암호화 장치를 이용한 거부적 암호화 방법에 있어서,

상기 거부적 암호화 장치의 거부적 인코딩부가 주어진 제 1 평문을 확률적 언어 모델(probabilistic language model)에 기반한 매핑 정보를 사용하여 제 1 이진 데이터(binary data)로 변환하는 단계;

상기 거부적 암호화 장치의 암호화부가 상기 제 1 이진 데이터를 암호화하여 제 1 암호문을 생성하는 단계;

상기 거부적 암호화 장치의 복호화부가 주어진 제 2 암호문을 복호화하여 제 2 이진 데이터를 생성하는 단계; 및

상기 거부적 암호화 장치의 거부적 디코딩부가 상기 제 2 이진 데이터를 상기 확률적 언어 모델에 기초하여 제 2 평문으로 변환하는 단계;를 포함하되,

상기 제 2 암호문이 상기 제 1 암호문과 동일할 경우,

진짜 복호화 암호키를 사용하여 복호화한 경우에는 상기 제 2 평문은 상기 제 1 평문과 동일하며,

가짜 복호화 암호키를 사용하여 복호화한 경우에는 상기 제 2 평문은 상기 제 1 평문과 상이한 거부적 암호화 방법.

청구항 4

제 3 항에 있어서,

상기 매핑 정보는 주어진 데이터 집합에서의 각 문자의 누적 빈도 분포 및 대응되는 이진 코드 정보이며,

누적 분포 훈련(training)을 통해, 상기 주어진 데이터 집합으로부터 추출되는 거부적 암호화 방법.

청구항 5

거부적 암호화 장치를 이용한 거부적 암호화 방법에 있어서,

상기 거부적 암호화 장치의 거부적 인코딩부가 상기 제 1 평문을 확률적 언어 모델(probabilistic language model)에 기반한 매핑 정보를 사용하여 제 1 이진 데이터(binary data)로 변환하는 단계;

상기 거부적 암호화 장치의 암호화부가 상기 제 1 이진 데이터를 진짜 키로 암호화하여 제 1 암호문을 생성하는 단계;

상기 거부적 암호화 장치의 복호화부가 주어진 제 2 암호문을 가짜 키로 복호화하여 제 2 이진 데이터를 생성하는 단계; 및

상기 거부적 암호화 장치의 거부적 디코딩부가 상기 제 2 이진 데이터를 상기 확률적 언어 모델에 기초하여 상기 제 2 평문으로 변환하는 단계;를 포함하는 거부적 암호화 방법.

청구항 6

제 5 항에 있어서,

상기 매핑 정보는 주어진 데이터 집합에서의 각 문자의 누적 빈도 분포 및 대응되는 이진 코드 정보이며,

누적 분포 훈련(training)을 통해, 상기 주어진 데이터 집합으로부터 추출되는 거부적 암호화 방법.

청구항 7

거부적 암호화 장치를 이용한 거부적 암호화 방법에 있어서,

상기 거부적 암호화 장치의 거부적 인코딩부가 상기 제 2 평문을 확률적 언어 모델(probabilistic language model)에 기반한 매핑 정보를 사용하여 제 2 이진 데이터(binary data)로 변환하는 단계;

상기 거부적 암호화 장치의 암호화부가 상기 제 2 이진 데이터를 가짜 키로 암호화하여 제 2 암호문을 생성하는 단계;

상기 거부적 암호화 장치의 복호화부가 주어진 제 1 암호문을 진짜 키로 복호화하여 제 1 이진 데이터를 생성하는 단계; 및

상기 거부적 암호화 장치의 거부적 디코딩부가 상기 제 1 이진 데이터를 상기 확률적 언어 모델에 기초하여 상기 제 1 평문으로 변환하는 단계;를 포함하는 거부적 암호화 방법.

청구항 8

제 7 항에 있어서,

상기 매핑 정보는 주어진 데이터 집합에서의 각 문자의 누적 빈도 분포 및 대응되는 이진 코드 정보이며,

누적 분포 훈련(training)을 통해, 상기 주어진 데이터 집합으로부터 추출되는 거부적 암호화 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 거부적 코딩 방식을 이용한 거부적 암호화 시스템에 관한 것이다.

배 경 기 술

[0002] 일반적인 암호화 시스템은 송신자 또는 수신자가 제3의 인물에게 암호화 키를 제공해야 하는 경우에는 원래의 평문을 공개해야 한다는 문제가 있다. 예를 들어, 을이 병에게 암호화된 메시지를 발송하였으나, 갑이 을의 약점을 갖고 있거나 상사일 경우 을은 어쩔 수 없이 비밀성을 포기해야 하는 문제가 생길 수 있다.

[0003] 이러한 문제점을 극복하기 위해서 나온 암호화 기법이 거부적 암호화(Deniable Encryption)이다. 즉, 진짜 키를 갖고 복호화하면 숨겨진 진짜 평문을 얻을 수 있지만, 가짜 키를 이용하여 복호화할 경우 일반적인 암호화 시스템은 말이 안되는 데이터를 결과값으로 만들지만 거부적 암호화에서는 말은 되는 하지만 숨겨진 평문과는 다른 중요성이 떨어지는 평문이 나오게 하는 것이 바로 이 거부적 암호화이다.

[0004] 하지만, 1996년에 Ran Canetti에 의해서 처음 제시된 이후로 이론적으로는 가능한 것으로 알려져 있지만, 너무 많은 연산과 낮은 성능으로 인해 실제로는 널리 이용되지 않고 있다.

[0005] 따라서 효율적이면서 실생활에 이용 가능한 거부적 암호화 시스템이 필요하다.

[0006] 본 발명과 관련하여 논문("Deniable Authentication with RSA and Multicasting", 2005년 2월 24일, Daniel R. L. Brown 등)에는 RSA 암호화에 거부적 인증(deniable authentication)을 적용하는 구성이 개시되어 있다.

[0007] 또한, 논문("Deniable Storage Encryption for Mobile Devices", 2013년 4월 3일, Adam Skillen)에는 휴대 기기에 거부적 암호화를 적용하는 구성이 개시되어 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 설계, 구현 및 이해가 쉽고 안전성 증명 역시 쉬운 거부적 암호화 시스템을 설계하고 구현하는데 그 목적이 있다.

과제의 해결 수단

[0009] 상기와 같은 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 거부적 암호화 장치는 거부적 암호화 장치는, 확률적 언어 모델(probabilistic language model)에 기반한 매핑 정보를 저장하는 데이터베이스; 주어진 제 1 평문을 상기 매핑 정보를 사용하여 제 1 이진 데이터(binary data)로 변환하는 거부적 인코딩부; 상기 제 1 이진 데이터를 암호화하여 제 1 암호문을 생성하는 암호화부; 주어진 제 2 암호문을 복호화하여 제 2 이진 데이터를 생성하는 복호화부; 및 상기 제 2 이진 데이터를 상기 확률적 언어 모델에 기초하여 제 2 평문으로 변환하는 거부적 디코딩부;를 포함하되, 상기 제 2 암호문이 상기 제 1 암호문과 동일할 경우, 진짜 복호화 암호키를 사용하여 복호화한 경우에는 상기 제 2 평문은 상기 제 1 평문과 동일하며, 가짜 복호화 암호키를 사용하여 복호화한 경우에는 상기 제 2 평문은 상기 제 1 평문과 상이한 것을 특징으로 한다.

[0010] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 거부적 암호화 장치를 사용한 거부적 암호화 방법은 상기 거부적 암호화 장치의 거부적 인코딩부가 주어진 제 1 평문을 확률적 언어 모델(probabilistic language model)에 기반한 매핑 정보를 사용하여 제 1 이진 데이터(binary data)로 변환하는 단계; 상기 거부적 암호화 장치의 암호화부가 상기 제 1 이진 데이터를 암호화하여 제 1 암호문을 생성하는 단계; 상기 거부적 암호화 장치의 복호화부가 주어진 제 2 암호문을 복호화하여 제 2 이진 데이터를 생성하는 단계; 및 상기 거부적 암호화 장치의 거부적 디코딩부가 상기 제 2 이진 데이터를 상기 확률적 언어 모델에 기초하여 제 2 평문으로 변환하는 단계;를 포함하되, 상기 제 2 암호문이 상기 제 1 암호문과 동일할 경우, 진짜 복호화 암호키를 사용하여 복호화한 경우에는 상기 제 2 평문은 상기 제 1 평문과 동일하며, 가짜 복호화 암호키를 사용하여 복호화한 경우에는 상기 제 2 평문은 상기 제 1 평문과 상이한 것을 특징으로 한다.

[0011] 상기와 같은 목적을 달성하기 위한 본 발명의 제 3 측면에 따른 거부적 암호화 장치를 이용한 거부적 암호화 방법은, 상기 거부적 암호화 장치의 거부적 인코딩부가 상기 제 1 평문을 확률적 언어 모델(probabilistic language model)에 기반한 매핑 정보를 사용하여 제 1 이진 데이터(binary data)로 변환하는 단계; 상기 거부적 암호화 장치의 암호화부가 상기 제 1 이진 데이터를 진짜 키로 암호화하여 제 1 암호문을 생성하는 단계; 상기 거부적 암호화 장치의 복호화부가 주어진 제 2 암호문을 가짜 키로 복호화하여 제 2 이진 데이터를 생성하는 단계; 및 상기 거부적 암호화 장치의 거부적 디코딩부가 상기 제 2 이진 데이터를 상기 확률적 언어 모델에 기초하여 상기 제 2 평문으로 변환하는 단계;를 포함하는 것을 특징으로 한다.

[0012] 상기와 같은 목적을 달성하기 위한 본 발명의 제 3 측면에 따른 거부적 암호화 장치를 이용한 거부적 암호화 방법에 있어서, 상기 거부적 암호화 장치의 거부적 인코딩부가 상기 제 2 평문을 확률적 언어 모델(probabilistic language model)에 기반한 매핑 정보를 사용하여 제 2 이진 데이터(binary data)로 변환하는 단계; 상기 거부적 암호화 장치의 암호화부가 상기 제 2 이진 데이터를 가짜 키로 암호화하여 제 2 암호문을 생성하는 단계; 상기 거부적 암호화 장치의 복호화부가 주어진 제 1 암호문을 진짜 키로 복호화하여 제 1 이진 데이터를 생성하는 단계; 및 상기 거부적 암호화 장치의 거부적 디코딩부가 상기 제 1 이진 데이터를 상기 확률적 언어 모델에 기초하여 상기 제 1 평문으로 변환하는 단계;를 포함하는 것을 특징으로 한다.

발명의 효과

[0013] 본 발명은 종래의 거부적 암호화가 새로운 암호화 시스템을 설계하고 개발하는데 많은 노력이 들고 또한 암호적 특성을 분석하는데 어려움이 있다는 문제를 극복하여, 종래의 암호화 모듈을 그대로 활용하고, 암호화의 안전성이 종래의 암호화 모듈의 안전성을 그대로 상속한다는 장점을 가진다.

[0014] 또한, 암호화 키 공간상의 모든 값을 가짜 키 (fake key)로 사용할 수 있다. 종래의 거부적 암호화 시스템은 두 가지 평문(진짜 평문과 가짜 평문)과 그에 해당하는 두개의 키(진짜 키와 가짜 키)만으로 운영되지만, 본 발명에서는 만약 키의 값이 128비트이라면 0부터 2^128-1까지의 임의의 값이 모두 가짜 키로 이용될 수 있으므로, 사용자가 가짜 키를 외울 필요가 없다. 또한 종래의 거부적 암호화 시스템과 달리 가짜 평문을 송신자가 고려할 필요가 없으므로 좀더 효율적이다.

[0015] 또한, 송신자가 수신자에게 보내는 메시지가 암호화된 난수가 아닌 가짜 평문이므로, 제 3자가 해당 메시지가 암호화된 메시지인지 알지 못하는 은닉 암호화(steganography)를 제공하는 효과가 있다.

도면의 간단한 설명

[0016] 도 1은 거부적 암호화 장치의 개념을 도시함.

도 2는 본발명의 일실시예에 따른 거부적 암호화 장치의 구조를 도시함.

도 3은 본발명의 일실시예에 따른 거부적 암호화 장치의 방법의 거부적 인코딩 단계의 흐름을 도시함.

도 4는 본발명의 일실시예에 따른 거부적 암호화 장치의 방법의 거부적 디코딩 단계의 흐름을 도시함.

도 5는 본발명의 일실시예에 따른 거부적 암호화 장치의 방법의 가짜 평문 발송 단계의 흐름을 도시함.

도 6은 본발명의 일실시예에 따른 거부적 암호화 장치의 방법의 진짜 평문 추적 단계의 흐름을 도시함.

도 7은 종래 기술에 따른 거부적 암호화를 도시함.

도 8은 종래 기술에 따른 인코딩 및 디코딩의 개념을 도시함.

도 9는 본발명의 일실시예에 따른 거부적 암호화의 개념을 도시함.

도 10은 본발명의 일실시예에 따른 인코딩의 개념을 도시함.

도 11은 본발명의 일실시예에 따른 디코딩의 개념을 도시함.

도 12는 첫번째 문자에 대한 통계적 언어 모델을 도시함.

도 13은 r번째 문자에 대한 통계적 언어 모델을 도시함.

도 14는 본발명의 일실시예에 따른 거부적 암호화의 실시예를 도시함.

발명을 실시하기 위한 구체적인 내용

[0017] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도 부호를 붙였다.

[0018] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0019] 본 명세서는 먼저 도 1 내지 도 6을 통해 본 발명의 일실시예에 따른 거부적 암호화에 대해 대략적인 내용을 설명한 후, 도 7 내지 도 14를 통해 본 발명의 일실시예에 따른 거부적 암호화에 대해 좀더 구체적으로 설명한다.

[0020] 도 1 및 도 2는 본발명의 일실시예에 따른 거부적 암호화 장치를 도시하고 있다.

[0021] 도 1은 거부적 암호화 장치의 개념을 도시하고 있다.

[0022] 거부적 암호화 장치(10)는 암호문(C1) 및 이를 복호화할 키(Kdecrypt 또는 Kdecrypt_fake)를 입력받아 평문(P1 또는 P2)을 출력한다. 진짜 키(Kdecrypt)를 입력받으면 진짜 평문(P1)이, 가짜 키(Kdecrypt_fake)를 입력받으면

가짜 평문(P2)이 출력된다.

[0023] 이때, 평문(plain message)은 송신자가 수신자에게 보내기를 원하는 진짜 메시지를 의미하며, 텍스트 형식에 한정되지 않는다. 즉, 본 명세서에서 평문이라 함은 디지털화된 모든 종류의 데이터를 의미한다. 예를 들어 평문은 일반적인 텍스트 문자열, 이진 데이터(binary data), 및 이미지, 동영상 등의 멀티미디어를 포함한다.

[0024] 암호문(encrypted message)은 평문을 암호화(encryption)한 메시지이며, 암호문(C1)을 복호화(decryption)하면 평문이 생성된다.

[0025] 진짜 평문(P1)이란 암호화하기 전의 원래 평문을 의미하며, 진짜 평문(P1)을 암호화하면 암호문(C1)이 생성된다. 가짜 평문(P2)이란, 진짜 평문(P1)이 아닌 평문을 말한다.

[0026] 올바른 키 또는 진짜 키(Kdecrypt)는 암호문(C1)에서 진짜 평문(P1)을 생성할 수 있는 암호화 키를, 잘못된 키 또는 가짜 키(Kdecrypt_fake)는 암호문(C1)에서 가짜 평문(P2)을 생성하는 암호화 키를 의미한다.

[0027] 도 2는 본발명의 일실시예에 따른 거부적 암호화 장치의 구조를 도시하고 있다.

[0028] 거부적 암호화 장치(10)는 거부적 인코딩부(100), 거부적 디코딩부(200), 암호화부(300), 복호화부(400), 및 데이터베이스(500)를 포함한다.

[0029] 도 1은 종래의 거부적 암호화 시스템을 나타낼 수 있다. 거부적 암호화부(300)를 통해서 잘못된 키와 진짜 키에 따라서 숨겨진 평문과 가짜 평문(P2)이 나온다.

[0030] 전술한 바와 같이, 종래에는 이러한 거부적 암호화 시스템을 종래의 암호화 시스템과 전혀 별개의 것으로 개발하려고 했기 때문에 어려움이 있었다. 본 발명의 목적 중 하나는 이러한 거부적 암호화 시스템에 대한 효율적이면서 실생활에 이용 가능한 거부적 암호화 시스템을 만드는 것이다. 특히, 본 발명은 도 2에 도시된 바와 같이 평문의 특징을 이용하여 인코더와 디코더 부분에 거부 능력(Deniability)을 부여함으로써 종래 기술과 전혀 다른 새로운 방식으로 거부적 암호화 시스템을 용이하게 만드는 효과를 갖는다.

[0031] 도 2는 본 발명의 일실시예에 따른 거부적 암호화 시스템으로, 도시되어 있는 바와 종래의 RSA, DES, AES와 같은 전통적인 암호화 시스템을 내부에 탑재하며 그 상단과 하단에 거부 능력을 보유한 인코더와 디코더를 부착함으로써 거부적 암호 능력을 갖게 된다.

[0032] 이는 여러 가지 면에서 종래의 거부적 암호화 시스템과는 다른 방식의 시스템이다.

[0033] 첫째, 가장 큰 차이점은 종래의 거부적 암호화 시스템은 암호화 기법 자체에 거부 능력(Deniability)을 부여하고자 함으로써 종래의 DES, RSA, AES등과 같은 전통적이면서 보편화된 암호화 시스템과 관련이 없는 우리가 사용하지 않고 있으며 새로이 배워야 하는 새로운 암호화 시스템을 개발해온 반면, 본 발명은 거부적 암호화 시스템을 구현하기 위해서 새로운 암호화 시스템을 구축하는 것이 아니라 DES, AES, RSA와 같은 종래의 대칭키 및 비대칭키 암호화 시스템을 그대로 사용하면서 암호화부(300) 및 복호화부(400)의 입력과 출력 부분의 인코더(Encoder)와 디코더 (Decoder)가 거부능력을 보유하게 한다는 것이다.

[0034] 이러한 인코더와 디코더를 본 발명에서는 거부적 인코딩부(100), 즉, 거부적 인코더(deniable encoder), 및 거부적 디코딩부(200), 즉, 거부적 디코더(deniable decoder)라 한다. 거부적 인코더와 거부적 디코더를 합쳐 거부적 코더(deniable coder)라고 할 수 있으며, 암호화부(300) 및 복호화부(400)를 합쳐 암호화 모듈이라고 할 수 있다.

[0035] 이렇듯 종래의 암호화 모듈(300, 400)을 그대로 사용하면서 그 위에 거부적 인코더 및 거부적 디코더(각각 100, 200)를 부착하여 거부적 암호화의 기능을 제공할수 있다.

[0036] 이에 따라 본 발명은 거부적 암호화 시스템은 새로운 암호화 시스템을 설계하고 개발하는데 많은 노력이 들고 또한 암호적 특성을 분석하는데 많은 어려움이 있는 종래 기술과 달리, 암호의 안전성이 내부에 사용되는 종래의 대칭키나 비대칭키 암호화 시스템의 안전성과 일치하므로 설계와 개발 및 안전성 체크에서 현격하게 수월하다는 장점을 가진다.

[0037] 둘째, 키(key) 공간상의 모든 값을 가짜 키(fake key)로 사용할 수 있다. 종래의 거부적 암호화 시스템은 두 가지 평문(진짜 평문(P1)과 가짜 평문(P2))과 그에 해당하는 오로지 두개의 키(진짜 키와 가짜 키)를 갖고 운영되지만, 본 발명에서는 만약 키의 값이 128비트이라면 0부터 2^128-1까지의 모든 값이 가짜 키로 이용될 수 있기에 가짜 키를 외울 필요가 없다. 또한 종래의 거부적 암호화 시스템과 달리 가짜 평문(P2)을 송신자가 고려할

필요가 없기에 보다 더 효율적이다.

[0038] 셋째, 본 발명은 송신자가 암호화된 난수가 아닌 가짜 평문(P2)을 직접 보냄으로써 은닉암호(steganography)의 기능을 갖는다.

[0039] 마지막으로, 거부적 디코딩으로 나온 값들이 모두 의미를 가지므로 전수 조사에 의한 암호 분석을 막을 수 있다는 장점이 있다.

[0040] 이하 도면들을 통해 본 발명의 일실시예에 따른 거부적 암호화 장치 및 방법의 구성 및 동작에 대해 좀더 구체적으로 설명한다.

[0041] 도 3은 거부적 인코더부(100) 및 암호화부(300)을 사용하여 주어진 평문(P1)으로부터 암호문(C1)을 생성하는 과정을 도시하고 있으며, 도 4는 복호화부(400)와 거부적 디코더부(200)를 사용하여 주어진 암호문(C1)으로부터 진짜 평문(P1) 또는 가짜 평문(P2)을 얻게 되는 과정을 도시하고 있다.

[0042] 설명의 편의를 위해 송신자가 평문(P1)을 암호화하여 수신자에게 보내면, 수신자가 수신한 암호문(C1)을 복호화하여 원래의 평문(P1)을 복원한다는 일반적인 암호화 시스템의 흐름을 가정하나, 여기에 한정되는 것은 아니다. 예를 들어, 송신자와 수신자가 동일 장치의 사용자일 수 있다.

[0043] 먼저, 도 3은 본발명의 일실시예에 따른 거부적 암호화 장치의 방법의 거부적 인코딩 단계의 흐름을 도시하고 있다.

[0044] 진짜 평문(P1)을 입력받아(S110), 거부적 인코딩한다(S120). 이때 확률적 언어 모델 기반의 데이터베이스(500)를 사용할 수 있다. 구체적인 내용은 도 12 내지 13을 통해 후술한다.

[0045] 거부적 인코딩된 데이터를 암호화 암호키(Kencrypt)로 암호화하면(S130) 암호문(C1)이 출력된다(S140).

[0046] 다음, 도 4는 본발명의 일실시예에 따른 거부적 암호화 장치의 방법의 거부적 디코딩 단계의 흐름을 도시하고 있다.

[0047] 암호문(C1)을 입력받아(S210), 복호화 암호키(Kdecrypt 또는 Kdecrpt_fake)로 복호화한다(S220).

[0048] 거부적 인코딩(S130)과 같은 확률적 언어 모델 기반의 데이터베이스(500)를 사용하여 거부적 디코딩한다(S230)하면, 평문(P1 또는 P2)이 출력된다(S240). 이때, 전술한 바와 같이, 진짜 복호화 암호키(Kdecrypt) 사용시에는 진짜 평문(P1)이, 가짜 복호화 암호키(Kdecrypt_fake) 사용시에는 가짜 평문(P2)이 출력된다.

[0049] 도 5 및 도 6은 도 3 및 도 4에서 설명한 거부적 인코딩 및 거부적 디코딩을 사용한 암호화 및 복호화를 활용하여, 송신자가 가짜 평문(P2)을 송신하고, 수신자가 진짜 평문(P1)을 추적하는 실시예를 설명하고 있다.

[0050] 먼저, 도 5는 송신자가 진짜 평문(P1)으로 얻어진 직접적인 암호문(C1)이 아닌 가짜 평문(P2)을 수신자에게 보내는 시스템에 대한 도면으로, 암호화와 복호화 과정이 동시에 존재하며 각각 다른 종류의 두개의 키가 사용된다.

[0051] 진짜 평문(P1)을 입력받아(S310), 거부적 인코딩한다(S320). 이때 확률적 언어 모델 기반의 데이터베이스(500)를 사용할 수 있다. 구체적인 내용은 도 12 내지 13을 통해 후술한다.

[0052] 거부적 인코딩된 데이터를 진짜 암호화 암호키(Kencrypt)로 암호화하여(S330), 제 1 암호문(C1)을 출력한다(S340).

[0053] 제 1 암호문(C1)을 가짜 복호화 암호키(Kdecrpt_fake)로 복호화한 후(S350), 거부적 인코딩(S320)과 같은 확률적 언어 모델 기반의 데이터베이스(500)를 사용하여 거부적 디코딩하면(S360), 가짜 평문(P2)이 출력된다(S370).

[0054] 도 6은 도 5에 기술된 방식으로 얻어진 가짜 평문(P2)을 받아서 원래의 숨겨진 진짜 평문(P1)을 찾는 과정을 도식화한 도면이다.

[0055] 수신한 가짜 평문(P2)을 입력받아(S410), 거부적 인코딩(S320)과 같은 확률적 언어 모델 기반의 데이터베이스(500)를 사용하여 거부적 인코딩한다(S420).

[0056] 거부적 인코딩된 데이터를 가짜 암호화 암호키(Kencrypt_fake)로 암호화하여(S430), 제 2 암호문(C2)을 출력한다(S440).

[0057] 제 2 암호문(C2)을 진짜 복호화 암호키(Kdecrpt)로 복호화한 후(S450), 거부적 인코딩(S320)과 같은 확률적 언어 모델 기반의 데이터베이스(500)를 사용하여 거부적 디코딩하면(S460), 진짜 평문(P1)을 출력된다(S470). 이때, 사용된 암호화 또는 복호화 키가 다르면 또다른 가짜 평문(P3)이 출력한다.

[0058] 이상 설명한 내용을 요약하면, 본 발명에서 제안되는 거부적 암호화는 크게 두 가지 형태로 사용이 가능하다.

[0059] 첫 번째 모델은 송수신에서 사용되는 데이터가 암호문(C1)일 경우이며, 도 3 및 도 4에 도시되어 있다.

[0060] 송신자: 평문->거부적 인코딩->암호화-> 암호문(C1)

[0061] 수신자: 암호문(C1)->복호화->거부적 디코딩-> 평문

[0062] 즉, 송신자는 한번의 거부적 인코딩과 암호화 과정을, 수신자는 한번의 복호화와 한번의 거부적 디코딩 과정을 거친다.

[0063] 이때, 복호화를 진짜 키를 이용하여 수행하면 평문은 진짜 키를 갖고 반대로 잘못된 키를 이용하면 가짜 평문(P2)이 나온다.

[0064] 두 번째 모델은 송수신에서 사용되는 데이터가 평문 형태(P2)일 경우이며, 도 5 및 도 6에 기술되어 있다.

[0065] 송신자: 진짜 평문(P1)-> 거부적 인코딩->암호화(진짜 키 사용)->복호화(가짜 키 사용)->거부적 디코딩->가짜 평문(P2)

[0066] 수신자: 가짜 평문(P2)->거부적 인코딩->암호화(가짜 키 사용)->복호화(진짜 키 사용)->거부적 디코딩-> 진짜 평문(P1)

[0067] 즉, 송신자와 수신자 모두 한번씩의 거부적 인코딩-암호화-복호화-거부적 디코딩 과정을 거친다.

[0068] 이때, 수신자가 복호화에 사용된 키가 진짜 키가 아닌 가짜 키인 경우에는 또다른 가짜 평문(P3)이 생성되므로, 송신자가 암호문(C1)이 아닌 가짜 평문(P2)을 전송하더라도 진짜 평문(P1)이 노출되는 것을 막을 수 있다.

[0069] 본 발명의 일실시예에 따른 거부적 암호화 시스템(10)의 이러한 기능은 스테가노그래피(steganography) 기법의 일종으로, 송신자가 수신자에게 전송한 메시지가 평문 형태이기 때문에, 제 3 자는 송신자가 이를 위해 진짜 평문(P1)을 암호화하여 가짜 평문(P2)으로 가공한 후 전송하였다는 사실을 눈치채지 못한다. 또한 잘못된 키를 사용하더라도 또다른 가짜 평문(P2)이 생성되므로, 진짜 평문(P1)이 따로 있다는 사실을 알아채지 못한다.

[0070] 이상 도 1 내지 도 6을 통해 본 발명의 일실시예에 따른 거부적 암호화에 대해 대략적인 내용을 설명하였다. 이제 도 7 내지 도 14를 통해 본 발명의 일실시예에 따른 거부적 암호화에 대해 좀더 구체적으로 설명한다.

[0071] 도 7은 종래 기술에 따른 거부적 암호화를 도시하고 있다.

[0072] 공개키(public key) 기반과 공유키(shared key) 기반 기술을 포함하는 종래의 거부적 암호화 기술은 다음과 같은 문제가 있다.

[0073] 첫째, 거부적 암호화 시스템을 구축하기 위해서는 암호화 시스템에 거부능력(Deniability)을 추가해야 하는데, 종래의 암호화 시스템에서 거부 능력은 암호화 모듈에 추가된다. 따라서 암호화 모듈이 RSA, DES, AES 등의 종래 암호화 기술을 활용할 수 없으며, 거부 능력을 갖는 새로운 암호화 기법이 필요하다. 그러므로, 종래의 방법은 거부적 암호화 시스템 전체를 다시 설계해야 한다는 문제가 있다. 또한 새로운 암호화 기법은 보안성(security) 및 안전성(safety)이 검증되어야 채용될 수 있으므로, 새로운 시스템이 실제 구현되고 사용되기까지 시간이 소요된다.

[0074] 둘째, 종래 기술은 송신자를 위한 가짜 알고리즘인 내부 함수를 갖는데, 적절한 내부 함수를 찾고 구축하는 것이 용이하지 않다. 종래 기술 중 하나는 확률 모델을 사용하여 내부 함수를 구축하는데, 대부분의 경우에 있어, 이를 이해하고 구현하는 것이 쉽지 않다.

[0075] 셋째, 종래 기술은 연산 복잡도 및 공간 복잡도가 크다는 문제가 있다. 즉, 연산량이 많고 많은 기억 공간을 필요로 하므로 실용적이지 않다. 예를 들어, 종래 기술은 대용량 텍스트를 거부적 암호화하기에 적절하지 않다.

[0076] 넷째, 종래 기술은 가짜 메시지를 필요로 한다. 따라서 사용자는 진짜 메시지(원래의 평문), 가짜 메시지, 및 이에 대응하는 진짜 키 및 가짜 키를 동시에 가지고 있어야 거부화 암호화 시스템을 사용할 수 있다.

[0077] 다섯째, 종래 기술은 복호화를 위해서도 진짜 키(K1)와 가짜 키(K2)를 모두 필요로 한다. 송신자와 수신자가 모

두 이를 필요로 하므로, 가짜 키(K2)가 없으면 송신자와 수신자 모두 원래의 평문을 복원해낼 수 없다. 또한, 이러한 경우 원래의 평문이 노출되어 버린다는 더 심각한 문제가 있다. 임의의 키(K3)를 사용하여 복호화하면(즉, K3≠K2,K3≠K1), 의미없는 문장이 생성되기 때문이다.

[0078] 예를 들어, 을이 "사랑"이라는 평문과 "회사"라는 가짜 텍스트를 각각 대응되는 키(K1 및 K2)와 함께 병에게 송신하면서 갑에게는 이를 숨기려 한다면, 갑이 암호화된 메시지의 키를 요구할 경우를 대비하여 을은 암호화에 가짜 키 K2를 사용하여 원래의 평문인 "사랑"을 숨기려 할 것이다. 그러나 을이 가짜 키 K2를 잊거나 분실하여, 임의의 다른 키 K3를 주었을 경우, K3로 메시지를 복호화하면 의미없는 임의의 문자열이 생성되기 때문에, 을의 거짓말은 쉽게 들통나게 된다.

[0079] 도 8은 종래 기술에 따른 인코딩 및 디코딩의 개념을 도시하고 있다.

[0080] 암호화 및 복호화 과정은 일반적으로 2단계로 이루어진다.

[0081] 먼저, 암호화 과정을 먼저 설명하면, 암호화(encryption) 전에 먼저 인코딩(encoding) 과정이 있다. 예를 들어, 도시되어 있는 예에서 평문 "crypto"는 ASCII 코드 테이블을 사용하여 "63 72 79 70 74 6F"라는 16진수 데이터로 변환된다. 따라서 암호화 모듈에 입력되는 것은 "crypto"가 아니라 16진수, 즉, 이진수 코드이다.

[0082] 복호화 과정도 마찬가지로, 복호화(decryption) 후에 디코딩(decoding) 과정을 더 거쳐야 평문 "crypto"가 복원된다.

[0083] 본 발명의 일실시예에 따른 거부적 암호화 장치 및 방법은 이러한 사항을 거부적 암호화에 사용한다는 점에서 종래 기술과 현저히 구분된다. 현재까지 암호학자들은 암호화 모듈 및 복화화 모듈, 즉, 거부적 암호화 알고리즘 자체를 개발하는 데에만 노력을 기울여왔으나, 본 발명은 암호화 모듈 및 복호화 모듈이 아닌 인코딩 코듈 및 디코딩 모듈을 사용함으로써, 전술한 바와 같은 종래 기술들이 가지고 있는 여러 가지 문제들을 효과적으로 해결한다. 이에 대해 도 9를 통해 설명한다.

[0084] 도 9는 본발명의 일실시예에 따른 거부적 암호화의 개념을 도시하고 있다.

[0085] 도시되어 있는 바와 같이, 본 발명의 일실시예에 따른 거부적 암호화 방법에서는 인코딩부(100) 및 디코딩부(200)를 종래의 암호화부(300) 및 복호화부(400)를 감싸는(warpping) 래퍼(wrapper) 모듈로 구성하고 있다.

[0086] 이러한 구성 덕분에 본발명의 일실시예에 따른 거부적 암호화 장치 및 방법은 RSA, DES, AES 등 종래의 암호화 기법을 그대로 사용하여도 인코딩부(100) 및 디코딩부(200) 변경만으로 거부 능력이 있는 암호화 시스템을 구축할 수 있다. 또한, 이에 따라 본 발명의 일실시예에 따른 거부적 암호화 장치 및 방법의 보안성 및 안전성은 암호화부(300) 및 복호화부(400)에 사용된 종래 암호화 기법의 보안성 및 안전성을 그대로 따른다는 장점이 있다.

[0087] 이제, 도 10 및 도 11을 통해 본 발명의 일실시예에 따른 인코딩부(100) 및 디코딩부(200)가 어떻게 거부 능력을 전체 시스템에 제공하는지 설명한다.

[0088] 도 10은 본발명의 일실시예에 따른 인코딩의 개념을 도시하고 있다.

[0089] 본 발명의 일실시예에 따른 인코딩 방법은 이진수 데이터로 변환할 때, 종래의 ASCII 코드 테이블을 사용하는 대신에, 데이터베이스(500)에 기반한 언어 모델 또는 확률적 언어 모델(probabilistic language model)을 적용한다.

[0090] 확률적 언어 모델은 공지 기술이므로 다음과 같이 간략하게 설명한다.

[0091] 확률적 언어 모델은 일련의 문자열에 확률을 할당하는 확률 모델이다. 예를 들어, 영어 단어 또는 문장에서 e라는 알파벳이 나올 확률, 단어의 첫번째 글자에 e가 나올 확률, 영어 문장에서 the라는 단어가 나올 확률, 또는 the 라는 단어 다음에 love라는 단어가 나올 확률 등을 모델링한 것이 확률적 언어 모델이다.

[0092] 예를 들어, m개의 알파벳 또는 문자로 이루어진 단어 또는 문자열 S에 대해 상태 공간(state space)이라고 불리는 계수 가능한 집합 A에 있는 값을 갖는 랜덤 변수(random variable) xi(0<i<m)를 정의하면(이때, 각 xi는 N=card(A) 개의 값들 중 하나를 갖는 불연속 변수임), 언어 모델은 불연속 시간 프로세스(discrete-time process)로 설명될 수 있다.

[0093] 예를 들어, 마코프 조건(Markov condition)을 갖는 k차 마코프 프로세스(k-order Markov process) x는 다음과 같이 정의될 수 있다.

[0094] <수학식 1>

$$p(x_i = s_i | x_{1:i-1} = s_{1:i-1}) = p(x_i = s_i | x_{i-k:i-1} = s_{i-k:i-1})$$

[0095]

[0096] 문자열을 모델링하는 일반적인 방법은 확률을 인수분해(factorizing)하여 수학식 2와 같은 k차 마코프 모델(k-order Markovian model)로 단순화하는 것이다.

[0097] <수학식 2>

$$p(s_{1:m}) = \prod_{i=1}^{m} p(s_i | s_{1:i-1}) = \prod_{i=1}^{m} p(s_i | s_{i-k:i-1})$$

[0098]

[0099] 일반적으로 확률 모델은 n-그램(n-gram) 통계, n개의 연속된 단어 집합의 빈도(frequency) 테이블을 사용한다. n그램 모델은 (n-1)차 마코프 체인((n-1)th order Markov chain)으로 해석될 수 있다.

[0100] 도면을 참조하면, 평문(P1)은 먼저, ASCII 코드 테이블 대신에, 이상과 같이 설명한 언어 모델에 기반한 데이터베이스(500)를 사용하여 이진 코드(binary code)로 변환된다. 도시되어 있는 바와 같이 본 명세서는 이를 거부적 인코딩(deniable encoding)이라고 부른다.

[0101] 다음, 상기와 같이 거부적 인코딩부(100)에 의해 거부적 인코딩된 이진 코드가 암호문(C1)으로 암호화된다. 전술한 바와 같이 암호화부(300)은 이를 종래의 암호화 기법을 사용하여 수행된다.

[0102] 도 11은 본발명의 일실시예에 따른 디코딩의 개념을 도시하고 있다.

[0103] 먼저, 이진 코드 형태의 암호문(C1)이 전술한 바와 같이 복호화부(400)에 의해 종래의 암호화 기법을 사용하여 복호화된다.

[0104] 다음, 복호화된 이진 코드를 거부적 디코딩부(200)가 전술한 바와 같은 언어 모델에 기반한 데이터베이스(500)를 사용하여 디코딩하면 평문(P1)이 생성된다. 도시되어 있는 바와 같이 본 명세서는 이를 거부적 디코딩(deniable decoding)이라고 부른다.

[0105] 이때, 도면의 하단에 도시되어 있는 바와 같이, 사용된 키(K)가 진짜 키이면 원래의 평문 P1이 복원되지만, 가짜 키이면 전혀 다른 가짜 평문(P2) 메시지가 생성된다.

[0106] 이제, 본 발명의 일실시예에 따른 거부적 인코딩 및 거부적 디코딩에 사용되고 있는 언어 모델 기반의 데이터베이스(500)의 일실시예에 대해 도 12 내지 도 13을 통해 살펴본다.

[0107] 도 12는 첫번째 문자에 대한 통계적 언어 모델을 도시하고 있다.

[0108] 도면의 (a)는 영어 문장의 첫번째 글자의 빈도 즉, p(X1=w)일 확률을 나타내고 있으며, (b)는 (a)가 나타내는 확률의 누적 분포를 도시한 것이다. w는 영어 알파벳({a, b, …, z}의 원소)이며, 숫자 또는 특수 문자(예: 문장 부호)일 수도 있다.

[0109] 도면의 (c)는 각 요소가 L 비트 길이의 이진 코드인 2^L x 1 크기의 래티스 공간이다. 이는 실제적인 물리 공간은 아니며, 평문의 각 문자가 이 중 하나의 요소로 대응(mapping)되어 인코딩된다. 즉, 래티스 공간의 각 요소는 각 문자의 누적 분포에 대응되는 이진 코드를 나타낸다.

[0110] 본 발명의 일실시예에 따른 거부적 암호화 방법은 도시되어 있는 언어 모델을 다음과 같이 활용한다.

[0111] 먼저, 도면의 (b)에 도시되어 있는 누적 분포에서 첫번째 문자인 t의 위치를 찾는다. 다음, 도면의 (c)에서 해당 위치에 대응하는 L 비트 길이의 이진 코드 집합을 찾는다.

[0112] 도시되어 있는 바와 같이 대응하는 후보가 다수 개 존재할 수 있다. 이런 경우에는 첫번째 후보를 선택할 수 있다.

[0113] 예를 들어, 평문 "the school"을 암호화하려고 할 때, (b)에서 t는 72.749%~ 89.420% 구간에 위치해 있다. (c)에서 이 위치에 대응하는 요소는 음영이 있는 구간이다. 도시되어 있는 바와 같이, 후보가 다수 개 존재하므로, 첫번째 후보인 10…11을 선택한다. 따라서 t는 10…11로 인코딩된다.

[0114] 디코딩 과정은 역으로 수행하면 되므로, 설명을 생략한다.

[0115] 도 13은 r번째 문자에 대한 통계적 언어 모델을 도시하고 있다.

[0116] 이후 문자들의 인코딩도 유사하게 수행된다. 단, 이 경우에는 조건부 확률이 고려된다.

[0117] 예를 들어, 'the school'이라는 문자열의 3번째 알파벳인 e에 대한 인코딩은 첫번째 글자가 t이고 두번째 글자가 h일 때 세번째 글자가 e일 확률(p(X3= e | X2= h, X1= t))을 구하여 수행될 수 있다.

[0118] 도시되어 있는 바와 같이, 이 확률의 누적 분포에 대응되는 구간인 인코딩 후보가 다수 개 존재하므로, 도 12에서와 마찬가지로, 첫번째 후보인 01…10이 선택된다.

[0119] 디코딩 과정은 역으로 수행하면 되므로, 설명을 생략한다.

[0120] 이상과 같은 거부적 인코딩 및 거부적 디코딩을 통해, 가짜 키를 사용하여 가짜 텍스트를 생성할 수 있다. 복호화부(400)가 종래의 암호화 방법을 통해, 주어진 암호문(C1)을 가짜 키를 사용하여 복호화하면 전혀 의미가 없는 이진 코드가 생성될 것이다. 그러나 이러한 디코딩부(200)가 상기 이진 코드를 전술한 방법을 디코딩하면 의미가 있어 보이는 평문이 생성된다.

[0121] 예를 들어, the school을 인코딩하고 암호화한 암호문(C1)을 복호화하고 디코딩한 평문이 종래 기술에서 생성되는 " @8hk*s"과 같이 전혀 의미없는 문자열이 아닌 "an apple"과 같이 의미있는 문자열이 되는 것이다.

[0122] 상술한 각 문자의 누적 분포 및 대응되는 이진 코드 정보(이하 매핑 정보)는 데이터베이스(500)에 저장되는데, 이는 공개 정보이다. 따라서 누구나 여기에 접근할 수 있다. 예를 들어, 전술한 예에서 을과 병뿐 아니라 갑도 여기에 접근할 수 있다. 그렇기 때문에 갑이 암호문(C1)을 복호화해서 얻게 되는 평문은 종래 기술과 같이 의미없는 문자열이 아닌 의미 있어 보이는 평문이 될 수 있는 것이다.

[0123] 각 문자의 누적 분포는 훈련(training) 과정을 통해 얻을 수 있다. 이는 사용자가 개인화된 데이터베이스(500)를 사용할 수 있음을 의미한다. 예를 들어, 어떤 사용자가 성경을 통해 언어 모델을 구축한다면, 데이터베이스(500)는 성경의 누적 분포를 갖게 될 것이다. 이는 경제 뉴스를 통해 언어 모델을 구축했을 때의 누적 분포와 상당히 차이가 있을 것임을 쉽게 알 수 있다. 예를 들어, 성경에서는 "사랑"이라는 단어의 빈도가 높을 것이나, 경제 뉴스에서는 "계좌"라는 성경에는 나오지 않을 법한 단어의 빈도가 높을 것이다.

[0124] 사용자는 이러한 특성을 활용하여, 원하는 스타일의 가짜 메시지를 자동 생성할 수 있다. 즉, 사용자는 원래의 평문 없이도 본 발명의 일실시예에 따른 거부적 암호화 장치 및 방법을 사용하여 진짜처럼 보이는 문장들을 만들어낼 수 있다.

[0125] 즉, 매핑 정보는 주어진 데이터 집합에서의 각 문자의 누적 빈도 분포 및 대응되는 이진 코드 정보이며, 누적 분포 훈련(training)을 통해, 주어진 데이터 집합으로부터 추출되어 데이터베이스(500)에 저장된다.

[0126] 도 14는 본발명의 일실시예에 따른 거부적 암호화의 실시예를 도시하고 있다.

[0127] 도면의 첫번째 열은 누적 분포 훈련에 사용한 자료를 도시하고 있다. NASA 문서, 로미오와 줄리엣, 암호학 문서, 성경, 클래식 음악 문서가 사용되었다.

[0128] 두번째 열은 각 경우에 사용된 평문을 도시하고 있다. 즉, 암호문(C1)의 복호화에 진짜 키(K1)가 사용되었을 때 복원되는 평문이다.

[0129] 세번째 열은 각 경우 임의로 선택된 가짜 키(K2 또는 K3)가 사용되었을 경우 생성되는 평문을 도시하고 있다. 도시되어 있는 바와 같이, 전혀 다른 평문이 생성되면서도, 종래의 거부적 암호화 방법과 달리, 의미있어 보이는 평문이 생성되고 있다. 또한, 이때 생성되는 각 평문들은 훈련에 사용한 자료에 따라 다름을 알 수 있다. 예를 들어, 암호학 문서를 사용했을 때는 암호학 문서에 나올 법한 구 또는 절이, 클래식 음악 문서를 사용했을 때는 음악 문서에 나올 법한 구 또는 절이 가짜 평문(P2)으로 생성됨이 도시되어 있다.

[0130] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령

어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0131] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0132] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0133] 10: 거부적 암호화 장치

100: 거부적 인코딩부

200: 거부적 디코딩부

300: 암호화부

400: 복호화부

500: 데이터베이스

K1, Kdecrpyt: 진짜 키(진짜 복호화 암호키)

K2, K3, Kdecrypt_fake: 가짜 키(가짜 복호화 암호키)

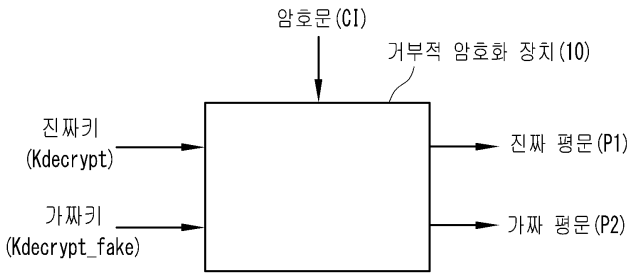
C1: 암호문(C1)

P1: 진짜 평문(P1)

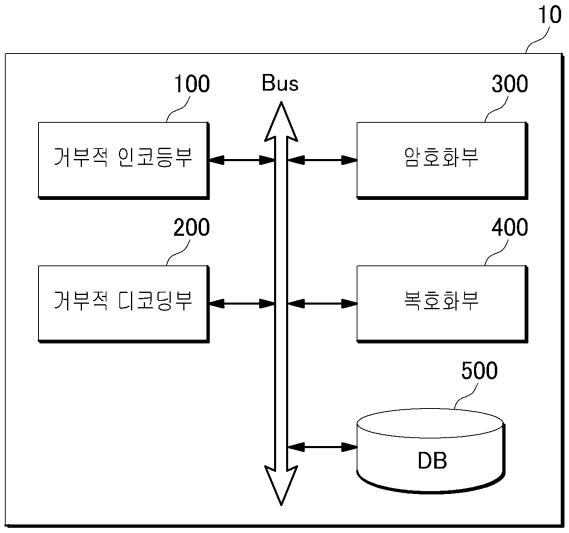
P2: 가짜 평문(P2)

도면

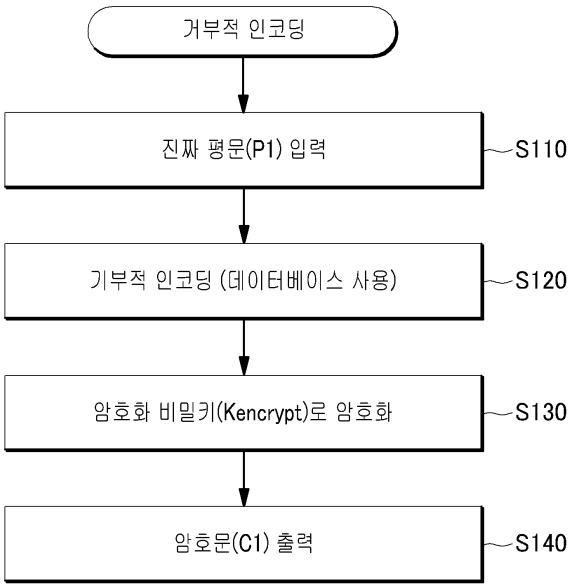
도면1



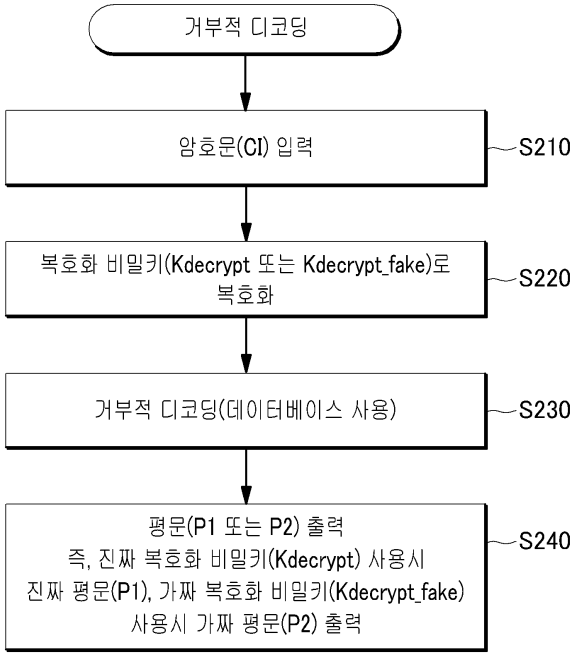
도면2


10
100
Bus
300
거부적 인코등부
암호화부
200
400
거부적 디코딩부
복호화부
500
DB

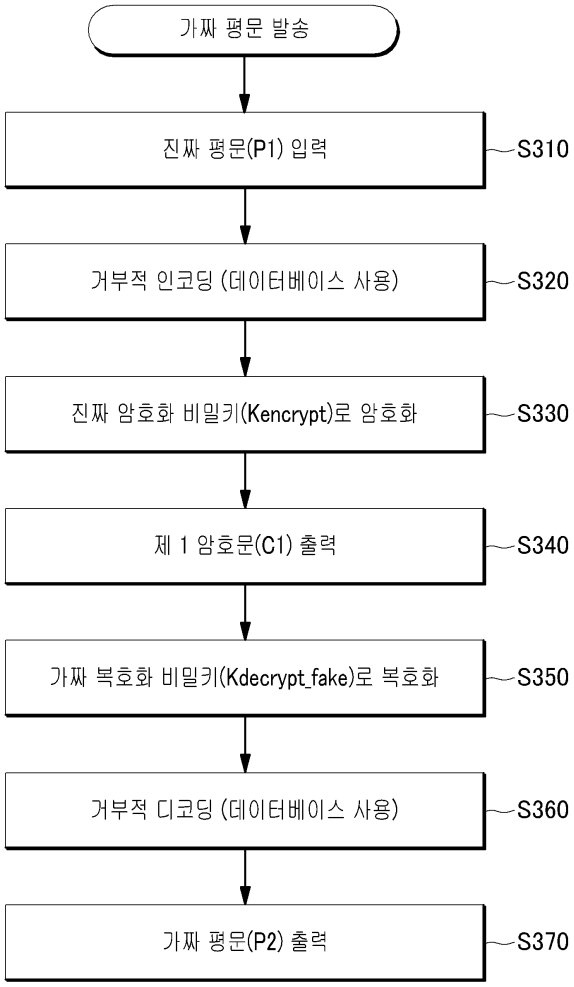
도면3


거부적 인코딩
진짜 평문(P1) 입력
S110
기부적 인코딩 (데이터베이스 사용)
S120
암호화 비밀키(Kencrypt)로 암호화
S130
암호문(C1) 출력
S140

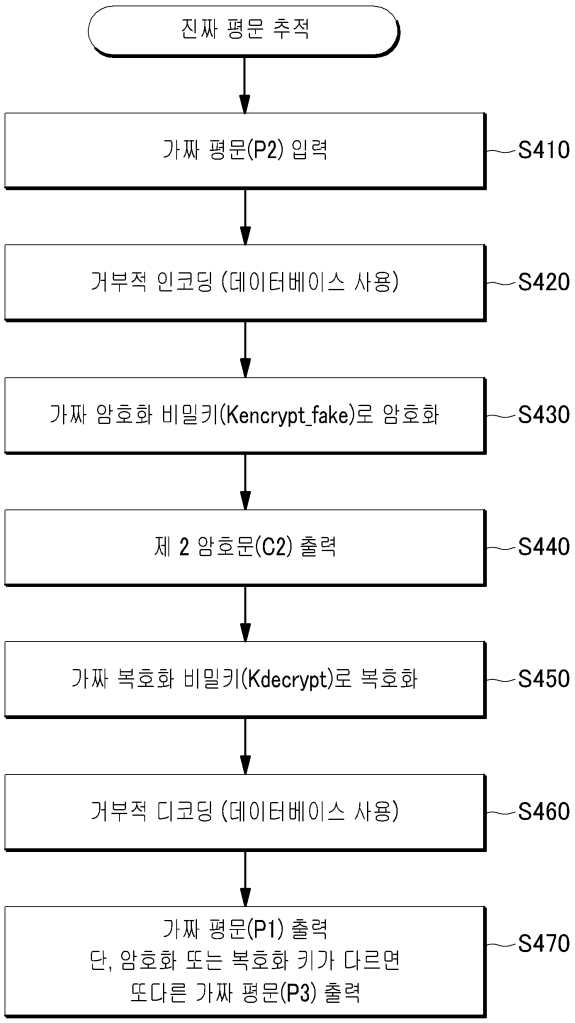
도면4


거부적 디코딩
암호문(CI) 입력
S210
복호화 비밀키(Kdecrypt 또는 Kdecrypt_fake)로 복호화
S220
거부적 디코딩(데이터베이스 사용)
S230
평문(P1 또는 P2) 출력
즉, 진짜 복호화 비밀키(Kdecrypt) 사용시 진짜 평문(P1), 가짜 복호화 비밀키(Kdecrypt_fake) 사용시 가짜 평문(P2) 출력
S240

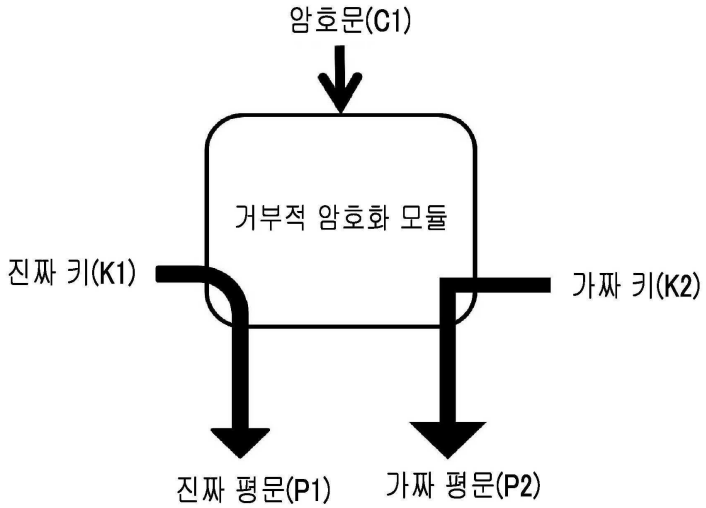
도면5


가짜 평문 발송
진짜 평문(P1) 입력
S310
거부적 인코딩 (데이터베이스 사용)
S320
진짜 암호화 비밀키(Kencrypt)로 암호화
S330
제 1 암호문(C1) 출력
S340
가짜 복호화 비밀키(Kdecrypt_fake)로 복호화
S350
거부적 디코딩 (데이터베이스 사용)
S360
가짜 평문(P2) 출력
S370

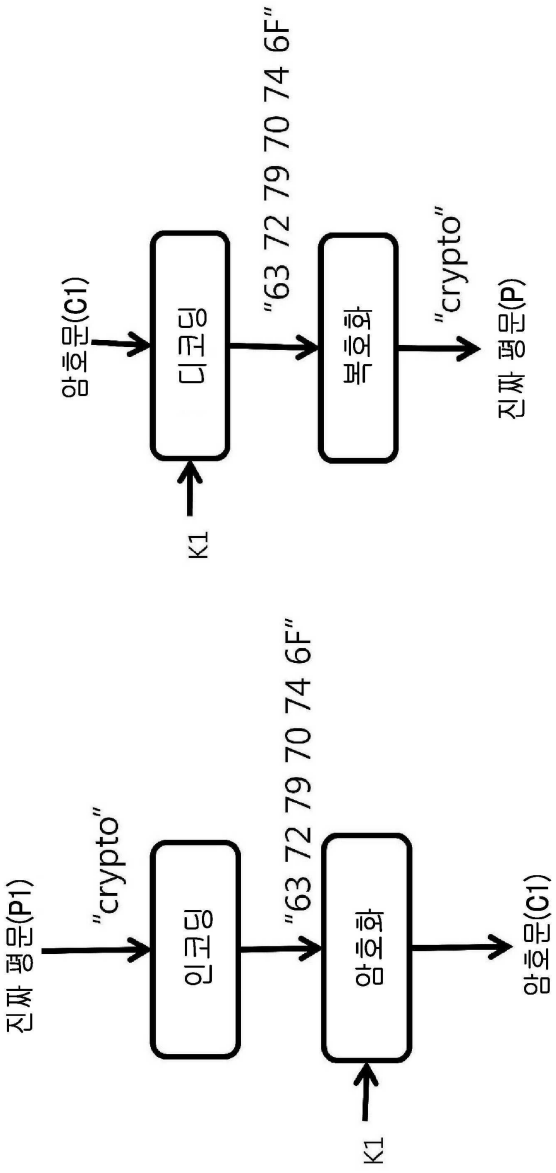
도면6


진짜 평문 추적
가짜 평문(P2) 입력
S410
거부적 인코딩 (데이터베이스 사용)
S420
가짜 암호화 비밀키(Kencrypt_fake)로 암호화
S430
제 2 암호문(C2) 출력
S440
가짜 복호화 비밀키(Kdecrypt)로 복호화
S450
거부적 디코딩 (데이터베이스 사용)
S460
가짜 평문(P1) 출력
단, 암호화 또는 복호화 키가 다르면
또다른 가짜 평문(P3) 출력
S470

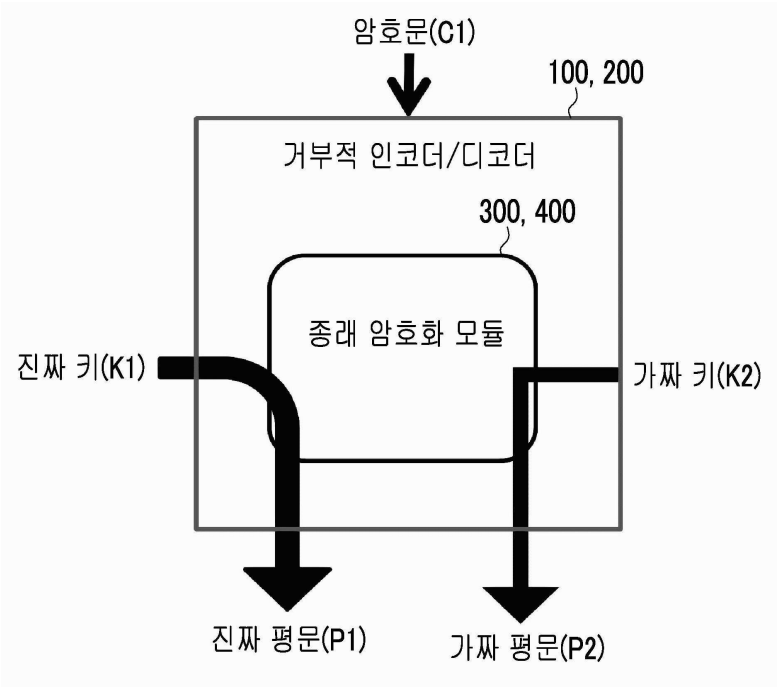
도면7


암호문(C1)
거부적 암호화 모듈
진짜 키(K1)
가짜 키(K2)
진짜 평문(P1)
가짜 평문(P2)

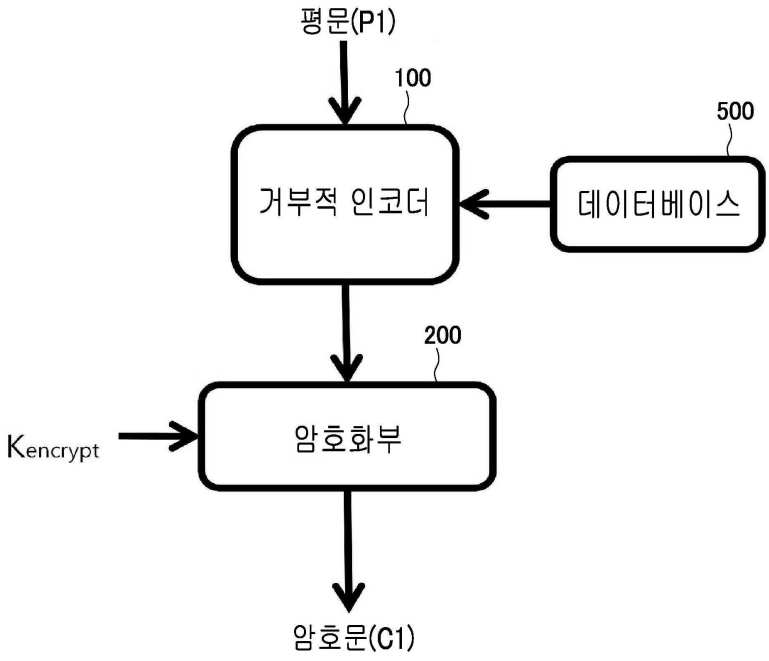
도면8


암호문(C1)
디코딩
"63 72 79 70 74 6F"
복호화
"crypto"
진짜 평문(P)
K1
진짜 평문(P1)
"crypto"
인코딩
"63 72 79 70 74 6F"
암호화
암호문(C1)
K1

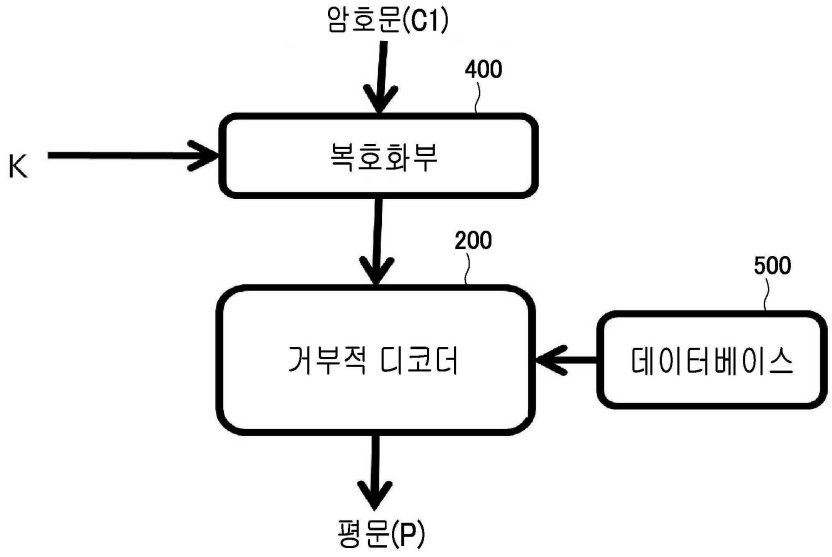
도면9


암호문(C1)
100, 200
거부적 인코더/디코더
300, 400
종래 암호화 모듈
진짜 키(K1)
가짜 키(K2)
진짜 평문(P1)
가짜 평문(P2)

도면10


평문(P1)
100
500
거부적 인코더
데이터베이스
200
Kencrypt
암호화부
암호문(C1)

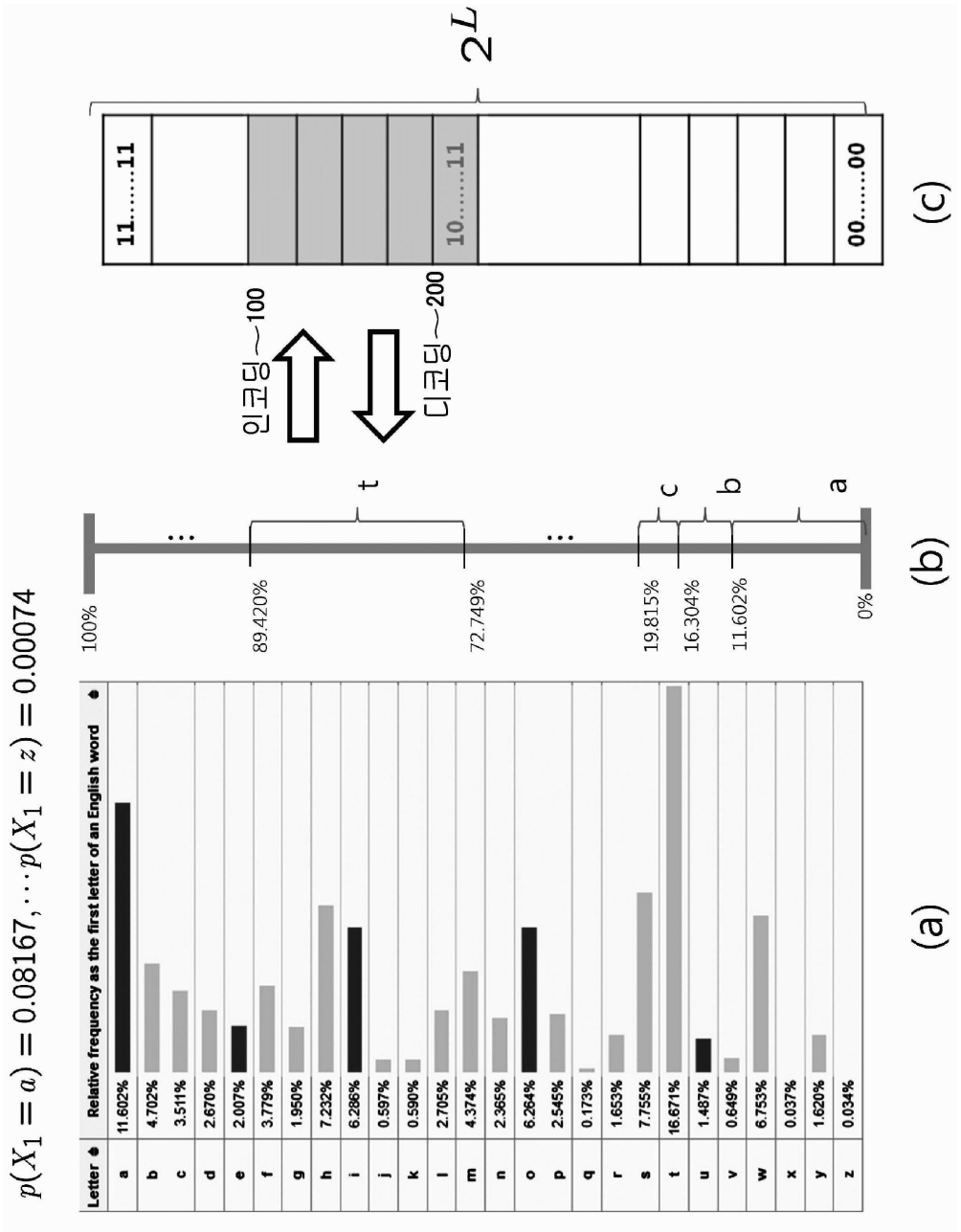
도면11



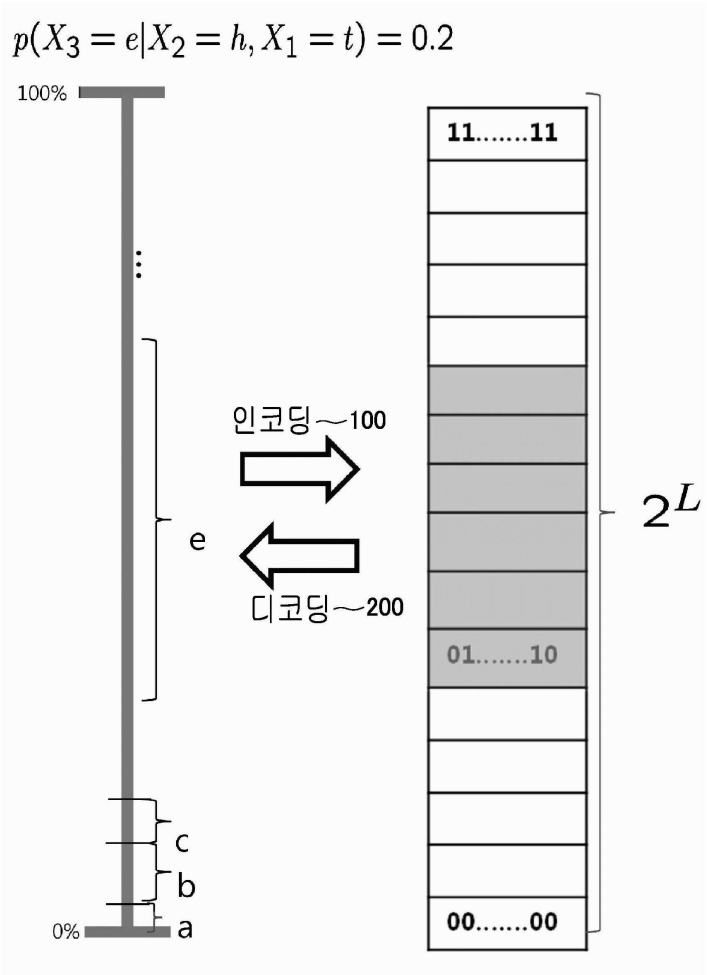
If $K = K_{decrypt}$, $P = P1$

If $K \neq K_{decrypt}$, $P \neq P1$

도면12


$p(X_1 = a) = 0.08167, \cdots p(X_1 = z) = 0.00074$
Letter
Relative frequency as the first letter of an English word
a 11.602%
b 4.702%
c 3.511%
d 2.670%
e 2.007%
f 3.779%
g 1.950%
h 7.232%
i 6.286%
j 0.597%
k 0.590%
l 2.705%
m 4.374%
n 2.365%
o 6.264%
p 2.545%
q 0.173%
r 1.653%
s 7.755%
t 16.671%
u 1.487%
v 0.649%
w 6.753%
x 0.037%
y 1.620%
z 0.034%
(a)
100%
89.420%
72.749%
19.815%
16.304%
11.602%
0%
t
c
b
a
(b)
인코딩~100
디코딩~200
2^L
11.....11
10.....11
00.....00
(c)

도면13



도면14

학습 데이터	진짜 키(K1) 사용	임의로 선택된 가짜 키(K2) 사용	임의로 선택된 가짜 키(K3) 사용
NASA 문서	'deniable encryption...'	'the scout's payload ac'	'the spacecraft and the'
로미오와 줄리엣 (소설)	'deniable encryption...	'what show the project'	'scene iii. scene iii'
암호학 문서	'deniable encryption...	'the secret key signatu'	'the probabilistic tech'
성경	'deniable encryption...	'and the children of th'	'and the lord was not b'
클래식 음악 문서	'deniable encryption...	'sym orch phil. Classic'	'beethoven l.v. sym com'