(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년12월08일
(11) 등록번호 10-1469857
(24) 등록일자 2014년12월01일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G06F 7/00* (2006.01)
(21) 출원번호 10-2013-0091749
(22) 출원일자 2013년08월01일
심사청구일자 2013년08월01일
(56) 선행기술조사문헌
KR1020120070874 A*
KR101106604 B1
JP2012073816 A
US20050147240 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
정재열
서울 성북구 안암로9가길 55, 304호 (안암동5가)
정익래
서울 광진구 긴고랑로4길 53, 203호 (중곡동, 호동아파트)
(74) 대리인
특허법인엠에이피에스

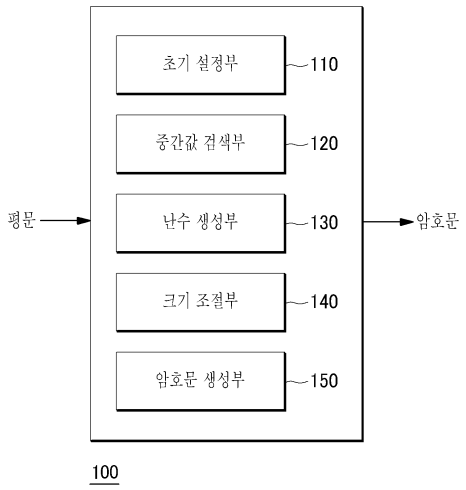
전체 청구항 수 : 총 10 항 심사관 : 구본재

(54) 발명의 명칭 **암호문 생성 장치 및 방법**

(57) 요 약

본 발명에 암호문 생성 장치는 복수의 파라미터 값에 기초하여 평문 공간, 암호문 공간 및 비밀키를 설정하는 초기 설정부, 상기 평문 공간상에서 중간값을 검색하는 중간값 검색부, 균등 분포에 기초하여 상기 암호문 공간상에서 상기 중간값에 대응하는 난수를 생성하는 난수 생성부, 상기 검색된 중간값에 기초하여 상기 평문 공간의 크기를 조절하고, 상기 생성된 난수에 기초하여 상기 암호문 공간의 크기를 조절하는 크기 조절부 및 암호화하기 위한 평문과 상기 중간값이 일치하는 경우, 상기 중간값과 대응하는 난수를 선택하여 최종 암호문으로 생성하는 암호문 생성부를 포함한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 KI002113
부처명 지식경제부
연구관리전문기관 한국산업기술평가관리원
연구사업명 SW컴퓨팅산업원천기술개발
연구과제명 Car-헬스케어 보안 기술 개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2013.03.01 ~ 2014.02.28

특허청구의 범위

청구항 1

암호문 생성 장치에 있어서,

복수의 파라미터 값에 기초하여 평문 공간, 암호문 공간 및 비밀키를 설정하는 초기 설정부,

상기 평문 공간상에서 중간값을 검색하는 중간값 검색부,

균등 분포에 기초하여 상기 암호문 공간상에서 상기 중간값에 대응하는 난수를 생성하는 난수 생성부,

상기 검색된 중간값에 기초하여 상기 평문 공간의 크기를 조절하고, 상기 생성된 난수에 기초하여 상기 암호문 공간의 크기를 조절하는 크기 조절부 및

암호화하기 위한 평문과 상기 중간값이 일치하는 경우, 상기 중간값과 대응하는 난수를 선택하여 최종 암호문으로 생성하는 암호문 생성부를 포함하되,

상기 난수 생성부는 상기 평문 공간과 대응되는 암호문 공간을 제외한 나머지 암호문 공간에 포함된 난수를 생성하는 것인 암호문 생성 장치.

청구항 2

제 1 항에 있어서,

상기 파라미터는 상기 평문의 최대 크기, 상기 암호문의 최대 크기 및 상기 비밀키의 길이인 것인 암호문 생성 장치.

청구항 3

제 1 항에 있어서,

상기 난수 생성부는 상기 중간값과 상기 비밀키를 기준값으로 설정하고, 상기 기준값에 기초하여 난수를 생성하는 것인 암호문 생성 장치.

청구항 4

제 1 항에 있어서,

상기 초기 설정부는 상기 암호문 공간의 크기를 상기 평문 공간의 크기보다 더 크게 설정하는 것인 암호문 생성 장치.

청구항 5

삭제

청구항 6

암호문 생성 장치에서의 암호문 생성 방법에 있어서,

(a) 평문 공간, 암호문 공간 및 비밀키를 설정하는 단계,

(b) 상기 평문 공간상에서 중간값을 검색하는 단계,

(c) 상기 암호문 공간에서 균등 분포에 기초하여 상기 중간값에 대응하는 난수를 생성하는 단계,

(d) 상기 평문 공간 및 상기 암호문 공간의 크기를 조절하는 단계 및

(e) 최종 암호문을 생성하는 단계를 포함하되,

상기 (d) 단계는 상기 중간값에 기초하여 상기 평문 공간을 조절하고, 상기 난수에 기초하여 상기 암호문 공간을 조절하며,

상기 (e) 단계는 암호화하기 위한 평문과 상기 중간값이 일치하는 경우, 상기 중간값에 대응하는 난수를 최종 암호문으로 선택하되,

상기 암호화하기 위한 평문과 상기 중간값이 일치할 때까지 상기 (b) 단계 내지 상기 (d) 단계를 반복하고,

상기 난수는 상기 평문 공간과 대응되는 암호문 공간을 제외한 나머지 암호문 공간에서 생성되는 것인 암호문 생성 방법.

청구항 7

제 6 항에 있어서,

상기 (a) 단계는 파라미터 값을 결정하는 단계를 더 포함하되,

상기 파라미터는 상기 평문의 최대 크기, 상기 암호문의 최대 크기 및 상기 비밀키의 길이인 것인 암호문 생성 방법.

청구항 8

제 6 항에 있어서,

상기 (c) 단계는,

상기 중간값과 상기 비밀키를 기준값으로 설정하고, 상기 기준값에 기초하여 난수를 생성하는 것인 암호문 생성 방법.

청구항 9

제 6 항에 있어서,

상기 암호문 공간의 크기는 상기 평문 공간의 크기보다 더 크게 설정되는 것인 암호문 생성 방법.

청구항 10

암호문 생성 장치에 의해 암호화된 암호문을 복호화하기 위한 장치에 있어서,

평문 공간상에서 중간값을 검색하는 복호화 중간값 검색부,

암호문 공간에서 균등 분포에 기초하여 상기 중간값에 대응하는 난수를 생성하는 복호화 난수 생성부,

상기 검색된 중간값에 기초하여 상기 평문 공간의 크기를 조절하고, 상기 생성된 난수에 기초하여 상기 암호문 공간의 크기를 조절하는 복호화 크기 조절부 및

암호문과 상기 생성된 난수가 일치할 경우, 상기 난수와 대응되는 중간값을 최종 복호문으로 선택하는 복호문 선택부를 포함하되,

상기 복호화 중간값 검색부는 상기 암호문 공간과 대응되는 평문 공간을 제외한 나머지 평문 공간에 포함된 중간값을 검색하는 것인 복호화 장치.

청구항 11

암호문 생성 장치에 의해 암호화된 암호문을 복호화하는 방법에 있어서,

(a) 평문 공간상에서 중간값을 검색하는 단계,

(b) 암호문 공간에서 균등 분포에 기초하여 상기 중간값에 대응하는 난수를 생성하는 단계,

(c) 상기 평문 공간 및 상기 암호문 공간의 크기를 조절하는 단계 및

(d) 최종 복호문을 선택하는 단계를 포함하되,

상기 (c) 단계는 상기 중간값에 기초하여 상기 평문 공간을 조절하고, 상기 난수에 기초하여 상기 암호문 공간을 조절하며,

상기 (d) 단계는 상기 생성된 난수와 암호문이 일치하는 경우, 상기 난수에 대응하는 중간값을 최종 복호문으로

선택하되,

상기 암호문과 상기 난수가 일치할 때까지 상기 (a) 단계 내지 상기 (c) 단계를 반복하고,

상기 중간값은 암호문 공간과 대응하는 평문 공간을 제외한 나머지 평문 공간에서 검색되는 것인 복호화 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 암호문 생성 장치 및 방법에 관한 것으로서, 구체적으로 순서 유지 암호화 기술을 이용하여 데이터를 암호화할 수 있는 암호문 생성 장치 및 방법과, 암호문을 복호화할 수 있는 복호화 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근 들어 정보화 사회가 고도화됨에 따라, 개인 및 기업 등에서 처리하는 데이터 양이 점점 증가하고 있는 추세이다. 이에 따라 데이터를 효율적으로 관리하기 위해 요구되는 자원의 양도 함께 증가하고 있다. 이와 더불어, 데이터를 효율적으로 관리하기 위해서 필요로 하는 비용 또한 증가하고 있으며, 이를 위해 외부 데이터베이스 서비스를 이용하여 정보를 저장하기도 한다.

[0003] 그러나 외부 데이터베이스를 활용함에도 불구하고 주민등록번호나 계좌번호와 같은 개인 정보 유출 사례가 증가하고 있어 사회적으로 문제가 되고 있다. 이와 같은 문제를 해결하기 위한 방법 중 하나로서 순서 유지 암호화 기술을 이용하여 데이터를 암호화하는 방법이 있다.

[0004] 순서 유지 암호화 기술은 평문의 순서를 암호문에서도 그래도 유지하는 암호화 기술이다. 예를 들어, 순서가 존재하는 두 개의 평문 P1, P2에 대하여 순서 유지 암호화 함수인 OPE_Enc를 이용하여 암호화하면, 두 개의 암호문 OPE_Enc(P1), OPE_Enc(P2)가 만들어진다. 이때, 평문의 대소 관계가 P1<P2일 경우, 두 암호문에도 평문과 같이 OPE_Enc(P1)<OPE_Enc(P2)의 관계가 유지된다.

[0005] 이와 같이 순서 유지 암호화 기술은 암호문을 통해 평문의 대소 관계를 알 수 있기 때문에 다른 암호들에 비하여 안전성이 다소 떨어지게 된다. 그러나 이러한 특징으로 인하여 다양한 분야에서 활용할 수 있으며, 특히 데이터베이스의 보안 분야에서 활용도가 높은 편이다.

[0006] 일반적인 데이터베이스 보안은 데이터를 암호화하여 저장하는 것으로 데이터를 보호할 수 있지만, 데이터베이스 본래의 목적인 데이터 검색에 있어 심각한 효율성 저하를 야기시킨다. 예를 들어, 1부터 100 사이의 평문을 검색할 경우, 데이터베이스에 저장된 모든 암호문을 복호화한 후 그 데이터를 검색하여 검색 결과를 사용자에게 알려준다. 하지만, 순서 유지 암호화 기술을 사용할 경우에는 1의 암호문과 100의 암호문 사이의 암호문들만 복호화해서 사용자에게 알려주면 되기 때문에 매우 효율적이다.

[0007] 한편, 순서 유지 암호화 기술은 2004년도에R. Agrawal, J. Kiernan, R. Srikant, Y. Xu에 의해 발표된 ” Order-Preserving Encryption for Numeric Data” 표제의 논문에서 처음으로 제안되었다. 하지만, 해당 기법의 경우 저장해야 하는 비밀 정보가 매우 많으며, 데이터의 추가 및 삭제가 자유롭지 못해 현실적으로 사용하기에 부적합하다는 문제가 있다.

[0008] 이와 더불어, 2009년도에 A. Boldyreva, N. Chenette, Y. Lee, A. O'Neill의해 발표된 논문인 “Order-Preserving Symmetric Encryption.”에서는 높은 안전성을 만족하는 순서 유지 암호화 기술이 제안되었다. 그러나 이 기법은 암호화할 때, 사용되는 난수 생성 함수가 복잡하여 비효율적이기 때문에 실제 대용량 데이터베이스에서 사용하기 부적합하다는 문제가 있다.

[0009] 이와 관련하여 한국공개특허 제2009-0066497호(발명의 명칭: 데이터 암호문 생성 장치와 이를 이용한 암호화 방법)에는 순서 유지 암호화 기법과 순서 교란 기법을 이용하여 데이터를 암호화하고 이를 통해 데이터 검색을 제공하는데 적합한 데이터 암호문 생성 장치와 이를 이용한 암호화 방법이 개시되어 있다.

[0010] 또한, 한국공개특허 제2009-0066063호(발명의 명칭: 버킷 내 부분 순서 보존을 통한 데이터베이스 처리 방법)에는 데이터베이스에 숫자데이터를 안전하게 암호화하여 저장하고, 효율적으로 검색하는데 적합한 데이터베이스 암호화 및 검색 기술이 개시되어 있다.

[0011] 다만, 위 선행기술과 더불어 현재까지 제안된 대부분의 순서 유지 암호화 기술은 다음과 같은 문제점을 가지고

있다.

[0012] 첫째로, 암호화 및 복호화 연산이 효율적인 경우, 추가적인 저장 공간이 필요하거나 데이터의 추가 및 삭제가 비효율적이라는 문제점이 있다. 둘째로, 높은 안전성을 제공하는 기술의 경우, 암호화 및 복호화 연산이 매우 비효율적이라는 문제점이 있다. 셋째로, 길이가 긴 평문의 경우에는 블록 단위로 잘라서 각각을 암호화해야 하는 경우도 있으며, 이 경우 암호화할 수 있는 평문의 크기가 크지 않을 경우 전수조사에 취약하다는 문제점이 있다. 예를 들어, 5byte를 암호화할 수 있는 순서 유지 암호가 있다고 가정할 경우, 10byte 평문을 암호화하더라도 평문의 최대 안전성은 5byte밖에 보장받을 수 없게 된다.

[0013] 따라서, 암호화 및 복호화 연산이 매우 효율적으로 이루어질 뿐만 아니라 높은 안전성을 제공하며, 추가적인 제약 사항이 없어 실제 대용량 데이터베이스에서 사용 가능한 현실적인 순서 유지 암호화 기술이 필요한 실정이다. 이와 더불어 평문의 길이에 제약을 받지 않는 순서 유지 암호화 기술의 개발이 필요하다.

발명의 내용

해결하려는 과제

[0014] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 본 발명의 일부 실시예는 순서 유지 암호화 기술을 적용하여 데이터를 암호화하기 위한 것으로서, 평문 공간에서 중간값을 검색하고, 암호문 공간에서 균등 분포에 기초하여 중간값에 대응하는 난수를 생성하며, 평문 공간 및 암호문 공간의 크기를 조절하는 단계를 거쳐 최종 암호문을 생성하는 암호문 생성 장치 및 방법을 제공하는 것을 그 목적으로 한다.

[0015] 또한, 암호문 생성 장치에 의해 암호화된 암호문을 순서 유지 암호화 기술을 이용하여 복호화하는 복호화 장치 및 방법을 제공하는 것을 그 목적으로 한다.

과제의 해결 수단

[0016] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 암호문 생성 장치는 복수의 파라미터 값에 기초하여 평문 공간, 암호문 공간 및 비밀키를 설정하는 초기 설정부, 상기 평문 공간상에서 중간값을 검색하는 중간값 검색부, 균등 분포에 기초하여 상기 암호문 공간상에서 상기 중간값에 대응하는 난수를 생성하는 난수 생성부, 상기 검색된 중간값에 기초하여 상기 평문 공간의 크기를 조절하고, 상기 생성된 난수에 기초하여 상기 암호문 공간의 크기를 조절하는 크기 조절부 및 암호화하기 위한 평문과 상기 중간값이 일치하는 경우, 상기 중간값과 대응하는 난수를 선택하여 최종 암호문으로 생성하는 암호문 생성부를 포함한다.

[0017] 또한, 본 발명의 제 2 측면에 따른 암호문 생성 장치에서의 암호문 생성 방법은 (a) 평문 공간, 암호문 공간 및 비밀키를 설정하는 단계, (b) 상기 평문 공간상에서 중간값을 검색하는 단계, (c) 상기 암호문 공간에서 균등 분포에 기초하여 상기 중간값에 대응하는 난수를 생성하는 단계, (d) 상기 평문 공간 및 상기 암호문 공간의 크기를 조절하는 단계 및 (e) 최종 암호문을 생성하는 단계를 포함하되, 상기 (d) 단계는 상기 중간값에 기초하여 상기 평문 공간을 조절하고, 상기 난수에 기초하여 상기 암호문 공간을 조절하며, 상기 (e) 단계는 암호화하기 위한 평문과 상기 중간값이 일치하는 경우, 상기 중간값에 대응하는 난수를 최종 암호문으로 선택하되, 상기 암호화하기 위한 평문과 상기 중간값이 일치할 때까지 상기 (b) 단계 내지 상기 (d) 단계를 반복한다.

[0018] 또한, 본 발명의 제 3 측면에 따른 암호문 생성 장치에 의해 암호화된 암호문을 복호화하기 위한 장치는 평문 공간상에서 중간값을 검색하는 복호화 중간값 검색부, 암호문 공간에서 균등 분포에 기초하여 상기 중간값에 대응하는 난수를 생성하는 복호화 난수 생성부, 상기 검색된 중간값에 기초하여 상기 평문 공간의 크기를 조절하고, 상기 생성된 난수에 기초하여 상기 암호문 공간의 크기를 조절하는 복호화 크기 조절부 및 암호문과 상기 생성된 난수가 일치할 경우, 상기 난수와 대응되는 중간값을 최종 복호문으로 선택하는 복호화문 선택부를 포함한다.

[0019] 또한, 본 발명의 제 4 측면에 따른 암호문 생성 장치에 의해 암호화된 암호문을 복호화하는 방법은 (a) 평문 공간상에서 중간값을 검색하는 단계, (b) 암호문 공간에서 균등 분포에 기초하여 상기 중간값에 대응하는 난수를 생성하는 단계, (c) 상기 평문 공간 및 상기 암호문 공간의 크기를 조절하는 단계 및 (d) 최종 복호문을 선택하는 단계를 포함하되, 상기 (c) 단계는 상기 중간값에 기초하여 상기 평문 공간을 조절하고, 상기 난수에 기초하여 상기 암호문 공간을 조절하며, 상기 (d) 단계는 상기 생성된 난수와 암호문이 일치하는 경우, 상기 난수에 대응하는 중간값을 최종 복호문으로 선택하되, 상기 암호문과 상기 난수가 일치할 때까지 상기 (a) 단계 내지 상기 (c) 단계를 반복한다.

발명의 효과

[0020] 전술한 본 발명의 과제 해결 수단의 어느 실시예에 의하면, 평문을 분할하지 않고 그대로 암호화하기 때문에, 블록 단위로 암호화한 후, 블록에 해당하는 암호문을 붙여 전체 암호문을 만들 필요가 없다. 따라서, 기존의 블록 단위로 암호화하는 대칭키 기반의 순서 유지 암호화보다 더 높은 안전성을 가질 수 있다.

[0021] 또한, 암호화할 때, 균등 분포를 이용하기 때문에 각 평문에 해당하는 암호문을 유추하기 어려우며, 종래의 순서 유지 암호화 기술에 비해 암호화 및 복호화 연산이 효율적이다.

[0022] 이와 더불어, 암호화 생성 단계에서 다양한 파라미터를 설정할 수 있어, 최적의 효율성 및 안전성을 제공할 수 있다.

도면의 간단한 설명

[0023] 도 1은 본 발명의 일 실시예에 따른 암호문 생성 장치의 블록도이다.

도 2 내지 도 6은 본 발명에 따른 암호문 생성 과정의 일 예시를 도시한 도면이다.

도 7은 본 발명의 일 실시예에 따른 암호문 생성 방법의 순서도이다.

도 8은 본 발명의 일 실시예에 따른 복호화 장치의 블록도이다.

도 9는 본 발명의 일 실시예에 따른 복호화 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0024] 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 도면 부호를 붙였다.

[0025] 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.

[0026] 도 1은 본 발명의 일 실시예에 따른 암호문 생성 장치(100)의 블록도이다.

[0027] 본 발명에 따른 암호문 생성 장치(100)는 초기 설정부(110), 중간값 검색부(120), 난수 생성부(130), 크기 조절부(140) 및 암호문 생성부(150)를 포함한다.

[0028] 참고로, 본 발명의 실시예에 따른 도 1 및 아래에서 설명할 도 8에 도시된 구성 요소들은 소프트웨어 또는 FPGA(Field Programmable Gate Array) 또는 ASIC(Application Specific Integrated Circuit)와 같은 하드웨어 구성 요소를 의미하며, 소정의 역할들을 수행한다.

[0029] 그렇지만 '구성 요소들'은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, 각 구성 요소는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다.

[0030] 따라서, 일 예로서 구성 요소는 소프트웨어 구성 요소들, 객체지향 소프트웨어 구성 요소들, 클래스 구성 요소들 및 태스크 구성 요소들과 같은 구성 요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다.

[0031] 구성 요소들과 해당 구성 요소들 안에서 제공되는 기능은 더 작은 수의 구성 요소들로 결합되거나 추가적인 구성 요소들로 더 분리될 수 있다.

[0032] 초기 설정부(110)는 복수의 파라미터 값에 기초하여 평문 공간, 암호문 공간 및 비밀키를 설정한다. 이때, 파라미터는 평문의 최대 크기, 암호문의 최대 크기 및 비밀키의 길이로 설정할 수 있다.

[0033] 초기 설정부(110)는 Setup(1^n)→params 함수를 이용하여 순서 유지 암호화 기술에서 사용할 다양한 파라미터 값

(params)을 결정하게 된다. 안전성 파라미터, 즉 사용자에 의해 선택된 안전성 레벨인 1^n에 기초하여 평문의 최대 크기 |plaintext|, 암호문의 최대 크기 |ciphertext| 및 비밀키의 길이 |key|를 설정하고, params=(|plaintext|, |ciphertext|, |key|) 함수를 출력하여 각 파라미터를 설정한다.

[0034] 또한, 초기 설정부(110)는 위 파라미터 값을 이용하여 실제 암호화 및 복호화 단계에서 사용할 비밀키를 Key(params)→key 함수를 이용하여 생성할 수 있다. 생성된 키는 난수를 생성할 때 기준값으로 사용될 수 있으며, 평문과 암호문의 크기 및 안전성을 고려한 결과에 따라 비밀키의 길이를 설정하게 된다.

[0035] 한편, 초기 설정부(110)는 암호문 공간의 크기를 평문 공간의 크기보다 더 크게 설정할 수 있다. 암호문 공간의 크기를 평문의 공간 크기보다 더 크게 설정하고, 이진 검색 기법을 통해서 평문의 공간을 줄여나가면, 암호화하기 위한 평문에 대응되는 암호문을 찾을 수 있다.

[0036] 중간값 검색부(120)는 평문 공간상에서 중간값을 검색한다. 이때, 중간값 검색부(120)는 위의 파라미터 값과 평문을 이용하여 중간값을 검색할 수 있으며, 이때 중간값 검색부(120)는 중간값을 검색하기 위하여 Middle(params, plaintext) →middle 함수를 이용할 수 있다. 중간값을 검색하기 위한 함수는 평문 공간에서만 적용되며, 암호문 공간에서는 적용할 수 없다.

[0037] 난수 생성부(130)는 균등 분포에 기초하여 암호문 공간상에서 중간값 검색부(120)에 의해 검색된 중간값에 대응하는 난수를 생성한다. 이때, 난수 생성부(130)는 중간값과 비밀키를 기준값으로 설정하고, 설정된 기준값에 기초하여 난수를 생성할 수 있다. 중간값과 비밀키를 기준값으로 설정함으로써, 동일한 평문을 암호화할 때 이전 암호문과 동일한 암호문을 생성할 수 있다.

[0038] 난수는 Rand(params, key, middle)→rand 함수를 이용하여 생성할 수 있으며, 균등 분포를 이용하기 때문에 암호문 공간에서 각 난수가 생성될 확률은 동일하다. 난수를 생성하는 위 함수는 암호문 공간에서만 적용되며, 평문 공간에서는 적용할 수 없다.

[0039] 한편, 초기 설정부(110)는 암호문 공간의 크기를 평문 공간의 크기보다 더 크게 설정할 수 있으므로, 이에 따라 난수 생성부(130)는 평문 공간과 대응되는 암호문 공간을 제외한 나머지 암호문 공간에 포함된 난수를 생성할 수 있다.

[0040] 크기 조절부(140)는 중간값 검색부(120)에 의해 검색된 중간값에 기초하여 평문 공간의 크기를 조절하고, 난수 생성부(130)에 의해 생성된 난수에 기초하여 암호문 공간의 크기를 조절한다.

[0041] 암호문 생성부(150)는 암호화하기 위한 평문과 중간값이 일치하는 경우, 중간값과 대응하는 난수를 선택하여 최종 암호문으로 생성한다. 이때, 암호문 생성부(150)는 OPE_Enc(params, plaintext, key)→cipherxext 함수를 이용하여 주어진 평문에 대해 비밀키를 이용하여 암호화를 수행하게 된다.

[0042] 한편, 암호화하기 위한 평문과 중간값이 불일치하는 경우, 중간값 검색부(120)는 크기가 조절된 평문에 대하여 다시 중간값을 검색하게 된다. 중간값이 검색되면, 난수 생성부(130)는 크기가 조절된 암호문 공간상에서 다시 난수를 생성하고, 크기 조절부(140)는 중간값 및 난수에 기초하여 평문 공간 및 암호문 공간의 크기를 줄여나가게 된다.

[0043] 이와 같은 단계는 암호화하기 위한 평문과 중간값이 일치할 때까지 반복하여 수행하며, 암호화하기 위한 평문과 중간값이 일치할 때의 중간값에 대응하는 난수를 선택하여 최종 암호문으로 생성하게 된다.

[0044] 이하에서는 도 2 내지 도 6을 참조하여 본 발명에 따른 암호문 생성 장치(100)에서의 암호문 생성 과정을 예를 들어 설명하도록 한다.

[0045] 도 2 내지 도 6은 본 발명에 따른 암호문 생성 과정의 일 예시를 도시한 도면이다.

[0046] 도 2를 참조하면 평문의 공간이 10이고 암호문 공간이 30이라고 할 때, 암호화하기 위한 평문이 2일 경우, 먼저 평문 공간상에서 1~10의 중간값인 5와 대응되는 난수를 암호문 공간상에서 산출해야 한다. 중간값 5에 대응하는 암호문 공간상의 난수는 5에서 25 사이에서 생성될 수 있다. 이는 평문 공간상에서 1~4 및 6~10에 대응하는 암호문 공간을 남겨둬야 하기 때문이다.

[0047] 다음으로, 도 3 및 도 4를 참조하면, 평문 공간상에서 검색된 중간값인 5에 대응하는 난수 21을 암호문 공간상에서 생성한다. 이때 암호화하기 위한 평문은 2이고, 이는 중간값으로 검색된 5와는 상이하기 때문에 1~10으로 설정된 평문 공간의 크기를 1~5로 조절한다. 그리고 암호문 공간의 크기 역시 1~30을 1~21로 조절한다. 암호문 공간의 크기를 조절한 후, 도 2와 같이 평문 공간상에서 1~5의 중간값인 3을 검색하고, 평문 공간상의 1~3 및

3~5와 대응하는 암호문 공간인 1~3, 19~21을 제외한 나머지 공간인 3~19에서 중간값인 3에 대응하는 난수를 생성하게 된다.

[0048] 다음으로, 도 5 및 도 6을 참조하면, 평문 공간상에서 검색한 중간값인 3에 대응하는 난수인 7을 암호문 공간상에서 생성한다. 이때 검색된 중간값인 3은 암호화하기 위한 평문 2와 상이한 값에 해당하므로 다시 평문 공간을 1~3으로 조절하고, 암호문 공간을 1~7로 조절한다.

[0049] 평문 공간 및 암호문 공간의 크기를 조절한 후, 평문 공간상에서 중간값을 다시 검색해야 하며, 그 결과 중간값은 2로 검색되고 이는 암호화하기 위한 평문 2와 동일한 값에 해당하므로, 중간값인 2와 대응하는 암호문 공간상의 난수인 3을 선택하여 최종 암호문으로 생성하게 된다.

[0050] 도 7은 본 발명의 일 실시예에 따른 암호문 생성 방법의 순서도이다.

[0051] 암호문 생성 장치(100)에서의 암호문 생성 방법은 먼저, 평문 공간, 암호문 공간 및 비밀키를 설정한다(S110). 이때, 평문 공간, 암호문 공간 및 비밀키 설정은 복수의 파라미터 값에 기초하여 설정될 수 있다. 복수의 파라미터는 평문의 최대 크기, 암호문의 최대 크기 및 비밀키의 길이로 설정할 수 있다.

[0052] 한편, 평문 공간 및 암호문 공간 설정시, 암호문 공간의 크기는 평문 공간의 크기보다 더 크게 설정될 수 있다. 암호문 공간의 크기를 평문 공간의 크기보다 더 크게 설정하고, 이진 검색 기법을 통해서 평문 공간 크기를 점점 줄여나가게 되면 최종적으로 암호화하기 위한 평문에 대응되는 암호문을 찾을 수 있다.

[0053] 다음으로, 평문 공간상에서 중간값을 검색하고(S120), 암호문 공간에서 균등 분포에 기초하여 중간값에 대응하는 난수를 생성한다(S130). 난수 생성시에는 중간값과 비밀키를 기준값으로 설정하고, 기준값에 기초하여 난수를 생성할 수 있다.

[0054] 한편, 평문 공간 및 암호문 공간 설정시 암호문 공간의 크기를 평문 공간의 크기보다 더 크게 설정할 수 있으므로, 이에 따라 난수는 평문 공간에 대응되는 암호문 공간을 제외한 나머지 암호문 공간에서 생성될 수 있다.

[0055] 다음으로, 평문 공간 및 암호문 공간의 크기를 조절한다(S140). 이때, 평문 공간의 크기는 중간값에 기초하여 조절하고, 암호문 공간의 크기는 생성된 난수에 기초하여 조절한다.

[0056] 다음으로, 암호화하기 위한 평문과 중간값이 일치하는지 여부를 판단하고(S150), 판단 결과 동일한 경우 중간값에 대응하는 난수를 선택하여 최종 암호문을 생성한다(S160). 이와 달리, 암호화하기 위한 평문과 중간값이 불일치하는 경우, 중간값을 검색하는 단계, 중간값에 대응하는 난수를 생성하는 단계 및 평문 공간 및 암호문 공간의 크기를 조절하는 단계를 암호화하기 위한 평문과 중간값이 일치할 때까지 반복 수행한다.

[0057] 한편, 암호문 생성 방법의 각 단계에서 적용되는 함수와 관련된 설명은 도 1에서 설명하였으므로 이에 관한 설명은 생략하도록 한다.

[0058] 위에서 설명한 암호문 생성 장치(100) 및 방법을 이용하여 데이터를 암호화할 경우, 평문을 분할하지 않고 그대로 암호화하기 때문에, 블록 단위로 암호화한 후 블록에 해당하는 암호문을 다시 붙이는 단계를 수행할 필요가 없게 된다. 따라서, 기존의 블록단위로 암호화하는 대칭키 기반의 순서 유지 암호화 기술보다 더 높은 안전성을 가질 수 있다.

[0059] 또한, 암호화할 때, 균등 분포를 이용하기 때문에, 각 평문에 해당하는 암호문을 유추하기 어렵다는 효과가 있다. 이와 더불어 균등 분포를 이용할 경우 종래의 순서 유지 암호화 기술에 비하여 암호화 및 복호화 연산의 효율성을 높일 수 있다.

[0060] 이하에서는 도 8 및 도 9를 참조하여 암호화 장치에 의해 암호화된 암호문을 복호화하기 위한 장치 및 그 방법에 대하여 설명하도록 한다.

[0061] 도 8은 본 발명의 일 실시예에 따른 복호화 장치(200)의 블록도이다.

[0062] 본 발명의 일 실시예에 따른 암호문 생성 장치(100)에 의해 암호화된 암호문을 복호화하기 위한 장치는 복호화 중간값 검색부(210), 복호화 난수 생성부(220), 복호화 크기 조절부(230) 및 복호문 선택부(240)를 포함한다.

[0063] 복호화 장치(200)에서의 복호화 단계는 도 1 내지 도 7에서 설명한 암호화 단계와 동일한 방법에 의해 수행된다. 즉, 중간값을 찾는 함수를 수행하고, 암호문 공간에서 난수를 생성하는 함수를 이용하여 중간값과 난수를 매칭시킨다. 그 다음, 평문 공간과 암호문 공간의 크기를 조절하고, 암호문과 생성된 난수를 비교하여 동일할 경우 그때 매칭된 중간값을 복호문으로 선택한다.

[0064] 이와 같이, 복호화 장치(200)는 순서 유지 암호화 기법을 이용하여 암호문 생성 장치(100)에서의 방법과 반대 과정을 수행함으로써 복호문을 찾을 수 있다. 이하에서는 복호화 장치(200)의 각 구성요소를 설명하도록 한다.

[0065] 복호화 중간값 검색부(210)는 평문 공간상에서 중간값을 검색한다. 이때, 중간값을 검색하기 위한 함수는 도 1의 암호문 생성 장치(100)의 중간값 검색부(120)에서 이용한 함수를 이용하여 중간값을 검색할 수 있다. 이와 같은 함수는 평문 공간에서만 적용되며, 암호문 공간에서는 적용할 수 없다.

[0066] 복호화 난수 생성부(220)는 암호문 공간에서 균등 분포에 기초하여 중간값에 대응하는 난수를 생성한다. 난수 생성시 적용되는 함수는 암호문 생성 장치(100)의 난수 생성부(130)에서 이용한 함수와 동일하며, 이와 같은 함수는 암호문 공간에서만 적용되며, 평문 공간에서는 적용할 수 없다.

[0067] 복호화 크기 조절부(230)는 검색된 중간값에 기초하여 평문 공간의 크기를 조절하고, 생성된 난수에 기초하여 암호문 공간의 크기를 조절한다.

[0068] 복호문 선택부(240)는 암호문과 생성된 난수가 일치할 경우, 난수와 대응되는 중간값을 최종 복호문으로 선택한다. 이때, 복호문 선택부(240)는 OPE_Dec(params, cipherxext, key)→plaintext 함수를 이용하여 주어진 암호문에 대하여 복호문을 선택할 수 있다.

[0069] 한편, 생성된 난수와 암호문이 불일치할 경우, 복호화 중간값 검색부(210)는 크기가 조절된 평문에 대하여 다시 중간값을 검색한다. 중간값을 검색하면, 복호화 난수 생성부(220)는 크기가 조절된 암호문 공간상에서 다시 난수를 생성한다. 그리고 복호화 크기 조절부(230)는 중간값 및 난수에 기초하여 평문 공간 및 암호문 공간의 크기를 줄여나가게 된다.

[0070] 이와 같은 단계는 암호문과 생성된 난수가 일치할 때까지 반복하여 수행하며, 암호문과 생성된 난수가 일치할 때, 난수에 대응하는 중간값을 최종 복호문으로 선택하게 된다.

[0071] 도 9는 본 발명의 일 실시예에 따른 복호화 방법의 순서도이다.

[0072] 암호문 생성 장치(100)에 의해 암호화된 암호문을 복호화하는 방법은, 평문 공간 상에서 중간값을 검색하고(S210), 암호문 공간에서 균등 분포에 기초하여 중간값에 대응하는 난수를 생성한다(S220).

[0073] 다음으로 평문 공간 및 암호문 공간의 크기를 조절한다(S230).

[0074] 다음으로, 생성된 난수와 암호문이 일치하는지 여부를 판단하고(S240), 판단 결과 일치할 경우 난수에 대응하는 중간값을 최종 복호문으로 선택한다(S250). 이와 달리, 생성된 난수와 암호문이 불일치할 경우, 중간값을 검색하는 단계, 중간값에 대응하는 난수를 생성하는 단계 및 평문 공간 및 암호문 공간의 크기를 조절하는 단계를 생성된 난수가 암호문과 일치할 때까지 반복 수행한다.

[0075] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행 가능한 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 판독가능 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 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0076] 본 발명의 방법 및 시스템은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍처를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다.

[0077] 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.

[0078] 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 것으

로 해석되어야 한다.

부호의 설명

[0079] 100 : 암호문 생성 장치

110: 초기 설정부

120: 중간값 검색부

130: 난수 생성부

140: 크기 조절부

150: 암호문 생성부

200: 복호화 장치

210: 복호화 중간값 검색부

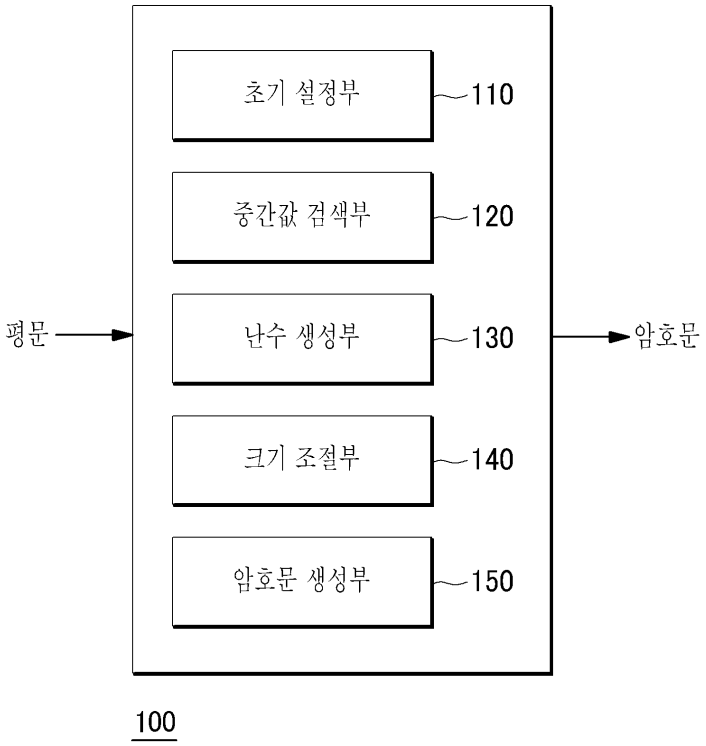
220: 복호화 난수 생성부

230: 복호화 크기 조절부

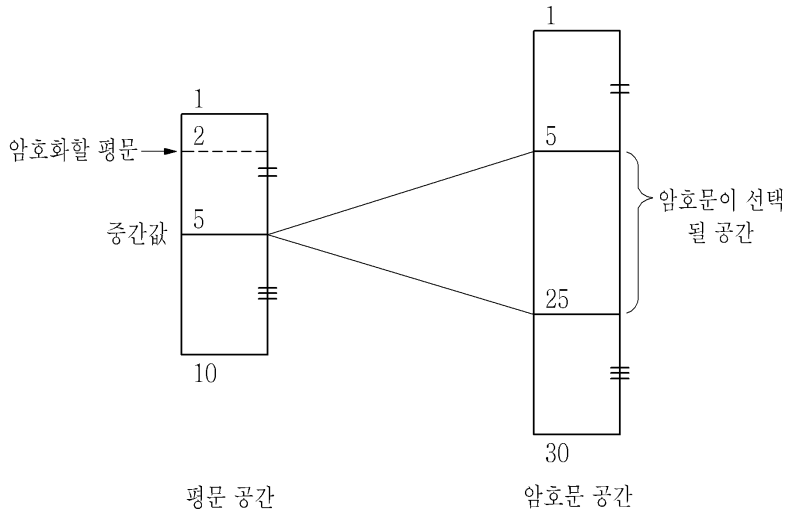
240: 복호문 선택부

도면

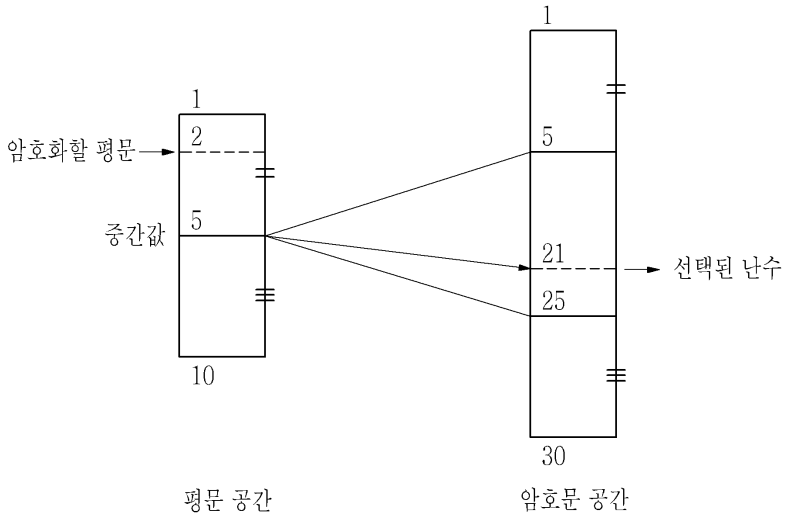
도면1



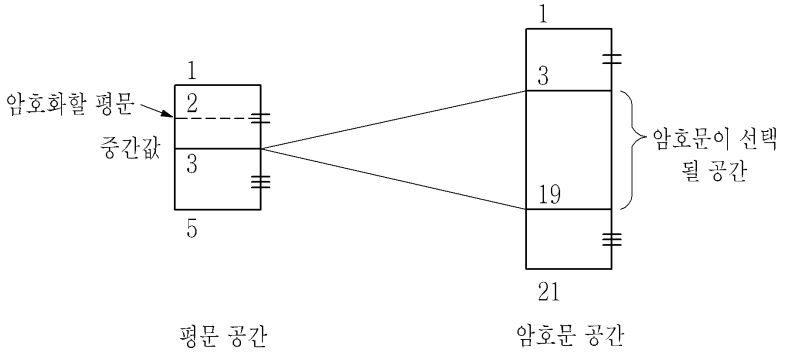
도면2


1
암호화할 평문
2
중간값
5
10
1
5
25
30
암호문이 선택
될 공간
평문 공간
암호문 공간

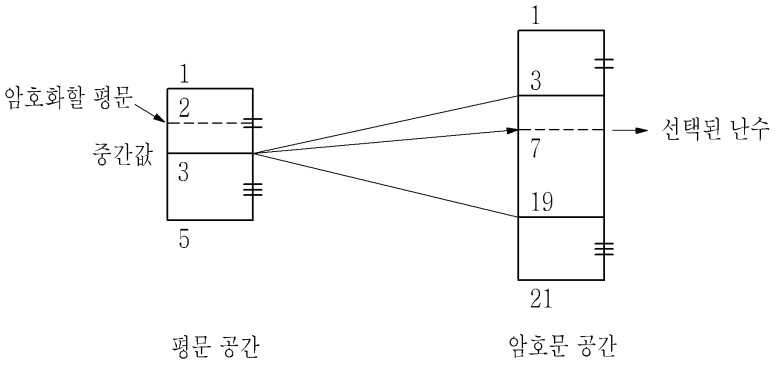
도면3


1
암호화할 평문
2
중간값
5
10
1
5
21
25
30
선택된 난수
평문 공간
암호문 공간

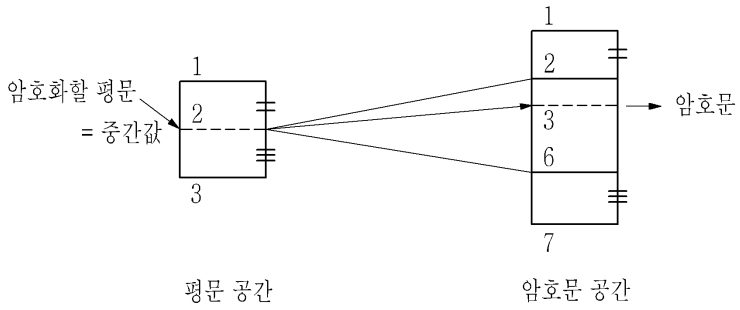
도면4


1
암호화할 평문
2
중간값
3
5
1
3
19
21
암호문이 선택
될 공간
평문 공간
암호문 공간

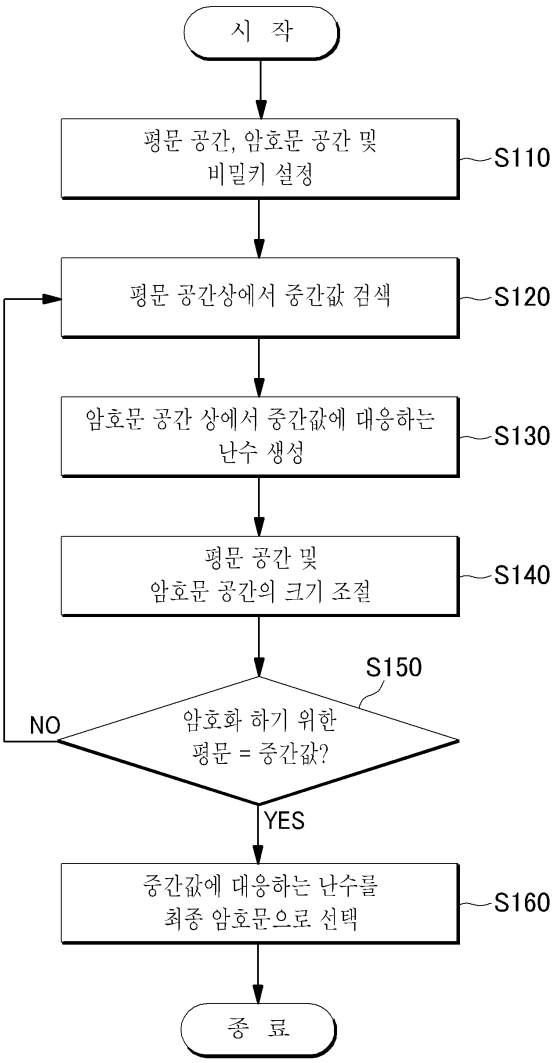
도면5


암호화할 평문
중간값
선택된 난수
1
2
3
5
1
3
7
19
21
평문 공간
암호문 공간

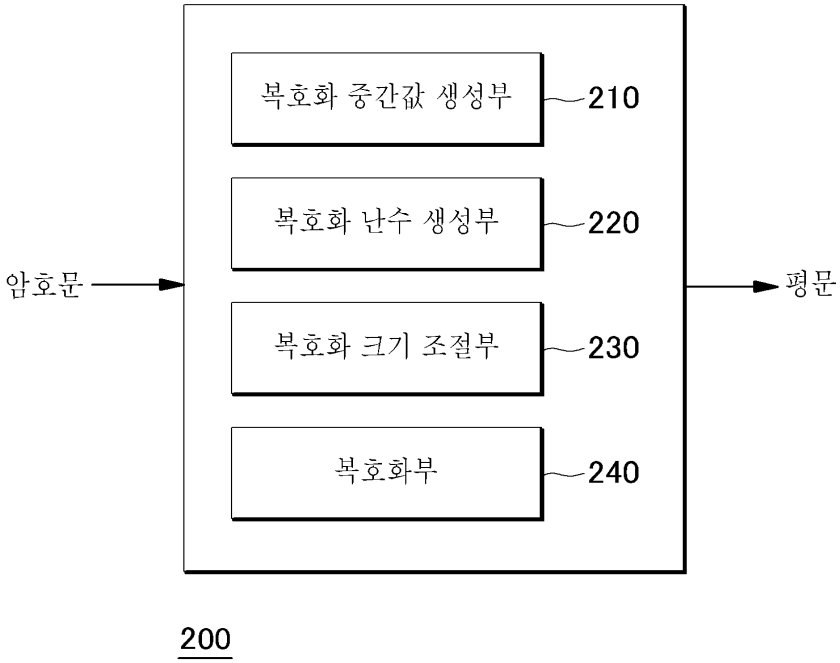
도면6


암호화할 평문
= 중간값
암호문
1
2
3
1
2
3
6
7
평문 공간
암호문 공간

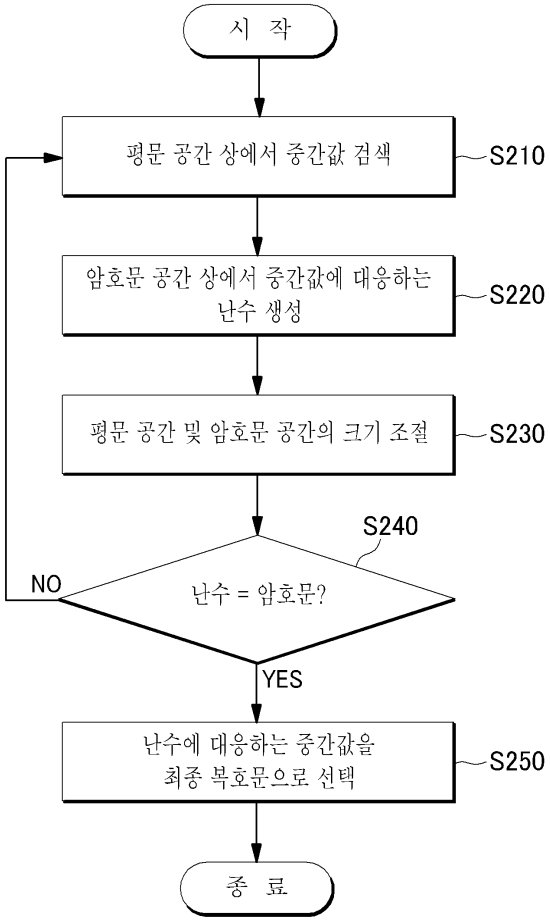
도면7


시 작
평문 공간, 암호문 공간 및 비밀키 설정
S110
평문 공간상에서 중간값 검색
S120
암호문 공간 상에서 중간값에 대응하는 난수 생성
S130
평문 공간 및 암호문 공간의 크기 조절
S140
S150
암호화 하기 위한 평문 = 중간값?
NO
YES
중간값에 대응하는 난수를 최종 암호문으로 선택
S160
종 료

도면8


복호화 중간값 생성부
210
복호화 난수 생성부
220
암호문
평문
복호화 크기 조절부
230
복호화부
240
200

도면9


시 작
평문 공간 상에서 중간값 검색
S210
암호문 공간 상에서 중간값에 대응하는 난수 생성
S220
평문 공간 및 암호문 공간의 크기 조절
S230
S240
난수 = 암호문?
NO
YES
난수에 대응하는 중간값을 최종 복호문으로 선택
S250
종 료