암호기술에 대하여

체계개발실 현지향

《모든 체신일군들과 근로자들은 체신에 대한 깊은 지식을 소유하고 체신부문의 세계적발전추세와 최신과학기술에 정통하기 위하여 꾸준히 노력하여야 합니다.》

김 정 일

1. 암호의 개요

2. 공통열쇠암호

3. 공개열쇠암호

4. 암호에 대한 해득 및 공격방법

5. 열쇠관리방식

6. 망에서의 암호화구간

1. 암호의 개요

1) 암호란 무엇인가?

암호란 문장에 대한 변환을 실시하여 제3자에게는 무엇이 씌여져있는가를 알수 없는 상태로 만드는것을 말한다.

변환전의 문 => 평문 변환후의 문 => 암호문

2) 암호의 리용목적

- 상대방인증(Entity authentication)

거래하고있는 상대방이 정확히 진짜상대방인가 하는것을 확인하기 위한 수단

- 통보문인증(Message authentication)

자료의 정확성을 확인하기 위한 수단

○ 자료완전성(Data integrity)

내용이 변경되지 않음의 보증, 확인

○ 부인방지(Non-repudiation)

송신측은 보냈다는것을 부정할수 없고 또 수신측은 받았다는것을 부정할수 없다는것을 보증 즉 《했다,안했다》고 하는것을 피하기 위한 수단

3) **암호알고리듬의 분류**

- 암호화대상으로 되는 자료의 종류

  수자신호, 상사신호

- 암호화알고리듬의 공개형/비공개형

- 암호화 및 복호화에 공통인 열쇠를 사용/ 다른열쇠를 사용

  공개열쇠암호(비대칭열쇠암호), 공통열쇠암호 (대칭열쇠암호)

- 통보문(평문)을 복원한다. /복원하지 않는다.

  공개열쇠암호의 한가지 응용으로서 수자서명기술이 있는데 이것을 복원을 필요로 하지 않는 비회복형알고리듬이다.

2. 공통열쇠암호

1) 기본구조

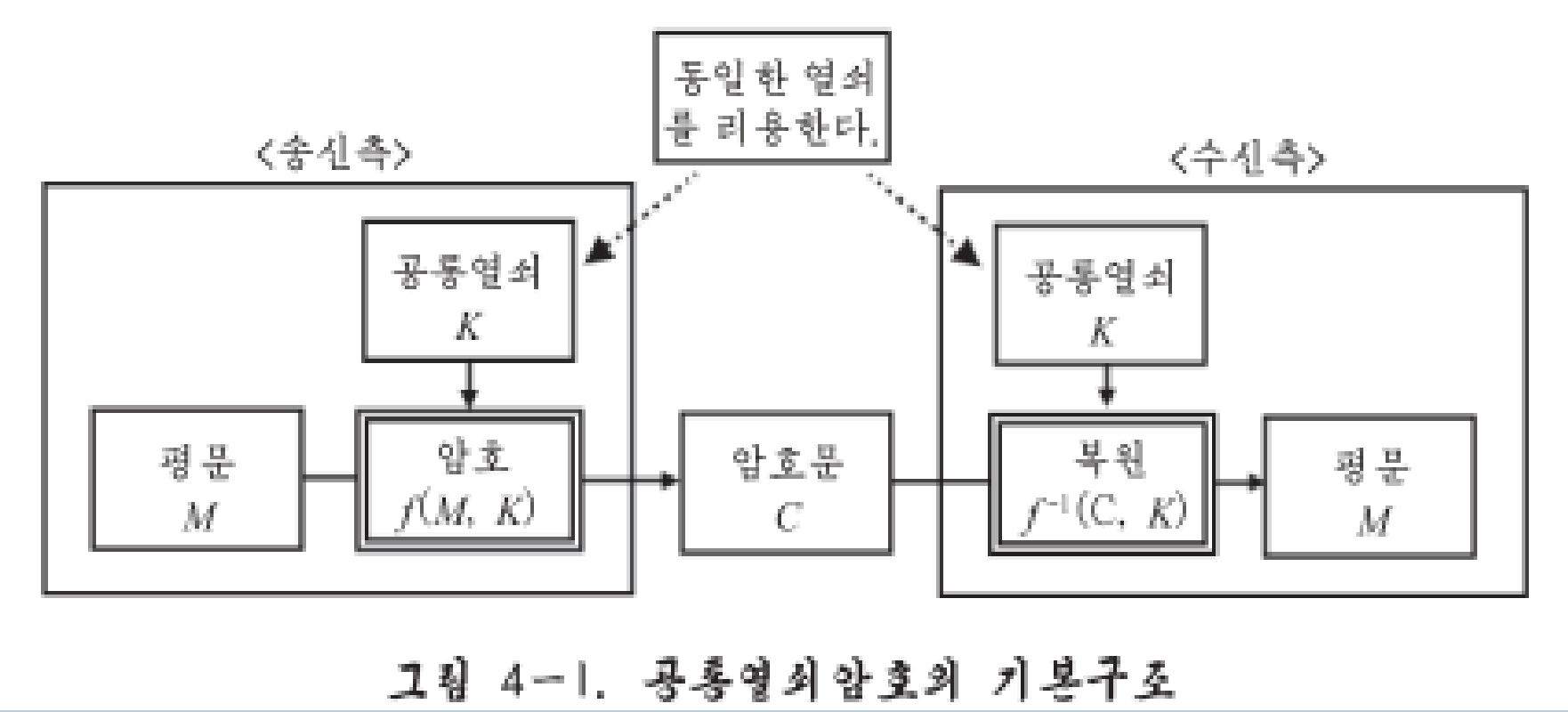

그림 4-1. 공통열쇠암호의 기본구조

공통암호열쇠는 입력자료의 처리단위가 1bit인가 그이상인가에 따라 흐름암호와 불로크암호로 나눈다.

2) 흐름암호

흐름암호는 평문을 1bit단위로 암호화하는 방식이다.

이 방식에서는 평문과 같은 길이의 열쇠가 필요하게 된다. 실례: 버남암호, RC4

실례로 ASCII코드의 매 비트에 대하여 암호열쇠와의 배타적론리합(xor)을 취하는 암호방식을 보자!

암호열쇠를 알고있는 경우는 암호문과 암호열쇠의 배타적론리합을 취함으로써 원래의 평문으로 복원할수 있다.

3) 블로크암호

평문의 여러개의 비트들을 한개 블로크로 하고 블로크단위로 암호화하는 방식을 블로크암호!

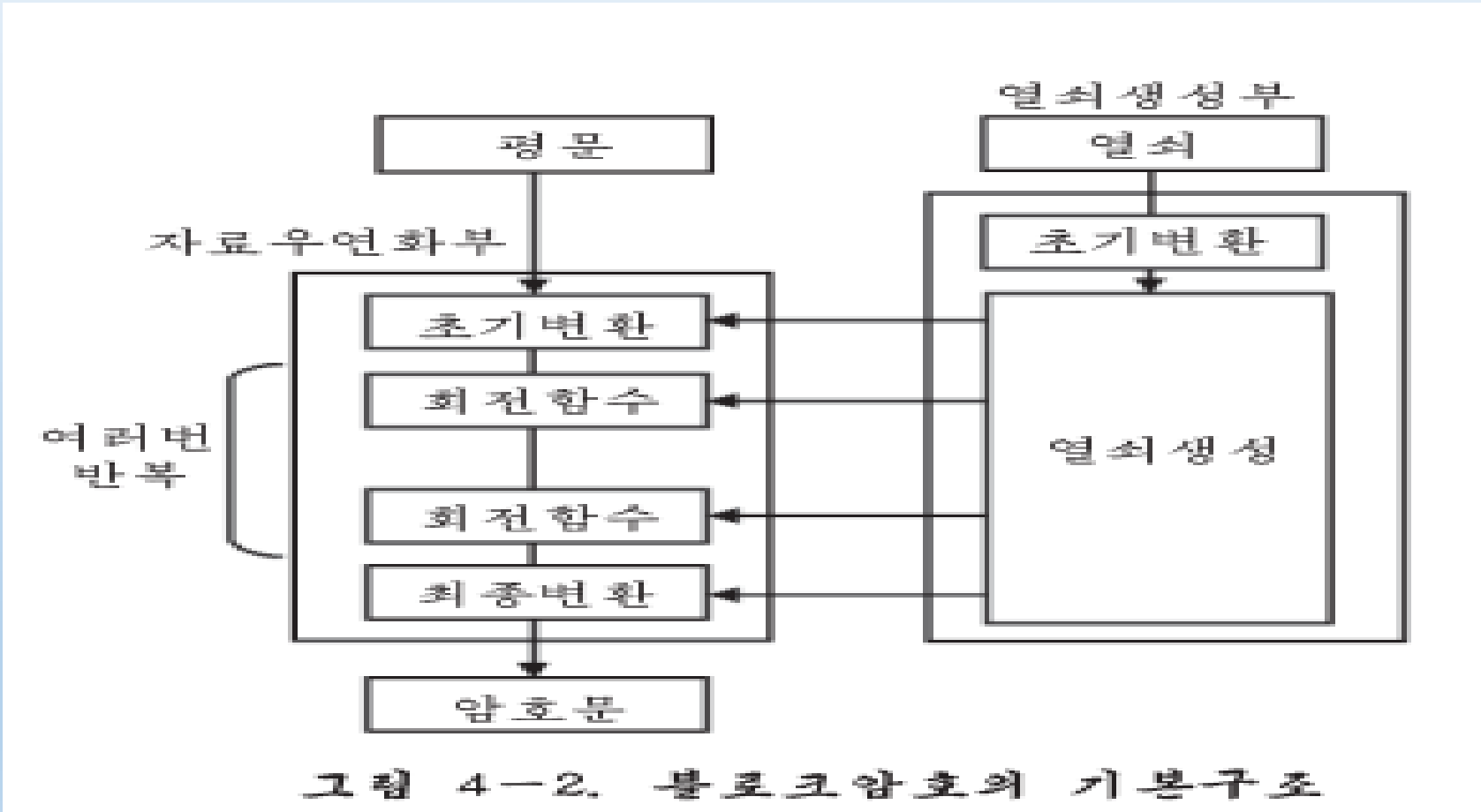

그림 4-2. 블로크암호의 기본구조

4). DES의 기본구조

DES의 명세는 아래와 같다.
블로크길이: 64bit
열쇠길이: 64bit, 여기서 8bit분은 기우성비트이므로 실지 유효한 비트길이는 56bit이다.

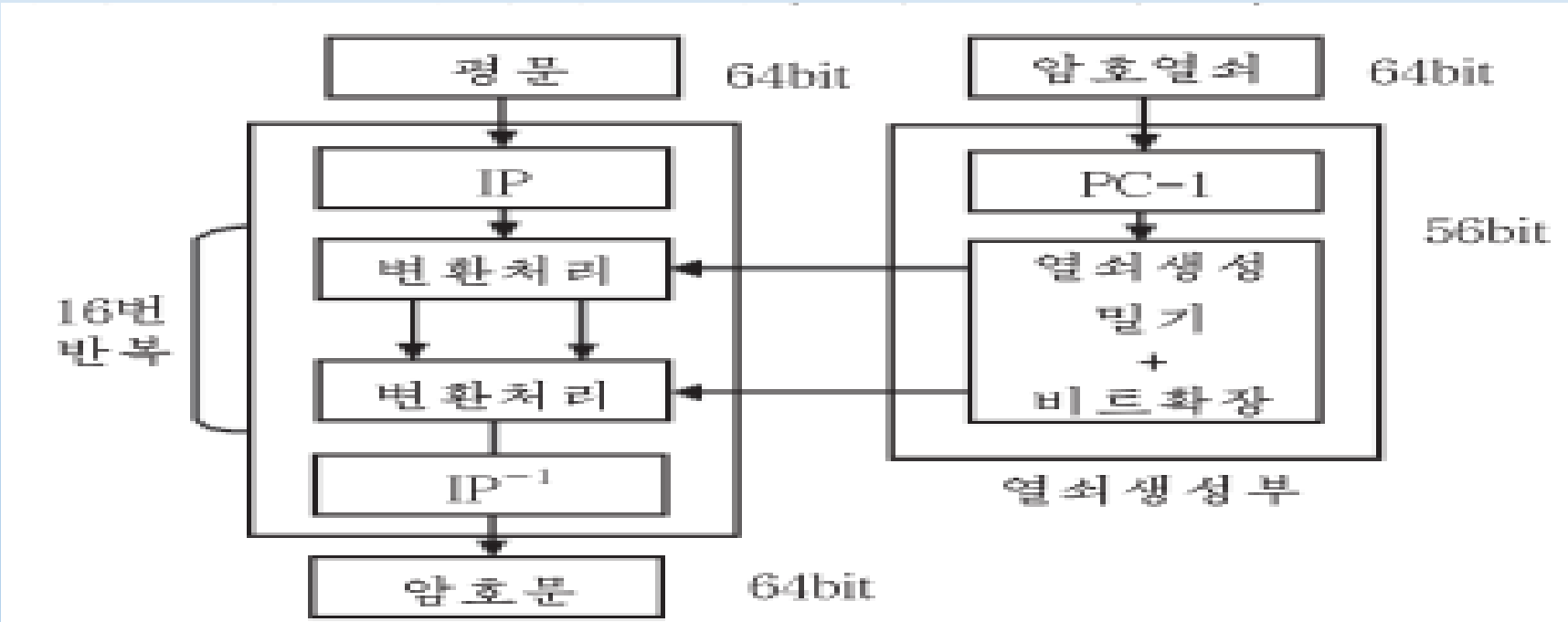

그림 4-5. DES기본구조

3. 공개열쇠암호

1) 기본구조

공통열쇠암호에서 복호처리는 암호처리의 거꿀연산으로서 진행된다.

공개열쇠암호는 한방향성함수를 암호화하기 위한 함수로서 리용하고 복호용의 함수와 복호용의 열쇠를 달리 갖추어 줌으로써 암호화알고리듬과 암호열쇠를 공개하여버리는 방법이다.

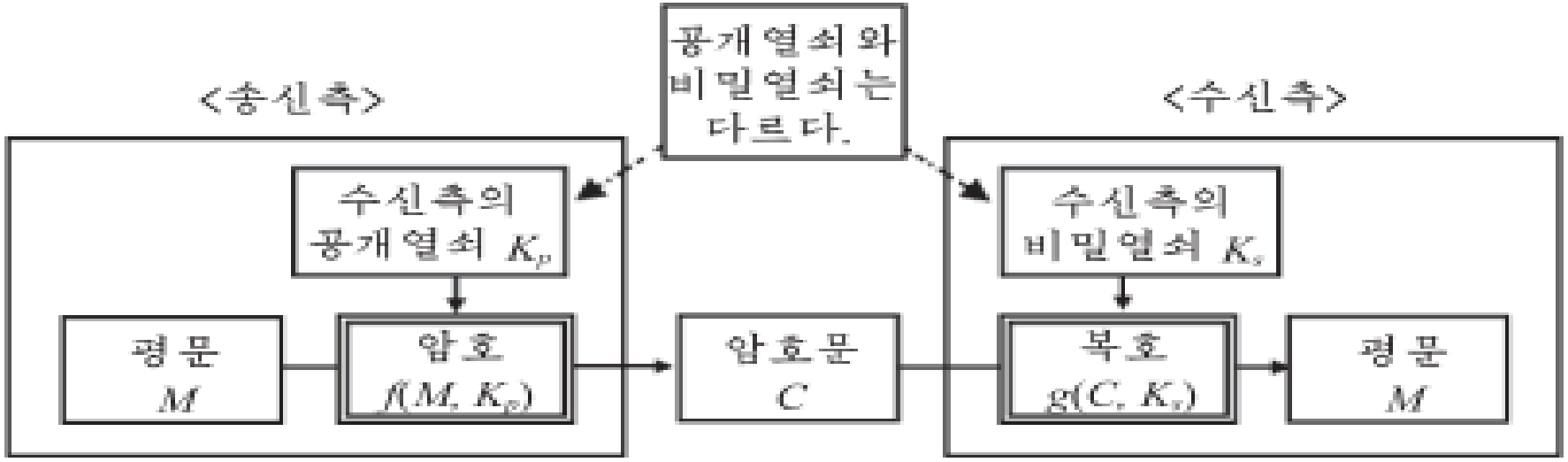

그림 4-13. 공개열쇠의 동작원리

2) 공개열쇠암호의 분류

- RSA

수학적원리는 2개의 씨수의 p,q의 적 n을 계산하는것은 쉽다. 큰 수 n을 p*q로 씨인수분해하는것은 곤난하다.

- Diffie-Hellman 열쇠배송,공유

씨수p,원시뿌리 a 를 공유정보로 한다.

어떤 수 x에 대하여 $b \equiv a^x \ (mod\ p)$ 을 계산하는것은 쉽다.

a,b,p로 부터 $b \equiv a^x (mod) p$ 를 만족시키는 x를 계산하는것은 곤난하다.

- EC Diffie-Hellman 열쇠배송,공유

유한체의 타원곡선상의 점에 대하여 더하기를 정의하고 여러번의 더하기를 스칼라배로 정의 한다.

타원곡선상의 점 G(기초점)을 공유정보로 한다.

어떤 수 x에 대하여 $y = xG$(타원곡선상의 스칼라배)를 계산하는것은 쉽다.

y,G로부터 $y = xG$에서 x를 계산하는것은 곤난하다.

4. 암호에 대한 해득 및 공격방법

1) 블로크암호에 대한 공격방법

- 전수탐사법
- 사전공격
  평문과 대응하는 암호문을 리용할수 있는 경우
- 계차해득법
- 부메랑 공격

2) 물리적공격방법

공개열쇠암호의 비밀열쇠의 보존수단으로서 IC카드가 주목되고 있다. IC카드는 자기카드와는 다르며 부정한 수단에 대하여 물리적정보의 읽기쓰기를 할수 없으므로 자기카드보다도 안전한것으로 되고 있는 데 이 IC카드 등의 물리적인 특성을 리용한 몇가지 공격방법이 있다.

3) DES Challenge

우의 이름으로 진행되는 경연이 RSA회사의 주최로 진행되고 있으며 실제로 DES가 해득된다. 가능한 모든 열쇠에 필용한 계산량은 2^{56} = 7205 794 37 027 936

4) 공개열쇠암호에 의한 공격방법

- IF형에 대한 공격방법
  IF형의 해득은 씨인수분해에 의해 진행된다.
- DL형에 대한 공격방법
  DL형의 해득은 리산로그문제를 풂으로써 진행된다. 대표적인 방법: 지수계산법
- EC형에 대한 공격방법