IT CookBook, 쉽게 배우는 데이터 통신과 컴퓨터 네트워크(개정) 17장 연습문제 해답

1. ① 암호문, ② 해독

2. ① 대칭키 (혹은 단일키), ② 비대칭키

3. 대체 암호화

4. 위치 암호화

5. ① DES, ② 56

6. ① 3DES, ② 168

7. ① RSA, ② 공개키, ③ 비공개키

8. ① 전자서명, ② 비밀키 (혹은 비공개키), ③ 공개키

9. 방화벽

10. ①, ②, ④, ⑤

(설명③) 암호화와 해독 과정에서는 키가 필요한데, 두 키는 서로 같은 값을 사용하는 방식과 다른 값을 사용하는 방식으로 나누어진다.

11. ②, ③, ⑤

(설명①) 특정 문자를 다른 문자로 1:1 대체하는 간단한 방식으로, 암호키와 해독키가 같으므로 대칭키 암호화 방식이다.

(설명④) 키워드 암호화는 대체 문자표의 오른쪽으로 갈수록 원문과 암호문의 문자표가 같아질 확률이 높으므로 시저 암호화보다 나쁜 결과를 얻을 수 있다.

12. ③, ⑤

(설명③) 컬럼 암호화를 두 번 수행하는 이중 컬럼 암호화 방식은 해독을 더 어렵

게 할 수 있다. 이때 첫 번째 컬럼 암호화와 두 번째 컬럼 암호화의 컬럼 길이를 다르게 하는 것이 유리하다.

(설명⑤) 암호문을 만드는 과정은 맨 왼쪽 컬럼부터 시작했던 컬럼 암호화와 다르게 키워드의 알파벳 순서를 따른다.

13. ②, ④, ⑤

(설명①) 암호문을 작성할 때 사용하는 암호키와 해독할 때 사용하는 해독키가 같기 때문에 비공개키 알고리즘에 속한다.

(설명③) DES 알고리즘의 동작 과정에서 위치 암호화는 시작과 끝에서 2번 수행된다.

14. 없음

15. ①, ②, ④, ⑤

(설명③) (공개키, 비공개키)의 조합은 다양하게 산출될 수 있기 때문에 서로 다른 조합에 표시된 공개키를 이용해 비공개키를 유추할 수 없도록 설계되었다.

16. ①, ④

(설명①) 전자 서명은 자신을 다수의 타인에게 증명하는 기능이다. 따라서 암호화 과정에서 자신만 알고 있는 비공개키인 전자서명을 사용해야 한다.

(설명④) 전자 서명의 해독 과정 역시 두 단계로 이루어진다. 암호화 단계의 반대 순서대로 RSA 알고리즘으로 해독한 후에 전자 서명 알고리즘으로 해독해야 한다.

17. ①, ③, ④, ⑤

(설명②) 데이터 링크 계층 암호화는 송수신 호스트 사이의 전송 선로에서의 감청 위협으로부터 데이터를 보호한다.

18. ②, ④

(설명②) 방화벽에서 패킷의 헤더를 검사하여 적절하지 못한 패킷의 전달을 제한하는데, 이와 같은 기능은 주로 라우터를 통하여 방화벽이 구현된다.

(설명④) 라우터의 방화벽 기능은 네트워크 계층과 전송 계층의 헤더 정보에 기초하여 이루어진다.

19.

암호화(Encryption)는 문서를 목적지에 전송할 때 외부 침입자로부터 보호하는 방법으로, 컴퓨터 네트워크가 보급되기 전부터 사용하던 방식이다. 이때 문서의 송수신자는 암호문을 작성하고 해석하는 과정에서 자신들만 아는 비밀키를 사용한다.

20.

시저 암호화(Caesar Cipher)는 줄리어스 시저가 처음 사용했을 것이라는 의미에서 붙은 이름이다. 알파벳 문자를 순차적으로 세 문자씩 오른쪽으로 이동하면서 대체 문자를 사용하는 방식이다. 시저 암호화 방식은 가장 초보적인 알고리즘임에도 불구하고, 원문서 없이 암호문만으로 원래의 문자를 찾기가 쉽지 않다. 장점은 단순함이다. 특히, 세 문자 간격으로 이동된 암호키를 쉽게 기억할 수 있으므로 암호문의 작성과 해독이 간단한 수작업만으로도 가능하다. 그러나 이런 단순함은 외부 침입자도 쉽게 해독할 수 있다는 단점도 된다(예는 교재 370p 참고).

21.

키워드 암호화(Keyword Cipher)는 키워드로 지정한 단어를 암호문 앞줄에 먼저 적고, 키워드에 표시된 문자를 뺀 나머지 문자를 알파벳순으로 기술한다. 키워드를 모르면 시저 암호화보다 대체 문자표를 추측하기가 훨씬 어렵다. 그러나 대체 문자표의 오른쪽으로 갈수록 원문과 암호문의 문자표가 같아질 확률이 높아 시저 암호화보다 나쁜 결과를 초래할 수 있다(예는 교재 370p 참고).

22.
컬럼 암호화(Column Cipher)는 첫 번째부터 마지막 컬럼까지 전체 문장을 컬럼을 기준으로 다시 배치한다. 특히 컬럼 암호화를 두 번 수행하는 이중 컬럼 암호화 방식은 해독을 더 어렵게 할 수 있다. 이때 첫 번째 컬럼 암호화와 두 번째 컬럼 암호화의 컬럼 길이를 다르게 하는 것이 유리하다(예는 교재 372p 참고).

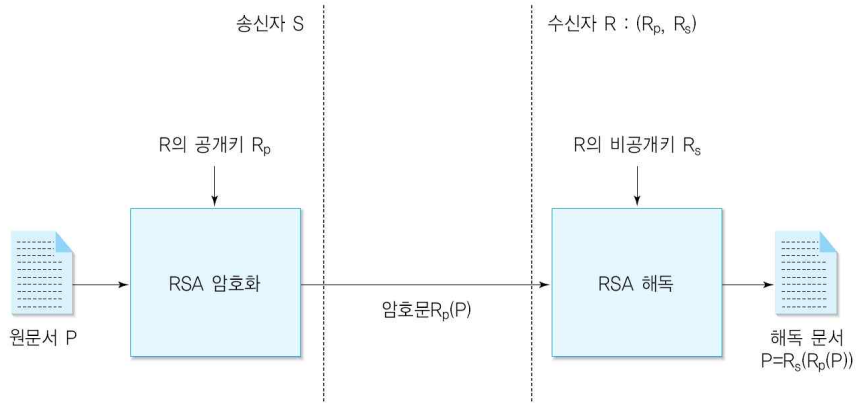
23.
키워드 암호화(Keyword Cipher)는 중복된 문자를 포함하지 않는 임의의 단어를 암호키로 제공하는 방식이다.
원리와 예는 교재 373p 참고

24.
비공개키 방식의 DES(Data Encryption Standard) 알고리즘은 미국 정부가 개발하여 여러 하드웨어와 소프트웨어에서 사용되어 왔다. 대체 암호화와 위치 암호화를 복잡하게 조합하여 개발한 DES 알고리즘은 암호화를 64비트 단위로 수행하며, 암호키의 크기는 56비트다.
동작 방식과 원리는 교재 374~376p 참고

25. 추가해야 함

26.
RSA 알고리즘은 공개키 알고리즘의 대표 예로, (공개키, 비공개키) 조합을 발생시키는 방법을 제시한다.

공개키 알고리즘은 암호화하는 키와 해독하는 키가 동일하지 않도록(혹은 하나로 다른 하나를 쉽게 유추할 수 없도록) 고안된 방식이다. 공개키 알고리즘을 이용하면, 암호문을 작성할 때 사용하는 암호키가 외부에 공개되어도 해독키를 모르면 암호문을 해독할 수 없다. 공개키 알고리즘에서는 사용자가 두 개의 암호키(공개키와 비공개키)를 사용하는데, 공개키(Public Key)는 원문서를 암호화하는 데 사용하므로 원칙적으로 누구에게나 공개된다. 따라서 송신 호스트는 공개키로 원문서를 암호화하여 전송한다. 수신 호스트에서는 암호문을 해독하기 위해 비공개키(Private Key)를 사용한다. 비밀키는 공개키와 다른 값을 갖는다.

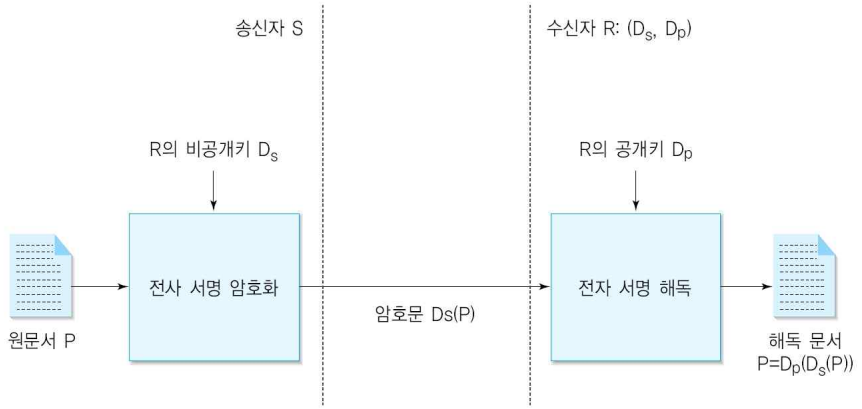


[그림 13-5] RSA 알고리즘

27.

전자 서명(Digital Signature)은 인터넷 환경에서 특정 사용자를 인증(Authentication)하려고 사용한다. 인증은 특정인이 진짜 그 사람인지를 확인하는 절차다. 이와 비슷한 기능으로 권한이 있고 없음을 확인하는 권한(Authorization)이 있는데, 인증과 다른 특징이 있다.

일반적으로 전자 서명의 인증 과정은 RSA 알고리즘과는 반대 원리며 비공개키 알고리즘과 공개키 알고리즘의 조합을 사용한다. 전자 서명은 자신을 다수의 타인에게 증명하는 기능이므로, 암호화 과정에서 자신만 아는 비밀키(전자 서명)를 사용한다. 암호화한 전자 서명은 다수의 타인이 확인하므로 해독 과정에서는 공개키를 사용한다.

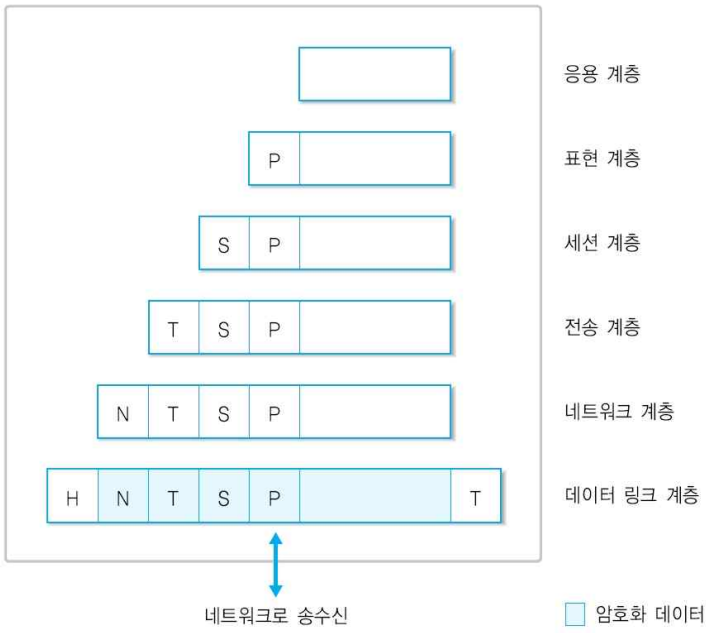


[그림 13-6] 전자 서명의 원리

전자 서명 암호화와 해독 과정은 교재 378~379p 참고

28.

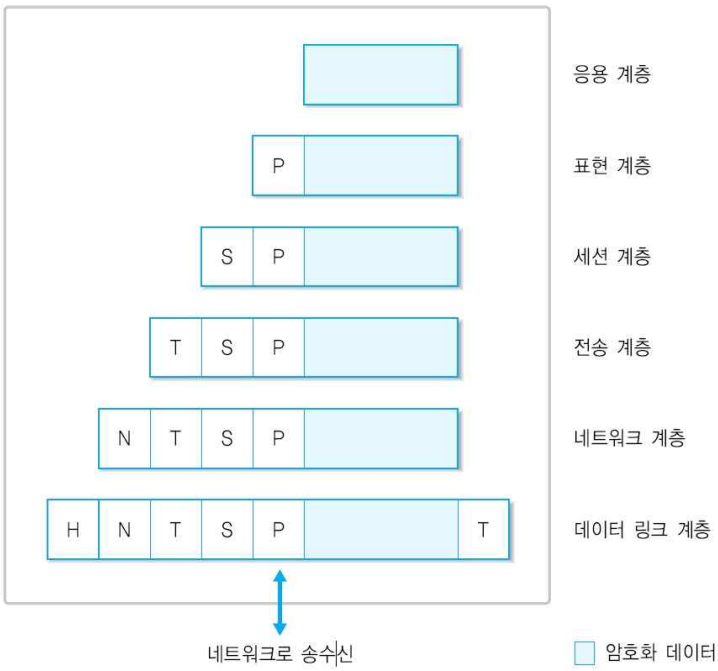
전송 직전인 데이터 링크 계층에서 암호화하여 전송하는 방식이 데이터 링크 계층 암호화다. 수신 호스트에서는 이와 반대로 암호화된 데이터를 수신하기 때문에 데이터 링크 계층에서 해독하여 상위 계층으로 전달해야 한다. 이 방식은 호스트 사이에 있는 전송 선로에서의 감청 위협으로부터 데이터를 보호한다.



[그림 13-9] 데이터 링크 계층 암호화

29.

응용 계층 암호화는 호스트 내부에서 보안을 지원하기 위해 사용하는 방식이다. 방식을 사용해야 한다. 송수신 과정의 끝단에 위치한 응용 계층에서 암호화한다.



[그림 13-10] 응용 계층 암호화

30.

인터넷의 확산으로 허가 받지 않은 사용자의 불법적인 사설 망 접근을 방지하는 문제가 중요한 이슈로 인식되고 있다. 따라서 개방적인 공중 인터넷망과 제한된 사용자 그룹에게 허가된 사설 망 사이에 보안 기능이 필요한데, 이를 방화벽(Firewall)이라고 한다.

31.

라우터의 차단 기능을 다양하게 사용할 수 있는데, 외부의 특정 호스트가 스팸 메일을 자주 보낼 때는 이 호스트를 발신자로 하는 모든 패킷을 차단할 수 있다. 반대로 내부 사용자가 불법 도박 사이트나 유해한 게임 사이트에 접근하는 것도 차단할 수 있다. 호스트의 IP 주소뿐만 아니라, 포트 번호를 이용한 응용 프로그램의 접근도 차단할 수 있다. FTP, 텔넷, 전자 메일 프로그램은 특정 포트 번호를 사용하기 때문에 이 포트 번호를 송신 주소나 목적지 주소로 갖는 패킷을 차단할 수 있다. 따라서 내부에서 외부로, 혹은 외부에서 내부로 특정 응용 서비스에 접근하는 것을 제어할 수 있다.

32.
프록시(Proxy)는 응용 환경에서 적절하게 처리할 수 있는 정보만 수신하도록 가상의 응용 프로그램을 시뮬레이션하는 방화벽이다. 프록시는 내부 네트워크의 호스트에는 외부 네트워크의 응용 연결처럼 보이고, 외부 네트워크에는 내부 네트워크의 응용 연결처럼 보인다.

웹 기능이 구현된 웹 프록시의 경우를 가정하면 내부 네트워크 사용자가 어떤 웹 서버를 어느 정도 방문하는 지에 대한 통계 등을 관리할 수 있다. 따라서 자주 방문하는 사이트 정보는 프록시에 저장하여 사용자에게 정보를 더 빠르게 제공할 수 있다.