문제지

9장

1. 메세지가 올바른 송신자에게 온것인지 확인하는것?
   :
2. 메세지의 무결성과, 인증을 확인 할 수 있는 코드
   :
3. 일방향 해시 함수와 MAC함수의 다른점
   :
4. 메세지 인증코드의 인증 순서
   :
5. 인증코드의 예 3가지
   :
6. 일방향 해시함수로 MAC값을 구하는 것
   :
7. 대칭암호와 인증코드를 조합하여 기밀성, 무결성, 인증을 충족시키는 암호
   :
8. MAC값을 보존, 반복 사용으로 하는 공격은?
   :
9. 위 공격을 방어하는 방법 3가지
   :
10. 키를 추측하여 공격하는것?
    :
11. 인증코드로 해결할수없는 문제 2가지
    :
12. 메세지에 붙여지는 작은 데이터 블록을 생성하기 위해 이것을 이용한다.
    :
13. 블럭암호 모드로 메시지 인증코드를 실현 한다면 무슨 모드?
    :
14. 블럭암호 CTR모드로 MAC값을 구하기 위해 덧셈과 뺄셈을 반복하는 해시 함수 사용하는 모드?

:

10장

1. 메세지를 개인키로 암호화 하는것?
   :
2. 위에것을 복호화 하는것
   :
3. 순서
   :
4. 메세지를 암호화하지 않고 디지털 서명만 한것?
   :
5. 디지털 서명에 취약한 공격은?
   :
6. 공격자가 올바른 디지털 서명을 할수도 있음을 표현하는 용어는?
   :
7. 당사자의 공개키를 인증기관에서 디지털 서명해준 것을?
   :
8. 공인인증서 종류 두가지
   :
9. 인증서의 표준 규격
   :
10. 인증서 관리, 키쌍 작성, 등록자 신원을 확인하는 기관
    :
11. 공개키 기반 구조(세글자 영어로)
    :
12. 위 구조의 4가지 구성요소
    :
13. 인증서 폐지목록 3글자(영어)?
    :

14. 최상위 인증기관을 가르키는 용어
    :
15. 자신의 공개키에 본인이 서명하는 것
    :
16. Lenovo 회사의 중대한 해킹 사건
    :
17. 인증서가 없으면 이 공격에 취약하다
    :
18. 연속된 인증 절차를 걸치게 되는데 이것을 무엇이라 하는가?
    :

11장

1. 키의 종류 두가지
   :
2. 복수의 단어로 이루어진 긴 패스워드
   :
3. 패스워드를 기초로한 암호(3글자 영어)
   :
4. 위 암호는 패스워드에 이 난수를 추가하는데 이 난수의 이름은?
   :
5. 위 난수를 추가 하게 되면 이 공격을 막을수 있다
   :
6. 키를 멜로리에게 들켜도 전체 메세지중 일부만 노출되는 구조
   :
7. 서로 키교환을 함 으로 공통의 비밀값을 얻는 키 교환 방법
   :
8. 원시근의 이미
   :
9. 일방향 해시함수의 횟수를 증가시키는 암호화 방법
   :
10. 모든 키들을 모아놓은 공간
    :

11. 키를 생성할 때 키가 갖추어야할 가장 중요한 성질은?
    :

13장

1. 난수를 사용하는 이유
   :
2. 난수의 용도 6가지
   :
3. 난수의 성질 3가지
   :
4. 난수의 성질에 따른 의사난수 이름 3가지
   :
5. 위 세가지 성질을 모두 만족하는 난수?
   :
6. 인텔에서 만든 회로내 잡음 현상을 이용한 난수생성 방식은?
   :
7. 난수 생성기와 의사난수 생성기의 차이
   :
8. 유명한 의사난수 생성 알고리즘으로 A배, C를 더하고 M으로 나눈 나머지를 의사난수열로 사용하는 방식은?
   :
9. PGP에서 사용하는 의사난수 생성기
   :
10. 랜덤한 비트열을 비축해 놓은 파일
    :
11. 의사난수 생성기를 영어 4글자로
    :

14장

1. PGP를 만든 사람의 이름은?
   :
2. PGP패키지 공개키 암호에 사용되는 알고리즘 3가지
   :

3. 암호문이나 디지털 서명 형식을 정한 규격
   :
4. 위 규격으로 만들어진 소프트 웨어
   :
5. 키고리 또는 키링 관리로 행해지는 기능은?
   :
6. PGP에서 이용자끼리 서로 정당성을 증명하는것,
   사용자의 개인 키를 일정 장소에 보관하는 방법
   :
7. 얼만큼 신뢰하는지 표현 용어
   :
8. 위 용어의 6가지
   :
9. PGP를 이용한 프로그램에서 암호화된 메시지를 아스키 문자열로 변화하는데 이렇게 하는 이유는 무엇을 보장 하기 위함?
   :

15장

1. 웹 브라우저와 웹 서버의 다른말
   :
2. 웹 서버와 웹 브라우저 사이에서는 이것을 이용해 통신을 한다.
   :
3. 암호기술의 추천 세트, 패키지
   :
4. TLS프로토콜 의 두가지 자식 프로토콜
   :
5. 핸드쉐이크 프로토콜의 4가지 자식 프로토콜
   :
6. 레코드 프로토콜에서 메세지를 이것 한다음 MAC값을 결합한다.
   :
7. 레코드 프로토콜에서 MAC값을 붙인다음 헤더를 붙이는데 헤더의 구성요소 3가지
   :

8. 클라이언트가 만든 난수
   :
9. 클라이언트와 서버가 합의한 비밀값
   :
10. SSL의 버그(취약한 성질)
    :
11. 패딩 오라클 공격 영문6글자
    :
12. 보안이 약한 암호 스위트를 사용시키는 공격
    :
13. 암호기술을 갈아끼울 수 있는 기술
    :
14. 웹서버와 웹 클라이언트가 상호작용하는 두가지 용어
    :
15. SSL/TLS로 통신할때 URL의 시작부분
    :
16. TLS 레코드 프로토콜에서 암호화하는 과정중 사용하는 블럭암호 모드는?
    :
17. 마스터 비밀을 생성하는 기초 자료 3가지
    :
18. TLS핸드쉐이크 프로토콜에서 사용하지 않는 암호 기술
    :

16장

1. 암호학자의 도구상자 기술 6가지
   :
2. 위 6가지를 활용한 흐름 암기
   :
3. 암호 압축기술 4가지
   :
4. 비트코인이 생길때 논문을 낸 사람
   :

5. 비트코인은 중앙은행이 없는대신 이용자끼리 분산해 관리하는 구조
   :
6. 비트코인의 거래는 이것과 이것 사이에서 이루어 진다.
   :
7. 위 정답은 사용자의 이것의 해시값으로 만든다.
   :
8. 비트코인용 어플
   :
9. 비트코인 공개 거래 기록부
   :
10. 비트코인 거래의 최소 단위
    :
11. 헤더에 구성요소 3가지
    :
12. 블럭을 추가하는것
    :
13. 블럭을 추가하여 본인이 한 일을 증명하는것
    :
14. 동시에 블록을 추가하여 분기가 만들어 졌을때 어떤 분기인지 인증하는것
    :
15. 앙자론을 이용한 양자 암호기술
    :
16. 위 기술을 제안한 두명
    :
17. 위 기술이 실용화 되면 이 암호기술이 실용화 된다.
    :
18. 위 기술이 실용화 되면 이 공격이 적절한 시간내에 가능해 진다
    :
19. 위 기술 해독의 궁극적 도구
    :
20. 내부에 사용하고있는 요소 기술을 교환 할 수있는 구조를 무었이라고 하는가?
    :