**네트워크 보안 중간시험**

4/28/05 주 복규

1. \_\_\_\_\_\_\_에 답을 쓰시오
   1. The codified language can be termed as **cipher**  text.
   2. In **substitution** cipher, characters are replaced by other characters.
   3. **Cryptanalyst** is a person who attempts to break cryptography solutions.
   4. Conversion of cipher text into plain text is called as **encryption**.
   5. In **stream** cipher, a bit of plain text is encrypted at a time.
   6. DES encrypts blocks of **64** bits.
   7. In asymmetric key cryptography, the **private** key must remain secret with an individual.
   8. While creating a digital envelope, we encrypt the one-time **session** key with the **reciever’s private key**.
   9. If the sender encrypts the message with her private key, it achieves the purpose of **digital signature**.
   10. When two different message-digests have the same value, it is called as **collision**.
   11. **MD5** is a message digest algorithm
   12. MAC stands for **Message Authentication Code**.
   13. PKI stands for **Public Key Infrastructure**.
   14. CRL stands for **Certification Revocation List**.
   15. A **Digital Certification** binds a user with the user’s public key.
   16. A **CA** can issue digital certificates.
   17. The **X.509** standard defines the structure of a digital certificate.
   18. The CA signs a digital certificate with its own **private key**
2. 기타 문제 (^는 지수 승을 나타냄)
   * 2^10 = **103**
   * 2^32 = **4x109** (대략)
   * 2^500 = **10150** (대략)

공개 키 시스템에서, A가 메시지 M을 B만 볼 수 있게 암호화 하는 방법과 그 암호문을 B가 복호화 하는 방법을 설명하라.  
  ,  

**메시지(원문)를 B의 Public Key로 Encryption 해서 B측으로 전송하면**

**B측에서 B의 Private Key로 Decryption하면 B만 메시지를 확인할 수 있다**.

1. 다음에 간단히 답하라 (1-2줄로)
   1. Diffie-Hellman Key exchange algorithm의 용도  
      **불안정한 통신채널에서 두당사자간 사전정보없이 비밀키를 공유(키교환후 대칭키 이용)**
   2. Triple DES with two keys의 원리. 어떻게 두 개의 key로 DES를 세 번 적용하는가?  
      **첫번째 K1으로 Encryption하고 K2로 Decryption한 다음 다시 K1으로 Encryption 한다.**
   3. 메시지에 전자 서명을 하는 방법은  
      **메세지 M 해쉬함수로 MD처리한 다음 자신의 Private Key로 Encryption 한다.**
   4. Replay attack이란  
      **이전에 전송된 메시지를 다시 이용하여 위장하는 방법.**
   5. MAC이 message digest와 다른 점은?

**MD와 거의 유사하지만 MAC은 Encryption/Decryption 기법이 추가된다.**

1. 메시지의 보안에 관한 네 가지 원칙을 간단히 설명하라.
   1. **Confidentiality(기밀성) : 비인가된 사람이 메시지를 볼수 없도록 보장.**
   2. **Integrity(무결성) : 메시지가 불법으로 변경되지 않도록 보장.**
   3. **Authentication(인증) : 상호간 서로 신뢰할 수 있는 개체임을 보장.**
   4. **Non-Repudiation(부인방지) : 메시지가 전송 또는 처리를 실행하고 사후 메시지 검증후 사실부인을 방지한다**.
2. 다음과 같은 측면에서 Public key system을 DES 같은 대칭 키 시스템과 비교하라.
   1. 속도 : **대칭키가 비대칭키에 비해 빠름**
   2. 용도 : **DES는 주로 암/복호에 사용, Public은 기밀성을 요하는 전자서명등.**
   3. 키 분배 : **대칭키에서는 문제가 크지만, Public Key에서는 문제가 없다.**
3. 기밀성을 위한 암호/복호에서 키의 길이가 왜 중요한 요소인가?  
   **현재의 컴퓨터성능과 발전속도에 따라 해독시간이 짧아지고 있는 추세이고, Key의 길이에 따라 해독가능여부가 변화한다.**
4. RSA알고리즘에서 두 키의 생성 방법을 설명하라.  
   **a. 매우큰 소수 2개를 구한다. P,Q**

**b. 소수의 곱 N=PxQ 값을 구한다.**

**c. Encryption(Public Key값)을 위한 E값을 구한다. (P-1)(Q-1)의 인수가 아닌수**

**d. Decryption(Private Key값)을 위한 D값을 구한다. (DxE)mod(P-1)(Q-1)=1 에서 D값을 구한다  
e. 암호화 CT= PTEmodN f. 복호화 PT= CTDmodN**

**네트워크 보안 기말시험**

6/16/05 주 복규

1. 다음 밑줄 친 부분을 채워라
   1. **Client authentication** is optional in SSL.
   2. The main purpose of **SET** is related to secure credit card payments in the Internet.
   3. Determining the identity of a user is called as **Authentication**.
   4. **Biometric** authentication works on the basis of human characteristics.
   5. **Application Gateway** are more secure than packet filters.
   6. Firewall is a specialized form of a **router**.
   7. ISAKMP/Oakley is the protocol used in IPSec for **Key management**.
2. 다음 영어 용어들에 대해 약자를 풀어 쓰고 간단히 (1~2줄로) 설명하라.
   * VPN : **Virtual Private Network**

**공중망을 이용하여 사설망을 구축할 수 있는 기술.**

* + FRR : **False Reject Rate**

**오거부율(시스템이 개인을 식별할 때 잘못 거부하는 비율**

* + PGP **: Pretty Good Private**

**데이터를 암호화하고 해석하는 프로그램**.

* + DMZ : **DeMilitarized Zone**

**사설 네트워크와 외부네트워크 사이 중립지역에 삽입된 호스트 또는 네트워크.**

1. SET의 기본 개념을 다음과 같이 설명하라:
   1. SET의 주요 참여자 들 : **Cardholder(카드소지자), Merchant(상인), Issure(카드발급자),  
       Acquirer(카드전표매입사), PaymentGateway, CA(인증기관).**
   2. 상품구입시 지불이 어떻게 이루어지는가 :

**1.상인이 카드소지자의 금융기관에 지불승인 요청, 2.승인확인후 주문확인을 카드소지자에 발송, 3.상품을 발송후 카드소지자의 금융기관에 지불요청**.

* 1. 어떻게 소비자의 신용카드 정보를 상인으로부터 보호하는가?  
     **거래당사자가 모두 서명하는 이중서명방식 사용**

1. Firewall에 대해:
   1. 무엇? : **외부네트워크로부터 내부네트워크의 중요한 정보 및 자원을 보호하는 시스템**
   2. 용도? : **내부정보(자원) 유출방지 및 유지. 외부침입방지**.
   3. 동작 원리?
2. Packet Filters : **IP,TCP/UDP헤더의 필드넘버 및 IP주소에 의한 필터링**.
3. Application Gateway : **Proxy서버, Bastion Host로도 불림.**

**내부호스트와 외부호스트의 중계역할(http,느세,ftp,telnet등)**

**Packet Filters보다 보안성이 뛰어나다.**

* 1. 한계(보안측면에서의 제한점)?

**Insider’s intrusion, Direct Internet traffic, Virus Attacks**

\* 아래 서술형 문제들에 간단히(3-4줄) 답하라.

5. Clear text password와 관련된 문제점들은 무엇이고, 그 해결 방안을 간단히 설명하시오  
**문제점 : 일반적으로 클라이언트에서 서버로 인증요구시 Clear Text를 사용한다.**

**Password가 ClearText로 DB에 보관된다.**

**해결방안 : MD Password를 사용.**

**서버의 DB에 ClearText를 저장하지 않고 MD-P/W를 저장한 후 같은방법으로 인증 처리.**

6. Authentication token의 용도와 동작원리는?  
**용도 : Password가 수시로 변경이 필요한 기기(휴대용소형기기,CreditCard등)**

**원리 : Token 즉 seed값을 이용한 인증방법.**

**Authentication Server는 주기적 혹은 요청에 의해 Token을 발생시킨다. 이Token은 user에게 seed값으로 주어지며 user는 이seed값을 입력하고 인증을 받는다. seed값은 LCD등의 소형단말기를 통해 확인할 수 있다.**

7. IPSec의 용도는 무엇이고 어떻게 구현되는지를 설명하라

**네트워크계층의 IP패킷의 정보 보호.**

**Transport layer와 Internet layer 사이에 위치하며, 아래와 같이 구성되어있다.  
AH(Athentication Header) : IP헤더의 변경되지 않는 필드에 대해서만 보안성제공.  
ESP(Encapsulating Security Payload) : 페이로드에 대해 AH외 추가적 기밀성제공.**

**SA : 접근제어,비연결형 무결성,발신인증등 제공.**

1. 전자서명(digital signature)이란 무엇이고 어떻게 구현되는가?  
   **문서작성자가 작성내용을 송수신과정에서 위변조 되지 않음을 증명하기 위한 방법(부인방지역할)  
   송신자는 문서를 MD처리한 다음 자신의 비밀키로 암호화(전자서명), 메시지(문서+전자서명+송신자의인증서)를 전송, 수신측에서는 메시지를 복호화한 후 문서를 MD처리하고, 전자서명내용을 송신자의 공개키로 복호화하여 두개의 MD를 비교 일치여부를 확인한다.**
2. Message digest란 무엇이고 그 용도는?

**임의 길이의 메시지를 해쉬함수 처리하여 일정한 길이의 형태로 만드는 것.**

**문서의 위변조를 방지. 부인방지.**

1. SSL과 IPSec의 차이를 설명하고, 네트워크 보안을 제공하는데 있어서의 장단점을 설명하라(5줄 이내).  
    **IPSec SSL**

**접근제어 : 네트워크 및 user단위 시스템 및 Application단위**

**SW : 전용 SW 필요 웹브라우저 외 불필요**

**장점 : 다양한 Application 사용 가능 사용 및 관리가 편리**

**End-to-End 보안적용가능 서버와 Client 인증가능**

**단점 : 서버나 Client인증불가 과부하 발생가능**

**운영 및 관리적요소 많음 사설IP기반 네트워크 적용이 어렵다**