2016년 2학기 정보보호 중간고사

1. Discuss why secret-key encryption/decryption cannot be used for non-repudiation. (10점)

2. Secret key cryptography 방식은 메시지의 암호화에 사용될 수도 있으며, message authentication에도 사용될 수 있다. 어떻게 하면 secret key cryptography 방식이 message authentication 용으로 사용될 수 있는지 가능한 동작 방법의 예를 보여라. (10점)

3. 메시지의 위조/변조 여부를 판단하기 위한 방식으로는 MAC(message authentication code)를 이용하는 방식과, cryptographic hash 함수를 이용하여 생성한 message digest를 이용하는 방식 등이 있다. 두 방식의 근본적인 차이점은 무엇인가? (10점)

4. 사용자 A로부터 인증서(certificate)를 받은 경우, 인증서에는 “A의 이름, 공개키, 서명 값” 등이 저장되어 있다. A로부터 받은 인증서에 있는 A의 공개키 값이 정말 A의 것이라는 것을 어떻게 확인할 수 있는지, 알기 쉽게 설명하라. (혹시 다른 사람이 A인 것으로 위장하여, A의 인증서라고 자신의 인증서를 보낸 경우, 우리는 이것을 어떻게 확인할 수 있을까?) (10점)

2016년 2학기 정보보호 기말고사

모든 문제의 답안은 source code 전체를 제출하여, 채점 시에 컴파일 하여 확인할 수 있도록 하라.

1. 공인인증서의 주요 내용은 “이름, 공개키, signature” 등을 들 수 있다. 이때, signature는 CA에서 생성한다. CA가 signature를 생성하는 방법을 알기 쉽고 자세하게 설명하라. (이론 문제) (10점)

2. openssl command를 이용하여 data.txt 파일의 hmac 값을 계산하여, 계산 값과 계산을 위한 openssl 명령을 exam.txt 파일에 저장하여 제출하라. (10점)
   - 키는 "0123456789“
   - Hashing algorithm은 sha1
   - “data.txt” 파일의 내용은 아래와 같음.

```
[temp]# cat data.txt
a HMAC is a specific type.
[temp]# hexdump data.txt -c
0000000   a       H   M   A   C       i   s       a       s   p   e   c
0000010   i   f   i   c       t   y   p   e   .  \n
000001b
[temp]#
```

3. argv[2] 파일을 decryption하여 argv[1] 파일에 저장하는 프로그램을 작성하라. 이때, decryption 함수를 호출하는 main 함수도 작성하여 제출하라. 사용되는 암호화 방식은 DES, ecb 모드로 하라. (10점)

4. 어떤 파일이 변경되었는지의 여부를 출력하는 다음과 같은 프로그램을 작성하라. (10점)
   - 입력
     - argv[1]: 변경여부를 검증할 파일이름
     - argv[2]: argv[1] 파일에 대한 (알려진) sha1 hash 값 (20 bytes)
   - 이 프로그램은 argv[1] 파일의 sha1 hash 값을 계산하며 (이 값을 “value1”이라고 함)
   - “value1” 값이, argv[2] 값과 일치하면, 변경되지 않은 것으로 판명한다.
   - “value1” 값이, argv[2] 값과 일치하지 않으면, 변경된 것으로 판명한다.

   힌트: 비교할 때 memcmp (...); 함수 사용. (man memcmp)

2017년 2학기 정보보안 중간고사

1. 어떤 보안 알고리즘이 다음과 같은 기능을 제공한다고 할 때, 이것이 무엇을 의미하는지 알기 쉽고 자세하게 설명하라.
   가) Confidentiality (5점)
   나) Integrity (5점)

2. 공인인증서(certificate)에 관한 다음 물음에 대하여 알기 쉽고 자세하게 기술하라.
   가) 공인인증서를 생성하는 전체 과정 (사용자의 동작 및 CA의 동작) (5점)
   나) 제3자로부터 수신한 공인인증서를 검증하는 과정 (5점)

3. 다음 표의 내용을 알기 쉽고 자세하게 기술하라. (2.5x8=20점)

	Symmetric key algorithms (AES)	Asymmetric key algorithms	
		RSA based	Elliptic curve based
키 길이	(가)	(나)	(다)
처리 속도	(라)	(마)	(바)
활용 (용도)	(사)	(아)	

4. IP security (IPsec)의 AH(authentication header) 방식과 ESP(encapsulating security payload) 방식에 관하여 아는 것을 전부 기술하라. (10점)

2017년 2학기 정보보안 기말고사

1. IPsec 프로토콜에 관한 다음 물음에 대하여 최대한 자세하게 기술하라. (10점)
   가) Transport mode와 tunnel mode에 관하여 설명하라. (5점)
   나) ESP (encapsulate security payload) 에 관하여 기술하라. (5점)

2. SSH 프로토콜의 local port forwarding 에 관하여 최대한 자세하게 기술하라. (10점)

3. SSL handshake 프로토콜에 관하여 최대한 자세하게 기술하라. (10점)

4. plaintext.txt 파일의 내용은 다음과 같다. (10점)

```
[tmp]$ cat plaintext.txt
Hello world.
This is test input.
[tmp]$
```

   가) plaintext 파일의 내용을 AES 128 bit CBC 모드로 암호화하여 ciphertext.bin 파일에 저장하는 openssl 명령을 기술하라. 이때 사용하는 key는 “0123456789012345”로 하고, iv는 “0123456789”로 하라. (5점)
   나) 가)에서 생성한 ciphertext.bin 파일의 내용을 decryption하는 openssl 명령을 기술하라. 이때 사용하는 key와 iv는 가)에서 사용한 값으로 한다. (5점)

2019년 2학기 정보보안 중간고사

1. 다음에 관하여 최대한 자세하게 기술하라. (2.5×4 = 10점)
   가) Brute force attack
   나) Message integrity
   다) Diffie-Hellman 알고리즘
   라) Block cipher의 모드 중 하나인 CTR (counter) 모드

2. 어떤 문서의 위변조를 검증하기 위한 보안 알고리즘인 HMAC과 RSA digital signature 두 방식의 장단점을 비교하기 위한 다음 내용을 기술하라. (5×4 = 20점)

	HMAC	RSA digital signature
사용하는 키의 종류	(가)	
상대적인 키 길이	(나)	
처리 속도	(다)	
non-repudiation 지원 여부	(라)	

3. 공개키 기반의 digital signature 방식에 관한 다음 물음에 대하여 알기 쉽고 자세하게 기술하라. (5×2 = 10점)
   가) 전자서명을 생성하는 과정
   나) 전자서명을 검증하는 과정

2019년 2학기 정보보안 기말고사

1. 다음에 관하여 최대한 자세하게 기술하라. (2.5×4=10점)
   가) OCSP (2.5점)
   나) IPsec에서의 SPI (2.5점)
   다) CSR (2.5점)
   라) CRL (2.5점)

2. IPsec에서 사용되는 IKE 프로토콜의 목적(5점)과 동작 방법(5점)에 관하여 최대한 자세하고 알기 쉽게 기술하라. (5×2=10점)

3. SSL 프로토콜을 구성하는 다음 sub protocol 들의 동작 및 기능에 관하여 아는 것을 전부 기술하라. (10점)
   가) SSL handshake protocol (4점)
   나) SSL change cipher spec protocol (1점)
   다) SSL alert protocol (1점)
   라) SSL application data protocol (1점)
   마) SSL record protocol (3점)

4. plaintext 파일의 내용을 암호화하고 복호화하기 위한 다음 물음에 답하라. (5×2=10점)
   가) plaintext 파일의 내용을 “Three key triple DES EDE in CBC mode”로 암호화하여 ciphertext 파일에 저장하는 openssl 명령을 기술하라. 이때 사용하는 key는 PBKDF2 알고리즘을 사용하여 password로 부터 만들어지도록 하라. (5점) (hint: man 사용)

   나) 가)에서 생성한 ciphertext 파일의 내용을 “Three key triple DES EDE in CBC mode”로 decryption 하는 openssl 명령을 기술하라. 이때 사용하는 key는 PBKDF2 알고리즘을 사용하여 password로 부터 만들어지도록 하라. (5점)

2020년 2학기 정보보안 중간고사

1. 다음에 관하여 최대한 자세하게 기술하라. (5점×4문제=20점)
   가) static DH (Diffie-Hellman)과 Ephemeral DH (DHE)
   나) PFS/FS (perfect forward secrecy/forward secrecy)
   다) chosen plaintext attack (CPA)
   라) hash function과 MAC function의 차이

2. Stream cipher cryptography의 동작 방식에 관하여 최대한 자세하게 기술하라. (encryption 5점 + decryption 5점 = 10점)

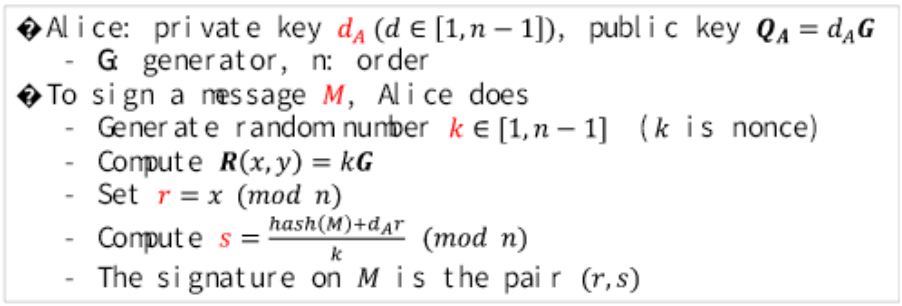
3. Nonce, iv (initialization vector), salt에 관하여 기술하라. (4/3/3=10점)

4. RSA에 관한 다음 물음에 답하라. (5점×2문제=10점)
   가) Textbook RSA의 문제점
   나) real life RSA에서 이 문제를 해결한 방법

2020년 2학기 정보보안 기말고사

1. 다음에 관하여 최대한 자세하게 기술하라. (5점×2문제=10점)
   가) CA (certificate authority)
   나) IPsec에서 transport mode와 tunnel mode

2. ECDSA의 sign 동작은 다음과 같다. Alice가 메시지 M에 sign하고, sign 생성시 사용한 nonce k 와 sign 값 (r, s)를 공개하면 attacker는 Alice의 비밀키 d_A 를 알아낼 수 있게 된다. Attacker가 Alice의 비밀키를 알아내는 방법을 기술하라. (10점)



3. 어떤 사용자가 공인인증서 C를 수신하였을 때, C의 내용이 위조되지 않고 정상임을 확인하는 방법을 기술하라. (10점)

4. SSL/TLS handshake protocol에 관하여 알기 쉽고 자세하게 기술하라. (10점)

2021년 2학기 정보보안 중간고사

1. 다음에 관하여 최대한 자세하게 기술하라. (2.5점×4문제=10점)
   가) Message Integrity
   나) chosen plaintext attack (CPA)
   다) Authenticated Encryption (or Authenticated Encryption with Associated Data)
   라) HMAC (keyed hashing with message authentication)

2. Secret key cryptography 방식과 public key cryptography의 비교에 관한 아래 테이블에 내용을 기술하라. (2.5점×4문제=10점)

	Secret key cryptography	public key cryptography
일반적인 키의 길이	(1)	(2)
상대적인 속도	(3)	
키 관리	(4)	

3. Public key algorithm을 이용한 전자 서명 (digital signature)에 관한 다음 물음에 답하라. (5점×2문제=10점)
   가) 서명하는 과정을 그림과 함께 최대한 자세하게 기술하라.
   나) 검증하는 과정을 그림과 함께 최대한 자세하게 기술하라.

4. Secret key cryptography 방식은 메시지의 암호화에 사용될 수도 있으며, message authentication에도 사용될 수 있다. 어떻게 하면 secret key cryptography 방식이 message authentication 용으로 사용될 수 있는지 가능한 동작 방법의 예를 보여라. (10점)

2021년 2학기 정보보안 기말고사

1. 다음에 관하여 최대한 자세하게 기술하라. (10점)
   가) Packet filtering firewall (5점)
   나) OCSP (Online Certificate Status Protocol) (5점)

2. ECDSA의 동작은 다음과 같다. Alice가 계산한 R 값이, 제 3자가 계산한 R' 값과 같아지게 되는 것을 증명하라. (10점)

- Alice: private key d_A ($d \in [1, n-1]$), public key $\boldsymbol{Q_A} = d_A \boldsymbol{G}$
  - G: generator, n: order
- To sign a message M, Alice does
  - Generate random number $k \in [1, n-1]$ (k is nonce)
  - Compute $\boldsymbol{R}(x, y) = k\boldsymbol{G}$
  - Set $r = x \pmod n$
  - Compute $s = \frac{hash(M) + d_A r}{k} \pmod n$
  - The signature on M is the pair (r, s)
- Verification
  - Compute $\boldsymbol{R'}(x', y') = \frac{1}{s}(hash(M)\boldsymbol{G} + r\boldsymbol{Q_A}) \pmod n$
  - If ($x' = r$)
    accept
    else reject

3. 공인인증서(certificate)에 관한 다음 물음에 대하여 알기 쉽고 자세하게 기술하라. (10점)
   가) 공인인증서를 생성하는 전체 과정 (사용자의 동작 및 CA의 동작) (5점)
   나) 제3자로부터 수신한 공인인증서를 검증하는 과정 (5점)

4. IPsec의 authentication header 방식에 관하여 아는 것을 전부 기술하라. (10점)

2022년 2학기 정보보안 중간고사

1. 다음에 관하여 최대한 자세하게 기술하라. (2.5점×4문제=10점)
   가) Authorization
   나) KPA (known plaintext attack)
   다) Pseudo-random (number) generator (PRG/PRNG)
   라) HMAC

2. Alice가 Bob에게 digital signature가 있는 문서와 자신의 공인인증서를 전송하였다.

   Alice --> "message contents (M), digital signature (sig)"
   Alice의 certificate (Cert_A) --> Bob

   Bob이 수신한 "M, sig", Cert_A를 이용하여, M의 내용이 변경되지 않은 것을 확인하는 방법을 알기쉽고 자세하게 기술하라. (10점)

3. 다음과 같은 두 방식으로 메시지를 암호화 할 때 어떤 차이가 있는지 기술하라. 결론에 이르게 된 원인도 자세하게 기술하라. (10점)

   $E_{k2}\ [\ E_{k1}(\text{Message})\ ]$

   $E_{k3}\ [\ \text{Message}\ ]$

   단, K1: m bits
   K2: m bits
   K3: m+n bits

4. EdDSA의 동작은 다음과 같다. EdDSA 검증과정에서 P1과 P2가 같아지게 되는 원인을 기술하라. (10점)

- **Key generation** (with a generator point G and a subgroup order q for the EC points)
  - Private key(integer): $pk \in [1, q-1]$
  - public key (EC point): pubKey = $pk \times G$
- **Sign**: EdDSA_sign(msg, pk) → { **R**, s }
  - r(integer) = hash[hash(pk)+msg] (mod q)
  - Calculate $R = rG$
  - h = hash[**R** + pubKey + msg] (mod q)
  - s = $(r + h \times pk)$ (mod q)
- **Verify**: EdDSA_verify(msg, pubKey, signature { **R**, s }) → valid/invalid
  - h = hash[**R** + pubKey + msg] (mod q)
  - P1 = sG
  - P2 = $R + h \times pubKey$
  - P1==P2 → valid, P1≠P2 → invalid

2022년 2학기 정보보안 기말고사

1. 다음에 관하여 최대한 자세하게 기술하라. (2.5점×4문제=10점)
   가) WAF
   나) SSH에서의 SOCKS
   다) IPsec에서의 ESP mode
   라) Linux iptables

2. Stateful firewall에 관하여 알기 쉽고 자세하게 기술하라. 가능하면, 예를 들어 설명하라. (10점)

3. SSL/TLS에 관한 다음 내용에 관하여 최대한 자세하게 기술하라. (10점)
   가) SSL/TLS 프로토콜의 목적은 무엇인가?
   나) SSL/TLS handshake protocol의 목적과 동작에 관하여 기술하라.

4. SSH 프로토콜의 local port forwarding에 관하여 최대한 자세하게 기술하라. (10점)