EZSUB S1

암호학 동형모의고사

SEASEON 01 01회

Date : 260612

cafe.daum.net/EZ-SUB

01 다음 보기에서 설명하는 용어는 무엇인가?

섀넌(Shannon)은 순환과 대치를 반복적으로 사용하여 평문과 암호문 사이의 관계 파악을 어렵게 만드는 합성암호를 소개하며, 암호문의 각각의 비트나 문자가 평문의 모든 비트나 특정 비트에 종속적으로 결정되어 암호문에 대한 통계적인 테스트를 통하여 평문을 찾고자 하는 공격자를 좌절시키는 개념을 소개하였다.

---

① 혼돈(Confusion)
② 확산(Diffusion)
③ 차분(Differential)
④ 선형(Linear)

02 다중문자 암호 방식에 해당하는 것만을 모두 고르면?

ㄱ. 비즈네르(Vigenère) 암호
ㄴ. 시저(Caesar) 암호
ㄷ. 플레이페어(Playfair) 암호
ㄹ. 아핀(Affine) 암호

---

① ㄱ, ㄷ
③ ㄴ, ㄷ
② ㄱ, ㄹ
④ ㄴ, ㄹ

03 블록암호 알고리즘을 구성하는데 사용되는 페이스텔(Feistel) 구조와 SPN 구조에 대한 설명으로 가장 적절한 것은?

① 정상적으로 복호화 과정이 수행되기 위해서 페이스텔 구조의 라운드 함수는 가역적(invertible)이어야 한다.
② 페이스텔 구조를 사용하는 대표적인 블록암호 알고리즘으로 AES가 있다.
③ SPN 구조는 Shannon의 혼동(confusion)과 확산(diffusion) 이론을 바탕으로 한 구조이다.
④ SPN 구조의 암호화 과정은 최소 2라운드 반복 수행해야 전체 평문이 암호화된다.

04 다음 문제가 모두 해결된 블록암호 운용 모드는?

- 평문 블록이 동일하면 암호문 블록이 같아지는 문제
- 암호문 블록에 오류가 발생하면 다음 블록의 복호화에 오류가 전파되는 문제

---

① ECB(Electronic CodeBook)
② OFB(Output FeedBack)
③ CFB(Cipher FeedBack)
④ CBC(Cipher Block Chaining)

05 SSL, IPSec 등 대부분의 네트워크 보안 프로토콜에서 RSA 공개키 암호를 이용하여 송신자(A)와 수신자(B) 간에 비밀 세션키를 공유하는 키분배 방식을 지원하고 있다. 이때, 송신자(A)가 수신자(B)에게 전달하는 세션키를 암호화할 때 필요로 하는 키 정보에 해당하는 것은?

① 송신자(A)의 개인키
② 송신자(A)의 공개키
③ 수신자(B)의 개인키
④ 수신자(B)의 공개키

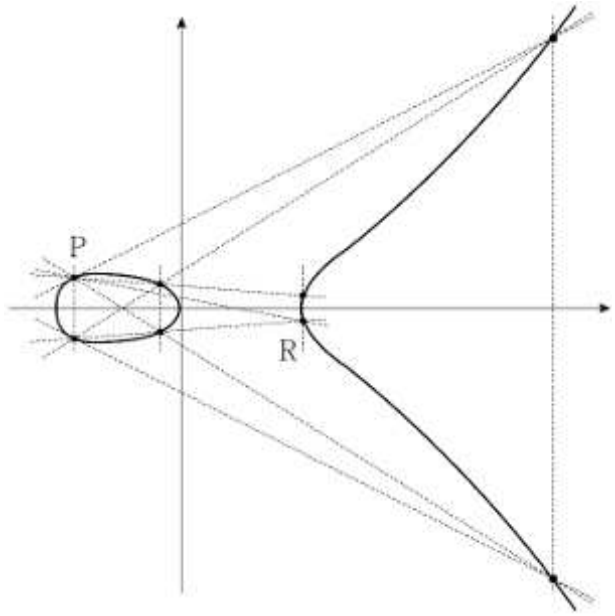
06 RSA 암호화 방식에서 공개키가 (7,33), 개인키가 (3,33)일 경우, 공개키로 암호화 한 값이 3이라고 할 때 이를 복호화 한 값은 무엇인가?

① 99
② 27
③ 2,187
④ 343

07 **ElGamal 등과 같이 이산 대수 문제를 기반으로 하는 암호화 기법에서 비밀키로 공개키를 계산할 때 원시근이 사용된다. 사용되는 소수가 13일 때, 원시근으로 사용될 수 있는 값은?**

① 6
② 8
③ 10
④ 12

08 **타원곡선 암호시스템(ECC)은 타원곡선 이산대수의 어려움을 이용한다. 그림과 같이 실수 위에 정의된 타원곡선과 타원곡선상의 두 점 P와 R이 주어진 경우, R = kP를 만족하는 정수 k의 값은?** (단, 점선은 타원곡선의 접선, 점을 연결하는 직선 또는 수직선을 나타낸다)



① 2
② 3
③ 4
④ 5

09 **해시함수 h의 성질에 관한 설명 중 틀린 것은?**

① 역상저항성은 주어진 임의의 출력값 y에 대해 y = h(x)를 만족하는 입력값 x를 찾는 것이 계산적으로 불가능한 성질이다.
② 두 번째 역상 저항성은 주어진 입력값 x에 대해 h(x)=h(x')를 만족하는 다른 입력값 x'을 찾는 것이 계산적으로 불가능한 성질이다.
③ 충돌 저항성은 h(x)=h(x')를 만족하는 두 입력값 x와 x'을 찾는 것이 계산적으로 불가능한 성질이다.
④ 충돌 저항성은 역상 저항성을 보장한다.

10 **NIST 표준(FIPS 186)인 전자서명 표준(DSS)에 대한 설명으로 옳지 않은 것은?**

① DSA(Digital Signature Algorithm)는 DSS에서 명세한 알고리즘으로 ElGamal과 Schnorr에 의해 제안된 기법을 기반으로 한다.
② 서명자는 공개키와 개인키의 쌍을 생성하고 검증에 필요한 매개 변수들을 공개해야 한다.
③ 서명 과정을 거치고 나면 두 개의 요소로 이루어진 서명이 생성되는데 서명자는 이를 메시지와 함께 수신자(검증자)에게 보낸다.
④ 검증 과정에서 검증자는 서명으로부터 추출한 값과 수신한 메시지로부터 얻은 해시값을 비교하여 일치하는가를 확인함으로써 서명을 검증한다.