



문 11. SSL(Secure Socket Layer)에서 메시지에 대한 기밀성을 제공하기 위해 사용되는 것은?  
 ① MAC(Message Authentication Code)  
 ② 대칭키 암호 알고리즘  
 ③ 해시 함수  
 ④ 전자서명

문 12. 메시지 인증에 사용되는 해시 함수의 요건으로 옳지 않은 것은?  
 ① 하드웨어 및 소프트웨어에 모두 실용적이어야 한다.  
 ② 다양한 길이의 출력을 생성할 수 있어야 한다.  
 ③ 해시를 생성하는 계산이 비교적 쉬워야 한다.  
 ④ 임의 크기의 메시지에 적용될 수 있어야 한다.

문 13. 사용자 A가 사용자 B에게 보낼 메시지 M을 공개키 기반의 전자서명을 적용하여 메시지의 무결성을 검증하도록 하였다. A가 보낸 서명이 포함된 전송 메시지를 다음 표기법에 따라 바르게 표현한 것은?

PUX: X의 공개키 PRX: X의 개인키 E(K,M): 메시지 M을 키 K로 암호화 H(M): 메시지 M의 해시   : 두 메시지의 연결
---

- ①  $E(PU_B, M)$                       ②  $E(PR_A, M)$   
 ③  $M || E(PU_B, H(M))$             ④  $M || E(PR_A, H(M))$

문 14. 대칭키 블록 암호 알고리즘의 운영 모드 중에서 한 평문 블록의 오류가 다른 평문 블록의 암호 결과에 영향을 미치는 오류 전이(error propagation)가 발생하지 않는 모드만을 묶은 것은?  
 (단, ECB: Electronic Code Book, CBC: Cipher Block Chaining, CFB: Cipher Feedback, OFB: Output Feedback)  
 ① CFB, OFB                              ② ECB, OFB  
 ③ CBC, CFB                              ④ ECB, CBC

문 15. 유닉스/리눅스 시스템의 로그 파일에 기록되는 정보에 대한 설명으로 옳지 않은 것은?  
 ① btmp - 실패한 로그인 시도  
 ② pacct - 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보  
 ③ loginlog - 성공한 로그인에 대한 내용  
 ④ utmp - 로그인, 로그아웃 등 현재 시스템 사용자의 계정 정보

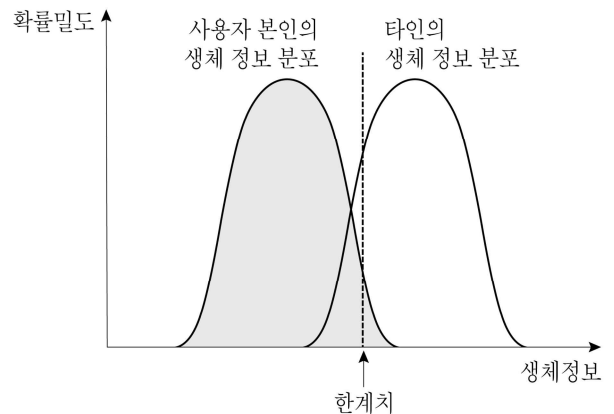
문 16. 「개인정보 보호법」상 개인정보처리자가 개인정보가 유출되었음을 알게 되었을 때에 지체 없이 해당 정보주체에게 알려야 할 사항에 해당하지 않는 것은?  
 ① 유출된 개인정보의 항목  
 ② 유출된 시점과 그 경위  
 ③ 조치 결과를 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고한 사실  
 ④ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

문 17. 인증서를 발행하는 인증기관, 인증서를 보관하고 있는 저장소, 공개키를 등록하거나 등록된 키를 다운받는 사용자로 구성되는 PKI(Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?  
 ① 인증기관이 사용자의 키 쌍을 생성할 경우, 인증기관은 사용자의 개인키를 사용자에게 안전하게 보내는 일을 할 필요가 있다.  
 ② 사용자의 공개키에 대해 인증기관이 전자서명을 해서 인증서를 생성한다.  
 ③ 사용자의 인증서 폐기 요청에 대하여 인증기관은 해당 인증서를 저장소에서 삭제함으로써 인증서의 폐기 처리를 완료한다.  
 ④ 한 인증기관의 공개키를 다른 인증기관이 검증하는 일이 발생할 수 있다.

문 18. 암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 옳은 것은?  
 ① 비결정적(non-deterministic) 알고리즘을 사용하여 재현 불가능한 수열을 생성해야 한다.  
 ② 시드(seed)라고 불리는 입력 값은 외부에 알려져도 무방하다.  
 ③ 생성된 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 없어야 한다.  
 ④ 생성된 수열의 비트는 정규분포를 따라야 한다.

문 19. 사용자 워크스테이션의 클라이언트, 인증서버(AS), 티켓발행서버(TGS), 응용서버로 구성되는 Kerberos에 대한 설명으로 옳은 것은? (단, Kerberos 버전 4를 기준으로 한다)  
 ① 클라이언트는 AS에게 사용자의 ID와 패스워드를 평문으로 보내어 인증을 요청한다.  
 ② AS는 클라이언트가 TGS에 접속하는 데 필요한 세션키와 TGS에 제시할 티켓을 암호화하여 반송한다.  
 ③ 클라이언트가 응용서버에 접속하기 전에 TGS를 통해 발급 받은 티켓은 재사용될 수 없다.  
 ④ 클라이언트가 응용서버에게 제시할 티켓은 AS와 응용서버의 공유 비밀키로 암호화되어 있다.

문 20. 생체 인식 시스템은 저장되어 있는 개인의 물리적 특성을 나타내는 생체 정보 집합과 입력된 생체 정보를 비교하여 일치 정도를 판단한다. 다음 그림은 사용자 본인의 생체 정보 분포와 공격자를 포함한 타인의 생체 정보 분포, 그리고 본인 여부를 판정하기 위한 한계치를 나타낸 것이다. 그림 및 생체 인식 응용에 대한 설명으로 옳은 것만을 고른 것은?



- ㄱ. 타인을 본인으로 오인하는 허위 일치의 비율(false match rate, false acceptance rate)이 본인을 인식하지 못하고 거부하는 허위 불일치의 비율(false non-match rate, false rejection rate)보다 크다.  
 ㄴ. 한계치를 우측으로 이동시키면 보안성은 강화되지만 사용자 편리성은 저하된다.  
 ㄷ. 보안성이 높은 응용프로그램은 낮은 허위 일치 비율을 요구한다.  
 ㄹ. 가능한 용의자를 찾는 범죄학 응용프로그램의 경우 낮은 허위 일치 비율이 요구된다.

- ① ㄱ, ㄷ                                      ② ㄱ, ㄹ  
 ③ ㄴ, ㄷ                                      ④ ㄴ, ㄹ