2018년 국가직 9급 합격예측서비스 분석과 정보보호론 향후 학습방향 안내

1. 목적

2018년 첫 번째 시험이 4월 7일(토)에 시행되었습니다. 합격권에 들어간 수험생도 있지만, 전년도와 다른 출제 경향으로 공무원 시험에 대한 회의감을 느끼며 방황하시는 분들도 많으리라 생각됩니다. 이에 이번 시험의 객관적 분석을 통해 향후 학습에 조금이나마 도움을 드리고자 합니다.

2. 합격예측서비스 분석

가. 지안 합격예측서비스 소개

지안 합격예측서비스는 전년도에도 높은 정확도를 보였습니다. 올해도 4월12일 10:00 현재 250명 이상이 입력하여 전년도와 비슷한 수준의 표본집단을 이루고 있습니다. 입력된 자료 중에 표본과 많은 차이를 보이는 점수대는 분석에서 제외하였습니다.

나. 예상 합격선 분석(전산일반 채용인원 : 50명)

점수	2018년	누계
81	2	2
80	2	4
79	1	5
78	4	9
77	5	14
76	6	20
75	9	29
74	8	37
73	9	46
72	7	53
71	6	59
70	10	69
69	11	80

※ 2017년 필기 합격선은 84점임

나. 전공과목 분석

점수	정보보호론		컴퓨터일반	
	2017년	2018년	2017년	2018년
100	3	1	3	
95	8	1	4	1
90	22	6	11	5
85	21	12	28	12
80	42	13	34	26
75	22	32	34	25
70	19	27	30	28
65	22	20	20	20
60	11	22	7	11

다. 평균 72점이상자의 전공점수

1) 정보보호론 75점 미만자 : 3명
2) 컴퓨터일반 75점 미만자 : 11명

→ 전공점수가 낮으면 합격권에 들어가기 힘들었고, 특히 정보보호론은 이번 시험에서 당락을 결정하는 중요 과목으로 나타남.

라. 특이한 합격예정자

이번 시험에서 안정적인 합격권에 들어가신 분들 중에는 특이한 분들이 있습니다. 모두 평균 79점(1명), 80(2명)점 받으셨는데, 컴퓨터일반과 정보보호론 과목의 점수가 각각 (60, 100), (75, 90), (70, 85)으로 난이도가 높았던 정보보호론이 효자과목의 역할을 톡톡히 한 것으로 판단이 됩니다.(3명 모두 지안학원 수강생였음)

3. 정보보호론 적중도 분석(95~98%)

쉬운 문제부터 많은 응용을 요하는 난이도가 높은 문제가 골고루 출제가 되었습니다. 특히 함정이 있는 보기 문항이 많아서 만족할만 점수를 못 받으신 분들도 많을 것 같습니다. 정보보호론은 전 영역에서 골고루 출제되었는데 전년도와 다른 점은 행안부 시험은 법규 문제가 통상 3문제가 출제되었는데, 이번 시험은 2문제가 출제되었습니다. 그리고 암호학파트가 6문제로 출제비율이 높았습니다. 지안학원의 정보보호론은 대다수 대학교재를 분석해서 이론서와 문제집을 만들어서 크게 벗

어난 내용은 없었습니다. 다만, CC 문제의 경우 교재에는 있었지만 수업시간에 강조를 못드린 것이 아쉬움으로 남고, UNIX 문제는 적중800제에서도 다루긴 했지만 정보보호직(시스템 보안)에서 보다 강조했던 부분이 정보보호론에서 출제가 되었습니다. 전체적으로 탑스팟 교재에서 95~98% 정도의 적중률을 보였습니다.

4. 정보보호론 성공 요인과 실패 요인 분석

가. 기준 점수

4월11일 19:00에 타학원 수험생을 포함하여 많은분들이 참석하여 해설 강의 후에 상담을 진행했습니다. 매년 반복되는 패턴이긴 하지만, 시장조사를 면밀히 하지 않고 공무원 시험을 시작해서 첫 시험이 끝나고 교재와 강의 선택에 문제가 있었다는 얘기를 하곤 합니다. 정보보호론 담당 선생의 입장에서 봤을 때 만약 본인이 이번 시험에서 **80점 이상**을 획득했다면 공부방법이 옳다고 볼 수 있고, 그 아래 점수를 받으셨다면 원인을 분석 후에 다음 시험에 임해야 하지 않을까 생각합니다.

나. 성공 사례(주관적일 수 있음)

- 이론 수업을 충실히 반복해서 들으신 분
- 최신 탑스팟 이론서를 확실히 이해하시는 분
- 적중 800제 등을 통해 응용 훈련을 충실히 하신 분
- 이론+기출문제+적중문제+모의고사를 일관성 있게 정리하신 분

다. 실패 사례(주관적일 수 있음)

- 전공 시험과목을 과소평가 하신 분(시장조사 소홀)
- 요약집 위주로만 정리, 얇은 수험서를 선호하시는 분
- 기출문제 위주로만 문제정리 하신 분
- 학원마다 모의고사만 찾아서 공부하신 분
- 오래된 수험서와 문제집으로 공부하신 분

5. 향후 학습방향

가. 정보보호론 향후 학습방향

이번 정보보호론 시험의 난이도나 출제경향은 처음있었던 것이 아닙니다. 전년도의 경우 하반기 9급 추가채용과 국가직 7급부터 보였던 경향입니다. 그리고 해마다 국가직 9급보다는 지방직 시험, 서울시, 7급 시험은 더 어려웠습니다. 올해는 군무원(8월11일 시험)까지 정보보호론으로 시험과목이 바뀌어서 정보보호론을 소홀히 하고서는 공무원의 꿈을 이루기는 쉽지 않아 보입니다. 모든 시험은 공부한 만큼 나오긴 하지만, 어떤 도구와 방법으로 하느냐도 점수를 좌우하는 요인입니다. 이론정리 → 기출문제 → 적중문제 → 모의고사 순으로 하는데 본인이 목표로 하는 시험의 남은 기간을 고려하여 보완하시길 바랍니다.[(적중→모의고사) or (기출→적중→모의고사) or (이론, 기출, 적중, 모의고사)]

나. 지안에듀의 향후 무료 학습지원

국가직 정보보호론은 해설자료와 함께 동영상이 같이 업로드됩니다. 정보보호직 시험(정보시스템보안, 네트워크보안) 해설 강의(해설자료 제외)도 순차적으로 업로드하여 지방직 시험전까지는 로그인 없이 누구나 수강가능하오니 이용바랍니다.

강의 링크 :
http://tech.zianedu.com/front/ProductVodView?a_lLinkCtgKey=0&a_lGKey=105246

6. 결언

시험을 잘 보든 못 보든 올해 첫 번째 시험이 끝났습니다. 만족할만 점수를 못 받으신 분은 냉철히 자기를 돌아보시고, 약점을 최대한 보완하셔서 원하는 시험에 합격하시길 바랍니다. 이때 주변 사람의 조언을 얻는 것도 좋은 방법일 수 있습니다.

저는 개인적으로 정보보안기사를 가장 많이 합격시키고 있고, 정보보호론을 최단 시간에 고득점을 올리는 방법과 도구를 모두 제공할 수 있는 유일한 선생이라고 자부합니다.

지안/탑스팟 가족이든 아니든 개인적으로 정보보호론 공부방법에 대해서 궁금한 내용이 있으신 분들은 kingsalt1102@naver.com으로 메일 보내시면 제가 아는 범위내에서 성심껏 답변드리도록 하겠습니다.

감사합니다.

2018년 국가직 9급 정보보호론

-2018년 4월 7일 시행

1.

전자우편 보안 기술이 목표로 하는 보안 특성이 아닌 것은?

① 익명성
② 기밀성
③ 인증성
④ 무결성

◘ 전자우편의 안정성 요구 조건
◦ 기밀성(Confidentiality) : 지정된 수신자 외 불특정 사용자들에게 전송된 메시지가 공개되지 않도록 보호하는 것이다.
◦ 메시지 무결성(Integrity) : 메시지가 원래 송신된 대로 복사, 추가, 수정, 순서 변경 또는 재전송되지 않았음을 수신자에게 보증하는 것이다.
◦ 인증(Authentication) : 송신자의 신분을 수신자에게 보증하는 것이다.
◦ 부인 봉쇄(Non-repudiation) : 송신자가 메시지를 전송하였음을 제3자에게 수신자가 증명할 수 있도록 하는 기법이다.

오답피하기 ① 익명의 전자우편은 메시지 작성자가 식별되지 않도록, 제3자의 서버를 통해 수신자에게 배달되는 메일로 전자우편 보안기술과는 거리가 멀다.

정답 ①

2.

프로그램이나 손상된 시스템에 허가되지 않는 접근을 할 수 있도록 정상적인 보안 절차를 우회하는 악성 소프트웨어는?

① 다운로더(downloader)
② 키 로거(key logger)
③ 봇(bot)
④ 백도어(backdoor)

◦ 다운로더(Downloader) : 악성 코드 유포 방식. 특정 웹 사이트에서 파일을 내려받고 그 파일이 다시 스파이웨어를 내려받게 한다. 이 스파이웨어는 사용자의 동의를 받지 않고 설치되며 기존 키 워드 검색 프로그램이나 특정 안티스파이웨어 프로그램을 삭제한다.
◦ 키로거 공격(Key logger attack) : 컴퓨터 사용자의 키보드 움직임을 탐지해 ID나 패스워드, 계좌 번호, 카드 번호 등과 같은 개인의 중요한 정보를 몰래 빼 가는 해킹 공격. 공격 도구는 공격 대상의 컴퓨터에 몰래 설치되어 공격 대상 컴퓨터에 입력되는 중요한 데이터를 공격자에게 전송한다.

오답피하기 ④ 트랩도어(Trap Door)라고도 불리는 백도어는 원래 시스템 관리자나 개발자가 유사시 트러블슈팅이나 유지보수 등을 할 관리적 목적으로 필요에 의해 시스템에 고의로 남겨 둔 보안 헛점의 일종이다. 그러나 이것이 순수한 목적으로 이용되지 않고 악의적으로 이용되는 경우 보안상 치명적인 문제를 일으킬 수 있다.

정답 ④

3.

프로그램을 감염시킬 때마다 자신의 형태뿐만 아니라 행동 패턴까지 변화를 시도하기도 하는 유형의 바이러스는?

① 암호화된(encrypted) 바이러스
② 매크로(macro) 바이러스
③ 스텔스(stealth) 바이러스
④ 메타모픽(metamorphic) 바이러스

◘ 은닉 전략에 따른 바이러스 유형
◦ 암호화된 바이러스(Encrypted virus) : 바이러스의 일부는 랜덤 암호화 키를 생성하고 바이러스의 남은 부분을 암호화한다.
◦ 스텔스 바이러스(Stealth virus) : 안티 바이러스 소프트웨어에 의해 탐지되지 않기 위해 자신을 감추도록 정교하게 설계된 바이러스 형태를 말한다.
◦ 폴리모픽 바이러스(Polymorphic virus) : 감염시킬 때마다 변형하는 바이러스이기 때문에 「특징(signature)」을 이용한 탐지가 불가능해진다.
◦ 메타모픽 바이러스(Metamorphic virus) : 폴리모픽 바이러스와 마찬가지로 메타모픽 바이러스는 감염시킬 때마다 변형한다. 메타모픽 바이러스는 모양만 변하는 것이 아니라 활동하는 방법까지도 변한다.

오답피하기 ④ 은닉 전략에 따라 바이러스를 분류할 때 자신의 형태뿐만 아니라 행동패턴까지 변화를 시도하는 바이러스는 메타포픽 바이러스이다.

정답 ④

4.

증거의 수집 및 분석을 위한 디지털 포렌식의 원칙에 대한 설명으로 옳지 않은 것은?

① 정당성의 원칙－증거 수집의 절차가 적법해야 한다.
② 연계 보관성의 원칙－획득한 증거물은 변조가 불가능한 매체에 저장해야 한다.
③ 신속성의 원칙－휘발성 정보 수집을 위해 신속히 진행해야 한다.
④ 재현의 원칙－동일한 조건에서 현장 검증을 실시하면 피해 당시와 동일한 결과가 나와야 한다.

◘ 연계 보관성의 원칙
◦ 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능해야 한다. 이를 연계 보관성(Chain of Custody)이라 한다.
◦ 연계 보관성을 만족하려면 증거를 전달하고 전달받는 데 관여한 담당자와 책임자를 명시해야 한다.

◘ 무결성의 원칙
◦ 수집된 정보는 연계 보관성을 만족시켜야 하고, 각 단계를 거치는 과정에서 위조 및 변조되어서는 안 되며, 이러한 사항을 매번 확인해야 한다.
◦ 하드디스크 같은 경우에는 해시값을 구해 각 단계마다 그 값을 확인하여 무결성을 입증할 수 있다.

오답피하기 ② 획득한 증거물을 변조가 불가능한 매체에 저장하는 것은 무결성 원칙과 관련되어 있다.

정답 ②

5.

웹 애플리케이션의 대표적인 보안 위협의 하나인 인젝션 공격에 대한 대비책으로 옳지 않은 것은?

① 보안 프로토콜 및 암호 키 사용 여부 확인
② 매개변수화된 인터페이스를 제공하는 안전한 API 사용
③ 입력 값에 대한 적극적인 유효성 검증
④ 인터프리터에 대한 특수 문자 필터링 처리

◘ SQL 인젝션에 대한 대응 방안
◦ 가능한 한 외부 인터프리터를 사용하지 않는다.
◦ 백엔드 데이터베이스를 호출할 경우, 입력 값을 주의 깊게 검증
◦ 데이터베이스와 연동을 하는 스크립트의 모든 파라미터들을 점검
◦ 사용자 입력 시 특수문자(' " / ₩ ; : – +등)가 포함되어 있는지 검사
◦ 웹 애플리케이션이 사용하는 데이터베이스 사용자의 권한을 제한(DB서버와 웹 서버 연동 시 DB서버에 웹 서버 전용 계정으로 접근 설정)

오답피하기 ① SQL Injection의 방어 대책으로는 특수 문자 등의 입력값 검증의 방법을 주로 사용한다. 암호화 방법을 이용하는 보안 프로토콜은 대책으로 적절치 않다.

정답 ①

6.

개인정보 보호법 상의 개인정보의 수집·이용 및 수집 제한에 대한 설명으로 옳지 않은 것은?

① 개인정보처리자는 정보주체의 동의를 받은 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
② 개인정보처리자는 개인정보 보호법 에 따라 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
③ 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.
④ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니하는 경우 정보주체에게 재화 또는 서비스의 제공을 거부할 수 있다.

◘ 제16조(개인정보의 수집 제한)
① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.
③ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

오답피하기 ④ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니하는 경우 정보주체에게 재화 또는 서비스의 제공을 거부할 수 없다.

정답 ④

7.

〈보기 1〉은 리눅스에서 일반 사용자(hello)가 'ls -al'을 수행한 결과의 일부분이다. 〈보기 2〉의 설명에서 옳은 것만을 모두 고른 것은?

보기1

-rwxr-xr-x 1 hello world 4096 Nov 21 15:12 abc.txt
ⓐ ⓑ

보기2

ㄱ. ⓐ는 파일의 소유자, 그룹, 이외 사용자 모두가 파일을 읽고 실행할 수 있지만, 파일의 소유자만이 파일을 수정할 수 있음을 나타낸다.
ㄴ. ⓑ가 모든 사용자(파일 소유자, 그룹, 이외 사용자)에게 읽기, 쓰기, 실행 권한을 부여하려면 'chmod 777 abc.txt'의 명령을 입력하면 된다.
ㄷ. ⓑ가 해당 파일의 소유자를 root로 변경하려면 'chown root abc.txt'의 명령을 입력하면 된다.

① ㄱ ② ㄱ, ㄴ
③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

◦ 접근권한 변경(chmod) : 기존 파일 또는 디렉터리에 대한 접근권한을 변경할 때 사용한다.
◦ 소유권 또는 그룹 변경(chown/chgrp) : 파일이나 디렉터리의 소유주나 그룹을 변경할 때 사용한다. 명령을 실행하고 나면 파일의 이전 소유주는 해당 파일에 이 명령을 다시 실행할 수 없다.

오답피하기 ② chmod 명령은 해당 파일의 소유주나 슈퍼 유저 root만 실행할 수 있다. chown 명령은 슈퍼 유저 root만 실행할 수 있다(보안의 특성상 슈퍼 유저만 사용).

정답 ②

8.

다음은 CC(Common Criteria)의 7가지 보증 등급 중 하나에 대한 설명이다. 시스템이 체계적으로 설계되고, 테스트되고, 재검토되도록 (methodically designed, tested and reviewed) 요구하는 것은?

보기

낮은 수준과 높은 수준의 설계 명세를 요구한다. 인터페이스 명세가 완벽할 것을 요구한다. 제품의 보안을 명시적으로 정의한 추상화 모델을 요구한다. 독립적인 취약점 분석을 요구한다. 개발자 또는 사용자가 일반적인 TOE의 중간수준부터 높은 수준까지의 독립적으로 보증된 보안을 요구하는 곳에 적용 가능하다. 또한 추가적인 보안 관련 비용을 감수할 수 있는 곳에 적용 가능하다.

① EAL 2 ② EAL 3
③ EAL 4 ④ EAL 5

CC의 등급별 보안수준

등급	목적
EAL1	기능적 시험 (Functionally tested)
EAL2	구조적 시험 (Structurally tested)
EAL3	방법론적 시험, 검사 (Methodically tested and checked)
EAL4	방법론적 설계, 시험, 검토 (Methodically designed, tested, and reviewed)
EAL5	준정형적 설계, 시험 (Semiformally designed and tested)
EAL6	준정형적 검증된 설계, 시험 (Semiformally verified design and tested)
EAL7	정형적 검증된 설계, 시험 (Formally verified design and tested)

오답피하기 ③ 방법론적 설계, 시험, 검토(Methodically designed, tested, and reviewed)는 EAL4 단계이다.

정답 ③

9.

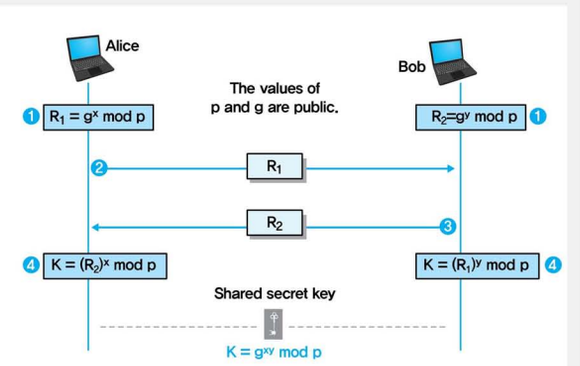
다음에 설명한 Diffie-Hellman 키 교환 프로토콜의 동작 과정에서 공격자가 알지 못하도록 반드시 비밀로 유지해야 할 정보만을 모두 고른 것은?

보기

소수 p와 p의 원시근 g에 대하여, 사용자 A는 p보다 작은 양수 a를 선택하고, $x = g^a \bmod p$를 계산하여 x를 B에게 전달한다. 마찬가지로 사용자 B는 p보다 작은 양수 b를 선택하고, $y = g^b \bmod p$를 계산하여 y를 A에게 전달한다. 그러면 A와 B는 $g^{ab} \bmod p$를 공유하게 된다.

① a, b
② p, g, a, b
③ a, b, $g^{ab} \bmod p$
④ p, g, a, b, $g^{ab} \bmod p$

Diffie-Hellman 방법



오답피하기 ③ 공개 요소는 p, g, $g^a \bmod p$, $g^b \bmod p$이다. 비공개 요소는 난수 a, b,와 공통 비밀키인 $g^{ab} \bmod p$이다.

정답 ③

10.

IEEE 802.11i에 대한 설명으로 옳지 않은 것은?

① 단말과 AP(Access Point) 간의 쌍별(pairwise) 키와 멀티캐스팅을 위한 그룹 키가 정의되어 있다.
② 전송되는 데이터를 보호하기 위해 TKIP(Temporal Key Integrity Protocol)와 CCMP(Counter Mode with Cipher Block Chaining MAC Protocol) 방식을 지원한다.
③ 서로 다른 유무선랜 영역에 속한 단말들의 종단간(end-to-end) 보안 기법에 해당한다.
④ 802.1X 표준에서 정의된 방법을 이용하여 무선 단말과 인증서버 간의 상호 인증을 할 수 있다.

802.11i

◦ 802.11i 표준은 두 개의 계층에서의 세 가지 구성요소로 되어 있다. 하위 계층은 암호화 알고리즘(TKIP와 CCMP)을 포함하며, 상위 계층은 802.1x를 포함한다.
◦ 802.11i 표준은 전체 프로토콜 스택을 다루지 않으며 OSI 계층 모델에서 단지 데이터 링크 계층에서 발생하는 것을 다룬다. 인증 프로토콜들은 이 계층보다는 상위에 위치하기 때문에 802.11i는 특정한 인증 프로토콜을 지정하지 않는다.
◦ 802.11i에는 WPA-1과 WPA-2 규격이 포함되어 있는데, 이는 암호화 방식에 따라 분류된 것으로 WPA-1은 TKIP(Temporal Key Integrity Protocol)을 WPA-2는 CCMP 암호화 방식을 사용하는 것으로 정의되어 있다.

키관리 방법

◦ 802.11i의 키들은 단말과 AP 간 키 핸드셰이크 과정을 마친 이후에 양쪽에 설치되며, 주요 암호키는 다음과 같다.
- PMK(Pairwise Master Key) : 단말과 AP 간의 마스터키
- PTK(Pairwise Transient Key) : PMK로부터 유도되어 생성되며, 하나의 단말과 AP 간 트래픽 보호에 사용
- GMK(Group Master Key) 및 GTK(Group Transient Key) : 그룹 주소로 전송되는 단말들과 AP 간 마스터키와 이를 이용해 유도되는 트래픽 보호용 키
- IGTK(Integrity GTK) : 그룹 주소로 전송되는 관리 프레임에 대한 무결성 제공

상호인증

◦ EAP-TLS 프로토콜은 인증서를 기반으로 하는 무선랜 사용자와 인증 서버간의 세션 키를 생성하는 상호 인증(양방향 인증)을 지원한다.

오답피하기 ③ 802.11i 표준은 OSI 계층 모델에서 단지 데이터 링크 계층에서 발생하는 것을 다루므로 종단간 보안 기법과는 거리가 멀다.

정답 ③

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

SSL/TLS 보안 서비스

◦ 기밀성 서비스 : DES, RC4와 같은 대칭키 암호화 알고리즘을 사용하여 제공되며, 이때 사용되는 비밀키는 Handshake Protocol을 통해 생성된다.
◦ 클라이언트와 서버 상호 인증 : 연결 설정 과정에서 서로 간에 신뢰할 수 있도록 인증을 사용하는데, 인증에는 RSA와 같은 비대칭키 암호 알고리즘, DSS와 같은 전자서명 알고리즘과 X.509 공개키 인증서가 사용된다.
◦ 메시지 무결성 서비스 : 안전한 해시 알고리즘을 사용해서 메시지 인증코드를 만들어 메시지에 포함시키기 때문에 신뢰성 있는 통신이 가능하다.

오답피하기 ② SSL은 대칭키 암호 알고리즘을 통해서 기밀성 서비스를 제공한다.

정답 ②

12.

메시지 인증에 사용되는 해시 함수의 요건으로 옳지 않은 것은?

① 임의 크기의 메시지에 적용될 수 있어야 한다.
② 해시를 생성하는 계산이 비교적 쉬워야 한다.
③ 다양한 길이의 출력을 생성할 수 있어야 한다.
④ 하드웨어 및 소프트웨어에 모두 실용적이어야 한다.

일방향 해시함수의 특징

◦ 임의 길이의 메시지로부터 고정 길이의 해시값을 계산한다.
◦ 해시값을 고속으로 계산할 수 있다.
◦ 일방향성을 갖는다.

오답피하기 ③ 해시함수는 어떤 길이의 메시지를 입력으로 주더라도 항상 고정 길이의 짧은 해시값을 생성하지 않으면 의미가 없다.

정답 ③

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?

보기

PU_X : X의 공개키
PR_X : 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 $M \,||\, E(PR_A, H(M))$

부가형 전자서명의 단계별 흐름

1. 앨리스는 일방향 해시함수로 메시지의 해시값을 계산한다.
2. 앨리스는 자신의 개인키로 해시값을 암호화한다.
3. 앨리스는 메시지와 서명을 밥에게 송신한다.
4. 밥은 수신한 서명을 앨리스의 공개키로 복호화한다.
5. 밥은 수신한 서명으로부터 얻어진 해시값과 앨리스로부터 직접 수신한 메시지의 해시값을 비교한다.

오답피하기 ④ 부가형 전자서명은 메시지 전체를 암호화하는 대신에 일방향 해시함수를 사용해서 메시지의 해시값을 구하고, 그 해시값을 암호화(해시값에 서명)하도록 하는 방법으로 보기는 이를 수식으로 표현한 것이다.

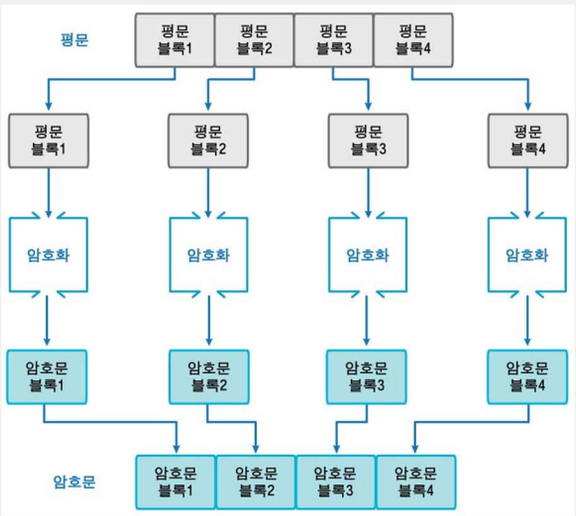
정답 ④

14.

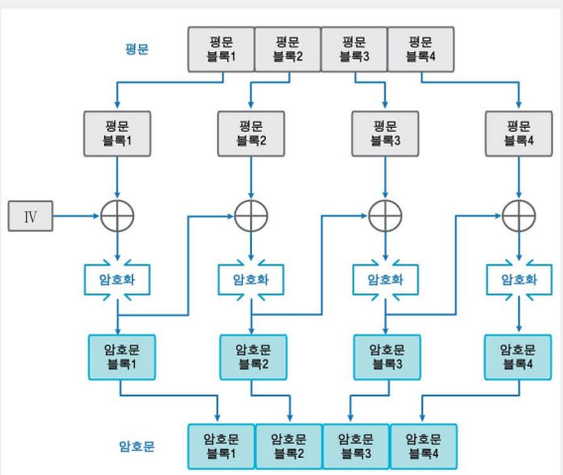
대칭키 블록 암호 알고리즘의 운영 모드 중에서 한 평문 블록의 오류가 다른 평문 블록의 암호 결과에 영향을 미치는 오류 전이(error propagation)가 발생하지 않는 모드만을 묶은 것은? (단, ECB: Electronic Code Book, CBC: Cipher Block Chaining, CFB: Cipher Feedback, OFB: Output Feedback)

① CFB, OFB
② ECB, OFB
③ CBC, CFB
④ ECB, CBC

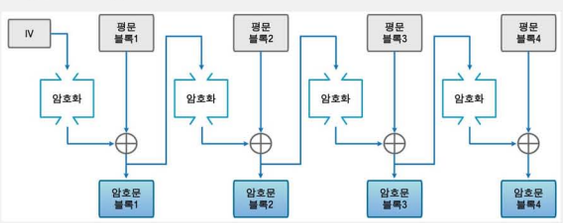
◦ ECB 모드 암호화



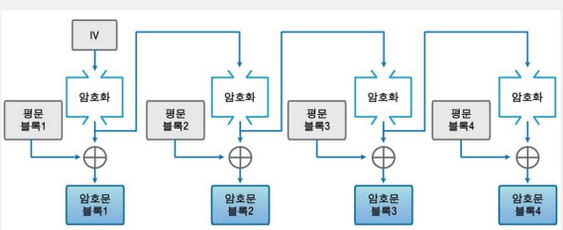
◦ CBC 모드 암호화



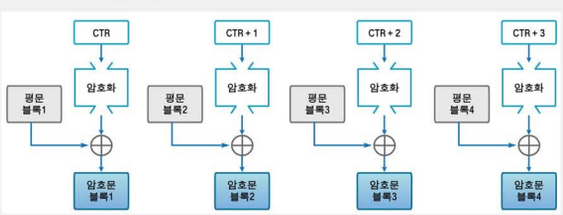
◦ CFB 모드 암호화



◦ OFB 모드 암호화



◦ CTR 모드 암호화



오답피하기 ② CBC, CFB 모드는 연쇄적 특징으로 한 평문 블록의 오류가 다른 평문 블록의 암호 결과에 영향을 미치는 오류 전이(error propagation)가 발생한다. 반면 ECB, OFB, CTR 모드에는 이런 특징이 발생하지 않는다.

정답 ②

15.

유닉스/리눅스 시스템의 로그 파일에 기록되는 정보에 대한 설명으로 옳지 않은 것은?

① utmp－로그인, 로그아웃 등 현재 시스템 사용자의 계정 정보
② loginlog－성공한 로그인에 대한 내용
③ pacct－시스템에 로그인한 모든 사용자가 수행한 프로그램 정보
④ btmp－실패한 로그인 시도

utmp(x) 로그

◦ utmp(x) 파일에 로그를 남기는 프로그램은 utmp 데몬이다. utmp 데몬은 유닉스의 가장 기본적인 로깅을 제공하는 데몬(/etc/lib/utmpd)으로 현재 시스템에 로그인한 사용자의 상태를 출력한다.
◦ utmp 데몬이 저장하는 로깅 정보의 형식은 /usr/include/utmp.h 파일에서 확인할 수 있다. utmp.h 파일에서 확인할 수 있는 utmp 구조체(struct)에는 로그인 계정 이름, 로그인한 환경(inittab id), 로그인한 디바이스(console, tty 등), 로그인한 셸의 프로세스 ID, 로그인한 계정의 형식, 로그오프 여부, 시간에 대한 저장 구조(structure) 등이 있다.
◦ utmp 파일에서는 utmp.h에서 정의된 구조체로 로그인 데이터를 저장하는데 이때 텍스트가 아닌 바이너리 형태로 저장하게 된다. 따라서 vi 에디터로는 확인할 수 없고, 특정 명령을 이용해 확인할 수 있다. utmp 데몬에 저장된 로그를 출력하는 명령에는 w, who, users, whodo, finger 등이 있다.

오답피하기 ② loginlog는 실패한 로그인 시도에 대한 로깅을 수행한다.

정답 ②

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

제34조(개인정보 유출 통지 등)

① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체

없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정안전부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

오답피하기 ③ 개인정보처리자는 개인정보가 유출된 경우 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 하나 이런 신고한 사실을 정보주체에게 알릴 필요는 없다.

정답 ③

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.

키 쌍을 작성하는 두 가지 방법

- PKI의 이용자 스스로가 수행하는 경우
- 인증기관이 수행하는 경우
  - –인증기관은 한 쌍의 공개키와 개인키를 작성
  - –안전한 방법으로 「개인키를 이용자에게 보내는」일을 할 필요가 있다.

오답피하기 ③ 인증서를 폐기할 때는 인증기관의 저장소(repository) 또는 디렉터리(directory) 시스템 등에 등재하여 신뢰 당사자가 언제든지 이 목록을 검색할 수 있도록 하여야 한다.

정답 ③

18.

암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 옳은 것은?

① 생성된 수열의 비트는 정규분포를 따라야 한다.

② 생성된 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 없어야 한다.

③ 시드(seed)라고 불리는 입력 값은 외부에 알려져도 무방하다.

④ 비결정적(non-deterministic) 알고리즘을 사용하여 재현 불가능한 수열을 생성해야 한다.

난수의 성질 분류

- 무작위성 : 통계적인 편중 없이 수열이 무작위로 되어 있는 성질
- 예측 불가능성 : 과거의 수열로부터 다음 수를 예측할 수 없다는 성질
- 재현 불가능성 : 같은 수열을 재현할 수 없다는 성질. 재현하기 위해서는 수열 그 자체를 보존해두는 수밖에 없다.

무작위성(임의성, Randomness)

- 무작위성이란 간단히 말하면 「아무렇게」 보이는 성질을 가리킨다.
- 의사난수열의 통계적인 성질을 조사해서 치우침이 없다면 그 의사난수열은 무작위하다고 여겨진다.
- 다음의 두 가지 기준은 수열의 무작위성을 평가하는데 사용된다.
  - –균일 분포(Uniform Distribution) : 수열의 비트 분포가 균일해야 한다; 즉, 0과 1의 출현빈도가 거의 동일해야 한다.
  - –독립성(Independence) : 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 없다.

의사난수 생성기

- 난수(실제로는 의사난수)를 생성하는 소프트웨어를 의사난수 생성기(PRNG, pseudo random number generator)라 부른다. 소프트웨어만으로는 진정한 난수를 생성할 수 없기 때문에 「의사」난수 생성기라 부른다.
- 소프트웨어만으로 재현 불가능성을 갖는 난수열을 만들 수 없다. 소프트웨어로는 의사난수열밖에 만들 수 없다.

진정한 난수생성기

- 진정한 난수생성기(TRNG, true random number generator)는 무작위 생성에 비해 비결정적인 소스를 사용한다.

오답피하기 ① 생성된 수열의 비트는 정규분포가 아닌 균일분포를 따라야 한다. ③ 의사난수의 「종자」는 랜덤한 비트열이다. 「종자」에 의해 자신만이 사용할 의사난수열을 생성할 수 있다. 의사난수 생성기는 모두가 공유하지만, 「종자」는 자신만의 비밀로 하지 않으면 안 된다. ④ 무작위성과 예측 불가능성을 만족하는 난수를 의사난수라고 하고, 재현불가능성까지 만족하는 난수를 진정한 난수라고 한다.

정답 ②

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.

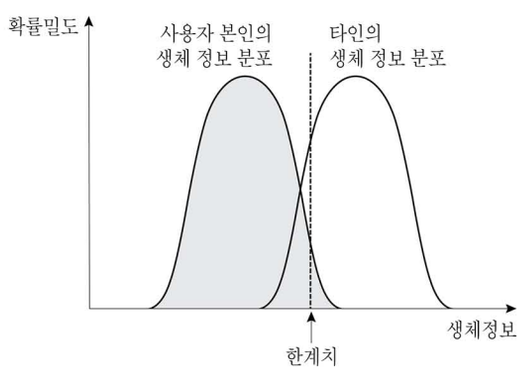
④ 클라이언트가 응용서버에게 제시할 티켓은 AS와 응용서버의 공유 비밀키로 암호화되어 있다.

오답피하기 ① 클라이언트는 자신의 등록된 ID를 이용 평문으로 AS에 자신의 요청을 보낸다.(패스워드는 제외) ③클라이언트가 응용서버에 접속하기 전에 TGS를 통해 발급 받은 티켓은 유효기간 동안 재사용될 수 있다. ④ 클라이언트가 응용서버에게 제시할 티켓은 오직 TGS와 응용서버만 아는 키로 암호화되어 있다.

정답 ②

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?



보기

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

◦ 부정거부율 : 인식돼야 할 사람이 얼마나 자주 시스템에 의해서 인식이 되지 않는지를 나타내는 값이다. FRR은 총 시도 횟수 중 부정 거부의 횟수가 얼마인지를 백분율로 나타낸 것이다.

◦ 부정허용률 : 인식되어서는 안 될 사람이 얼마나 자주 시스템에 의해서 인식이 되는지를 나타내는 값이다. FAR은 총 시도 횟수 중 부정 허용의 횟수가 얼마인지를 백분율로 나타낸 것이다.

◦ FRR(False Rejection Rate) ≒ Type Ⅰ Error ≒ FPR(False Positive Rate) ≒ 오탐

◦ FAR(False Acceptance Rate) ≒ Type Ⅱ error ≒ FNR(False Negative Rate) ≒ 미탐

오답피하기 ① ㄴ. 한계치를 우측으로 이동시키면 FRR은 줄어들어 편의성은 강화되지만 FAR은 늘어나서 보안상은 저하된다. ㄹ. 가능한 용의자를 찾는 범죄학 응용프로그램의 경우는 엉뚱한 사람을 용의자로 몰아갈 수 있으므로 오탐을 낮춰야 한다.

정답 ①