2018년도 지방공무원 공개(경력)경쟁임용시험

정보보호론

B형

※ 다음 각 물음에 알맞은 답을 골라 답안지의 같은 번호에 컴퓨터용 수성 사인펜으로 정확히 표기하시오.

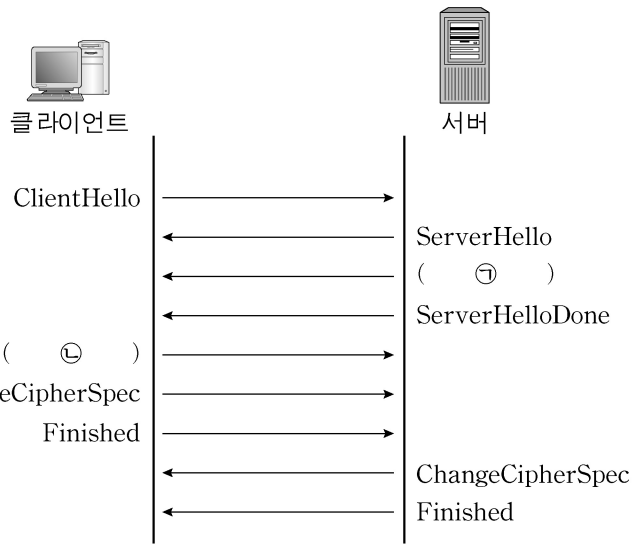
정보보호론

1. 다음 설명을 모두 만족하는 정보보호의 목표는?

> ○ 인터넷을 통해 전송되는 데이터 암호화
> ○ 데이터베이스와 저장 장치에 저장되는 데이터 암호화
> ○ 인가된 사용자들만이 정보를 볼 수 있도록 암호화

① 가용성 ② 기밀성 ③ 무결성 ④ 신뢰성

2. 그림은 SSL/TLS에서 상호인증을 요구하지 <u>않는</u> 경우의 핸드쉐이크(handshake) 과정이다. ㉠, ㉡에 들어갈 SSL/TLS 메시지를 바르게 짝지은 것은?



	㉠	㉡
①	ClientRequest	ClientHelloDone
②	ServerKeyExchange	ClientHelloDone
③	ClientKeyExchange	ServerKeyExchange
④	ServerKeyExchange	ClientKeyExchange

3. 다음 스푸핑(spoofing) 공격에 대한 설명 (가)~(다)를 바르게 짝지은 것은?

> (가) 공격 대상이 잘못된 IP 주소로 웹 접속 유도
> (나) 권한 획득을 위하여 다른 사용자의 IP 주소 강탈
> (다) MAC 주소를 속여 클라이언트에서 서버로 가는 패킷이나 그 반대 패킷의 흐름을 왜곡

	(가)	(나)	(다)
①	IP 스푸핑	ARP 스푸핑	DNS 스푸핑
②	ARP 스푸핑	IP 스푸핑	DNS 스푸핑
③	ARP 스푸핑	DNS 스푸핑	IP 스푸핑
④	DNS 스푸핑	IP 스푸핑	ARP 스푸핑

4. 리눅스 시스템에서 침해사고 분석 시 wtmp 로그파일에서 확인할 수 있는 정보로 <보기>에서 옳은 것만을 모두 고른 것은?

<보기>

ㄱ. 재부팅 시간 정보
ㄴ. 사용자의 로그인/로그아웃 정보
ㄷ. 로그인에 실패한 사용자의 IP 주소

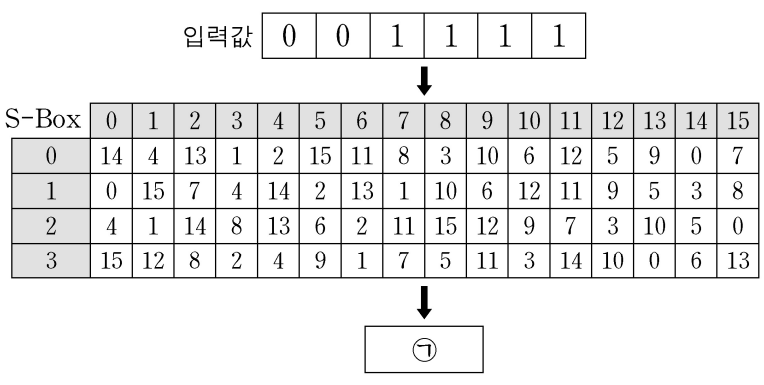
① ㄱ ② ㄴ ③ ㄱ, ㄴ ④ ㄱ, ㄴ, ㄷ

5. 다음은 신문기사의 일부이다. 빈칸 ㉠에 공통으로 들어갈 용어로 옳은 것은?

> ㉠ 은(는) 하나의 PC로 제어되는 대규모 온라인 기기 모음이며, 악성 소프트웨어를 이용해 빼앗은 다수의 좀비 컴퓨터로 구성되는 네트워크라고 볼 수 있다. 일반적으로 PC, 공유기, 스마트 폰, 웹캠, 태블릿 등을 악성코드에 감염시켜 사용한다. ㉠ 은(는) 특정 온라인 서버를 표적으로 다운시키거나 대규모 스팸 캠페인을 전달하는 DDoS 공격에 사용할 수 있다. 또한 사용자는 자신의 기기에 있는 악성코드를 인식하지 못하기 때문에 사생활 침해 사기에 개인 정보를 쉽게 도용당할 수 있다.
>
> – 2017년 ○월 ○일자 –

① 웜(worm)
② 봇넷(botnet)
③ 루트킷(rootkit)
④ 랜섬웨어(ransomware)

6. 그림은 DES(Data Encryption Standard)에서 S-Box를 통과하는 과정이다. 입력 값이 $001111_{(2)}$일 때 출력 비트 ㉠은?



① $0001_{(2)}$ ② $0010_{(2)}$ ③ $0110_{(2)}$ ④ $0111_{(2)}$

7. 블록암호 운영모드 중 CTR(counter) 모드에 대한 설명으로 <보기>에서 옳은 것만을 모두 고른 것은?

<보기>

ㄱ. 운영모드에서 시프트 레지스터를 사용한다.
ㄴ. 패딩이 필요 없으며 평문 블록과 키 스트림을 XOR 연산하여 암호문을 생성한다.
ㄷ. 암호화는 각 블록에 독립적으로 적용되기 때문에, 블록 단위 에러 발생 시 해당 블록에 영향을 준다.

① ㄱ ② ㄱ, ㄴ ③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

8. 다음의 개인정보보호법 제17조 ①항에 따라 개인정보처리자가 정보주체의 개인정보를 수집한 목적범위 안에서 제3자에게 제공할 수 있는 경우로 <보기>에서 옳은 것만을 모두 고른 것은?

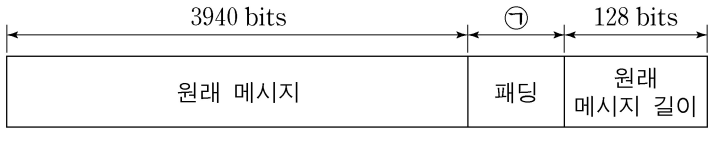
제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

<보기>

ㄱ. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
ㄴ. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
ㄷ. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

① ㄱ ② ㄷ ③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

9. 해시함수 SHA-512를 이용하여 해시값을 구하려고 한다. 원래 메시지가 3940 비트일 때, 그림에서 ㉠ 패딩의 비트 수는?



① 24 ② 28 ③ 32 ④ 36

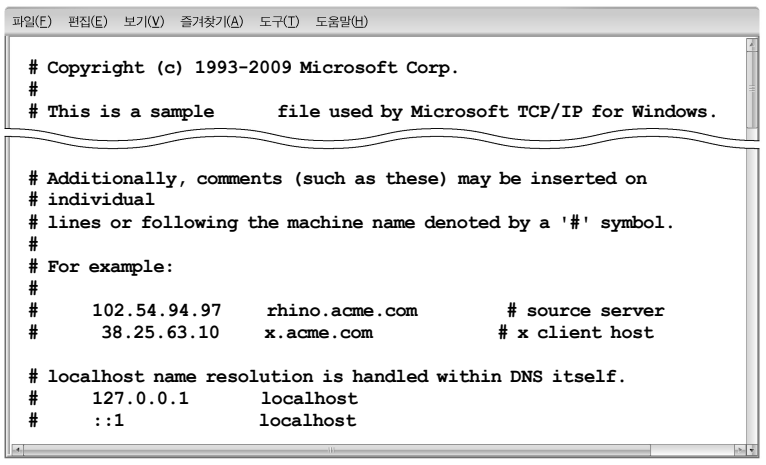
10. 데이터베이스 서버와 어플리케이션 서버로 분리하여 운용할 경우, 데이터베이스 암호화 방식 중 암·복호화가 데이터베이스 서버에서 수행되는 방식으로 <보기>에서 옳은 것만을 모두 고른 것은?

<보기>

ㄱ. API 방식
ㄴ. 플러그-인 방식
ㄷ. 필터(filter) 방식
ㄹ. TDE(Transparent Data Encryption) 방식

① ㄱ, ㄴ ② ㄱ, ㄷ ③ ㄴ, ㄹ ④ ㄴ, ㄷ, ㄹ

11. 그림은 DNS 보다 우선 적용되는 파일로, 해커는 이 파일을 변조하여 파밍(pharming)에 사용할 수 있다. 이 파일명으로 옳은 것은?



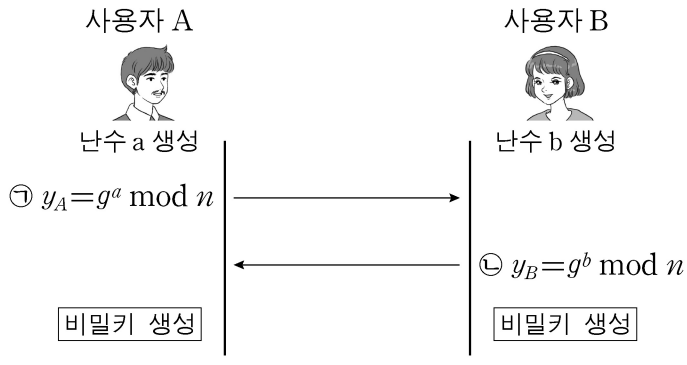
① hosts ② networks
③ protocol ④ services

12. 다음 설명을 모두 만족하는 공개키 기반구조(PKI)의 구성요소는?

○ LDAP을 이용하여 X.500 디렉터리 서비스 제공
○ 인증서와 사용자 관련 정보, 상호 인증서 쌍, CRL 등을 저장하고 검색하는 데이터베이스

① 사용자(user)
② 저장소(repository)
③ 등록기관(registration authority)
④ 인증기관(certification authority)

[13~14] 그림은 Diffie-Hellman의 키 교환 방법이다. 다음 그림을 보고 물음에 답하시오.



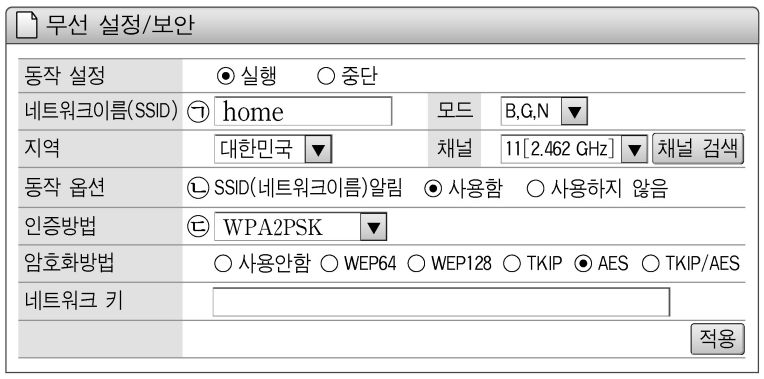
13. 위 그림의 식 ㉠, ㉡에서 n이 7일 때, g로 사용할 수 있는 것은?

① 2 ② 3 ③ 4 ④ 7

14. 위 그림에서 사용자 A, B가 생성하는 비밀키 값과 동일한 값을 구하는 식은? (단, mod는 나머지를 구하는 연산자이고, $\phi(n)$는 오일러의 Totient 함수이다.)

① $g^{a \times b} \bmod n$ ② $g^{a+b} \bmod n$
③ $g^{a \times b} \bmod \phi(n)$ ④ $g^{a+b} \bmod \phi(n)$

15. 그림은 무선 AP(Access Point)를 설정한 결과 화면의 일부이다. ㉠~㉢에 대한 설명으로 옳지 않은 것은?



① ㉠의 'home'은 관리자가 변경할 수 없다.
② ㉡을 '사용함'으로 설정하였기 때문에, 클라이언트의 무선 네트워크 연결 목록에서 'home'을 볼 수 있다.
③ 무선 네트워크 연결 목록에서 'home'을 볼 수 없게 하여 접속시도를 줄이려면, ㉡을 '사용하지 않음'으로 설정을 변경한다.
④ ㉢을 'WPA2PSK'로 설정하였기 때문에, '암호화 방법'으로 AES를 사용할 수 있다.

16. AES(Advanced Encryption Standard) 알고리즘에서 사용되는 함수들이다. 암호화 과정의 마지막 라운드에서 수행되는 함수를 <보기>에서 옳은 것만을 모두 골라, 호출 순서대로 바르게 나열한 것은?

<보기>

ㄱ. SubBytes( ) /* 바이트 치환 */
ㄴ. ShiftRows( ) /* 행 이동 */
ㄷ. MixColumns( ) /* 열 혼합 */
ㄹ. AddRoundKey( ) /* 라운드 키 더하기 */

① ㄱ－ㄷ ② ㄱ－ㄴ－ㄹ
③ ㄴ－ㄱ－ㄹ ④ ㄹ－ㄱ－ㄴ－ㄷ

17. 네트워크 기반 침입탐지시스템(Intrusion Detection System)의 특징에 대한 설명으로 <보기>에서 옳은 것만을 모두 고른 것은?

<보기>

ㄱ. 어플리케이션 서버에 설치되어 관리가 간단하다.
ㄴ. 네트워크상의 패킷을 분석하여 침입을 탐지한다.
ㄷ. 방화벽 내부의 내부 네트워크와 방화벽 외부의 DMZ에 모두 배치 가능하다.

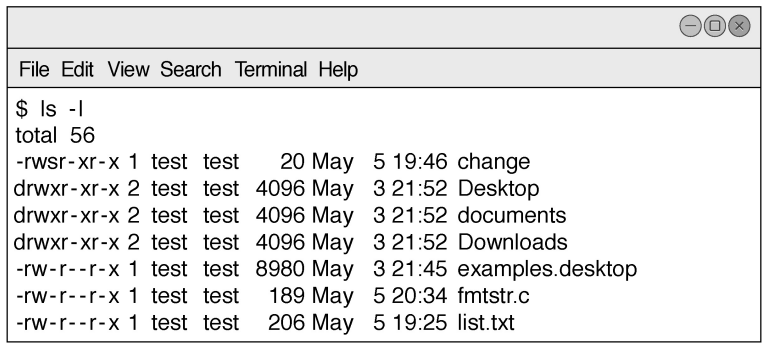
① ㄱ ② ㄴ ③ ㄱ, ㄷ ④ ㄴ, ㄷ

18. 다음 설명을 모두 만족하는 OTP(One-Time Password) 생성 방식은?

> ○ 해시체인 방식으로 계산된다.
> ○ 생성된 일회용 패스워드의 사용 횟수가 제한된다.
> ○ 검증 시 계산량이 적기 때문에 스마트카드와 같은 응용에 적합하다.

① S/KEY 방식
② 시간 동기화 방식
③ 이벤트 동기화 방식
④ Challenge-Response 방식

19. 그림은 리눅스에서 ls -l 명령을 실행한 결과이다. change 파일에 대한 설명으로 옳은 것은?



① change 파일은 setGID 비트가 설정되어 있다.
② change 파일의 접근 권한을 8진수로 표현하면 754이다.
③ test 외의 사용자는 change 파일에 대해 쓰기 권한을 가진다.
④ change 파일은 test 외의 사용자가 실행할 때 유효 사용자 ID(effective UID)는 test가 된다.

20. 그림은 C 언어 소스코드의 일부이다. 이 소스코드 ㉠~㉣에서 오버플로우 취약점을 가진 행은?

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#define BUFSIZE 10
int main(int argc, char **argv)
{
   char *dest = NULL; ---------- ㉠
   dest = (char *)malloc(BUFSIZE); ------ ㉡
   strcpy(dest, argv[1]); ---------- ㉢
   free(dest);
   return 0; ---------- ㉣
}
```

① ㉠ ② ㉡ ③ ㉢ ④ ㉣