【정보보호론】

1. 어떤 블록 암호 모드들의 복호화 정의가 아래와 같을 때, 각각의 암호화 정의로 가장 적절한 것은? (단, C_i는 i번째 암호화문, P_i는 i번째 평문, $E_K(P_i)$는 P_i를 암호화, $D_K(C_i)$는 C_i를 복호화)

복호화	$P_i = D_K(C_i) \oplus C_{i-1}$	$P_i = E_K(C_{i-1}) \oplus C_i$
암호화	㉠	㉡

	㉠	㉡
①	$C_i = E_K(P_i) \oplus C_{i-1}$	$C_i = E_K(C_{i-1}) \oplus P_i$
②	$C_i = E_K(P_i) \oplus C_{i-1}$	$C_i = D_K(C_{i-1}) \oplus P_i$
③	$C_i = E_K(P_i \oplus C_{i-1})$	$C_i = E_K(C_{i-1}) \oplus P_i$
④	$C_i = E_K(P_i \oplus C_{i-1})$	$C_i = D_K(C_{i-1}) \oplus P_i$

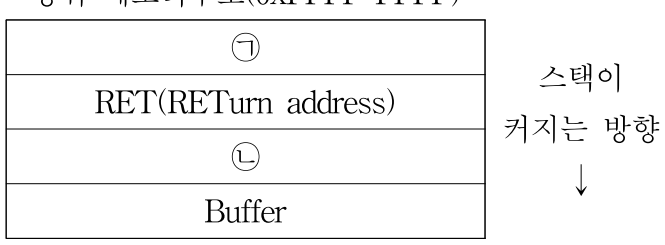
2. ITU-T 권고안 X.800에 관한 내용 중 가장 적절하지 **않은** 것은?
① OSI 보안 구조인 ITU-T 권고안 X.800은 보안 요구사항을 만족하는 체계적인 접근 방법을 규정하고 있다.
② 보안 기법(Mechanism)은 보안 공격을 탐지, 예방하고 그로부터 복구하기 위한 제반 기법이다.
③ 보안 서비스는 조직의 데이터 처리 시스템 및 정보 전송에 대한 보안을 강화하기 위한 제반 서비스이며, 데이터 기밀성, 데이터 무결성, 인증, 라우팅 제어 등이 있다.
④ 보안 서비스를 제공하기 위한 보안 기법은 암호화, 데이터 무결성, 디지털서명, 트래픽 패딩, 접근제어 등이 있다.

3. 다음 지문의 ㉠~㉣에 들어갈 값으로 가장 적절한 것은?

> 현재 10명이 사용하는 암호시스템을 30명이 사용할 수 있도록 확장하려면 키의 수도 증가한다. 대칭키 암호시스템을 채택할 때에는 10명일 경우 (㉠)개, 30명일 경우에는 (㉡)개가 필요하며, 확장에 추가로 필요한 키의 수는 (㉢)개이다. 반면, 공개키 암호시스템을 채택할 때 확장에 추가로 필요한 키의 수는 (㉣)개이다.

	㉠	㉡	㉢	㉣
①	45	435	390	40
②	90	870	780	40
③	45	435	390	60
④	90	870	780	60

4. 스택 버퍼 오버플로우(stack buffer overflow) 공격에 대응하기 위해 스택 가드(stack guard) 방법을 사용하는 경우, 다음의 논리적 메모리에 주입하는 위치와 값이 가장 적절한 것은?



	주입위치	값
①	㉠	canary
②	㉡	canary
③	㉠	Global RET
④	㉡	Global RET

5. Diffie-Hellman 키교환 알고리즘에서 소수 13과 원시근 6, 사용자 A와 B의 개인키가 각각 4, 3일 때, 공유 비밀키의 값으로 가장 적절한 것은?
① 1 ② 2 ③ 3 ④ 4

6. SSL/TLS에 관한 설명 중 가장 적절한 것은?
① SSL/TLS는 서버와 클라이언트 인증, 데이터 기밀성과 무결성을 제공하고, 통신을 수행할 때 URL은 "https://"로 시작한다.
② 공개키 암호 혹은 키 교환 기술을 이용하고 있기 때문에, 의사난수 생성기의 품질은 낮아도 된다.
③ 공개키가 서버로부터 오기 때문에, 클라이언트가 서버의 공개키를 하나도 가지고 있지 않아도 서버를 인증할 수 있다.
④ 종단 대 종단 보안 서비스인 SSL/TLS는 현재는 신뢰할 수 없는 프로토콜이다.

7. 각 용어에 대한 설명으로 가장 적절하지 **않은** 것은?
① Honeypot : 보안 위협을 사전에 대응할 목적으로 해킹 공격과 악성코드 감염을 고의로 유도함으로써 해킹 기법과 악성코드 특성과 행위를 분석하여 그에 대한 예방책을 세우도록 하는 시스템
② Bufferbloat : 데이터통신망에서 패킷 손실을 막기 위하여 버퍼의 크기를 크게 만들었지만, 이로 인하여 오히려 응답문자(ACK : acknowledgement)와 같이 작은 크기의 패킷들이 정체되어 패킷 전송이 느려지는 현상
③ Authentication, Authorization : Authentication은 사용자에 따라 적절한 접근 권한을 부여하는 것이고, Authorization은 암호를 제시함으로써 사용자를 인증하는 것
④ Grayware : 인터넷 사용자가 어쩔 수 없이 자신의 컴퓨터에 설치하도록 유도한 후(ActiveX 설치요구 등), 설치가 된 후에는 사용자의 기대와 다른 동작을 하여 시스템 성능을 악화시키거나 사용 불편을 초래하는 소프트웨어들을 총칭

8. 유클리드 알고리즘을 이용하여 2740과 1760의 최대공약수를 계산하였다. 각 위치에서의 값이 가장 적절한 것은?

q(몫)	r_1	r_2	r(나머지)
1	2740	1760	980
1	1760	㉢	780
1	980	780	200
3	780	200	㉣
1	200	180	20
㉠	180	20	0
	㉡ (최대공약수)	0	

	㉠	㉡	㉢	㉣
①	9	20	480	90
②	5	10	480	90
③	5	10	980	180
④	9	20	980	180

9. 다음 설명에 해당하는 공격으로 가장 적절한 것은?

> 컴퓨터의 소프트웨어나 하드웨어 및 컴퓨터 관련 전자 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 만들어진 절차나 일련의 명령, 스크립트, 프로그램 또는 특정한 데이터 조각을 말하며, 이러한 것들을 사용한 공격 행위를 이르기도 한다. 주로 공격 대상 컴퓨터의 제어 권한 획득이나 서비스 거부 공격(DoS) 등을 목적으로 한다.

① Trojan Horse ② Exploit
③ Hoax ④ Bonk

10. '2021 국가정보보호백서'에 게재된 PKI(Public-Key Infrastructure) 공인인증기관(CA, Certification Authority)으로 지정되지 **않은** 곳은?

① ㈜코스콤 ② 한국정보인증㈜
③ ㈜한국무역정보통신 ④ ㈜한국거래소

11. IoT(Internet of Things)에 관한 설명으로 가장 적절하지 **않은** 것은?

① IoT 기기를 대상으로 한 악성코드는 미라이(Mirai), 다이어(Dyre) 등이 있다.
② 네트워크 카메라 제품에 관한 주요 보안 위협에는 공격 대상자의 사진, 동영상을 공격자의 서버 및 이메일로 전송하는 방법 등이 있다.
③ IoT 제품의 보안 요구사항에는 시큐어 코딩, 알려진 보안 취약점 및 취약점 제거, 안전한 소프트웨어 사용 등이 있다.
④ 안전한 IoT 사용을 위해 ARIA, SEED, EC-KCDSA 사용을 권장한다.

12. 대칭키 블록 암호 알고리즘 중 키 길이가 256bit인 것으로 가장 적절한 것은?

① RSA ② SHA-3
③ Blowfish ④ ARIA

13. 매스메일러형 웜 바이러스에 관한 설명으로 가장 적절하지 **않은** 것은?

① SMTP 서버의 네트워크 트래픽을 증가시킨다.
② 버퍼오버플로우나 포맷 스트링과 같은 취약점을 이용하여 확산 및 공격한다.
③ 매스메일러형 웜 바이러스에는 베이글, 넷스카이, 소빅 등이 있다.
④ 매스메일러형 바이러스는 내부 교육을 통해 충분히 예방할 수 있다.

14. 다음에서 Elgamal 암호화 방식에 관한 설명으로 올바르게 짝지어진 것은?

㉠ RSA 알고리즘과 동일한 안전성을 제공하기 위해서 더 짧은 길이의 키를 필요로 한다.
㉡ 이산대수에 근거해서 만든 시스템이다.
㉢ 암호화와 디지털 서명 알고리즘을 모두 지원한다.
㉣ Rabin, ECC 알고리즘과 비교할 때 가장 빠르다.

① ㉠㉢ ② ㉠㉣ ③ ㉡㉢ ④ ㉡㉣

15. 정보시스템 및 네트워크의 취약점 분석도구로 가장 적절하지 **않은** 것은?

① Nipper
② COPS(Computer Oracle and Password System)
③ Nessus
④ BotSnipper

16. 다음 설명에 해당하는 공격유형으로 가장 적절한 것은?

· 사용자가 인증한 세션이 특정 동작을 수행하여도 계속 유지되어 정상적인 요청과 비정상적인 요청을 구분하지 못하는 점을 악용하는 공격이다.
· 사용자의 브라우저 내에서 서버가 유지하고 있는 신뢰를 이용해서 웹 서버를 공격하며 악성 스크립트를 서버에 요청한다는 특징이 있다.
· 데이터 등록·변경의 기능이 있는 페이지에서 동일 요청으로 매회 등록 및 변경 기능이 정상적으로 수행이 되면 이 공격에 취약할 가능성이 있다.

① Session Hijacking ② CSRF
③ SQL Injection ④ XSS

17. 다음에서 설명하는 웹 공격에 해당하는 용어가 올바르게 짝지어진 것은?

㉠ 해커가 웹사이트 화면을 원하는 화면으로 바꾸어 해킹 성공을 알리는 공격으로써 공격자가 자신의 존재감을 알리는 목적으로 활용
㉡ 클라이언트의 명령을 서버에서 실행시켜주는 프로그램으로, 공격자가 악의적인 목적을 가지고 웹서버에서 임의의 명령을 실행할 수 있도록 제작한 프로그램
㉢ 웹 표적으로 삼은 특정 집단이 자주 이용하는 웹사이트를 감염시키고, 피해 대상이 그 웹사이트를 방문할 때까지 기다리는 웹 기반 공격

	㉠	㉡	㉢
①	인젝터	워터링 홀	웹 쉘
②	디페이스	웹 쉘	워터링 홀
③	인젝터	웹 쉘	워터링 홀
④	디페이스	워터링 홀	웹 쉘

18. 생체 인증 기법 중 신체학적 특성을 이용한 인증으로 가장 적절하지 **않은** 것은?

① 지문 ② 얼굴 ③ 홍채 ④ 걸음걸이

19. CSA(Cloud Security Alliance)에서 2019년에 발표한 클라우드 환경에서의 위협, 리스크 및 취약점에 관한 11대 보안 위협 요인에 포함되지 **않은** 것은?

① 계정 하이재킹
② 데이터 유출
③ 클라우드 서비스 남용 및 악용
④ 가상화 취약점

20. 다음에서 설명하는 전자우편 보안 프로토콜의 특징이 올바르게 짝지어진 것은?

㉠ S/MIME 보안 서비스에는 메시지에 대한 송신 사실 부인 방지가 포함되지 않는다.
㉡ PGP는 기밀성, 메시지 인증, 사용자 인증, 송신 부인방지, 단편화와 재조립에 대한 보안 기능을 지원한다.
㉢ PEM은 IETF가 채택한 인터넷 표준 프로토콜로 다소 구현이 복잡하고 높은 보안성을 가지고 있지만, 현재는 많이 사용하지 않고 있다.
㉣ PGP는 IDEA, 3DES로 메시지를 암호화하여 전송하고, S/MIME은 AES 128bit로 메시지를 암호화하고 압축하여 전송한다.

① ㉡㉢㉣ ② ㉠㉢ ③ ㉡㉢ ④ ㉠㉡㉢㉣