정보보호론	국가 전산 7급	2023년 9월 23일

♠ 필기합격인원/합격선(52명/79점) - 선발예정인원 38명 ♠

1. 검증을 마친 시스템 사용자가 시스템 자원에 접근할 수 있도록 허락하는 과정은? [2023년 국가 7급]

① Authentication ② Authorization
③ Audit ④ Accounting

♤ **인증과 허가**

authentication	인증, 입증, 증명
authorization	인가, 허가(권한 부여)
audit	회계 감사, (품질수준에 대한) 검사, 회계를 감사하다.
accounting	회계 (업무)

// 인증과 허가

authentication	• 인증은 **식별** 또는 **신원 확인**이 목적이다. • 서버가 현재 요청을 보내는 클라이언트가 누구인지 식별하는 프로세스 • 인증은 사용자 측에서는 '**로그인**' 부분이다.
authorization	• 허가(인가)는 자원에 접근할 수 있는 **권한 부여**가 목적이다. • 허가는 권한의 **차등적 부여**를 위한 프로세스이다.**(권한은 사용자마다 다름)** • 허가는 인증 결과를 활용하기도 하지만, 필수요건은 아니다.

• 일반적으로, 인증을 진행한 후에 허가가 진행된다.
• 일반적으로, 인증과 허가 사이는 시간으로 선후관계는 존재한다고 볼 수 있다.
• 하지만, 인증과 허가는 별개의 목적을 가지는 전혀 다른 프로세스이다.
• **예** : 인증 없이도 허가 프로세스를 진행할 수 있고, 허가 없이 인증만 진행할 수 있다.

// 왜 대부분 사람들은 '인증/허가'를 묶어서 취급할까?
• 먼저, 개발에서 두 로직은 별개이지만 현실적으로 두 로직은 **밀접**하게 **연결**되어 있다.
• 서버가 사용자의 인증 요청을 받으면 누구인지 식별한 후 서버는 사용자를 인증하게 되고
• 서버는 인증 결과를 바탕으로 권한 정보를 조회하여 자원에 대한 접근 권한을 부여한다.
• 즉, 사용자가 인증 후 접근 권한을 요청하지 않아도 서버가 미리 **알아서** 권한을 부여한다.

정답 : ②

2. 도출된 위험에 대하여 보안 대책 마련을 위한 추가적인 비용의 투입이나 외부와의 연계 · 협력을 고려하지 않고, 잠재적 위험을 자체적으로 감수하거나 일부 시스템 기능의 사용 포기에 따른 불편함을 감수하는 방식의 위험 대처에 해당하는 것만을 모두 고르면? [2023년 국가 7급]

ㄱ. 위험수용	ㄴ. 위험회피
ㄷ. 위험감소	ㄹ. 위험전가

① ㄱ, ㄴ ② ㄱ, ㄹ ③ ㄴ, ㄷ ④ ㄷ, ㄹ

♤ **위험관리**

// 위험수용

- 위험에 대한 조치를 취하지 않고, 현 상태의 위험을 허용하기로 결정하는 것이다.
- 위험 처리 비용이 과도하면, 일정 수준의 위험은 그냥 받아들이는 것이다.
- 위험이 조직에 발생시키는 결과에 대한 책임을 관리층이 지는 방식이다.

// 위험회피

- 위험이 존재하는 프로세스나 사업을 포기하는 것이다.

// 위험전가

- 잠재적 위험 비용을 제3자에게 이전하거나 할당하는 것이다.
- 위험에 대한 보험을 들거나 다른 기관과 계약을 통하여 잠재적 손실을 제3자에게 이전하는 것

// 위험감소

- 위험을 감소시킬 수 있는 효과적인 대책을 채택하여 구현하는 것이다.

정답 : ①

3. 해시충돌을 바르게 나타낸 것은? (단, 해시함수 $h_1 \neq h_2$, 해시 입력값 $k_1 \neq k_2$) [2023년 국가 7급]

① $h_1(k_1) = h_2(k_1)$ ② $h_1(k_1) = h_1(k_2)$

③ $h_1(k_1) \neq h_1(k_2)$ ④ $h_1(k_1) \neq h_2(k_2)$

♤ **해시충돌**

- 해시충돌 : 동일한 해시함수가 서로 다른 입력값에 대해 같은 해시값을 출력하는 것!
- h(2) = 2 % 7 = 2
- h(9) = 9 % 7 = 2
- h(2) = h(9) = $h_1(k_1) = h_1(k_2)$ = **2**

정답 : ②

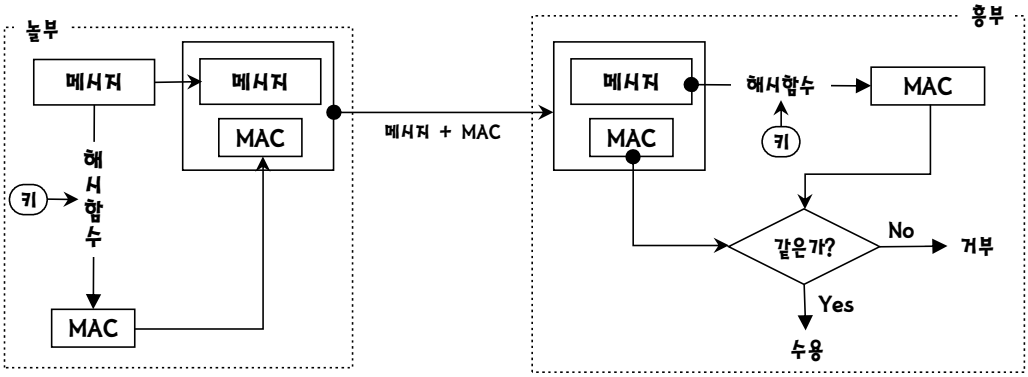
4. 메시지인증코드(MAC)에 대한 설명으로 옳지 않은 것은? [2023년 국가 7급]

① MAC을 사용하기 위해서는 송·수신자만의 공유 비밀키가 필요하다.
② MAC의 길이는 메시지의 길이와 같다.
③ 메시지와 함께 전달되어 메시지 무결성 검증에 이용된다.
④ 수신자는 검증을 통해 메시지가 송신자로부터 전송된 것을 확인할 수 있다.

♤ **메시지인증코드**

• MAC의 길이는 메시지의 길이와 같다.**(×)**
→ MAC는 메시지를 압축한 **작은 고정길이 값**이다.(예:256bit)

• MAC는 메시지 **인증과 무결성**을 제공한다.(MAC는 키를 사용)



• 키는 송수신자 사이에 공유된 비밀키이다.(shared secret key) – **키는 사전에 교환**

① MAC는 키를 사용하는 해시함수에 의한 출력값(해시값)이다.
• MAC는 "메시지와 **비밀키**"를 기초로 해서 생성되는 고정길이 값이다.
• MAC는 메시지 인증을 위해 메시지에 덧붙여지는 작은 데이터 블록이다.
② MAC 함수는 비밀키를 파라미터로 가지며, 다음 특성을 만족해야 한다.
• 키를 모르는 공격자가 메시지에 대한 MAC값을 위장하는 것은 계산상 불가능하다.
• computation-resistance(계산 저항성)
③ MAC의 안전성은 사용하는 해시 알고리즘의 안전성에 의존한다.
④ MAC에서 메시지 **인증**
• 즉, 메시지를 보낸 사람의 "신분 확인"을 위한 것이다.
• 단, 공개키 방식이 아닌 대칭키 방식이므로 **부인방지를 위한 법적인 효력은 없다.**
⑤ MAC 해시함수 : CBC-MAC, HMAC(Hashed MAC)

정답 : ②

5. 리눅스 파일의 접근 권한을 설정하기 위하여 다음과 같은 명령을 실행한 경우, 해당 파일에 부여된 권한을 바르게 나타낸 것은? [2023년 국가 7급]

chmod 2755 file1

① -rwxr-xr-x
② -rwsr-xr-x
③ -rwxr-sr-x
④ -rwsr-sr-x

♤ chmod에서 숫자를 이용한 권한 설정

4 : 읽기 권한 2 : 쓰기 권한 1 : 실행 권한	• 읽기, 쓰기, 실행 권한 설정 : 4 + 2 + 1 = 7 (2진수로 111) • 읽기, 쓰기 권한 설정 : 4 + 2 = 6 (2진수로 110) • 읽기, 실행 권한 설정 : 4 + 1 = 5 (2진수로 101) • 읽기 권한 설정 : 4 (2진수로 100) • 쓰기, 실행 권한 설정 : 2 + 1 = 3 (2진수로 011) • 쓰기 권한 설정 : 2 (2진수로 010) • 실행 권한 설정 : 1 (2진수로 001)

// 특별한 퍼미션 setuid, setgid, sticky bit

모드	퍼미션	퍼미션 설정
s	setuid	• setuid가 설정된 파일은 실행되는 동안 **파일 소유자 권한**으로 **실행** • setuid의 **심볼릭 모드는 's'이고, 8진수 모드는 4000**이다. # chmod 4755 sample → sample 파일에 setuid 퍼미션 설정
s	setgid	• setgid가 설정된 파일은 **파일 소유자 그룹의 권한**으로 **실행** • setgid의 **심볼릭 모드는 's'이고, 8진수 모드는 2000**이다. # chmod 2755 sample → sample 파일에 setgid 퍼미션 설정
t	sticky bit	• sticky bit는 디렉터리에 있는 파일을 보호하기 위한 퍼미션 • sticky bit의 **심볼릭 모드는 't' 이고, 8진수 모드는 1000**이다. # chmod 1777 aaa → aaa 디렉터리에 sticky bit 설정

chmod 755 file1	chmod 2755 file1
-rwx r-x r-x	-rwx r-s r-x

• 파일 소유자가 속한 그룹의 권한 : r-s

정답 : ③

6. 「정보통신기반 보호법」상 주요정보통신기반시설을 관리하는 관리기관의 장이 국가정보원장에게 우선적으로 기술적 지원을 요청하여야 하는 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설이 아닌 것은? [2023년 국가 7급]

① 도로 · 철도 · 지하철 · 공항 · 항만 등 주요 교통시설
② 전력, 가스, 석유 등 에너지 · 수자원 시설
③ 금융 정보통신기반시설 등 개인정보가 저장된 정보통신기반시설
④ 원자력 · 국방과학 · 첨단방위산업관련 정부출연연구기관의 연구시설

♤ **정보통신기반 보호법 – 제7조(주요정보통신기반시설의 보호지원)**

① 관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 과학기술정보통신부장관과 국가정보원장등 또는 필요한 경우 대통령령으로 정하는 전문기관의 장에게 다음 각 호의 업무에 대한 기술적 지원을 요청할 수 있다.
〈개정 2007. 12. 21., 2008. 2. 29., 2013. 3. 23., 2017. 7. 26., 2020. 6. 9.〉
1. 주요정보통신기반시설보호대책의 수립
2. 주요정보통신기반시설의 침해사고 예방 및 복구
3. 제11조에 따른 보호조치 명령 · 권고의 이행

② 국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. 〈개정 2007. 12. 21.〉
1. 도로 · 철도 · 지하철 · 공항 · 항만 등 주요 교통시설
2. 전력, 가스, 석유 등 에너지 · 수자원 시설
3. 방송중계 · 국가지도통신망 시설
4. 원자력 · 국방과학 · 첨단방위산업관련 정부출연연구기관의 연구시설

③ 국가정보원장은 제1항 및 제2항에도 불구하고 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니된다.
〈개정 2007. 12. 21., 2020. 6. 9.〉

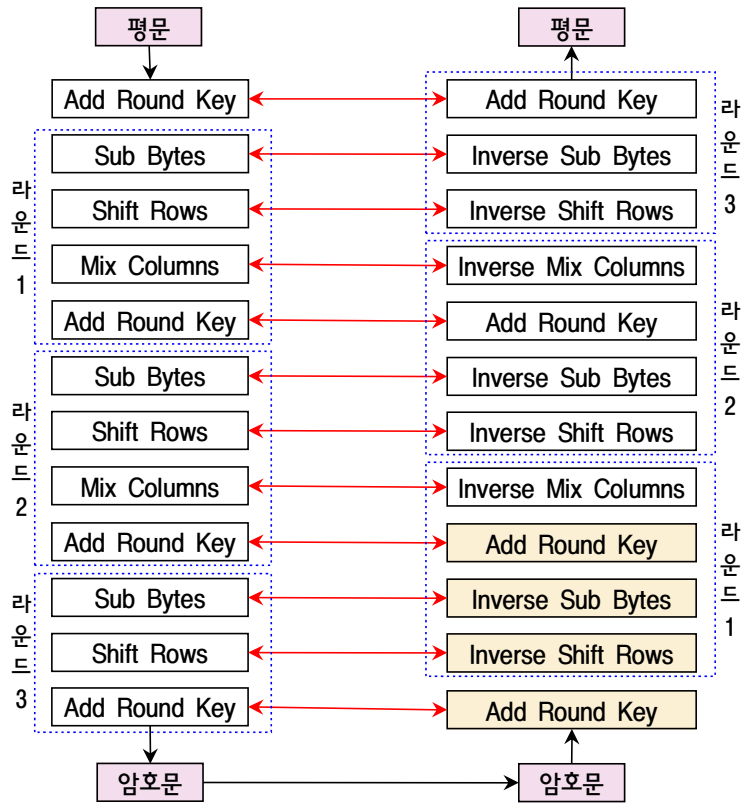
정답 : ③

7. AES 알고리즘의 복호화 과정에서 한 암호 블록에 대해 실행되는 처음 4개의 오퍼레이션을 첫 번째부터 네 번째까지 순서대로 바르게 나열한 것은?(ARK: Add Round Key, IMC: Inverse Mix Columns, ISR: Inverse Shift Rows, ISB:Inverse Substitute Bytes) [2023년 국가 7급]

① ARK - IMC - ISR - ISB　　② ARK - ISB - ISR - IMC
③ ARK - ISR - ISB - ARK　　④ IMC - ISR - ISB - ARK

♤ AES – 암복호화 과정 : 핵심 부분만 설명

- AES 암호는 안전성을 위해 각 라운드는 **4가지 단계의 변환**을 적용한다.**(문제 참조)**
- 암호의 **마지막 라운드**는 MixColumns을 제외한 **3단계의 변환**을 사용한다.
- 다음은 간단하게 **3 라운드** 기준으로 AES 암호의 암복호화 과정을 그린 것이다.



모든 라운드가 같은 라운드 4이면	암호 과정 : SB-SR-MC-RK 순일 때 복호 과정 : ARK-IMC-ISR-ISB 순처럼 될 수도 있다.	
모든 라운드가 라운드 4가 아니면	암호 과정 : SB-SR-MC-RK 순일 때 복호 과정 : ARK-ISR-ISB-ARK 순처럼 될 수도 있다.	주어진 문제의 정답

정답 : ③

8. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3의 일부이다. (가)와 (나)에 들어갈 용어를 바르게 연결한 것은? [2023년 국가 7급]

> **(가)**는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 **(나)**로 지정하고 과학기술정보통신부장관에게 신고하여야 한다.

	(가)	(나)
①	정보통신서비스 제공자	정보보호 최고책임자
②	정보통신서비스 제공자	개인정보 보호책임자
③	개인정보처리자	정보보호 최고책임자
④	개인정보처리자	개인정보 보호책임자

♤ **정보통신망 이용촉진 및 정보보호 등에 관한 법률 – 제45조의3(정보보호 최고책임자의 지정 등)**

① **정보통신서비스 제공자**는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 **정보보호 최고책임자**로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다. 〈개정 2014. 5. 28., 2017. 7. 26., 2018. 6. 12., 2021. 6. 8.〉

② 제1항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다. 〈신설 2014. 5. 28.〉

③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다. 〈신설 2018. 6. 12.〉

④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. 〈개정 2021. 6. 8.〉

1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
   가. 정보보호 계획의 수립 · 시행 및 개선
   나. 정보보호 실태와 관행의 정기적인 감사 및 개선
   다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련
   라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행
2. 정보보호 최고책임자는 다음 각 목의 업무를 겸할 수 있다.
   가. 「정보보호산업의 진흥에 관한 법률」 제13조에 따른 정보보호 공시에 관한 업무
   나. 「정보통신기반 보호법」 제5조제5항에 따른 정보보호책임자의 업무
   다. 「전자금융거래법」 제21조의2제4항에 따른 정보보호최고책임자의 업무
   라. 「개인정보 보호법」 제31조제2항에 따른 개인정보 보호책임자의 업무
   마. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

정답 : ①

9. 리눅스에서 사용자 계정의 패스워드를 변경한 후 그 패스워드를 그대로 사용해야 할 최소기간과 사용할 수 있는 최대기간을 지정하기 위한 명령어와 그 명령의 실행 결과가 저장되는 파일을 바르게 연결한 것은? [2023년 국가 7급]

	명령어	파일
①	usermod	/etc/passwd
②	chage	/etc/passwd
③	usermod	/etc/shadow
④	chage	/etc/shadow

♤ **chage : 사용자의 패스워드 만기 정보 변경 및 설정하는 명령어**

• chage -M 90 user02	패스워드 유효기간을 90일로 지정
• chage -M 9999 user02	패스워드 유효기간을 9999일로 지정
• chage -M 99999 user02	패스워드 유효기간을 무제한으로 지정

- 옵션 **-M**은 패스워드 최종 변경일로부터 패스워드 변경 없이 사용할 수 있는 최대일수 설정
- 리눅스 사용자 정보는 /etc/passwd 파일에 기록되어 있다.
- 하지만, /etc/passwd 파일의 **패스워드** 항목은 보안상 **/etc/shadow** 파일에서 별도로 관리한다.
- chage는 패스워드 정보를 수정하는 명령어이므로 **/etc/shadow** 파일도 동시에 갱신된다.

정답 : ④

10. 서비스 거부(DoS) 공격에 대한 대응 방법으로 옳지 않은 것은? [2023년 국가 7급]

① Smurf 공격에 대응하기 위해 브로드캐스트 IP 주소로 전송되는 ICMP 패킷을 차단한다.
② Land 공격에 대응하기 위해 출발지와 목적지의 IP 주소가 동일한 패킷을 차단한다.
③ TCP SYN Flooding 공격에 대응하기 위해 서버의 TCP 연결 테이블의 크기를 감소시킨다.
④ Slowloris 공격에 대응하기 위해 특정 클라이언트로부터 전송된 일정시간 동안의 불완전한 HTTP 요청 개수와 연결 유지시간을 제한한다.

♤ **서비스 거부 공격에 대한 대응 방법**

- TCP SYN Flooding 공격에 **대응**하기 위해 서버의 TCP **연결 테이블**의 **크기**를 **감소**시킨다.**(×)**
  → 서버의 TCP 연결 테이블의 크기를 **증가**시켜야 한다.**(백로그큐 크기 증가)**
- 그런데, **백로그큐 크기 증가**는 임시적인 대응이고 **신쿠기** 기능을 사용해야 한다.

정답 : ③