ICT의 가치를 이끄는 사람들!!

126회

정보관리기술사 기출풀이 4교시

T 02.724.1831 E kpcitpe@kpc.or.kr H www.kpc.or.kr C cafe.naver.com/kpcitpe

국가기술자격 기술사 시험문제

정보처리기술사 제 126 회 제 4 교시

분야	정보처리	종목	정보관리기술사	수험번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 25 점)

1. 메타버스(Metaverse)는 현실과 가상을 혼합하는 기술이다. 메타버스로 구현된 세계에는 편리한 면도 있지만 보안적, 사회적으로 많은 문제가 내포되어 있다. 다음과 같은 측면으로 설명하시오.
   1) 메타버스의 특징
   2) 정보시스템 측면의 메타버스의 보안 위협
   3) 메타버스에서 발생 할 수 있는 사회적 문제점
   4) 안전한 메타버스를 위한 방안

2. Real Time Scheduling 이 갖는 문제 중 우선순위 역전(Priority Inversion)이 있다. Task 1, Task 2, Task 3 순으로 우선순위가 낮다고 할 때 우선순위 역전을 사례기반으로 설명하고, 우선순위 역전을 해결하기 위한 2 가지 기법에 대하여 설명하시오.(단 P, V 연산을 사용한다)

3. 미라이 봇넷(Mirai Botnet)에 대하여 설명하시오
   1) 미라이 봇넷의 개념
   2) IoT 서비스 생애주기별 보안위협 및 해결 방안
   3) IoT 공통보안 7 대원칙

4. VPN(Virtual Private Network)과 Tor 에 대하여 설명하시오.

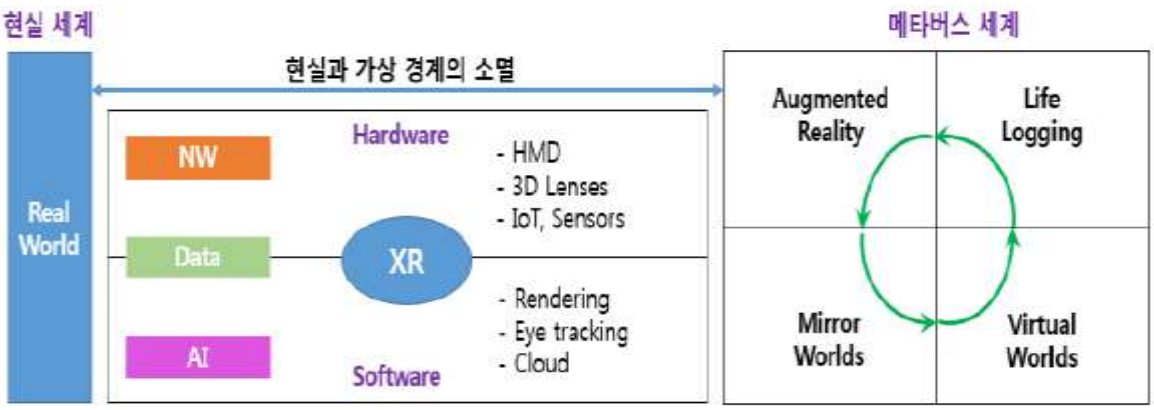
5. RSA(Rivest-Shamir-Adleman)알고리즘과 DSA(Digital Signature Algorithm)을 비교하여 설명하시오.

6. 디지털 포렌식 (Digital Forensic)의 증거수집기술 중 하나인 파일카빙(FC : File Carving)에 대하여 설명하시오.
   1) 파일 카빙에 대한 개념
   2) 파일 카빙의 4 종류 기법의 특징

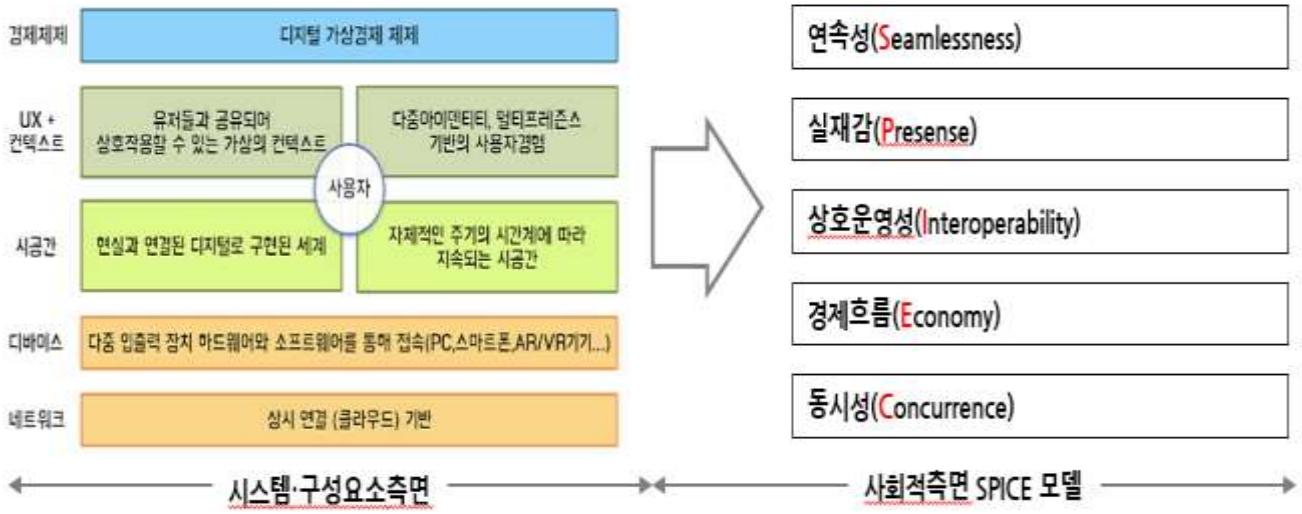
문 제	1. 메타버스(Metaverse)는 현실과 가상을 혼합하는 기술이다. 메타버스로 구현된 세계에는 편리한 면도 있지만 보안적, 사회적으로 많은 문제가 내포되어 있다. 다음과 같은 측면으로 설명 하시오. 1) 메타버스의 특징 2) 정보시스템 측면의 메타버스의 보안위협 3) 메타버스에서 발생할 수 있는 사회적 문제점 4) 안전한 메타버스를 위한 방안
출 제 영 역	디지털서비스 / 난 이 도 ★★★★☆
출 제 배 경	2022 년 보안분야의 10 대 핫 키워드 중 비대면 시대 상징하는 메타버스의 특징을 고려한 맞춤형 전략 수립 필요성
출 제 빈 도	-125 회 관리 1 교시-메타버스 개념 -123 회 관리 2 교시-개념, 운영사례, 시사점 -합숙(22.01) 응용 -메타버스 보안취약점과 대응방안 및 윤리적 이슈 -합숙(22.07) 관리 -메타버스 핵심기술 및 주요 유형 -모의(21.12) 공통 – 메타버스의 정의 및 텔레프레즌스와 텔레오퍼레이션 -모의(21.10) 관리 – 메타버스개념, 자율트윈, 서비스 동향 -모의(21.06) 관리 – 메타버스의 핵심 기술 및 주요유형
참 고 자 료	- 2021 년 한국산학기술학회 추계 학술발표논문집 메타버스 기술 동향 및 관련 사이버 위협 조사분석 - 메타버스(metaverse)의 현황과 향후과제/국회입법조사처 제/(21.7.28)
Keyword	지속성, 반응성, 상오운용, 가상화폐, 저작권, XR, AR, 윤리적 이슈, 중독
풀 이	서 OO 기술사(제 124 회 정보관리기술사/yhsuh2107@naver.com)

I. 현실세계의 비중 축소와 새로운'확장가상세계'로의 진화, 메타버스 (Metaverse)의 개념 및 특징

가. 메타버스(Metaverse)의 개념

정의	가상과 현실이 상호작용하며 공진화하고 그 속에서 사회·경제·문화 활동이 이루어지면서 가치를 창출하는 세상 또는 확장가상세계
구성	

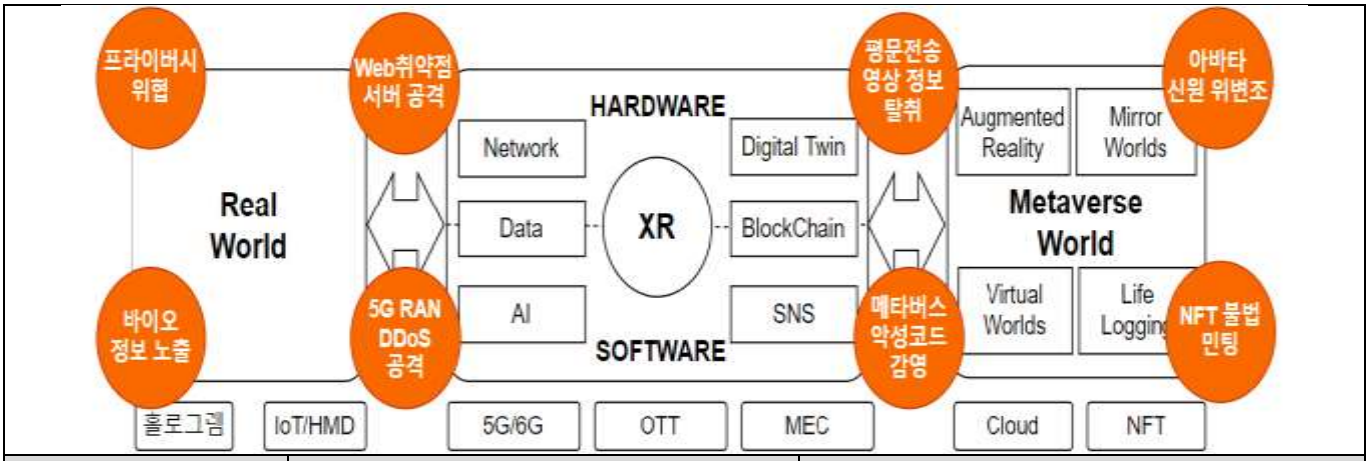
나. 메타버스(Metaverse)의 특징



지속성	Persistent	지속적이고 계속적으로 존재하는 장소; 온라인에서는 오프라인에서 든 사람들의 삶은 지속될 것임
반응성	Reactive	가상 환경과 그곳에 거주하는 사람들이 실시간으로 사용자의 행동에 대응하고 반응할 것
상호운영성	Interoperable	어떤 플랫폼에도 얽매이지 않고, 경험, 소유물 및 정체성의 변화 없이 플랫폼 간 상호 이동할 것
창의성	Creative	사람들이 콘텐츠를 수동적으로 소비하지 않고 적극적으로 참여하는 창의성과 영감의 촉매제가 될 것
사용자정의	User-defined	삶을 살고, 연결하고, 창조하고, 참여하는 사람들에 의해 소유되고 형성될 것
탈중앙화	Decentralize	소유권이 집중 화되지 않을 것
일상화	Everyday	일상 활동과 업무와 완벽하게 연결
무한성	Limitless	사용자 수, 경험 또는 월드에 대한 제한이 없을 것
시회화	Social	새로운 사람을 만나고 교류하며, 기존의 관계를 강화하고, 새로 운 공동체를 만드는 장소

II. 정보시스템 측면의 메타버스의 보안 위협

가. 정보시스템 인프라 측면의 메타버스의 보안위협 개념 및 상세설명



구분	대상	보안위협-
인프라 및 시스템	가상환경 플랫폼 및 시스템(VR,AR SW, 플랫폼)	제로데이(Zero Day)공격 악성코드/랜섬웨어 유포
	가상환경, 메타버스 서비스구축 인프라	물리적 및 SW 보안 취약점
	메타버스 플랫폼 및 서비스 이용을 위한 Web, 어플리케이션	웹 어플리케이션 취약점
네트워크	가상환경/메타버스와 서비스 이용자간 네트워크	-정보탈취 및 시스템 해킹, 서비스 공격 -Dos/DDos 공격 -MAC Spoofing, DNS Spoofing 등
데이터	메타버스 플랫폼 서비스에 저장된 개인정보, 콘텐츠	- 데이터 위 변조 및 유출 - 개인정보 암호화 또는 가명처리 미흡
	아바타, 가상화폐, NFT 등	- 가상자산에 대한 탈취 및 불법 복제
서비스	가상화폐, 메타버스 이용단말기	- 디바이스 펌웨어 취약점 - 보안 패치 미적용 또는 자체 취약점
	실시간 정보수집 서비스 (위치, 프라이버시, 민감정보 등)	- 사생활 침해 및 유출, 변조 - 신원 사칭 등

나. 정보시스템 구성 측면의 메타버스의 보안위협 및 상세설명

구분	보안위협	설명
Real World	- 개인정보 유출 - 프라이버시 위협 - 불법 권한상승 - 자산 탈취 - 바이오 정보 노출 - 지리정보 노출	- 메타버스 연결 디바이스의 SW 악성코드 삽입·감염 위협 (사례)제페토: 유사도 높은 얼굴 이미지 노출 - 개인정보 데이터 프로파일링 (라이프 로깅) (사례)포트나이트: 특정링크 클릭 시 로그인 정보 유출 - Brute Force, 크리덴셜스터핑, 사회공학 공격, 루팅, 탈옥 (사례)동물의 숲: 닌텐도 계정유출로 상품 구매 가능

		- 디지털 트윈 (나의 모습과 공간 투영) (사례)Second Life: 스파이 작업을 통해 사적인 영역 침범 - 실시간 개인정보 처리(소비습관, 위치정보, 생체정보 공유) (사례)나이키 피트니스: GPS위치, 러닝기록공유 생활루틴 노출
Interface	- 송출 데이터 스니핑 위협 - 메타버스 로그 삭제 - 5G RAN DDoS	- MITM공격, ARP Spoofing통한 패킷 캡쳐 유출 (사례)Second Life: 버그를 통해 채팅의 염탐이 가능 - 이용자 접속, 결제 정보 등 주요한 정보 삭제 위협 (사례)펌웨어 업데이트 미실시로 Zero-Day 공격 보안 위협 - 5G RAN(Radio Access Network) DDoS로 인한 서비스 지연 (사례)IoT봇넷 재밍 공격, 네트워크 슬라이싱 위협
Metaverse World	- 신원 변조·도용 - 개인정보 불법 거래 - 불법행위와 사법권 - AI 창작물 저작권 침해	- 불안전한 인증수단과 취약한 비밀번호 사용으로 계정도용 (사례)도용된 계정으로 활동하는 아바타의 불법 행위 증가 - 아바타의 가상공간 개인정보 불법거래 경제활동 (사례)로블록스 해킹: 선정적인 이미지와 인종차별 메시지노출 - 가상 세계에서 도박, 사기, 매춘 등 범죄 발생으로 사회 문제 (사례)n번방과 유사한 비밀가상공간과 가상자산 추적 불가 - 메타버스 내 AI의 창작물에 대한 저작권 이슈 (사례)창작자가 아닌 다른 사람의 NTF 무분별 민팅(Minting)
관리적 측면	- 내부자 설계/관리 문제 - 데이터센터 관리 - 해커들의 타겟 - 피해 규모의 확산 - 키 도난 및 분실 - 취약한 키 생성	- 내부자의 실수에 의한 데이터 손실, 유출, 악의적 의도 파괴 - DR센터 관리 미흡 - 클라우드에 담긴 중요한 범위 탈취 - 악성 감염 파일의 전파 - 공격자에 의해 분실된 키 악용 - 취약한 키 생성 알고리즘, 키 재생성 공격
기술적측면	- 트래픽 도청 및 위·변조 - 시스템 설계상의 오류 - 침입탐지 어려움 - 가상머신의 이동성	- 인증 및 접근권한 탈취 데이터 손실 - 시스템 잠재적 취약점 - 불충분한 실사 - 공유기술 취약점과 악성 감염 전파
서비스측면	- 트래픽 도청 및 위·변조 - 시스템 설계상의 오류 - 침입탐지 어려움 - 가상머신의 이동성	- 거래사기, 자금세탁 등 비정상 거래 탐지 불가 - 거래사기, 자금세탁 등 비정상 거래 탐지 어려움 - 기능확장 등 연계 필요 시 책임주체 및 표준 규격 불명확

- 메타버스를 이용하여 개인정보의 탈취, 계정 및 권한 도용 등에 침해가 발생할 수 있으며 메타버스 플랫폼 제공자는 사이버 공격으로 인한 연쇄공격 노출 피해에 대한 예방 노력 필요

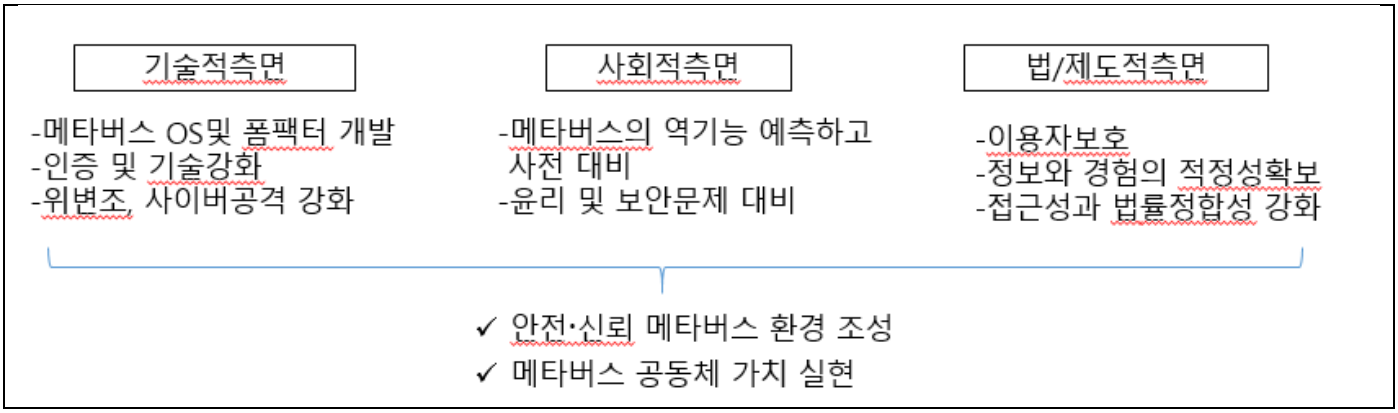
- 새롭게 대두되는 메타버스는 저작권, 국가간 이슈 등 사회적문제가 대두됨

III. 메타버스에서 발생할 수 있는 사회적 문제점

구분	문제점	해결방안
제도적 측면	창작물 저작권	창작물에 대한 귀속 및 제 3자 저작권 침해 방지
	상표권침해	메타버스내 생성된 콘텐츠의 복제. 공유 단속 제도
	개인정보보호	메타버스내 수집되는 개인정보보호 방안 및 제도 수립
	국가간 관할	다국적 플랫폼에서 발생하는 국가간 분쟁 해소
관리적 측면	공연사용료 징수	메타버스 공연료 관련 저작권 이슈 해소
	아바타 법적지위	아바타 채무 불이행, 명예훼손 등 불법 해소
	인공지능 기술악용	디지털 카르텔 등 인공지능 이슈 해소 방안 마련

- 메타버스 플랫폼들이 안고 있는 문제점에 대한 해결방안, 플랫폼의 보안성 강화 방안, 메타버스의 기술의 안정적인 정착을 위한 노력이 필요

IV. 안전한 메타버스를 위한 방안



- 메타버스의 여러 가능성들이 안전하게 시도될 수 있는 환경을 마련
- 예측가능한 안전장치안에서 신사업/신서비스가 발현될 수 있도록 생태계 구축과 활용 방안 마련 필요

기출풀이 의견

1. 출제자가 세분화된 문제를 제시하는 경우는 이유가 있습니다. 각 세분화된 문제를 엮어서 답안지에서 흐름이 읽힐 수 있도록 간

[참고] 메타버스에서 발생되는 문제

요인	문제점 및 해결 방안
메타버스 내의 불법 행위와 사법권	–세컨드 라이프와 같은 가상 세계에서 도박, 사기, 매춘 등 범죄가 발생하며 새로운 사회 문제가 되고 있음 –가상 세계는 물리적 장소 개념을 적용할 수 없어 법적 문제가 발생할 경우 재판 관할에 문제가 발생함 –현실 세계의 법질서를 가상 세계에도 동일하게 적용하자는 견해가 있음
가상화폐의 현금화	–가상 세계의 경제 규모가 커지면서 가상화폐의 현금화에 관한 논쟁이 발생하고 있음 –국내의 경우 게임산업진흥법에 의해 가상화폐 환전은 불법으로 취급되지만, 미국에서는 린든 달러 등의 가상화폐가 미화로 환전 가능한 상태
	–현실 세계에서는 물건을 팔아 번 돈과 장물을 팔아서 번 돈은 구분되기 때문에 합법적 자금과 불법적 자금으로 구분하여 불법 자금은 환수하거나 이를 근거로 체포도 가능 –가상화폐를 새로운 거래 수단으로 인정할 수 있는지에 대한 논쟁 발생 –인정 여부에 따라 가상 경제 활성화라는 긍정적 효과가 있는 반면, 게임 중독, 불법 거래, 탈세에 대한 우려가 교차하는 상황
가상 세계의 중독	–가상 세계에 지나친 몰입으로 인해 현실 일상이 황폐해지거나, 정체성 장애 등이 발생할 수 있음 –특히 게임 중독의 경우 다음과 같은 방안이 있음 1) 인터넷 중독으로 인해서 지장을 받는 일들에 대한 목록을 작성함 2) 새로운 일정표를 만들어 적절한 사용 시간과 우선 순위를 정함 3) 외부적인 요소를 활용(운동, 협력 기관, 상담사, 가족 치료, 치료센터, 약물 치료 등) 4) 특별히 문제가 되는 애플리케이션, 웹사이트, 습관 등을 그만둠 5) 리마인더(Reminder) 카드 활용 등

〈표 1〉 네 가지 유형의 메타버스 세계의 특징 비교

	증강현실 (Augmented Reality)	라이프로깅 (Life-logging)	거울세계 (Mirror Worlds)	가상세계 (Virtual Worlds)
정의	현실공간에 가상의 2D 또는 3D 물체가 겹쳐져 상호작용하는 환경	사물과 사람에 대한 일상적인 경험과 정보를 캡처, 저장, 전송하는 기술	실제 세계를 그대로 투영한 정보가 확장된 가상세계	디지털 데이터로 구축한 가상세계
구현 가치 (니즈)	현실세계와 판타지, 편의성을 결합한 몰입 콘텐츠 제공	방대한 현실세계의 경험과 정보를 언제든지 확인가능하며 타자와 공유 가능	외부정보를 가상공간에 통합, 확장함으로써 활용성 극대화	다양한 개인들의 활동이 가능한 현실에 없는 새로운 가상공간을 제공
핵심 기술	-비정형 데이터 가공 -3D 프린팅 -5G 네트워크	-온라인 플랫폼 -유비쿼터스센서 -5G 네트워크	-블록체인기술 -GIS 시스템 -데이터 저장, 3D기술	-그래픽기술, 5G 네트워크, 인공지능, 블록체인기술
서비스 사례	-포켓몬Go -운전석 앞의 HUD -SNOW앱 -코카콜라 프로젝트 -방탈출 게임 -3D아바타를 통한 SNS 활동 -에어버스, BMW의 증강현실 스마트 팩토리	-S-health, Apple -나이키+러닝 -차량 블랙박스 -SNS(인스타그램, 유튜브, 페북 등) 매체의 블로그, Vlog, 피드 등	-구글 Earth, 네이버, 카카오 지도 -에어비앤비 -미네로바스콜 -Zoom 회의실 -몰드잇 디지털 실험실 -배달의민족 -직방, 다방 등	-포트나이트 -마인크래프트 -로블록스 -동물의 숲 -제페토 -버버리 B서프 -시뮬레이션 플랫폼
주요 대표 기업	-나이앤틱 -잉그레스 -마이크로소프트 -아마존 -페이스북	-나이키 -삼성, 애플 -페이스북, 트위터 -마이크로소프트 -아마존	-구글, 네이버, 카카오 -에어비앤비 -마이크로소프트 -아마존 -페이스북	-Epic games -X-box game studio -네이버Z -닌텐도 -엔씨소프트 -마이크로소프트 -페이스북
부작용 (도전요소)	-현실이 중첩된 증강현실 공간 속의 혼란 -증강현실 속 캐릭터 등에 대한 소유권	-초상권 및 재산권 침해 -내부기밀 유출 및 겸업금지위반 등	-정보조작의 문제 -거대플랫폼 락인 효과로 불공정거래	-현실세계의 회피 -도덕적, 윤리적 문제를 일으킬 무질서 우려

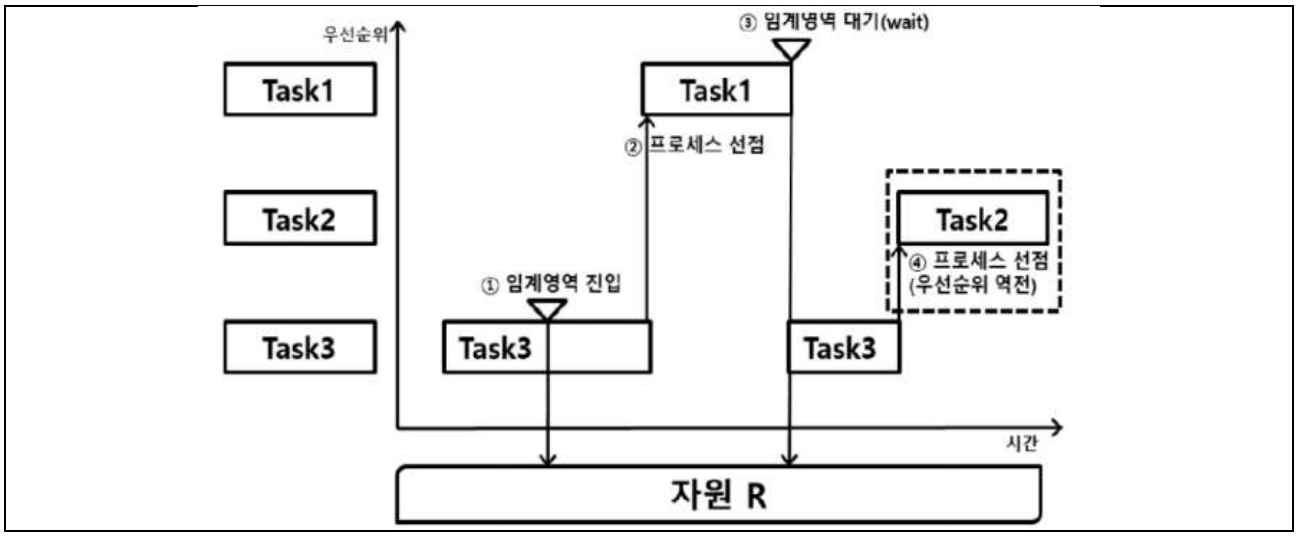
문 제	**2. Real Time Scheduling 이 갖는 문제 중 우선순위 역전(Priority Inversion)이 있다. Task1, Task2, Task3 순으로 우선순위가 낮다고 할 때 우선순위 역전을 사례기반으로 설명하고, 우선순위 역전을 해결하기 위한 2 가지 기법에 대하여 설명하시오. (단, P, V 연산을 사용한다)**
출 제 영 역	OS / 난 이 도 ★★★☆☆
출 제 배 경	운영체제의 기본 개념
출 제 빈 도	111 회 응용 1 교시 – 우선순위 상속 108 회 응용 4 교시 – 우선순위역전 발생 사례와 이를 해결하기 위한 방법(3 개 태스트로설명) 99 회 응용 4 교시 – 우선순위 상황 시나리오와 해결기법 2 가지 제시 96 회 관리 1 교시 – 우선순위 기반 CPU 스케줄링 알고리즘 합숙(19.08) 응용 - Task1, Task2, Task3 우선순위 역전 현상 및 해결 기법 합숙(19.04) 관리 – 우선순위 역전 현상 합숙(19.01) 관리 – 우선순위 역전 현상 모의(20.10) 응용 – 우선순위 상속, 올림 비교 모의(19.11) 공통 – 우선순위 해결기법
참 고 자 료	정보관리/응용 기출 풀이, 모의/합숙 기출풀이
Keyword	우선순위 상속, 우선순위 올림, 세마포어
풀 이	서 OO 기술사(제 124 회 정보관리기술사/yhsuh2107@naver.com)

I. Real Time Scheduling 이 갖는 문제 우선순위 역전(Priority Inversion)의 개념

- 낮은 우선순위를 가진 Task 에 의해 높은 우선순위를 가진 Task 가 임계영역 대기 때문에 블록 되어 수행되지 않는 현상

II. 우선순위 역전 사례기반 설명

가. Task1, Task2, Task3 순으로 우선순위 낮은 경우, 우선순위 역전 사례 개념도



- 우선순위가 가장 높은 Task1 이 결국 가장 나중에 완료.

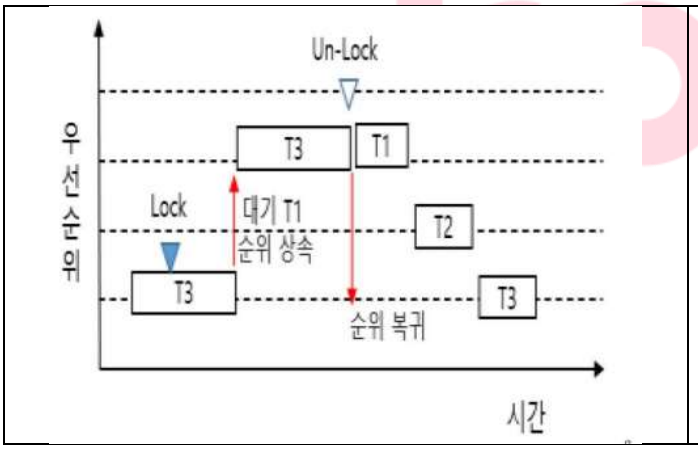
나. Task1, Task2, Task3 순으로 우선순위 낮은 경우, 우선순위 역전 사례 상세 시나리오

순서	우선순위 역전 발생 시나리오
1	task3 이 공유자원 접근 위해 바이너리 세마포어 획득
2	스케줄러에 의해 task1 이 수행 (문맥 교환)
3	task1 은 task3 이 획득한 세마포어를 얻으려 하고, task3 이 그 세마포어를 반환할 때까지 waiting 상태
4	스케줄러에 의해 task3 이 수행
5	스케줄러에 의해 task2 수행. 이 때, task1 의 우선순위가 task2 보다 높음에도 task2 가 먼저 수행. 우선순위 역전
6	task2 수행 종료 시 다시 task3 이 수행
7	task3 세마포어 반납
8	task1 세마포어 획득 후 수행 완료

- 우선순위 역전 현상을 해결기법은 "우선순위상속기법"과 "우선순위 올림 기법"이 있음.

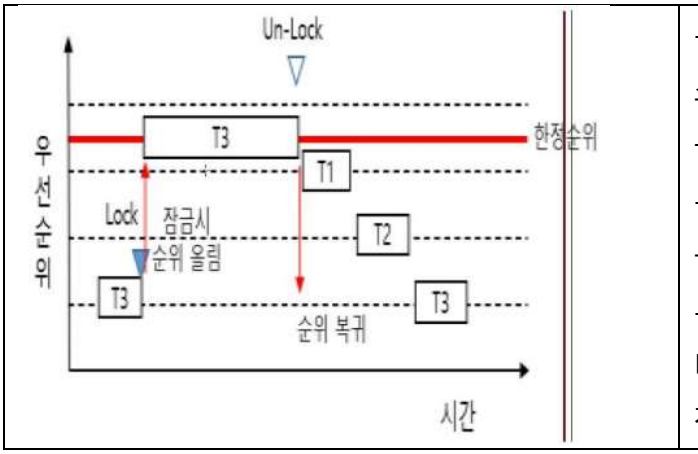
III. 우선순위역전을 해결하기 위한 2 가지 기법, 우선순위 상속기법과 우선순위 올림 기법

가. 우선순위상속(Priority Inheritance)기법



- 우선순위 낮은 Task3 을 임시로 자원요청한 상위우선순위를 부여해서 먼저 실행
-Deadlock 걸릴 확률 있음
(Task3 이 Task1 점유 자원을 요청하는 경우)

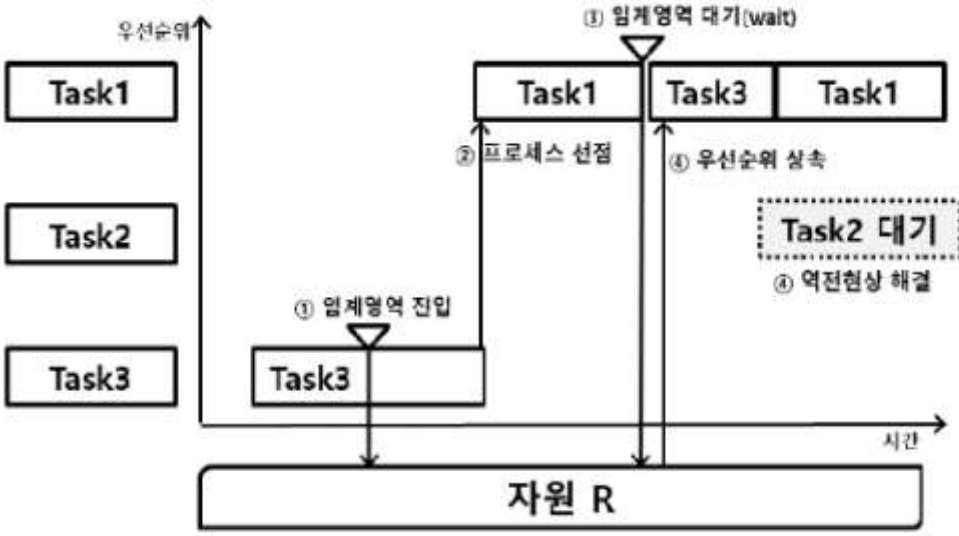
나. 우선순위올림(Priority Celling) 기법



- 어떤 스레드가 세마포어(뮤텍스)를 소유하고 있는 동안은 지정된 우선순위에서 동작
- 단, 스레드의 우선순위가 지정된 우선순위 올림 값보다 작은 경우에만 우선순위 변경
- 세마포어(뮤텍스)를 이미 잠근 쓰레드는 다른 쓰레드들에 의해 선점되지 않고 자신의 작업을 종료가능

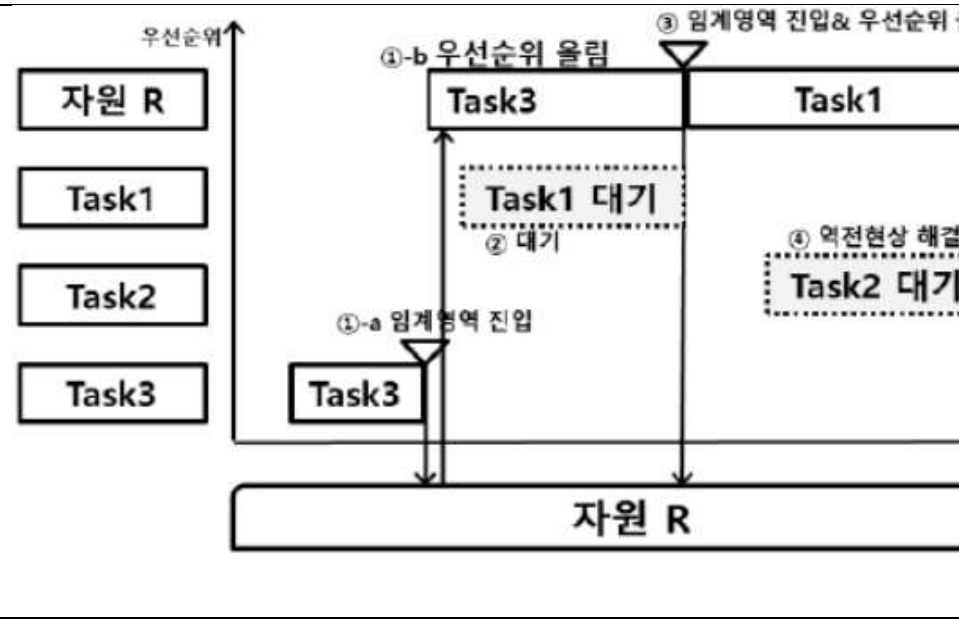
IV. 우선순위 상속기법과 우선순위 올림기법으로 해결 사례설명

가. 우선순위상속(Priority Inheritance)기법



개념	임계영역에 진입한 우선순위가 낮은 Task 의 우선순위를 진입 대기하는 높은 우선순위의 Task 와 동일하게 부여
방법	1) 임계영역진입- Task3 는 자원 R 을 사용하기 위하여 임계영역 진입 2) 프로세스선점-우선순위가 높은 Task1 은 Task3 선점하고 스케줄링 3) 우선순위 상속-Task1 은 수행 중 자원 R 이 필요하지만 Task3 가 진입하여 있으므로 대기하고 Task3 는 Task1 의 우선순위를 상속 4) 역전현상 해결-Task2 가 실행되어도 상속받은 우선순위 보다 낮아 역전현상 해결

나. 우선순위올림(Priority Celling) 기법



개념	임계영역의 자원 R 에 우선순위를 부여하고 해당 임계영역에 진입하는 Task 의 우선순위를 자원의우선순위로 올림
방법	1) 우선순위 올림-Task3 는 자원 R 을 사용하기 위하여 임계영역 진입하여 자원 R 의 우선순위로 올림 2) 대기-우선순위가 높은 Task1 은 자원 R 의 우선순위보다 낮으므로 대기 3) 임계영역 진입-Task1 은 Task3 가 종료된 이후 임계영역 진입하고 자원 R 의 우선순위로 올림 4) 역전현상 해결-Task2 가 실행되어도 올림 된 우선순위 보다 낮아 역전현상 해결

"끝"

기출풀이 의견

기본 토픽으로 우선순위 역전을 알고 있지만, 출제자는 사례기반으로 답안을 요청했습니다. 답안 작성 조건인 Task1, Task2, Task3와 사례를 작성하고, 사례기반으로 우선순위 역전 해결 기법의 개념과 1단락의 우선순위 역전현상을 제시한 기법을 활용하여 해결 사례를 작성하시면 좋을 거 같습니다.

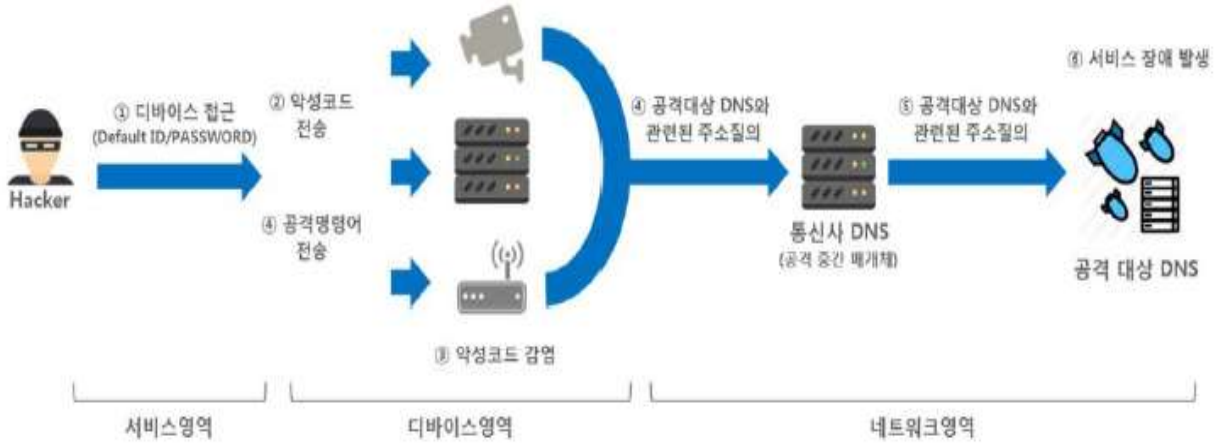
문 제	3. 미라이 봇넷(Mirai Bonet)에 대하여 설명하시오. 1) 미라이 봇넷의 개념 2) IoT 서비스 생애주기별 보안위협 및 해결방안 3) IoT 공통보안 7 개원칙
출 제 영 역	보안 / 난 이 도 ★★☆☆☆
출 제 배 경	급증하는 IoT 보안 위협, IoT 의 진화와 함께 보안 인식 제고 필요성
출 제 빈 도	모의(19.11) 공통- IoT 의 개념, 주요기술 IoT 보안 취약성과 방어기술 모의(18.01) 응용 – IoT 디바이스의 보안취약점 3 가지 이상 제시, 대응방안 합숙(17.08) 공통 - IoT 공통보안 7 원칙. 합숙(17.01) 공통 – IoT 의 보안 취약 점 및 디바이스 보안을 위한 Secure Boot 합숙(16.07) 공통 – IoT 보안의 주요 위협, 보안요구사항, 보안 기술, 보안전략 합숙(16.01) 응용 - IoT 보안위협, 보안요구사항, 보안 공통 7 대원칙
참 고 자 료	사물인터넷(IoT) 환경에서의 암호인증기술 이용 안내서_2017, IoT 공통보안 가이드
Keyword	사물인터넷(IoT), DDos, 봇넷, IoT 서비스주기, IoT 공통보안
풀 이	서 OO 기술사(제 124 회 정보관리기술사/yhsuh2107@naver.com)

I. 기업형 사물인터넷기기를 노리는 미라이 봇넷(Mirai Bonet)의 개요

가. 미라이봇넷의 개념

정의	- IoT기기들을 좀비화 해 대량의 트래픽을 유발시키는 방식(DDoS)으로 웹사이트를 공격하는 봇넷 - IoT기기들의 디폴트 계정을 통해 기기 통제권 획득하고 다량의 트래픽 발생해서 웹서비스를 다운 봇넷
특징	- HTTP 프로토콜을 기반으로 하는 봇넷의 한 종류 -보안 기능을 넣기 어려운 모든 사물인터넷 기기가 공격 대상

나. 미라이봇넷의 동작원리



① 디바이스접근	-IP 주소로 접근하여 해당 기기의 루트 권한을 획득 -루트 권한을 획득하기 위해 디폴트 계정 정보를 입력 - 루트 권한을 획득
② 악성코드전송	-쉘 스크립트를 실행 - 악성코드를 다운받고 이를 실행
③ 악성코드 감염	- 대상 기기를 완전히 감염
④ 공격 명령어 전송	- C&C 서버로 대기 명령을 전송
⑤ 공격대상 DNS 질의	-①~④ 반복하여 대규모 봇넷 구성
⑥ 서비스 장애 발생	- C&C 서버를 통해 공격 대상을 전달 대규모 봇넷 공격

-

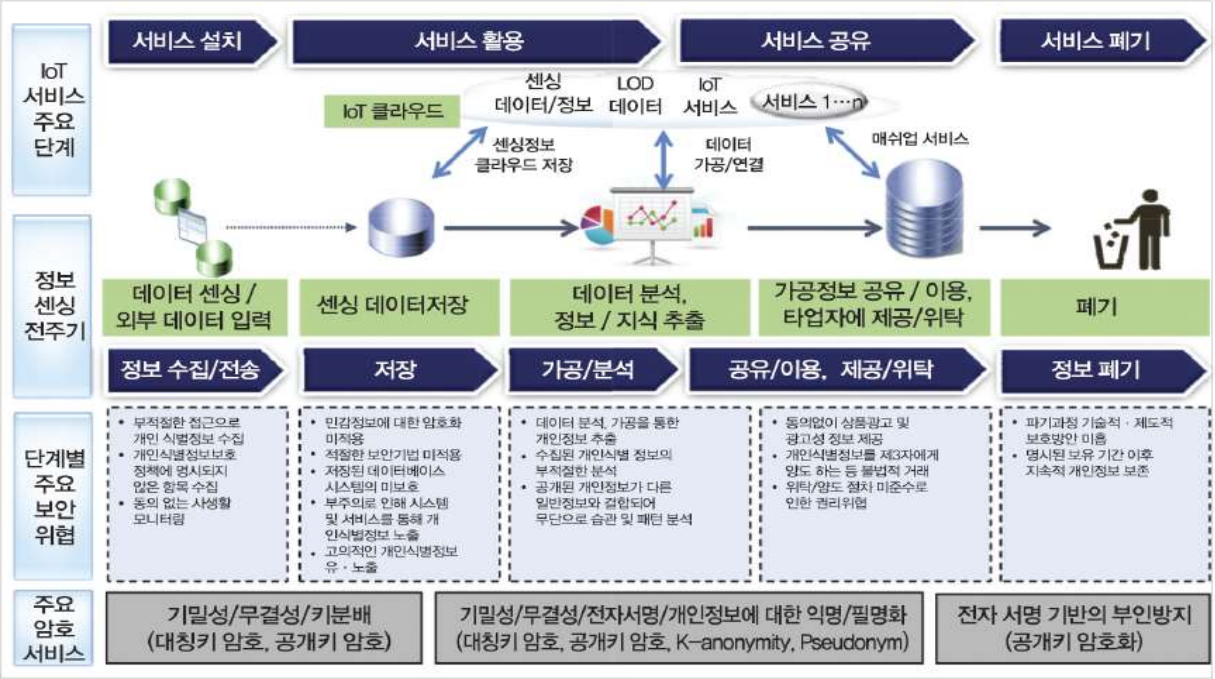
다. 미라이봇넷 취약점 및 대응방안

취약점	- 수백만 IoT가 존재하며 손쉬운 Default 암호 - 장치 소유주가 통상 보안 전문성이 없는 일반 소비자 또는 기업으로 악용 용이 - 보안프로그램 지원 미흡
대응방안	- 네트워크 연결을 끊는다. - 네트워크와 인터넷이 끊기면 재부팅 한다. Mirai 악성코드는 동적 메모리에서 동작하기에 재부팅 하여 메모리를 초기화하여 해결 - 재부팅이 끝나면 장치에 접근할 때 사용하는 암호를 강력한 암호로 변경 - 강력한 암호로 변경했으면 다시 네트워크에 연결하여 서비스를 실행. 만약 암호를 변경하기 전에 네트워크에 연결하면 다시 감염될 수 있음

- 미라이봇넷과 같은 악성코드 감염은 기기가 사용하는 네트워크를 통해 이뤄지기 때문에 안전한 보안 인식을 바탕으로 사물인터넷 기기를 설정하고 네트워크 보안을 강화-
- 사물인터넷 기술을 올바르게 활용하고 발전시키기 위해 사용자와 기업 모두가 보안성 확보를 위해 IoT 서비스 생애 주기 별 보안위협에 대응, 기본원칙 준수 필요.

II. IoT 서비스 생애 주기 별 보안 위협 및 해결방안

가 IoT 서비스 생애 주기 별 보안위협 개념도



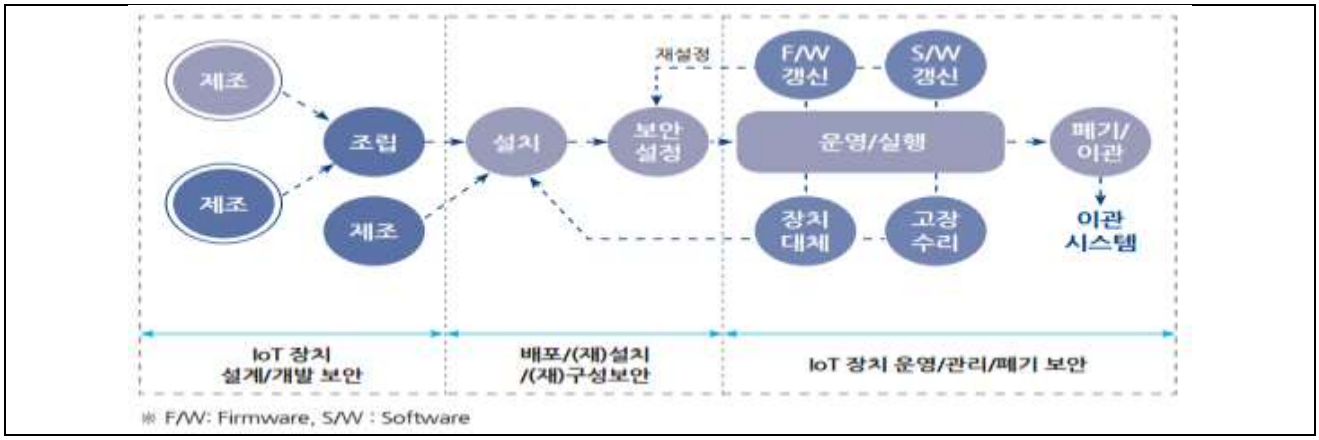
나 IoT 서비스 생애 주기 별 보안위협 및 해결방안 설명

단계	보안위협	해결방안	
		기술적	비기술적
서비스 설치	비 적합 키 설정	-키 관리/분배 기법제공	-서비스 규약 준수, 사용자 교육
	단순한 패스워드 사용	- 패스워드 안전도 검사 및 변경 - 패스워드 기밀성유지 및 무결성 확인	- 패스워드 강도 테스트 및 재설정 - 안전한 패스워드 설정 안내
	트랩도어 설정	-방화벽 설정 및 최초 설치 시 설치된 바이너리 인증 - 방화벽 설정	- 인증된 바이너리 사용만 허가
	기본 관리자 계정 이름과 패스워드 유지	- 관리자 계정 변경 강제 - 패스워드 안전도검사 - 패스워드 기밀성, 무결성	- 주기적 패스워드 관리
	다중 요소 인증 옵션 비 제공	-OTP 혹은 암호화된 2채널 이상 인증	-본인인증 및 정보관리 중요성 교육
	인증되지 않은 펌웨어 업로드	-펌웨어 서명 검증	- 비 인증 바이너리 사용시 경고
	필요한 이상의 권한 부여	- 다중 사용자에게 최소 권한 부여	- 서비스 규약 준수, 사용자 교육
	방화벽 미 설정	- 허가된 서비스 및 포트만 열기	- 무허가 포스 사용금지

서비스 활용	도청, 프라이버시 침해	- 암호기술 적용한 채널 통신	- 서비스 규약 준수, 사용자 교육
	데이터 위 변조	- 무결성, 불법수정 방지를 위한 서명된 인증성 기반의 통신채널 제공	- 개인정보 데이터위변조 피해유형 및 안정성 교육
	권한/접근 제어 위반	- ACL 권한 /접근제어	- 서비스 규약 준수, 사용자 교육
	취약점 보안 패지 무시	-주기적 자동 펌웨어, SW 업데이트, 패치적용 -무결성 검사	- 주기적 펌웨어 및 SW 업데이트
	인증되지 않은 패지 적용	- 펌웨어, SW 업데이터, 패치적용 시 미 인증된 패치 적용 방지	- 불법 루팅툴 및 비 인증 패치 위험성 교육
	암호화되지 않은 로그 파일 유출, 만료된 로그 파일 유지	- 로그파일 유효성 검사 및 기간 설정 - 유효기간 지난 로그파일 자동 파기	- 서비스 규약 준수, 사용자 교육
	DB중요 정보 비 암호화	- 암호화 및 인증 값 이용 정보 암호화	- 서비스 규약 준수, 사용자 교육
서비스 폐기	암호화 키 값 유출	- 내부 중요 데이터 저장장치 암호화	- 개인/민감정보 안전한 폐기 절차안내
	삭제되지 않은 저장 장치 파기	- 암호화 가능한 파일 시스템 이용	- 암호화기능 제공 저장장치 이용
	폐기되지 않은 인증서 유출	- 인증서 만료기간관리 - 유효한 인증서에 대한 암호화접근 제한	- 개인/민감정보 안전한 폐기처리절차 안내
	폐기되지 않은 계정 정보 유출	- 계정정보에 대한 암호화 - 2채널 인증의 계정인증	- 개인/민감정보 안전한 폐기처리절차 안내

Ⅲ. IoT 공통보안 7 개원칙

가. IoT 공통보안 구성도



나. IoT 공통보안 7 대 원칙

#	단계	원칙
1	설계/개발 보안	정보보호와 프라이버시 고려한 제품 설계
2		안전한 S/W, H/W 개발기술 적용 및 개발
3	배포/설치/구성보안	안전한 초기 보안 설정 방안 제공
4		보안 프로토콜 준수 및 안전한 파라미터 설정
5	운영/관리/폐기	취약점 보안 패치 및 업데이트 지속 이행
6		안전한 운영 관리위한 정보보호 관리체계 마련
7		침해사고 대응체계 및 추적성 확보 마련

"끝"

기출풀이 의견

기업형 사물인터넷기기를 노리는 신종 미라이봇넷에 대한 개념과 전파대상인 사물인터넷 기기들에 대한 이해와 인지와 기본적인 보안원칙을 알고 있는지를 묻는 문제였습니다.

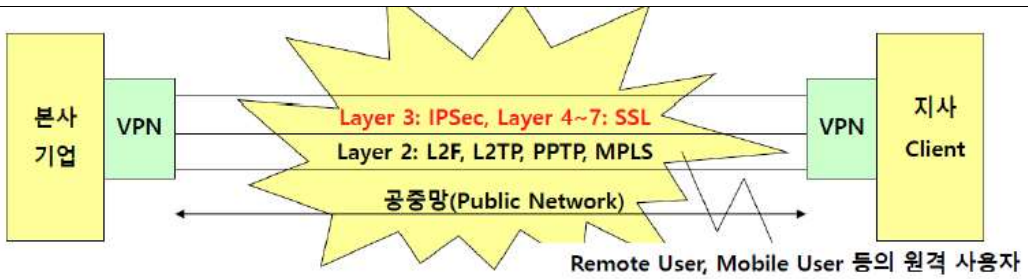
문 제	4. VPN(Virtual Private Network)와 Tor 에 대하여 설명하시오.		
출 제 영 역	보안	난 이 도	★★★☆☆
출 제 배 경	프라이버시 보장과 동시 익명성 보장의 중요성 증대에 따른 VPN 과 Tor 연관성		
출 제 빈 도	120 회 관리 3 교시 – VPN, NFV 비교 119 회 응용 2 교시 – VPN 구현방식, 서비스형태, SSL VPN 과 비교 104 회 관리 2 교시 – VPN, IPsec 모의(17.01) 응용- 토르 네트워크 모의(16.06) 응용- VPN 구성방식 합숙(21.01) 응용 –VPN 유형		
참 고 자 료	정보처리/응용기출풀이, 모의/합숙기출풀이		
Keyword	독립성보장 네트워크, SSL, IPSEC, OR, OP, 겹층암호화, Tor over VPN, VPN over Tor		
풀 이	서 OO 기술사(제 124 회 정보관리기술사/yhsuh2107@naver.com)		

I. 사설 전용망의 효과를 얻는 가상네트워크, VPN(Virtual Private Network)

가. VPN(Virtual Private Network)개요

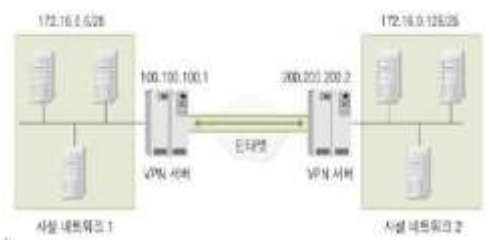
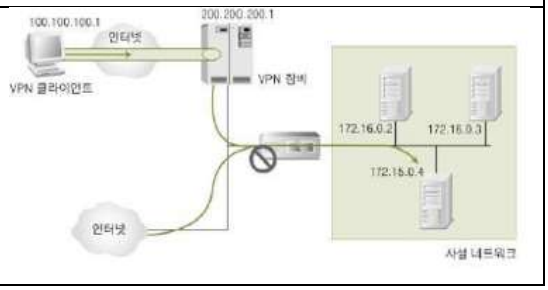
정의	인터넷 같은 공중망에서 터널링(Tunneling)기법을 사용해서 전용선에 비해 경제적이면서도 사설망과 같은 보안성과 연결성으로 안전하게 통신할 수 있는 보안 솔루션	
등장배경	- 전용선망의 고비용을 대체할 솔루션에 대한 요구 발생 - 이동 근무 지원으로 기업 생산성 향상에 대한 기대 - 인터넷 환경의 급속한 확산에 따라 보안성의 필요성 증가	
특징	뛰어난 보안성	- IPSec VPN, SSL VPN 터널링 구성으로 보안성 제공 - 전송 데이터에 암호화와 인증 등의 보안기능 제공
	유연한 확장성	- 네트워크 증설 및 감속의 용이성 - 통합구성으로 인한 관리의 편리성
	저렴한 구축비용	- 초고속망 기본 구성으로 인한 비용절감 - 본/지사 구축 시 비용절감

나. VPN 구성도 및 상세설명

구성도		
구현기술	기술	설명
	인증	- 네트워크를 통해 데이터를 보낸 자가 누구인지 인증 - PKI [Public Key Infrastructure] 기반의 비 대칭 키를 사용하여 세션을 성립하기 때문에 End-to-End인증 효과 - 추가적으로 MD-5, SHA-1 등의 해쉬 함수를 통한 메시지 다이제스트 구현으로 대상

		노드 및 데이터 무결성 인증
	터널링	- 인터넷 상에서 가상의 정보흐름 통로 - 패킷을 사전에 암호화하는 방법을 규정한 IPSec이 업계표준
	암호화	- 기밀성 보장을 위한 메커니즘 - 전송중인 정보의 공개 방지(DES,SEED 등 사용) - End-to-End 간의 세션 키를 기반으로 암호화/복호화 수행 - DES, 3-DES, AES, SEED 등의 블록 암호화 알고리즘 사용
	키 관리	- 사전에 공유한 암호화 키의 안전한 분배를 위한 키의 안전한 관리 메커니즘 - IKE(Internet Key Exchange; IPsec를 암호화하는데 사용 예) 프로토콜을 사용 - 비 대칭 키의 교환을 위해서는 RSA 암호화 프로토콜이 사용되며, End-to-End 간에 SA [Security Association]이 성립된 이후에는 해당 비 대칭 키로, 데이터의 암호화에 사용되는 세션 키(대칭 키, 비밀 키)를 생성 및 교환
	복수 프로토콜	- 공용 네트워크에서 일반적으로 사용되는 프로토콜을 처리

VPN 유형	기술	계층	표준	장점	단점
	IPSec	네트워크(3)계층	RFC2401	-높은보안수준 -다양한인터넷접속기술활용	-높은 초기도입비용 -트래픽제어,QoS 기능 미약
	MPLS	데이터링크(2,3)계층	RFC2547	-동일네트워크 多 VPN 제공 -단일네트워크에서 데이터,음성,비디오 처리	-동일 ISP 내부에서만 운용가능 -공중망 전송시 암호화기능 미약
	SSL	전송(4)~운용(7)계층	-	-Clientless VPN -사용성, 관리 편의성	-UDP 사용제한 -SSL 자체의 부하

구성 유형	구분	LAN To LAN	LAN To Client
	개념	두개의 네트워크를 VPN 으로 구성	원격지의 개인 사용자와 보호대상 네트워크 연결
	활용	본사-지사연결	원격지근무, 출장(외부 접근)
	인증	VPN 간 장비	VPN 장비와 Client 프로그램
	암호화	고속	저속
	이슈	성능	인증, 사용자 편의성
	기술	IPSec	SSL
	구성		

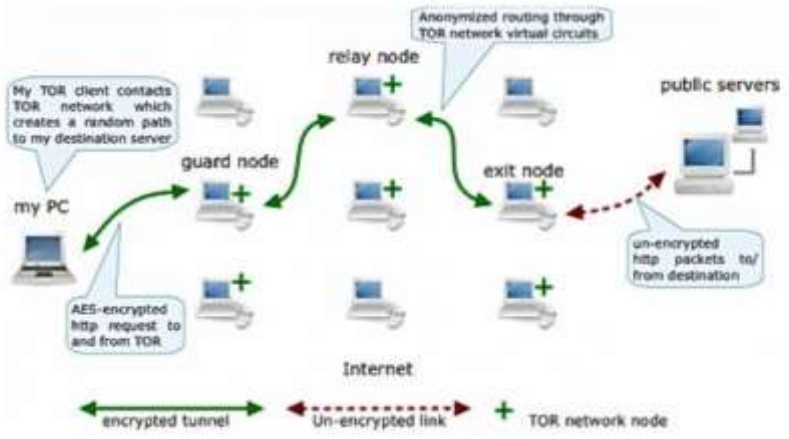
II. 익명성 보장 Tor (The Onion Router)

가. Tor의 개요

정의	온라인 상에서 트래픽 분석이나 IP 주소 추적을 불가능하게 하는 익명성 보장 네트워크	
특징	익명성 보장	– 출발, 목적지 주소 추적 불가
	겹 층 암호화	– 패킷은 여러 겹으로 암호화, 이동 시 복호화
	이동경로 삭제	– 패킷의 이동 경로 관련 정보 주기적 삭제

나. Tor 구성도 및 상세설명

구성도



	구분	핵심기술	설명
구성요소	Cell	512Byte 패킷	– Tor 네트워크를 통과하는 고정된 크기의 패킷
	Circuit	TLS 암호와 AES	– 각 TCP Stream 에 대한 전체 라우팅 경로
	OR (Onion Router)	Tor 패킷 전달	– Tor 네트워크 내 패킷 전달 노드(guard, relay, exit node)
	OP (Onion Proxy)	연결 관리 프록시	– Circuit 생성 및 연결 관리 사용 Proxy
	Director 서버	Circuit, OR 정보저장	– OR 정보 및 Circuit 정보 보유 서버
겹층암호화 기술요소	구간	Entry Guard	– Cell, Circuit
		Middle Relay	– Directory 서버, OR(Onion Router 3 개 이상), OP (Onion Proxy),
		Exit Note	-토르 브라우저, 디피헬만암호화
	라우팅	Cascade	– 미리 여러 경로 중에 하나를 선택하는 방식
		Stratified	- 각 단계별로 다른 경로의 해당 단계에 있는 노드를 선택할 수 있는 계층 (stratified) 방식
		Free-router	- 모든 노드를 자유롭게 선택할 수 있는 자유 경로(free route) 방식

- Tor 네트워크를 구성하는 각 노드는 겹층 암호화된 Layer 를 단계별로 복호화 하며 다음 IP 주소로 전달

- Tor 네트워크의 겹 층 암호화 기술을 이용해 파이어폭스 브라우저 취약점 악용 스크립트 사용 추적회피

기출풀이 의견

VPN과 Tor는 사설네트워크와 익명성보장네트워크를 각각 설명하고 각 토픽에 대해서 비교 또는 엮어서 마지막 단락을 작성하시면 좋은 답안이 가능합니다.

문 제	5. RSA(Rivest, Shamir, Adleman))알고리즘과 DSA(Digital Signature Algorithm)알고리즘을 비교하여 설명하시오.		
출 제 영 역	보안	난 이 도	★★★☆☆
출 제 배 경	SSL/TLS 에 가장 많이 사용되는 공개키 암호화 알고리즘		
출 제 빈 도	116 회 관리 1 교시- 전자서명 118 회 관리 4 교시 - 110 회 응용 4 교시 – 대칭 키 암호화, 비대칭키 암호화 합숙(20.01) 공통 - Diffie Hellman(디피헬만키교환법), RSA 암호 알고리즘 합숙(19.08) 응용- RSA 암호 알고리즘		
참 고 자 료	[Cryptography] 13. Digital Signature Standard, RSA and DSA Signing 강의노트		
Keyword	공개키, 개인키, 소인수 곱, 엘가멜, 검증, 전자서명, SSH2, SSH, 이산대수 문제, 키 생성, 암호화, 복호화		
풀 이	서 OO 기술사(제 124 회 정보관리기술사/yhsuh2107@naver.com)		

I. 비대칭 키 방식의 대표적 암호화 알고리즘, RSA 의 개요

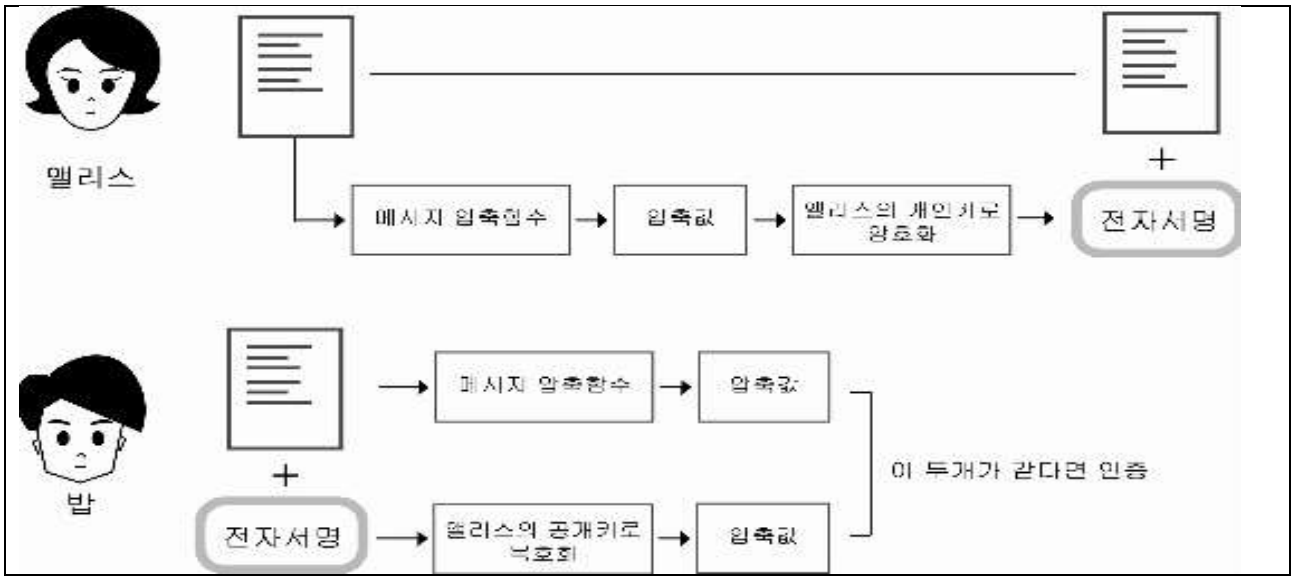
가. RSA(Rivest, Shamir, Adleman)의 정의

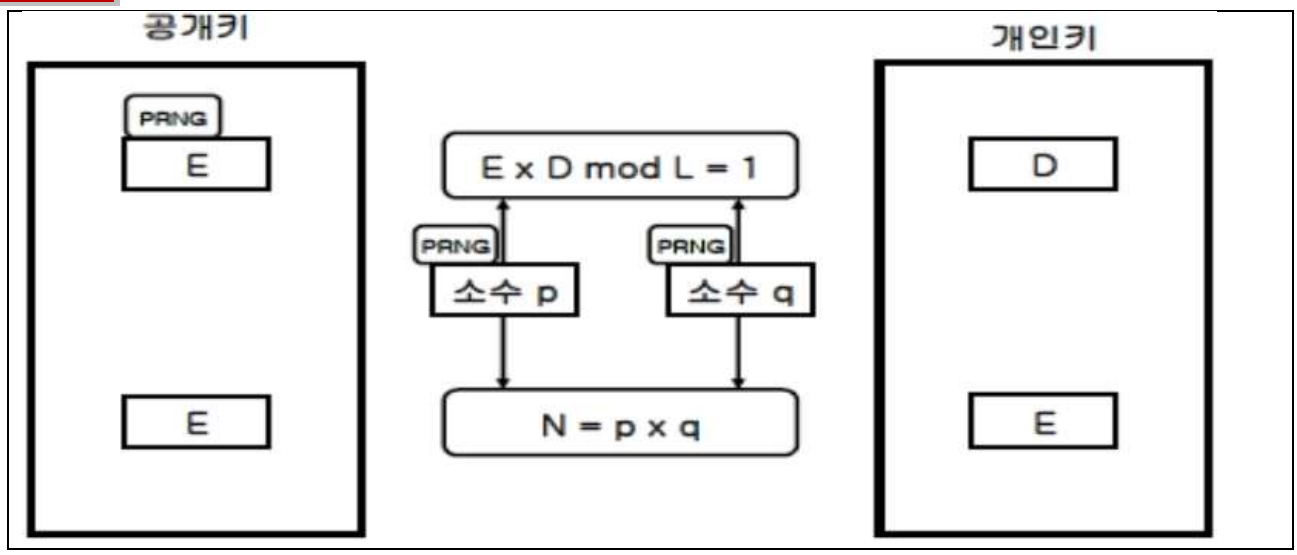
- Rivest, Shamir, Adleman 이 고안한 큰 소인수 곱 n=p*q 의 소인수 p, q 를 찾는 것이 어렵다는 것을 근간으로 만들어진 알고리즘

나. RSA 알고리즘의 특징

안정성, 신뢰성	안정성 신뢰성이 높은 알고리즘이지만 수행 시간이 많이 소요
소수 p, q 의존성	소수 p, q 에 의해 성능이 좌우됨
비대칭키 암호화	대표적인 비대칭키를 사용하는 암호화 알고리즘
랜섬웨어	랜섬웨어에 많이 사용되는 암호화 알고리즘(RSA 2048/4096)

다. RSA 알고리즘의 개념도





- PRNG(Pseudo Random Number Generator) – 블록 암호 알고리즘 기반 의사 난수 발생

라. RSA 알고리즘의 안정성 확보

구분	안정성 확보 설명
소수 선택	PRNG(Pseudo Random Number Generator) – 블록 암호 알고리즘 기반 의사 난수 발생
	p-1, q-1 은 큰 소수를 인수로 가져야 안전함
	p-1, q-1 의 치대 공약수는 작아야 안전함
키사이즈	1980 년까지 512 비트, 1996 년에는 1024 비트, 2005 년에는 2048 비트 권장

마. RSA 알고리즘의 활용

활용	설명
암호화/복호화	송신자는 수신자의 공개키로 메시지를 암호화, 수신자는 수신자의 개인키로 복호화
디지털서명	송신자는 송신자의 개인키로 메시지에 서명, 수신자는 송신자의 공개키로 검증함
키 교환	송신자는 수신자의 공개키로 세션키를 암호화하여 전달하고 수신자는 수신자의 개인키로 복호화 하여 세션키를 서로 공유

II. 전자서명 알고리즘, DSA 의 개요

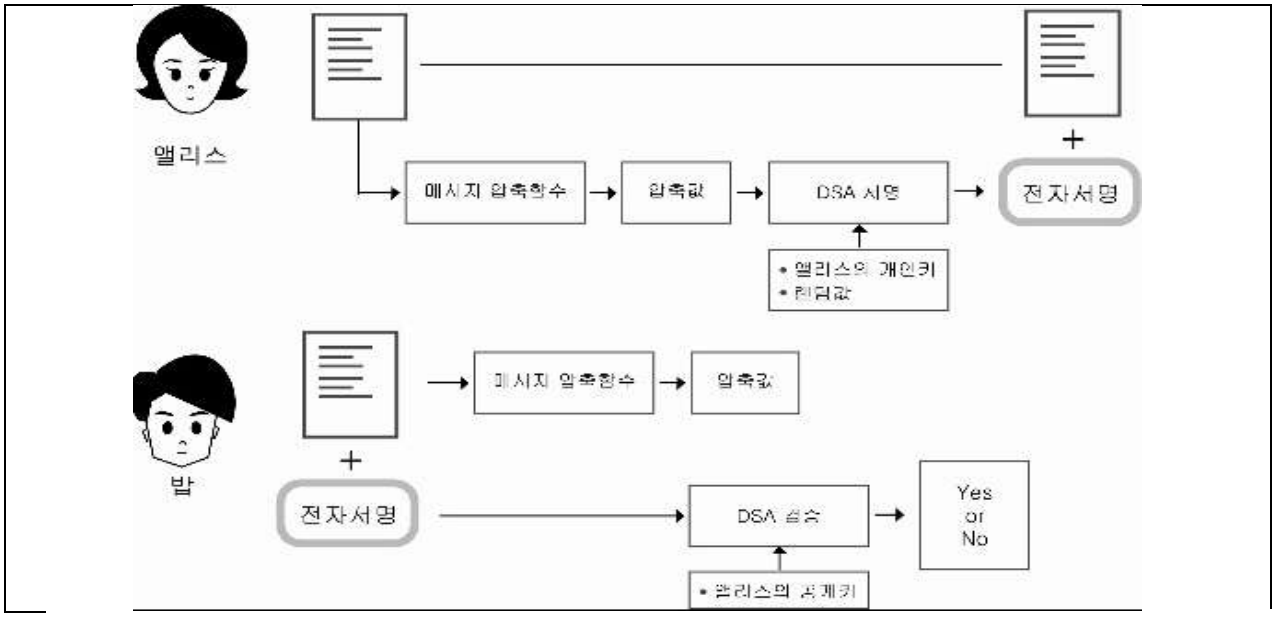
가. DSA(Digital Standard Algorithm) 정의

- 디지털 서명 알고리즘(Digital Signature Algorithm, DSA)은 디지털 서명을 위한 표준
- NIST 가 1991 년 8 월 DSS 라는 미국 전자서명 표준에서 이용하기 위해 정부용 전자서명 알고리즘으로 발표했으며, 현재는 DSA 와 함께 ECDSA, RSA 를 사용.

나. DSA 의 특징

키 생성 속도	RSA 보다 키 생성이 빠름
검증속도	RSA 보다 느림
원리	이산대수 문제의 어려움을 이용한 방법
서명	320bit 서명 생성
해시 함수	SHA1을 이용

다. DSA 개념도

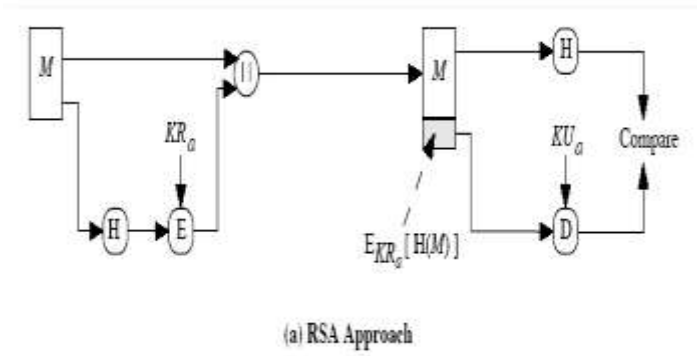
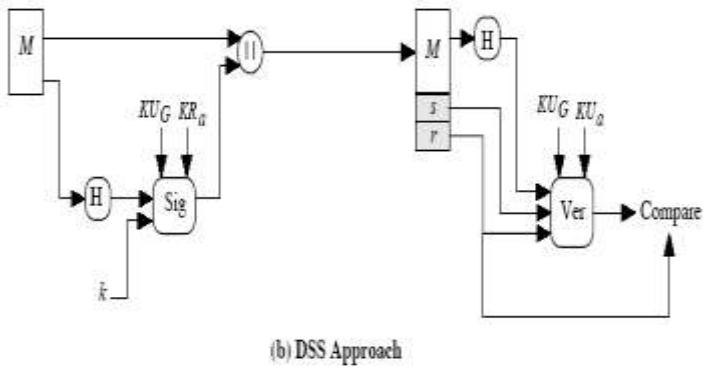


- El Gamal형 알고리즘으로 기밀성은 가지고 있지 않으며 전자서명 기능을 제공, 전자서명을 위한 3가지 함수 '키 생성', '서명', '검증' 역할을 하는

- 메시지를 압축하고 그 압축 값을 개인키로 암호화해서 전자 서명 값을 만드는 것은 RSA 와 DSA 동일
- RSA 전자서명 알고리즘은 메시지를 인증할 때 메시지를 압축 해시 값을 생성, 복호화 한 전자 서명 값과 비교하여 인증
- DSA 알고리즘은 검증결과가 바로 예 또는 아니오 로 출력(DSA 가 전자 서명/인증만을 위한 알고리즘)

III. 전자서명을 위한 알고리즘 RSA 알고리즘과 DSA 비교

가. RSA 알고리즘과 DSA 개념비교

RSA 알고리즘	DSA
 (a) RSA Approach	 (b) DSS Approach
소인수분해의 어려움을 기반으로 하는 공개키 암호화 방식으로 전자 서명의 공개키 암호화 시 이용되는 방식	이산 로그문제 어려움에 기반한 엘가멜 등의 공개키 암호화 기법 활용하여 전자서명에서 공개키를 암호화하는 방식

나. RSA 와 DSA 의 상세 비교

구분	RSA	DSA
암호화원리	소인수 분해의 어려움에 기반	이산로그문제의 어려움 기반
키생성속도	느림	빠름
검증속도	빠름	느림
서명속도	느림	빠름
장점	검증에 최적화	서명에 최적화
기법	소인수 분해	엘가멜기법
적용	SSH2	SSH

-SSH 에 적용시 DSA 를 사용하고 RSA 는 SSH2 에 적용하여 SSH 의 보안성을 높여 줌

[참고] 수학적 문제에 기반한 암호알고리즘 RSA, ECC 및 El Gamal 비교

항목	RSA	ECC	El Gamal
수학적문제	소인수분해	타원곡선 이산대수	이산대수
키 크기	큼	적음	큼
속도	상대적 느림	빠름	상대적 느림
암호문 크기	-	-	평문의 두배
메모리	ElGamal 에 비해 적음	가장 적게 차지	가장 많이 차지
비용	많이 소요	적게 소요	많이 소요

- 시스템 환경과 특성에 맞는 수학적 문제에 기반한 암호 알고리즘 적용 필요
- RSA/ECC 와 더불어 디지털 서명, 키 교환 알고리즘에 활용되는 El Gamal 키 생성/암호화/복호화
-

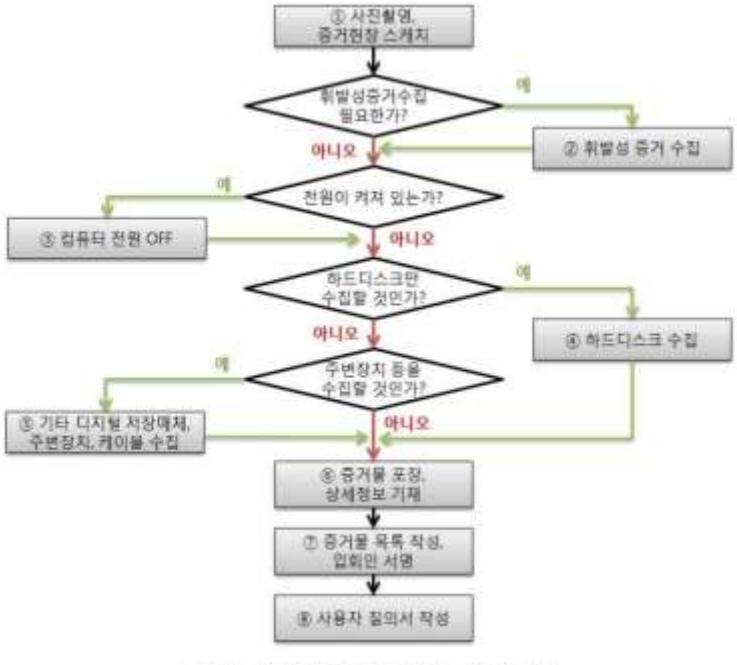
기출풀이 의견

1. 비교문제는 1단락에서부터 마지막 단락까지 비교로 작성하셔야 합니다.
2. RSA와 DSA의 차이 때문에 SSH2, SSH에 각 적용되고 클라우드에서 SSH에 암호 없이 접속하기 위해 RSA와DSA가 사용된 다라고 하시면 좋을 거 같습니다.

문 제	6. 디지털 포렌식(Digital Forensic)의 증거수집기술 중 하나인 파일카핑(File Carving)에 대하여 설명하시오. 1) 파일 카핑에 대한 개념 2) 파일 카핑의 4 종류 기법의 특징
출 제 영 역	보안 / 난 이 도 ★★★☆☆
출 제 배 경	디지털 증거의 수집·분석 및 관리 규정 2021.01 일부 개정
출 제 빈 도	121 회 관리 2 교시 - 디지털 포렌식의 필요성, 절차 및 활용되는 기술 118 회 관리 4 교시 – 디지털 포렌식 조사모델, 분야, 활용 소프트웨어, 고려사항, 5 대원칙 117 회 관리 4 교시 – 디지털 포렌식 증거수집기술과 증거분석기술 111 회 응용 1 교시 - 디지털 포렌식 모의(17.12) 응용 – 디지털 포렌식의 절차, 기술, 안티 포렌식 합숙(18.01) 공통 – 디지털 포렌식의 증거수집 및 분석기법
참 고 자 료	-디지털 포렌식 조사에서 효율적인 파일 복구를 위한 레코드 파일 카빙 기법(2013, vol.2, no.2)-정보처리학회 -http://cfpa.or.kr 사이버 포렌식 협회 -디지털 포렌식 기술 및 동향(전자통신동향분석 제 22 권 제 1 호 2007 년 2 월)
Keyword	파일시스템의 비 할당 영역, 헤더/푸터, 파일크기카빙, 파일 조각화, 시그니처기반
풀 이	서 OO 기술사(제 124 회 정보관리기술사/yhsuh2107@naver.com)

1. 디지털 포렌식의 증거수집

가. 디지털 포렌식의 증거수집 절차



(그림 4. 디지털증거 수집 절차도3))

① 사진촬영 및 현장 스케치
② 네트워크 정보 등 휘발성 증거 수집
③ 수집 대상물의 전원 확인
④ 본체 수집을 원칙으로 하되, 부득이한 경우 하드디스크만 분리하여 수집
⑤ 외장형 디스크, USB 등 기타 디지털 저장매체 수집
⑥ 증거물 포장 및 상세정보 기재
⑦ 입회인으로부터 압수확인서 및 압수증거물 목록에 서명 날인을 받음
⑧ 사용자 질의서 작성

- 경찰청, "디지털증거 처리 표준 가이드라인"
- 디지털 포렌식 증거 수집 프로세스에서 사용되는 도구들은 다양하게 존재

나. 디지털 포렌식 증거수집 주요기술

구분	증거복구	증거 수집 및 보관	증거분석
저장매체	-하드 디스크 복구 -메모리 복구	-하드디스크 복제 기술 -메모리 기반 장치 복제기술 - 저장매체 복제 장비	- 저장매체 사용 흔적 분석 - 메모리 정보분석
시스템	- 삭제된 파일 복구 - 파일 시스템 복구 - 시스템 로그온 우회기법	- 휘발성 데이터 수집 - 시스템 초기 대응 -포렌식 라이브 C/USB	- 윈도우 레지스트리 분석 - 시스템 로그분석 -프리패치분석 -백업 데이터 분석
데이터 처리	- 언어통계기반 복구 - 암호 해독/DB구축 -스테가노그래피 파일조각분석	-디지털 저장 데이터 추출 - 데이터 증거보존 - 디지털 증거 공증/인증	- 데이터 포뱃 별 분석 - 영상 정보분석 - 데이터베이스 정보 분석 - 데이터 마이닝
응용/네트워크	- 파일 포맷 기반 복구 - 프로그램 로그온 우회기법 - 암호 통신 내용 해독	- 네트워크 정보 수집 - 네트워크 역 추적 - 데이터베이스 정보수집 허니넷	- 네트워크 로그분석 -해시 데이터베이스 -바이러스/해킹분석 - 네트워크 시각화
기타	- 개인정보보호기술, 디지털 포렌식 수사 절차 정립, 범죄 유형 프로파일링 연구, 통합 타임라인 분석 - 디지털 포렌식 도구 비교 분석, 하드웨어/소프트웨어 역 공학, 회계부정 탐지 기술		

- 안드로이드 스마트폰, 태블릿 PC 등을 비롯한 안드로이드 운영체제를 기반으로 하는 여러 임베디드 기기 들이 증가
- 이러한 임베디드 기기 내부에는 사용자의 일상생활과 관련된 많은 데이터들이 저장 디지털 포렌식 조사 과정에서 매우 중 요한 분석 대상이 되고 있음.
- 파일 삭제 시 복구에 필 요한 정보가 초기화되기 때문에 삭제된 파일을 복구하 기 위해서는 비 할당 영역에서 파일 포맷 별 카빙을 수행

나. 디지털 포렌식 증거수집 도구

비교 항목		Forensic Explorer	X-Ways Forensics	Blacklight
증거 파일 마운트	물리 디스크 마운트	O	X	O
	논리 디스크 마운트	O	X	O
	이미지파일 마운트	O	O	O
물리메모리 분석	물리메모리 파일 추가	O	O	X
	물리메모리 Hex 뷰	O	O	X
	물리메모리 해석	X	X	X
저장매체 이미징	-	O	O	X
파일시그니처	오피스 파일	O	O	X

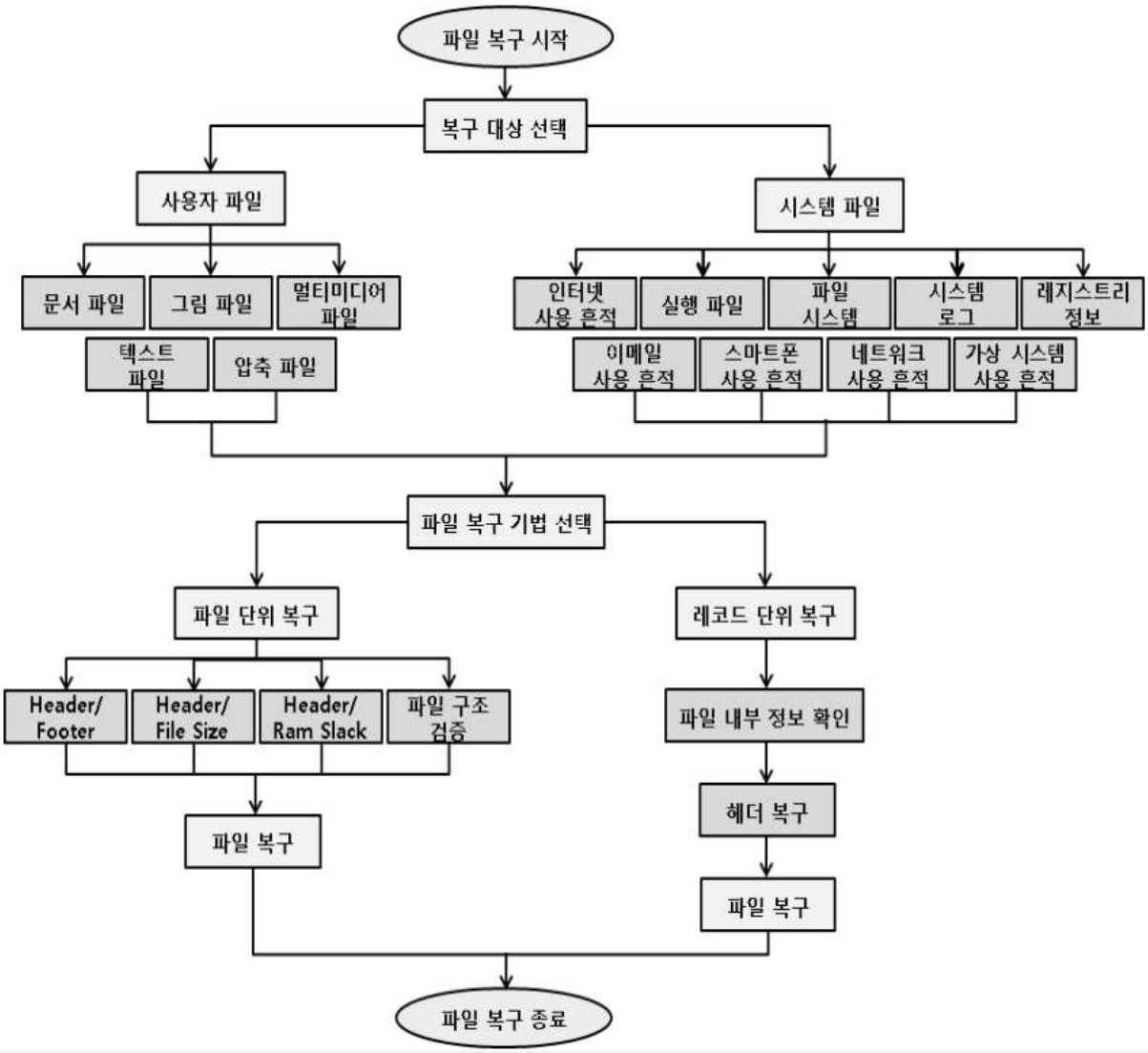
분류 기능	카메라 파일	O	△	X
	음악 파일	O	O	X
	비디오 파일	O	O	X
	인터넷 파일	O	O	X
	그래픽 파일	O	O	X
	문서 파일	O	O	X
	압축 파일	O	O	X
	이메일 파일	O	O	X
	데이터베이스 파일	O	△	X
	윈도우 시스템 파일	O	O	X
	사용자 정의	O	O	X
파일 해석 정보	그림파일 읽기 지원	O	O	O
	압축파일 브라우징	O	O	O
	Hex View 지원	O	O	O
Mac OS 분석 지원	파일시스템 브라우징	O	O	O
	사용자 아티팩트 분석	X	X	O
레지스트리 하이브파일	레지스트리 브라우징	O	O	X
	레지스트리 정보 해석	O	X	X
삭제된 파일 카빙	-	O	O	O
원격지 수집	-	O	O	X

II. 디지털 포렌식 증거수집기술 파일카빙에 대한 개념

가. 파일카빙의 정의 및 특징

개념	- 메타데이터(meta-data)와 같은 부가 정보가 없는 데이터의 단편 조각들 간 인접-상관도를 측정하여 원래 이미지 형태로 단편화 조각들을 재조합해 디지털 증거를 재현하는 기술 - 데이터 영역에 존재하는 **파일 자체 정보(시그니처, 논리구조, 파일 형식, 고유특성)을 이용**하는 방법으로, 디스크의 비 할당 영역을 처음부터 끝까지 스캔하여 삭제된 파일을 찾아보고 복원하는 방식

나. 파일카빙의 프로세스



다. 파일 카핑의 분류

구분	연속적 파일 카빙	비연속적 파일카핑
개념	데이터가 저장매체의 연속된 공간에 저장된 경우 수행하는 기법	데이터 단편화가 발생하여 저장매체 여러 부분에 조각나 저장된 경우 수행하는 기법
주요기법	헤더/푸터, 램 슬랙 카빙, 파일 크기 카빙, 파일 검증 카빙	파일 조각화 비율, 시그니처 기반 기법, 엔트로피 이용 기법

- 데이터의 단편화 여부에 따라 연속적, 비연속적 기법 적용여부 판단

라. 파일 카빙의 기법특징

구분	주요기법	특징
연속적 파일카빙	헤더/푸터	파일 고유의 헤더와 푸터 시그니처 활용
	램 슬랙 카빙	윈도우 시스템으 램 슬랙이 항상 0X00으로 채워지는 성질 이용
	파일 크기카빙	각 파일의 고유한 헤더 구조체를 이용

비연속적 파일카빙	파일 조각화 비율	각 파일의 조각난 수에 따라 단편화 된 부분을 복구하는 기법
	시그니처기반	각 파일의 시그니처를 기반으로 단편화 된 부분을 복구하는 기법
	엔트로피 이용	블록/클러스터의 엔트로피를 계산하여 특정 파일의 조각을 분류하는 기법

-카빙을 쉽게 적용하거나 오탐율을 줄이기 위해서는 연속적, 비연속적 파일 카빙기법을 혼용하여 사용.

- 암호화된 이미지의 단편조각을 읽어내는 파일카빙은 하드웨어 구조를 기반으로 개발, 이미지 단편조각 간 상관성을 계산하는 기술은 소프트웨어 포렌식 기술을 기반으로 개발

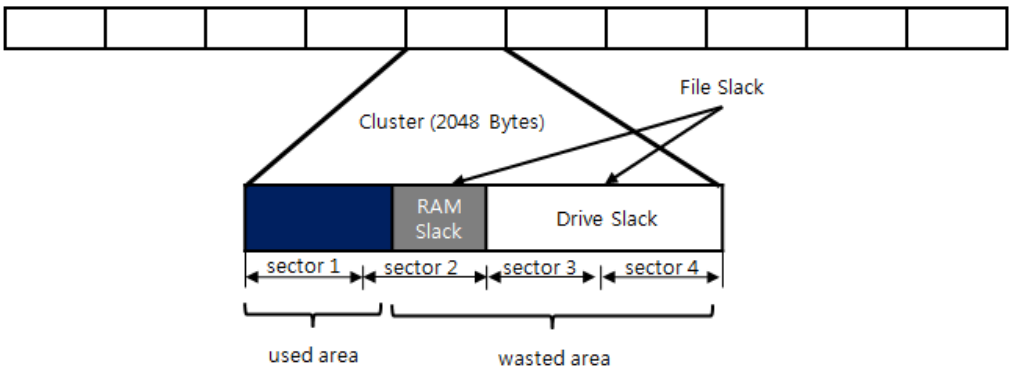
III. 연속적 파일 카빙 2 종류 기법 및 특징

가. 파일크기 파일카빙

개념	- 파일 가장 맨 윗단에 있는 파일 구조체를 이용 - 파일의 구조체 안에 파일의 크기 정보를 이용, 파일 구조체에서 제공해 주는 정보를 획득하여 카빙하는 방법
특징	- 파일 구조체 이용, 구조체 정보 획득
파일 포맷	파일 크기 획득 방법을 적용할 수 있는 파일 포맷

파일 포멧	시그니처	
	헤더(Hex)	푸터(Hex)
BMP	42 4D ("BM")	-
EXE	4D 5A ("PE")	-
DLL		-

나. 램슬랙카빙

개념	- 파일의 크기가 데이터 단위의 크기의 배수가 되지 않아 물리적, 논리적 구조의 차이로 발생하는 낭비 공간인 슬랙공간에 정보를 수집하는 방법
특징	- Footer 시그니처와 램 슬랙이용하여 오탐율 줄이는데 활용
램슬랙	

VI. 비연속적 파일카빙 2 종류 기법 및 특징

가. 시그니처기반 파일카빙

개념	파일 카빙은 메타 데이터를 이용하지 않기 때문에 고유의 특성으로 복구를 해야 하는데 각 파일의 포맷 별로 존재하는 파일 시그니처를 이용하는 방법
특징	- Header 시그니처와 Footer 시그니처가 존재 - Header 시그니처를 시작으로 Footer 시그니처를 확인하여 그사이 데이터를 해당 시그니처 파일 수집
파일 포맷	헤더, 푸터 시그니처를 모두 갖는 파일 포맷

파일 포맷	시그니처	
	헤더(Hex)	푸터(Hex)
JPEG	FF D8	FF D9
GIF]	47 49 46 38 37 61 ("GIF87a")	00 3B
	47 49 46 38 39 61 ("GIF89a")	
PNG	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44 AE 42 60 82
PDF	25 50 44 46 2D 31 2E ("PDF-1.")	25 25 45 4F 46 ("%%EOF")
HTML	"<HTML" or "<html"	"</HTML>" or "</html>"
	"<!DOCTYPE HTML" or "<!doctype html"	

나. 파일구조 검증방법 기반의 파일 카빙

개념	문서 파일과 같이 빈번한 수정이 이루어 지는 경우에 데이터 표현을 위해 고유한 계층 구조를 사용하는데 파일 구조 검증은 이러한 계층 구조를 검증해서 카빙하는 방식
특징	- Microsoft 복합 문서나 압축 파일 같은 경우에는 계층 구조 마다 고유한 시그니처가 존재 - 파일의 시작위치를 지정하고 계층 구조를 확인을 통해 수집
파일 포맷	파일 구조 검증 방법을 적용할 수 있는 파일 포맷

파일 포맷	시그니처	
	헤더(Hex)	푸터(Hex)
ZIP	50 4B 03 04	50 4B 05 06
ALZ	41 4C 5A 01	43 4C 5A 02
RAR	52 61 72 21 1A 07	3D 7B 00 40 07 00
Compound	D0 CF 11 E0 A1 B1 1A E1	-

기출풀이 의견

1. 디지털 포렌식의 개념을 물어보지 않았습니다. 질문에서 파일카빙을 물어봤습니다. 파일카빙에 대해서 작성하시고, 예전에는 연속된 파일 카빙 위주로 파일 추출을 하였으나, 비 연속 파일에 대한 파일 카빙 기술이 나오면서 진보된 증거수집이 이루어지고 있습니다. 이러한 부분을 마지막 단락에 작성하시면 좋을 거 같습니다.