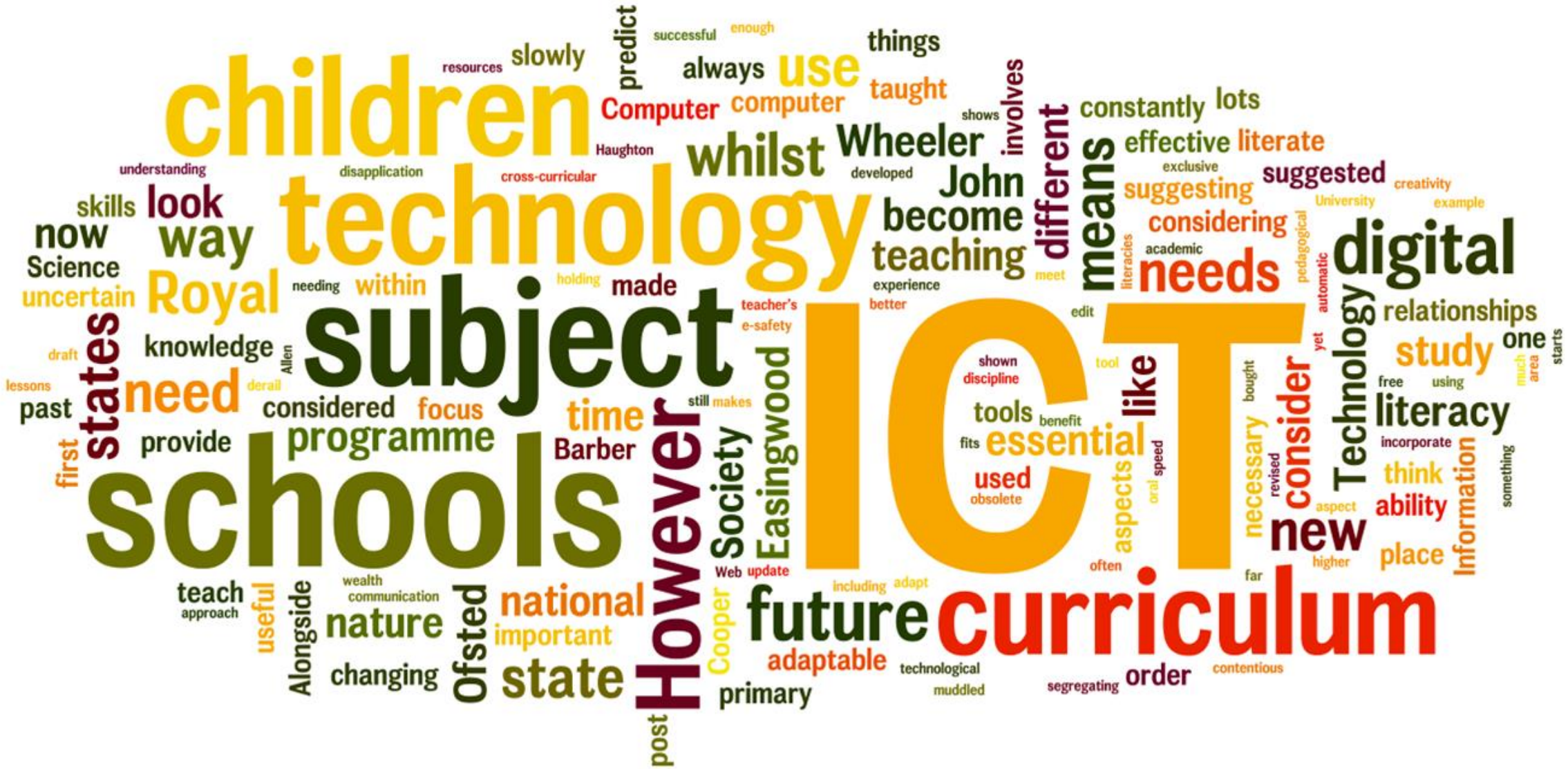

children
technology
subject
schools
ICT
curriculum
However
future
digital
needs
means
different
Wheeler
whilst
John
become
teaching
Computer
computer
always
use
things
taught
involves
constantly
lots
effective
literate
suggested
suggesting
considering
academic
exclusive
creativity
example
University
pedagogical
automatic
literacies
meet
experience
better
edit
relationships
study
one
starts
much
area
free
using
literacy
incorporate
think
ability
place
Information
something
Technology
consider
yet
bought
necessary
revised
aspect
higher
far
new
often
aspects
oral
speed
like
essential
used
obsolete
fits
tools
benefit
shown
discipline
tool
teacher's
e-safety
made
holding
within
needing
Royal
uncertain
Science
way
now
look
skills
understanding
disapplication
cross-curricular
Haughton
developed
slowly
resources
predict
successful
enough
Easingwood
Society
Web
update
Cooper
primary
post
adaptable
technological
muddled
segregating
order
contentious
including
adapt
national
important
state
Ofsted
changing
nature
wealth
communication
Alongside
useful
teach
approach
first
states
draft
lessons
past
need
knowledge
Allen
derail
provide
considered
focus
programme
time
Barber
still
makes
Haughton

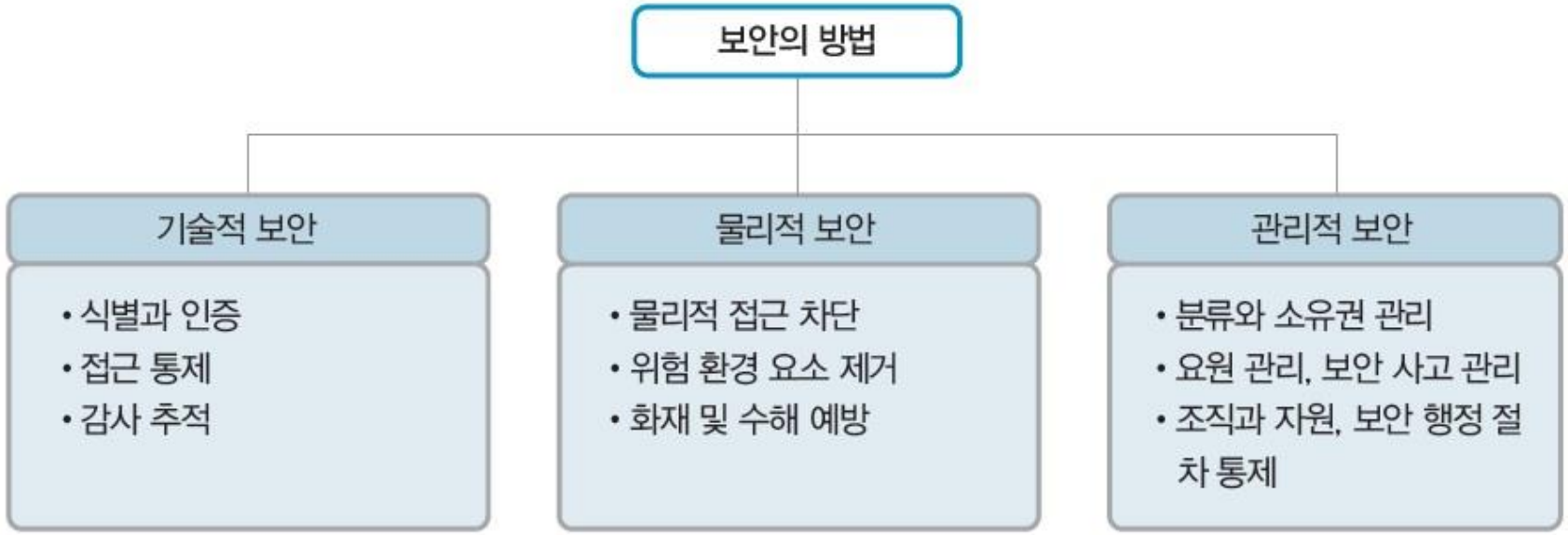
10 정보통신 보안과 윤리

정보통신 보안의 필요성

- 인간 생활에서 컴퓨터와 네트워크 의존도가 높아지면서 부작용도 증가
- 앞으로 정보통신 기술이 발전하는 만큼 정보통신 보안의 중요성이 더 커질 것

정보통신 보안의 개념

사용자의 시스템에 불법으로 침입하여 공격하는 위협으로부터 시스템을 보호하거나, 네트워크를 통해 데이터를 전송할 때 발생하는 데이터의 누설과 변조로부터 데이터를 보호하는 것을 정보통신 보안이라고 한다.

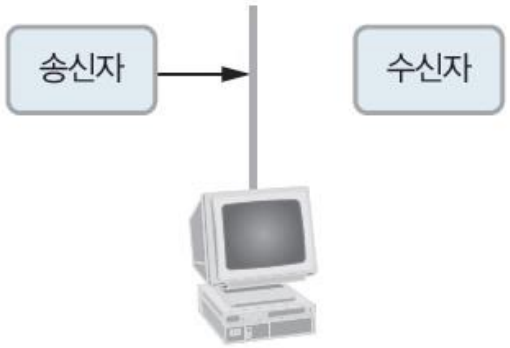


크래커(Cracker)

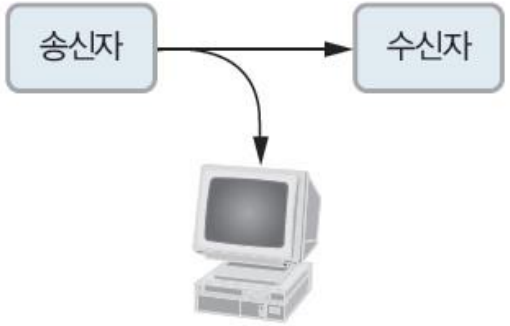
- 크래커(Cracker)와 불법 공격
  - 다른 사람의 컴퓨터 시스템에 무단으로 침입해 정보를 훔치거나 프로그램을 훼손하는 등 불법 행위를 하는 사람
- 크래커가 행하는 불법 공격의 유형
  - 방해(Interruption) : 송신자의 데이터를 수신자에게 전달하지 못하도록 시스템의 일부를 파괴하거나 사용할 수 없게 하는 것
  - 가로채기(Interception) : 송신자의 데이터를 수신자에게 전달할 때 통신선로 등을 가로채서 데이터를 얻는 행위
  - 변조(Modification) : 송신자의 데이터를 수신자에게 전달할 때 허가되지 않은 주체가 시스템에 불법으로 접근하여 데이터를 변경하는 것
  - 위조(Fabrication) : 송신자의 데이터를 수신자에게 전달할 때 허가되지 않은 주체가 시스템에 거짓정보를 삽입하여 수신자가 착각하게 만드는 것

크래커(Cracker)

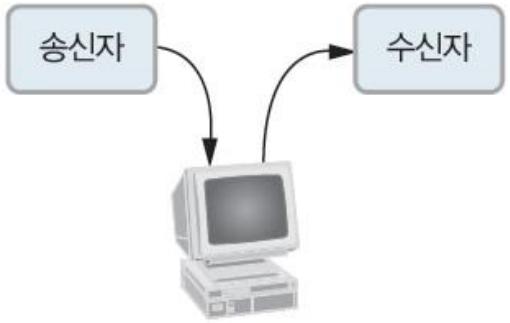
- 크래커가 행하는 불법 공격의 유형



(a) 방해



(b) 가로채기



(c) 변조

(d) 위조

악성 프로그램과 감염 형태

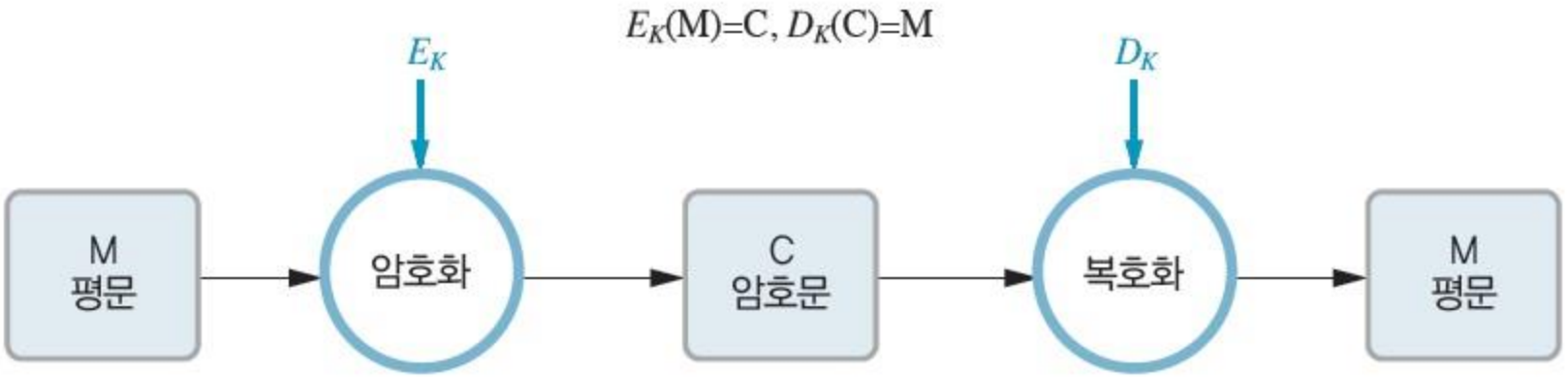
- 컴퓨터 바이러스(Computer Virus)
  - 컴퓨터에서 실행되는 프로그램의 일종
  - 자기 복제를 하며, 컴퓨터 시스템을 파괴하거나 작업을 지연 및 방
- 웜(Worm)
  - 실행 코드 자체로 번식하며, 주로 PC에서 실행됨
  - 전자우편을 이용해 다른 사람에게 전달되는 형태로 많이 출현하면서 일반인에게도 널리 알려짐
- 트로이 목마(Trojan Horse)
  - 컴퓨터 사용자의 정보를 빼 가는 악성 프로그램
  - 상대편이 눈치채지 못하게 프로그램을 다른 사람의 컴퓨터에 몰래 설치한다는 의미에서 트로이 목마라고 함

암호화 기술

- 암호를 사용하는 목적
  - 기밀성(Confidentiality) : 허가된 사람 이외에는 그 내용을 알 수 없게 함
  - 무결성(Integrity) : 외부의 요인으로 데이터가 변조되었는지 알 수 있게 함
  - 인증(Authentication) : 통신하는 상대방이 맞는지 확인한 후 서로에게 전송한 데이터가 위조되지 않았음을 확인할 수 있게 함
  - 부인방지(Non-repudation) : 통신 내용을 보낸 적이 없다고 속이지 못하게 함

암호화와 복호화

- 암호화(Encryption 또는 Encoding Processing)
  - 암호화되지 않은 상태의 평문을 암호문으로 만드는 것
- 복호화(Decryption 또는 Decoding Processing)
  - 암호문을 평문으로 바꾸는 것



암호화 기술의 분류

암호화 기술 동작 형태에 따른 분류	대치 암호
	치환 암호
평문 처리방법에 따른 분류	블록 암호화
	스트림 암호화
분류키에 따른 분류	관용 암호화(비밀키 암호화, 대칭키 암호화)
	공개키 암호화(비대칭키 암호화)

대치 암호(Substitution Cipher)

- 평문의 각 문자를 다른 문자나 기호로 일-대-일 대응시켜 암호문자로 변환

① 시저(Caesar) 암호 : 각 문자를 세 번째 뒤에 있는 문자로 대체한다.

M(평문)	a b c d e f g h i j k l m n o p q r s t u v w x y z
E_k(M)(암호문)	d e f g h i j k l m n o p q r s t u v w x y z a b c

② 단일 알파벳 암호 : 문자를 다른 문자로 일–대–일 매핑한다.

M(평문)	a b c d e f g h i j k l m n o p q r s t u v w x y z
E_k(M)(암호문)	o f j g z h r e k t a x d v q i s l u p m y n c b w

치환 암호(Transposition Cipher)

- 평문에 있는 문자의 위치를 바꾸는 방식

① 각 단어의 알파벳 순서를 뒤집어 끝부터 적는 방법으로, 간단하게 암호화한다.

M(평문)	data communication
E_k(M)(암호문)	atad noitacinummoc

② 각 단어의 알파벳 순서를 뒤집어 끝부터 적은 다음에 다섯 글자씩 묶어 상대적으로 복잡하게 암호화한다.

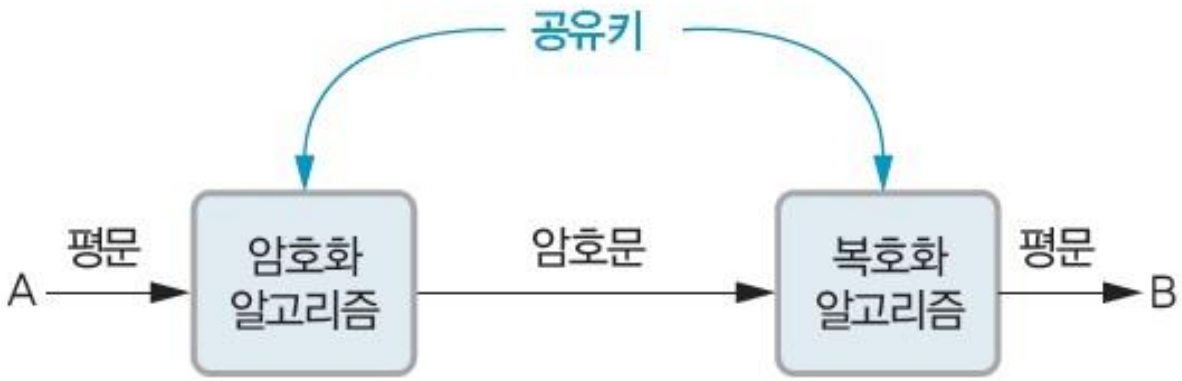
M(평문)	data communication
E_k(M)(암호문)	atadn oitac inumm oc

블록 암호화와 스트림 암호화

- 블록 암호화(Block Encryption)
  - 평문을 블록 단위로 모아 암호화하는 방식
  - 대표적인 블록 암호화 시스템으로는 DES, Triple-DES, 유럽에서 사용하는 IDEA, 일본에서 사용하는 FEAL 등이 있음
- 스트림 암호화(Stream Encryption)
  - 평문을 연속적으로 입력하여 암호화하는 방식

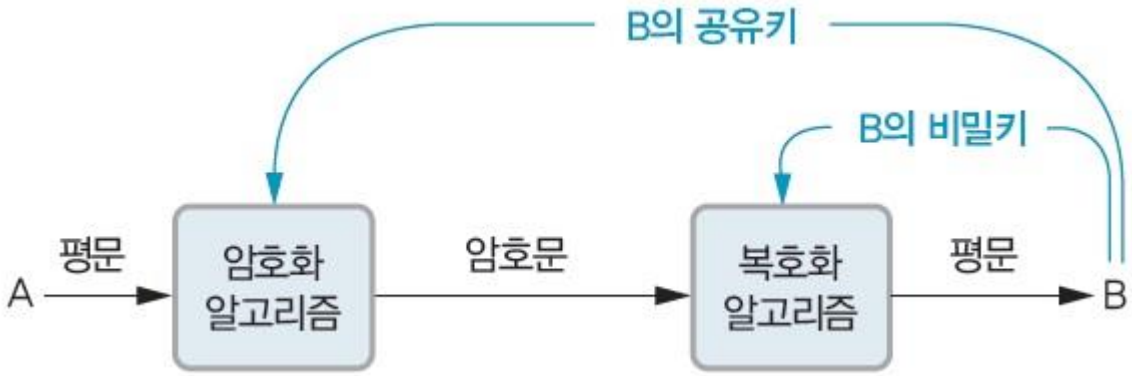
관용 암호화(Conventional Encryption)

- 암호화와 복호화에 쓰는 키가 같아 속도가 빠름
- 암호화할 때 쓴 키를 어떻게 상대방에게 전달할지가 문제
- 비밀키 암호화(Secret Key Encryption) 방식 또는 대칭키 암호화 방식이라고 함
- DES 암호화는 대칭키 암호화이면서 동시에 블록 암호화임



공개키(Public Key) 암호화

- 메시지를 암호화할 때 사용하는 암호화키와 그 암호문을 해독할 때 사용하는 해독키가 서로 다름
- 암호화키를 공개함으로써 키의 생성과 분배가 쉬움
- 관용 암호화보다 암호화와 복호화 속도가 느림
- 대표적인 예는 RSA 방식
- 비대칭키 암호와 방식이라고도 함



관용 암호화와 공개키 암호화의 비교

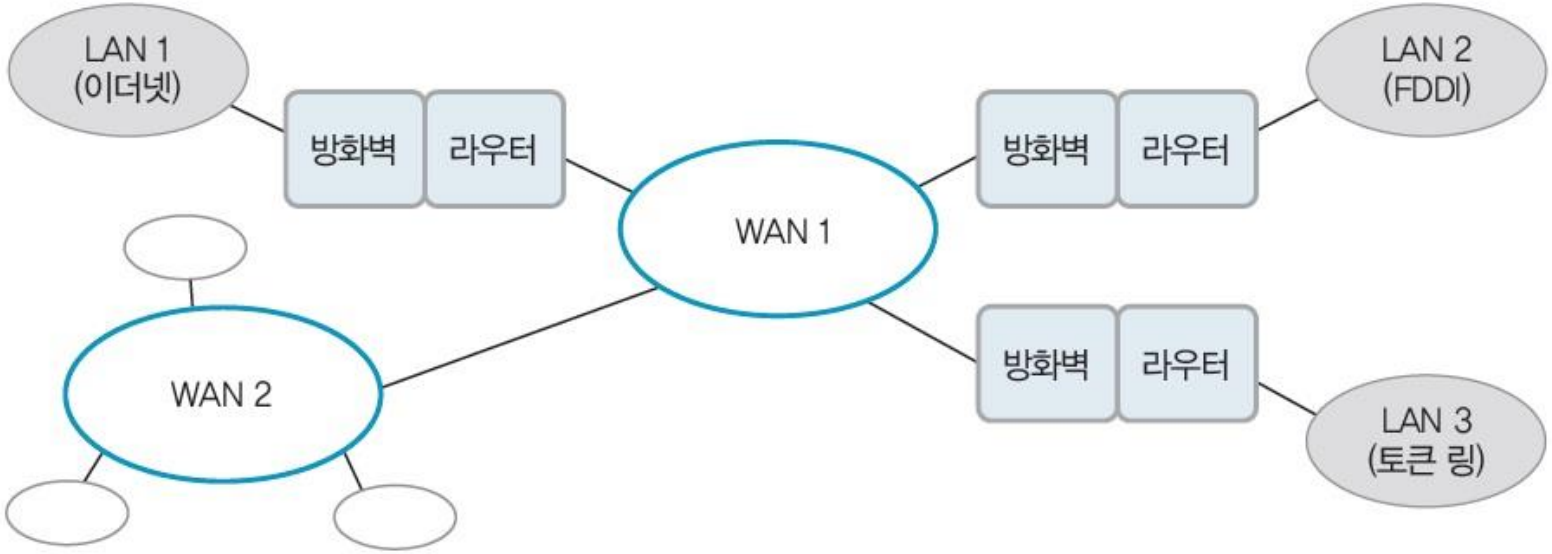
종류 / 항목	관용 암호화	공개키 암호화
키의 대칭 여부	대칭키 암호화로 암호화키와 복호화키가 동일	비대칭키 암호화로 암호화키와 복호화키가 다름
암호화키	비밀	공개
복호화키	비밀	비밀
비밀키 전송	필요	불필요
대표적인 예	DES, 3DES, AES	RSA
암호화 속도	고속	저속
키 분배	어려움	용이
키 길이	짧다	길다

응용 서비스 보호 기술

- 바이러스 백신
  - 컴퓨터 바이러스를 찾아 기능을 정지하거나 제거하는 프로그램
  - 감염된 바이러스를 찾아 기능을 정지하거나 삭제하는 역할
  - 바이러스의 감염을 사전에 막지는 못함
- 전자서명
  - 인터넷 등 가상공간에서 문서나 메시지를 송수신할 때 사용
  - 개인의 고유성을 주장하고 인정받기 위해 디지털 문서에 전자 방식을 이용해 서명하는 것
  - 전자서명은 공개키 암호화 기법을 이용

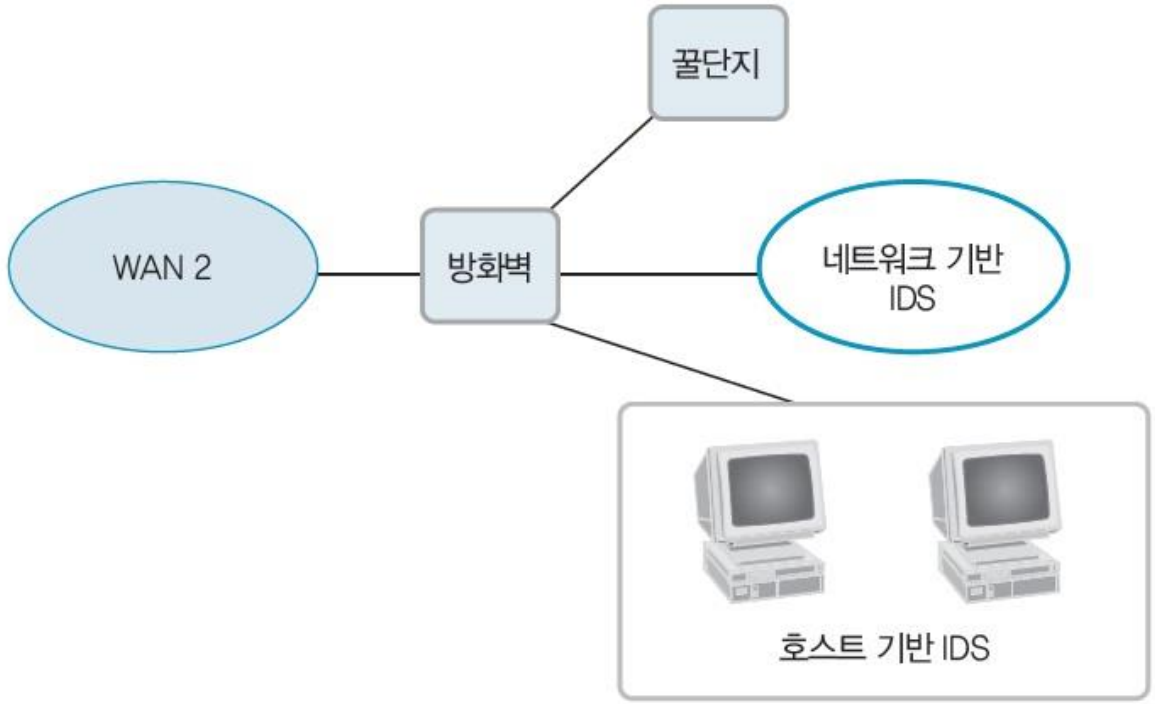
방화벽(Firewall)

- 내부 네트워크와 외부 네트워크 사이에 있는 하드웨어와 소프트웨어로 구성
- 보통은 라우터나 서버 등에 위치하는 소프트웨어



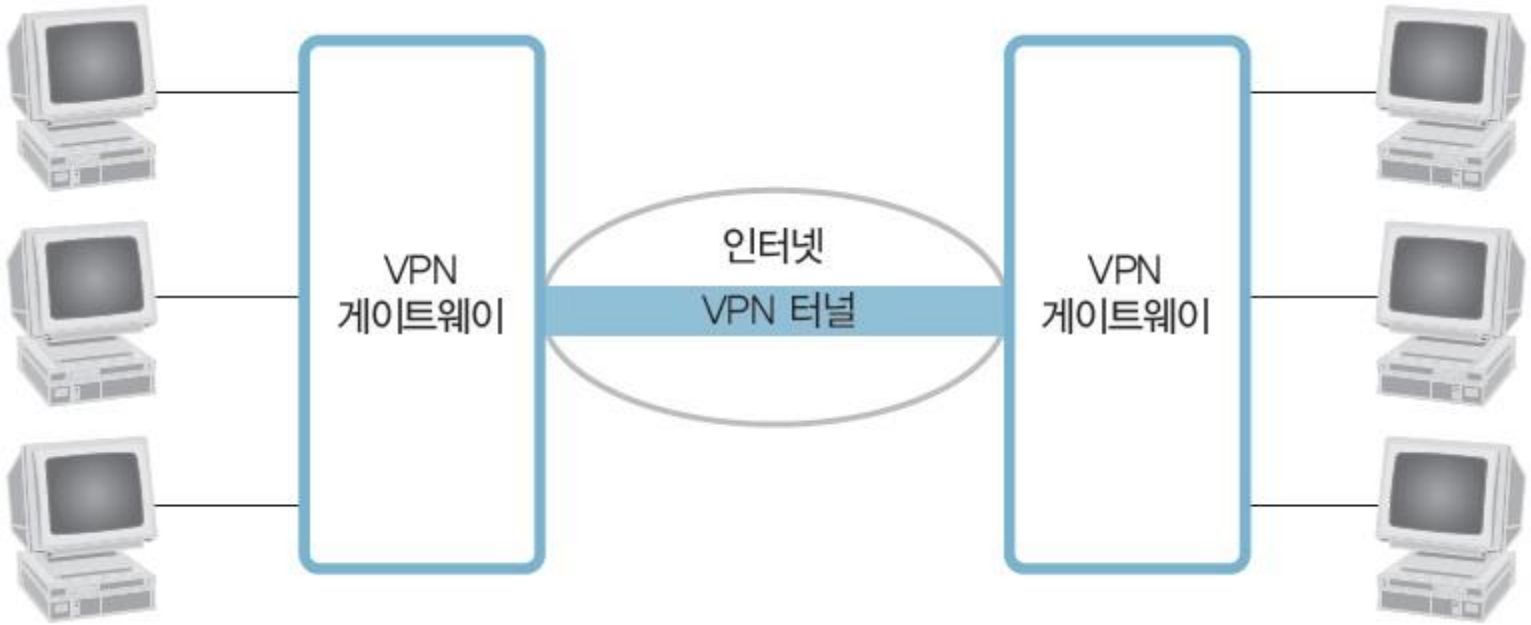
침입탐지시스템(IDS, Intrusion Detection System)

- 인증 절차를 거치지 않고 불법으로 침입한 사용자를 찾아내는 시스템
- H-IDS(Host-based IDS)
  - 호스트(컴퓨터)에서 일어나는 일련의 활동을 감시하고 침입 발생을 탐지하는 IDS
- N-IDS(Network-based IDS)
  - 네트워크에서 일어나는 활동을 감시하고 침입 시도를 탐지하는 IDS

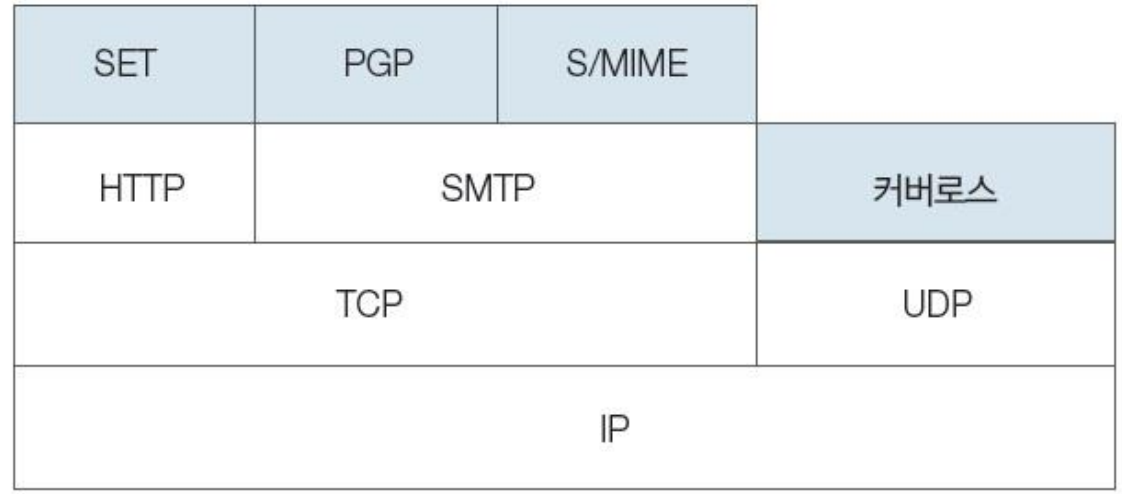


가상 사설망(VPN, Virtual Private Network)

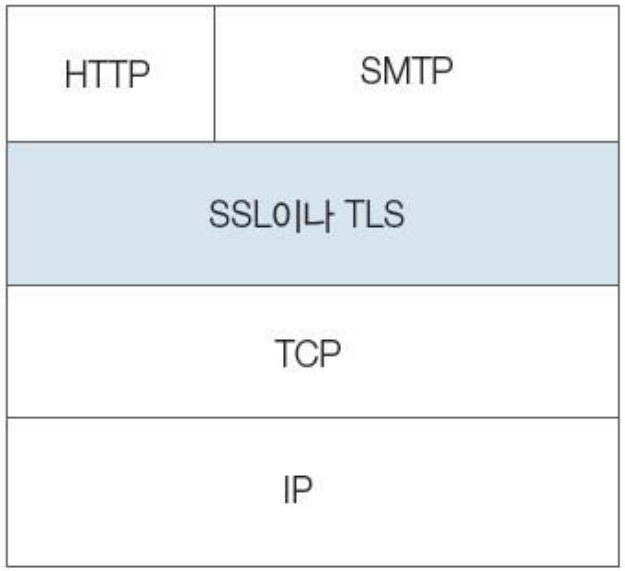
- 게이트웨이 사이에서 물리적으로 통신하되, 암호화 통신은 논리적으로 하는 방식
- 주로 단말과 단말 사이에 통신하는 패킷을 압축·암호화하여, 이 패킷을 터널링 기술을 이용해 전송



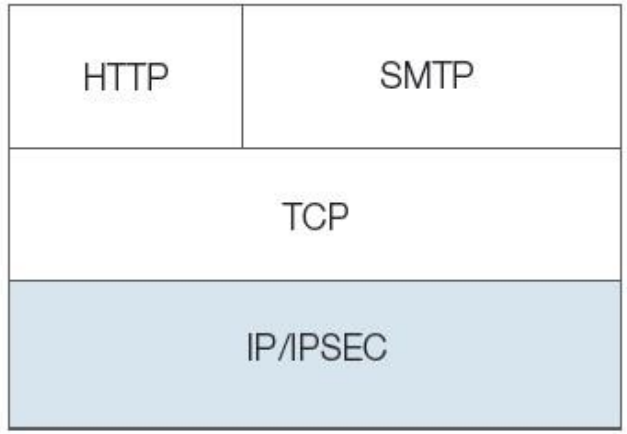
TCP/IP 보안



(a) 응용 계층



(b) 전송 계층



(c) 네트워크 계층

네트워크 보안 기술

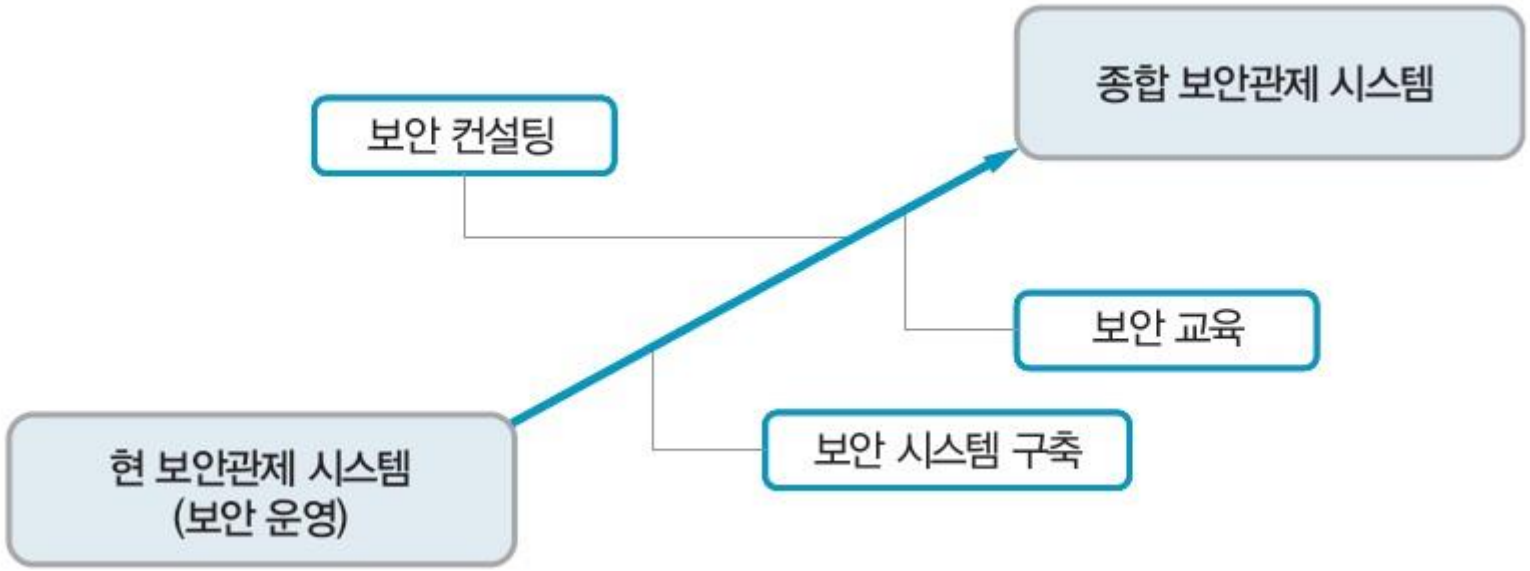
- IPSEC(IP SECurity)
  - 네트워크 계층에서 IP 패킷을 보호하는 인터넷 표준 방식
  - IPSEC 작업 그룹은 네트워크 계층에서 인터넷 보안 기술을 다루는 유일한 그룹
  - 인터넷 네트워크를 경유하는 IP 패킷의 보안 문제를 다룸
- SSL/TLS(Secure Sockets Layer/Transport Layer Security)
  - SSL
    - 넷스케이프에서 개발한 보안 프로토콜
    - TCP/IP에서 동작하도록 설계
    - 응용 계층과 전송 계층 사이에서 클라이언트와 서버 간 안전한 채널을 형성해 주는 역할
  - TLS
    - 통신 응용 프로그램 사이에서 개인의 정보 보호와 데이터의 무결성을 제공
    - 응용 프로토콜에 독립적

네트워크 보안 기술

- SET(Secure Electronic Transaction)
  - 오픈 네트워크에서 전자상거래를 안전하게 하도록 보장해 주는 보안 프로토콜
- PGP(Pretty Good Privacy)
  - 인터넷 전자우편을 암호화·복호화시켜 제3자가 알 수 없게 하는 보안 프로그램
- S/MIME(Secure Multi-purpose Internet Mail Extensions)
  - RSA 암호화를 사용해 전자우편을 안전하게 보내는 방법
- 커버로스(Kerberos)
  - 오픈 네트워크에서 인증과 통신의 암호화를 하여 보안성을 확보하는 알고리즘
  - 키분배센터(KDC)에서 클라이언트의 패스워드를 기초로 생성한 티켓을 발급하고 이를 사용해 패스워드의 누출 위험을 줄여 더 높은 상호 인증을 구현

보안관제 시스템

- 보안관제 시스템의 개념
  - 불법적인 접근으로부터 네트워크 자원을 보호할 목적으로 관제가 필요한 모든 시스템을 실시간으로 모니터링하여 즉각적으로 대응할 수 있도록 만든 시스템



차세대 보안관제 시스템

- 고화질의 영상정보를 확보하되 개인의 프라이버시 침해는 최소화해야 함
- 이미 발생한 사건에 대한 신속한 추적은 물론, 미연에 방지할 수 있어야 함

정보통신 기술이 사회에 미친 역기능

- 인간이 하는 일을 로봇이 대신 하면서 일자리가 줄어듦
- 각 부문이 네트워크로 연결되면서 시스템 한 곳이 정지되면 전체 시스템에 장애가 발생
- 원격통신을 이용한 업무 처리, 재택근무가 보편화되면서 인간관계가 소원해짐
- 검증되지 않은 정보가 인터넷을 통해 유출되어 개인의 인격이 훼손되는 문제 (악플이나 신상 털기 등)
- 집단 사이버 폭력이나 과몰입으로 인한 생활 파탄 등의 문제

사이버 공간과 현실세계의 차이점

- 사이버 공간은 내가 상상한대로 만들 수 있지만, 현실세계는 정신적, 육체적 노력과 사회적 환경이 뒷받침되어야 성과를 낼 수 있음
- 사이버 공간은 현실이 뒷받침되지 않으면 유지할 수 없음 (현실에 의존적)
- 사이버 공간은 현실세계에 비해 자유롭고 평등해서 일탈 행동으로 이어지기 쉽고, 익명성이 보장되어 정보를 왜곡시키거나 과장할 가능성이 있음
- 사이버 공간은 현실세계의 면대면 대화보다 더 복잡하고 다양한 방법으로 소통(이메일, 페이스북, 트위터, 스마트폰의 카톡, 밴드 등)
- 사이버 공간은 현실세계보다 공간적인 제약을 극복하기가 쉬워 정보가 실시간으로 확산됨

정보통신 윤리의 개념과 기본 원칙

- 정보통신 윤리의 개념
  - 정보통신 사회에서 야기되고 있는 윤리적 문제들을 해결하기 위한 규범 체계
- 정보통신 윤리의 기본 원칙
  - 정의(Justice)
    - 사이버 공간에서 사용자는 자신이 제공하는 정보의 진실성, 비편향성, 완전성, 공정한표현성 등을 추구해야 함 (타인의 기본적 자유와 권리를 침해하지 않아야 하기 때문)
  - 책임(Responsibility)
    - 정보 제공자는 자신의 행동이 어떤 결과를 가져오게 될지에 대해 미리 심사숙고해야 함
  - 존중(Respect)
    - 자신에 대한 존중과 타인에 대한 존중을 의미
  - 해악금지(Non-Maleficence)
    - 따뜻하고 정감 있는 공간을 만들기 위해 각자 타인의 복지를 증진시키는 방향으로 행동