

토픽이름	AES
분류	정보 보안 > 암호화 > AES
키워드	레인Deal(Rijndael), 대칭키, 미국 연방 정보처리 표준, DES 개선 요구 대응 특징 – 가변 길이의 블록, 가변길이 키 사용, 공격 저항력 높음, 속도와 코드의 간결성, 단순한 설계, 1회의 순열과 3회의 치환의 4단계 구성 암호화 절차 - 바이트 치환(Substitute bytes), 행이동 (Shift row), 열 혼합(Mix columns), 라운드 키 추가(Add Round Key)
암기법	

기출문제

번호	문제	회차
1	1. AES(Advanced Encryption Standard)에 사용되는 SPN(Substitution Permutation Network) 구조에 대하여 설명하시오.	102.컴시응.2.1
2	SNS 검열과 관련하여 암호화에 대한 관심이 고조되고 있다. 암호화 알고리즘의 개념에 대하여 설명하고 아래 알고리즘에 대해서 기술하시오. 가. RSA (Rivest, Shamir, Adleman) 나. SHA-2 (Secure Hash Algorithm) 다. AES (Advanced Encryption Standard)	응용.모의 2014.11.4

I. DES 를 대체하는 고급 암호화 표준 AES의 개요

가. AES의 정의

- 1998년 미국의 표준기술 연구소(NIST)에 의해서 수행된 암호화 알고리즘
- 공모전에 선정된 Rijndael 암호화 기술임

나. AES 의 등장배경

- DES의 암호화 강도가 발달하는 PC수준으로 약해짐
- DES 암호기술은 속도가 느림
- 속도가 빠르면서 3-DES 이상의 안전성과 효율성이 요구됨

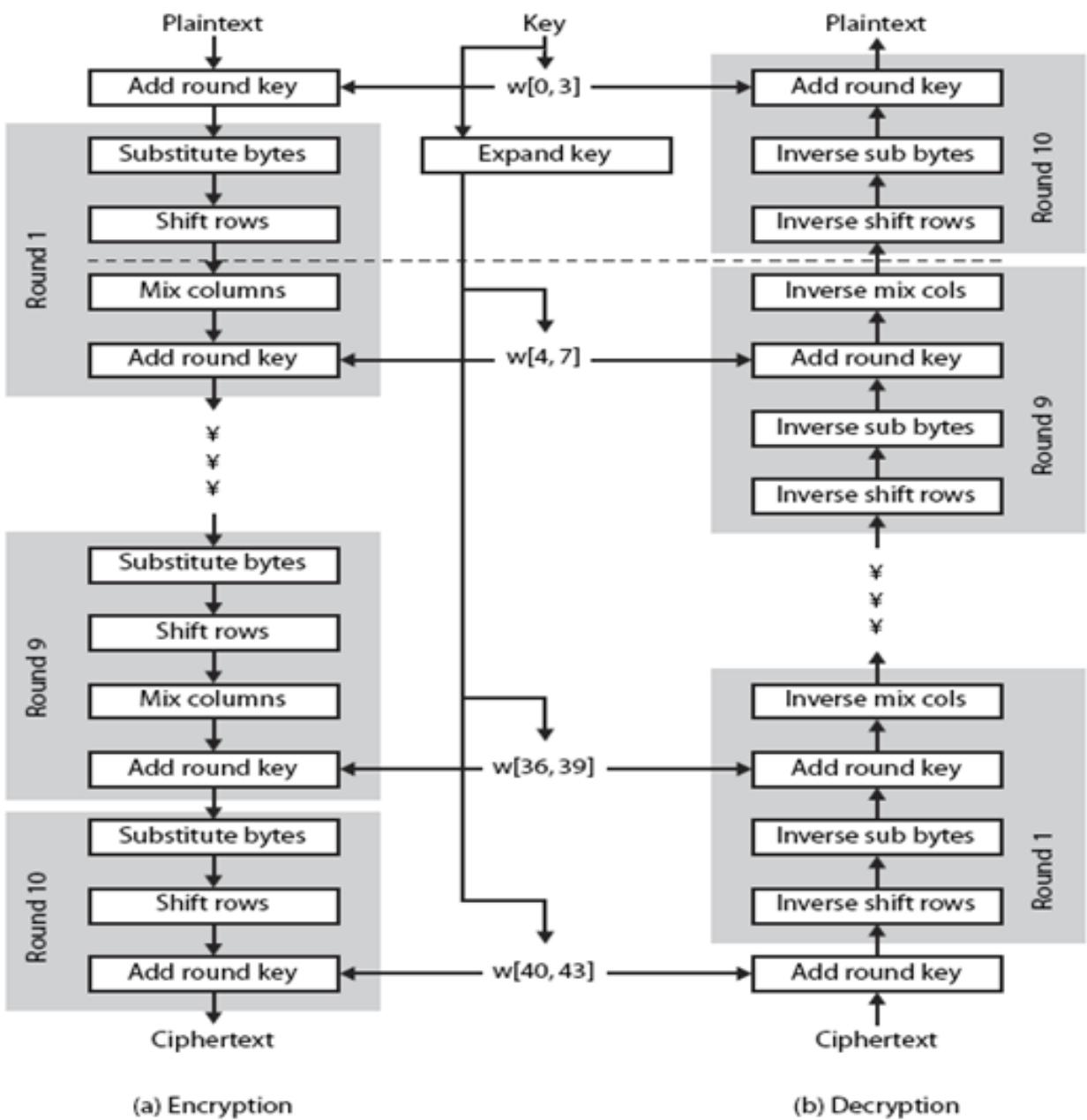
다. AES 특징

- 가변 길이의 블록과 가변 길이의 키 사용 가능(128,192,256)
- 모든 알려진 공격에 대한 저항력을 가짐
- 다양한 플랫폼에 대한 속도와 코드의 간결성이 있음
- 단순한 설계 (※워드/바이트/비트 순으로 표시)

키 길이	4/16/128	6/24/192	8/32/256
평문블록 사이즈	4/16/128	4/16/128	4/16/128
라운드 수	10	12	14
라운드 키 길이	4/16/128	4/16/128	4/16/128
확장 키 길이	44/176/1408	52/208/1664	60/240/1920

- 1회의 순열과 3회의 치환으로 구성된 4단계 사용

바이트 치환(Substitute bytes)	블록의 바이트 대 바이트 치환을 수행하기 위해 하나의 S-BOX를 사용
행 이동 (Shift row)	단순 순열
열 혼합(Mix columns)	GF 산술식을 사용한 치환
라운드 키 추가(Add Round Key)	현재 블록과 확장된 키의 일부로 단순 비트 단위의 XOR 연산



(a) Encryption

(b) Decryption

II. AES에서의 SPN 과정

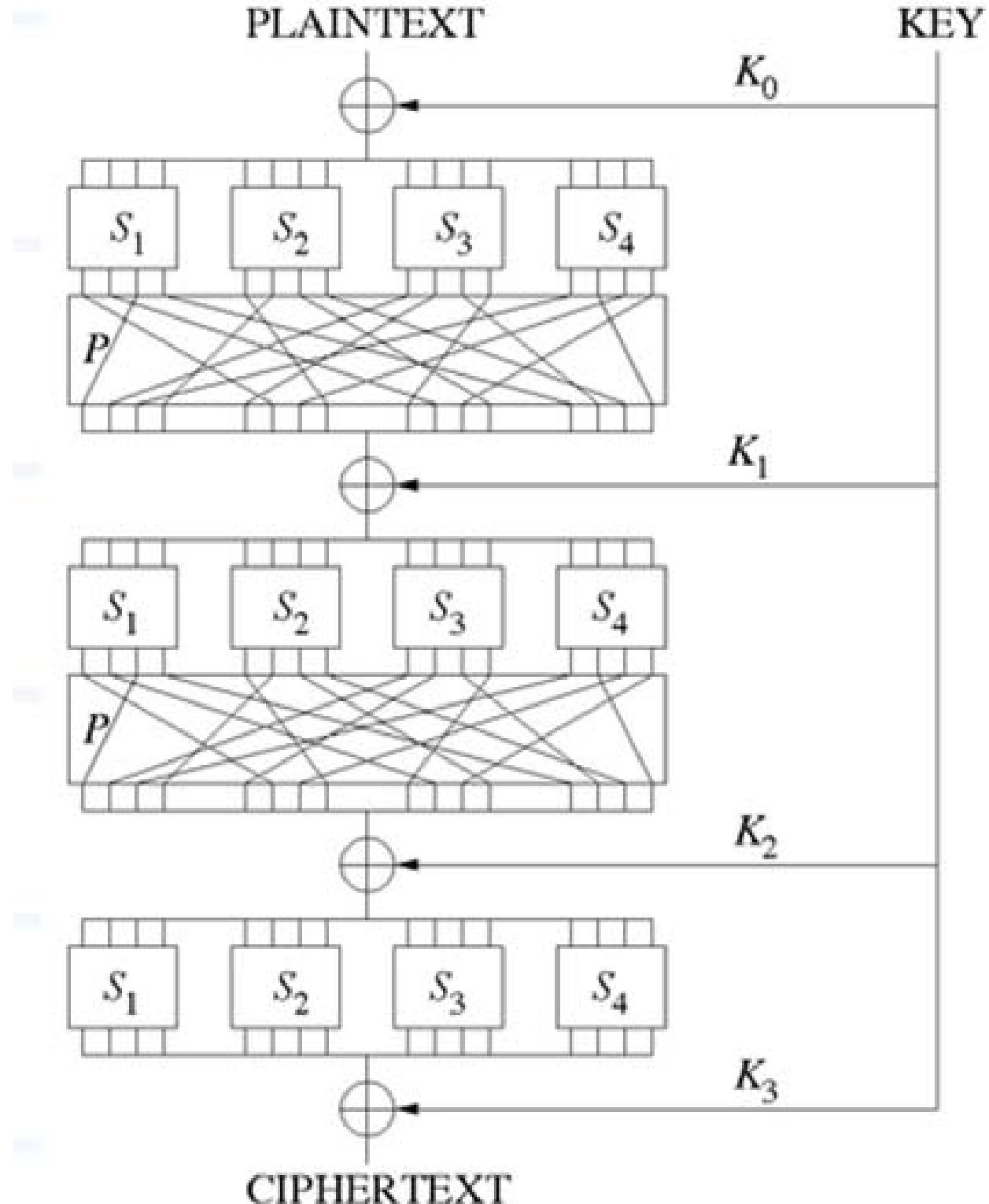
가. SPN(Substitution-Permutation Network)의 정의

- S-Box를 이용한 대체기법과 P-Box를 이용한 치환기법,
- 라운드 키를 이용한 반복적 연산으로 이루어지는 블록 암호화 알고리즘

나. SPN의 특징

- 병렬 연산이 가능하기 때문에, 알고리즘의 고속화 가능,
- 복호화 시 별도의 복호화 모듈 생성 필요
- AES, 3-Way, SAFER, SHARK

다. SPN의 구성도



라. SPN 구성요소

구 분	설 명
평문(Plain Text)	암호화 하고자 하는 문장
대체(S-Box)	평문을 n bit로 나누고, S-Box 테이블을 참조하여 다른 n bit로 대체
치환(P-Box)	S-Box 출력의 모든 Bit의 순서를 치환
라운드 키(Round Key)	P-Box의 출력을 변환하기 위한 암호화 키
암호문(Cipher Text)	평문을 암호화 알고리즘과 키를 이용하여 암호화 한 문장

마. ES에서의 SPN 변환과정

내용	설명
Plaintext의 State 변환	일반 텍스트의 16진수 변환과 State로의 변환
SubBytes()	Substitution 테이블을 통해 변환
ShiftRows()	State의 0번째 행은 건너뛰고 1번째 행부터 1바이트씩 왼쪽 순환 이동
MixColumns()	행렬 곱셈을 이용하여 바이트들을 뒤섞는 과정
AddRoundKey()	State 행렬에 라운드 키와 XOR 수행

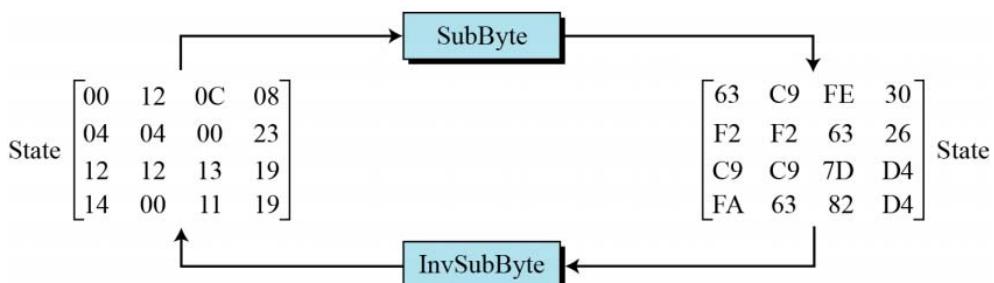
- Plaintext의 State 변환

- 일반 텍스트의 16진수 변환과 State로의 변환
- 일반 텍스트의 변환 예

Text	A E S U S E S A M A T R I X Z Z
Hexadecimal	00 04 12 14 12 04 12 00 0C 00 13 11 08 23 19 19
	$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix} \text{ State}$

- SubBytes()

- Substitution 테이블을 통해 변환
- 변환 예

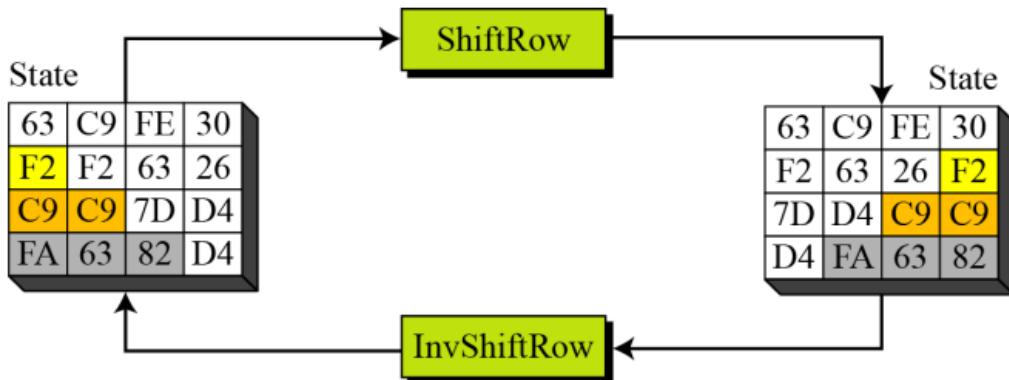


Substitution 테이블 (S-Box)

		y																
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	
x		0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0	
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15	
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75	
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84	
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf	
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8	
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2	
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73	
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db	
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79	
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08	
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a	
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e	
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df	
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16	

- ShiftRows()

- State의 0번째 행은 건너뛰고 1번째 행부터 1바이트씩 왼쪽 순환 이동
- ShiftRows() 변환 예

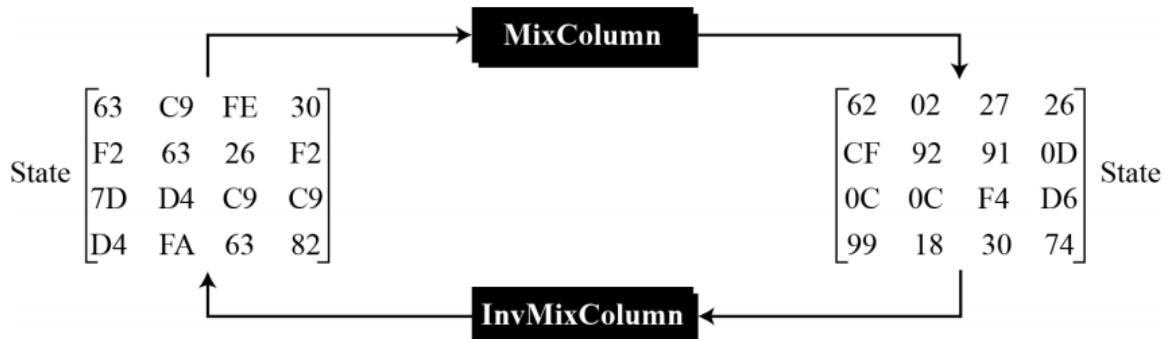


- MixColumns()

- 행렬 곱셈을 이용하여 바이트들을 뒤섞는 과정

$$\begin{array}{l}
 ax + by + cz + dt \\
 ex + fy + gz + ht \\
 ix + jy + kz + lt \\
 mx + ny + oz + pt
 \end{array} \rightarrow \left[\begin{array}{c} \text{New matrix} \\ \text{New matrix} \\ \text{New matrix} \\ \text{New matrix} \end{array} \right] = \left[\begin{array}{cccc} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{array} \right] \times \left[\begin{array}{c} \text{Constant matrix} \\ \text{Old matrix} \\ \text{Old matrix} \\ \text{Old matrix} \end{array} \right]$$

- MixColumns() 변환 예



- AddRoundKey()

- State 행렬에 라우드 키와 XOR 수행

The State

S0	S4	S8	S12
S1	S5	S9	S13
S2	S6	S10	S14
S3	S7	S11	S15

Subkey

K0	K4	K8	K12
K1	K5	K9	K13
K2	K6	K10	K14
K3	K7	K11	K15

AddRoundKey ()

XOR

New State

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

IV. AES와 타 암호화 알고리즘 비교

가. 3-DES, AES, SEED 비교

구분	3-DES	AES	SEED
장점	DES호환	안전성 우수 효율성이 높음 크래킹 위험이 낮음	안전성/속도 우수 크래킹 위험 낮음
단점	크래킹 위험 높음 쉽게 해독 가능	외국기술에 종속	국제적 범용성 낮음
키길이	56비트	128,192,256비트	128비트
블록크기	64비트	128비트	128비트
표준	레거시 시스템 표준	NIST표준	IETF/ISO표준

나. AES, Hash 함수 비교

구분	AES	Hash Function
주요 개념	암·복호화 가능한 암호화 기술	암호화만 가능하고 복호화 불가능 - 이것을 제1저항성이라 부름 (Preimage Resistance)
활용 분야	개인정보 전체 암호화 적용	비밀번호 암호화 (제3자가 절대로 알 수 없도록 함) 내부 개발 지원도 알 수 없음

[참고] S-Box, P-Box 개념

1단계 – 평문은 라운드 키를 이용해 XOR하고, 그 결과에서,

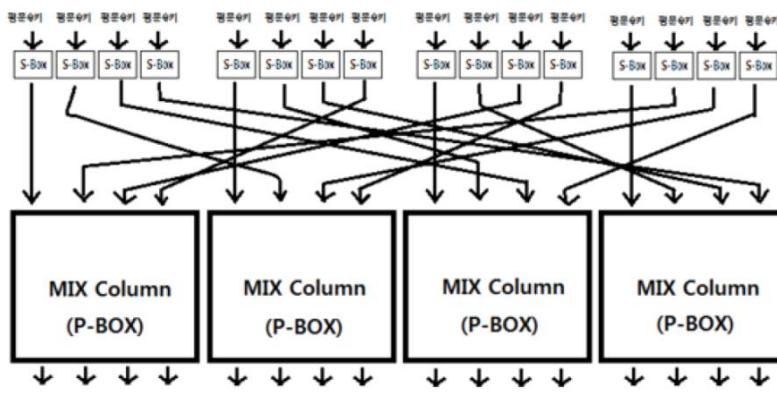
XOR한 각 바이트는 앞부분과 뒷부분(예를 들면, 16비트)로 다음의 S-Box 인덱스를 찾아가 변환; e9 -> 1e

hex	Y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

S-box (substitution-box)

라운드 키 : 고성능 핵심 기술로서, 키 생성 알고리즘에 의해 생성시킴

2단계 – P-Box를 이용해서, 위치 바꾸기(Rotation 진행)



[Mix Column] 을 P-Box라고 부름

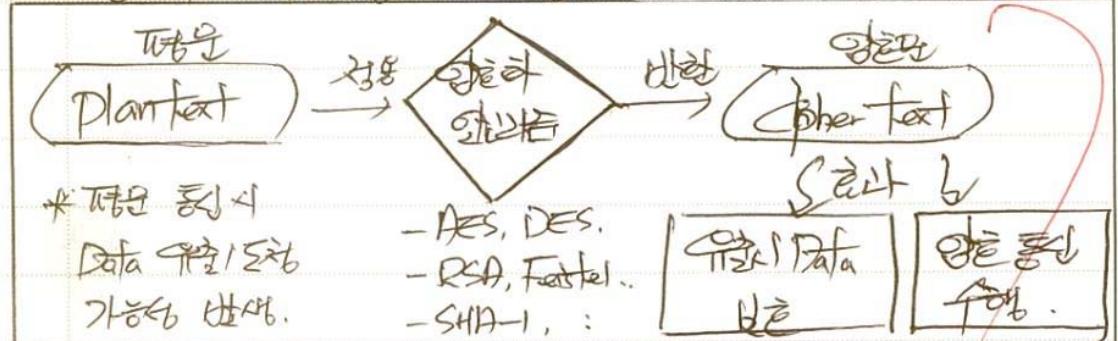
permutation box (or P-box)

- ④) 1) 암호화 암호화증 개념
 2) RSA, SHA-2, AES 설명.

5).

I. 디비터의 기밀성 위한 암호화 암호화증 개념.

가. 암호화 암호화증의 정의.



- 평문 Data의 안전한 송·수신 통한 "무결성", "기밀성", "기동성" 확보하기 위한 암호화증 기법.
- 평문의 암호화 암호화증 도입 통한 인증통제 수행.

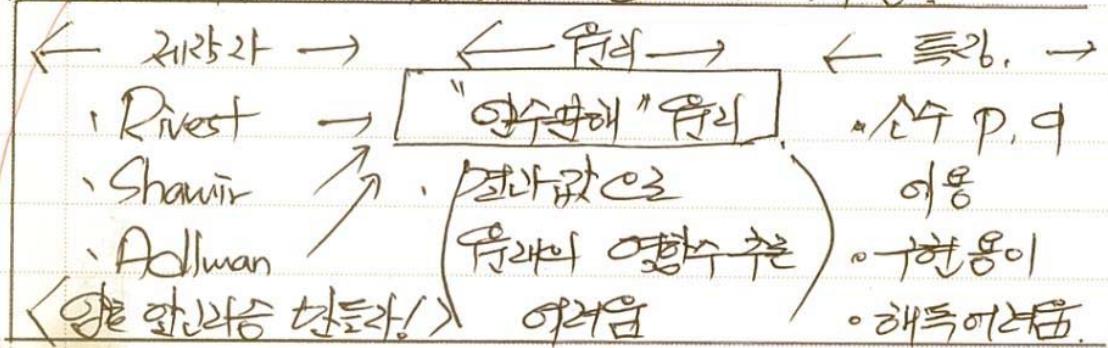
나. 암호화 암호화증의 유형별 분류.

분류	세부	설명 / 예제.
비대칭형	- 송·수신측이 서로 다른 암호 Key 사용.	
대칭형 (송·수신측) 같은 암호 Key 사용	복호 방식. (고장 길이)	RSA : 암호화 방식 암호화증 DES : Feistel 기반 암호화증 SPN : 고정 행렬 암호화증. SHA : 해시 기반 암호화증.
	스트링 암호.	- 가변길이의 암호문 생성 위한 암호화증 기법.

- 고장길이 축약을 위한 블록 암호 기법 대수 사용.

II. 암수분해 원리의 확장형 암호화, RSA 설명.

가) RSA (Rivest Shamir Adleman) 개념.



- 네명의 수학자가 암수분해의 원리를 창안하여 개발한 소수 P, q 중심의 암호화 알고리즘.
- 암수분해의 지수 통한 연환수 추출 어려움성 이용.

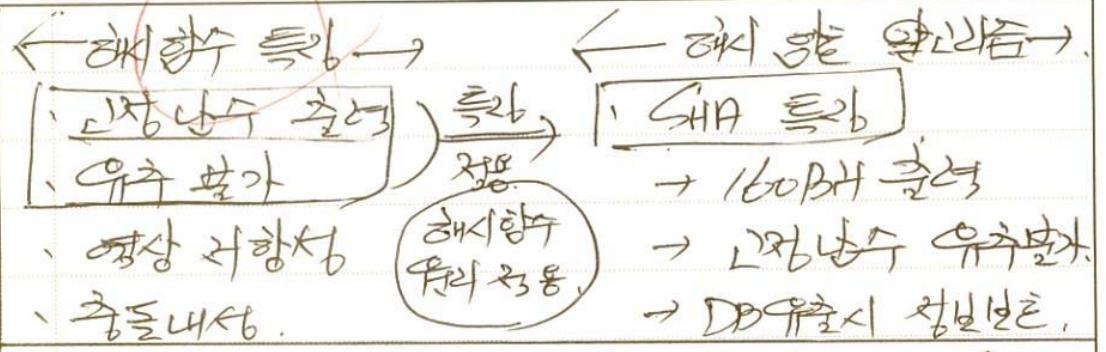
나) RSA의 수행 절차(방식)

1) 소수 P, q 찾기	→ 암호문 생성 ($C = P \text{ Mod } q$)	→ 복호화 (P) (평문생성)
→ ①에 가까운 4로 나누는 소수 생성.	$C = (P)^P \text{ Mod } q$ 계산 수행.	$P = (C)^P \text{ Mod } q$ 계산 수행.

- 소인수분해 통한 암호 복호화 수행 암호화 원리.

III 고장길이 낮은 축약, 해시원리, SHA-2 설명.

가) SHA-2 (Secure Hash Algorithm) 개념.



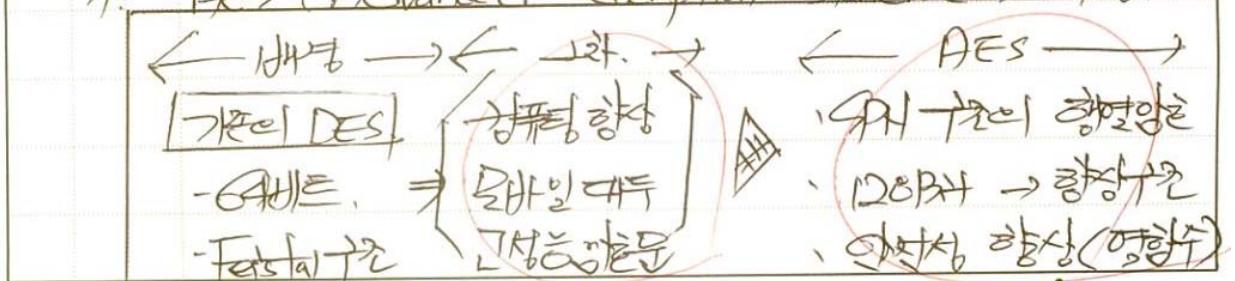
- 해시함수의 고장난이, 고장난수 유추 불가의 원인에 기반한 160Bit의 불투명한 알고리즘.

나 SHA-2의 주요 특징.

주요 특징	설명.
160Bit 고장 불투명 기법 난수 출현. 기정값 출현 암호값 사용	· 유전적 SHA 사용이 160Bit 출현 · 고장난이 출현의 불투명 알고리즘 · 출현된 난수로 유추 불가. · 특징 유출은 없에도 투명하지 않은 출현. · 해시값의 DB저장 → 유출시 절대보호.
- 160Bit의 불투명 알고리즘, 예상저항성, 유추불가.	

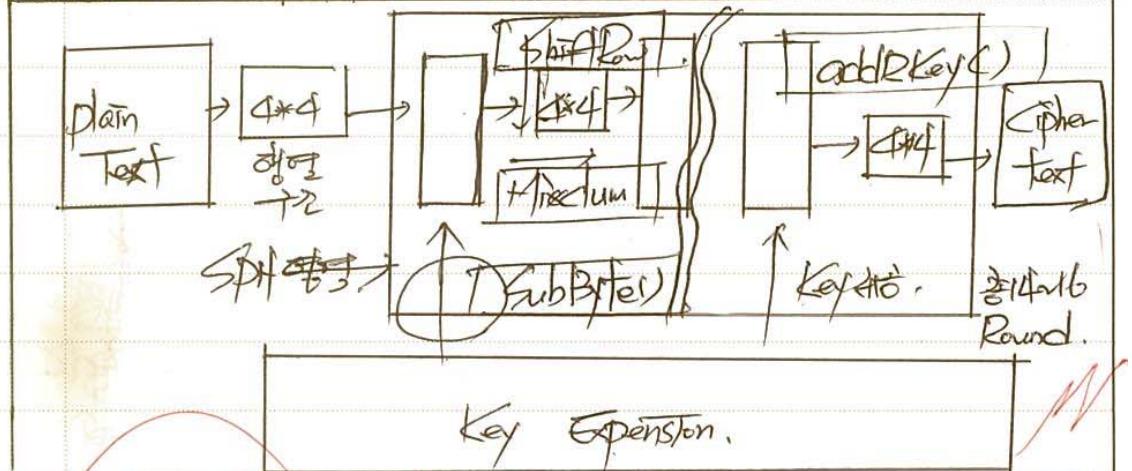
IV SPN 유리의 예상수, 128Bit, 대체행렬 방식, AES선행.

가. DES (Advanced Encryption Standard) 개념.



- 기존 DES의 취약점 개선을 위해 SPN의 허여 암호화를 대상으로 적용한 DES의 허여 암호화.
- 16비트/32비트 단위로 블록 단위로 처리

c. DES의 SPN 구조.

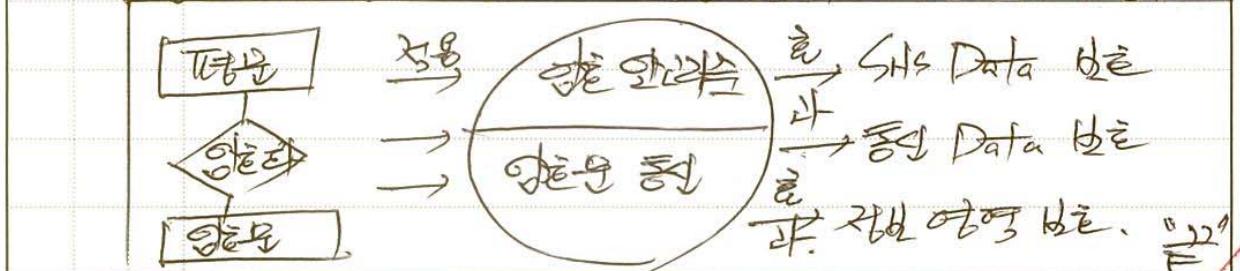


~~Sub Byte()~~
~~Shift Row()~~
~~Mix Column()~~
~~Add Round Key()~~

- Key의 확장, 행렬 단위 수행.
- Row 단위 간 치환 수행.
- Column 단위 간 교환 수행.
- XOR 연산 단위화 작업 수행.

- 4개 단계 수행 중 4번 16round 수행.

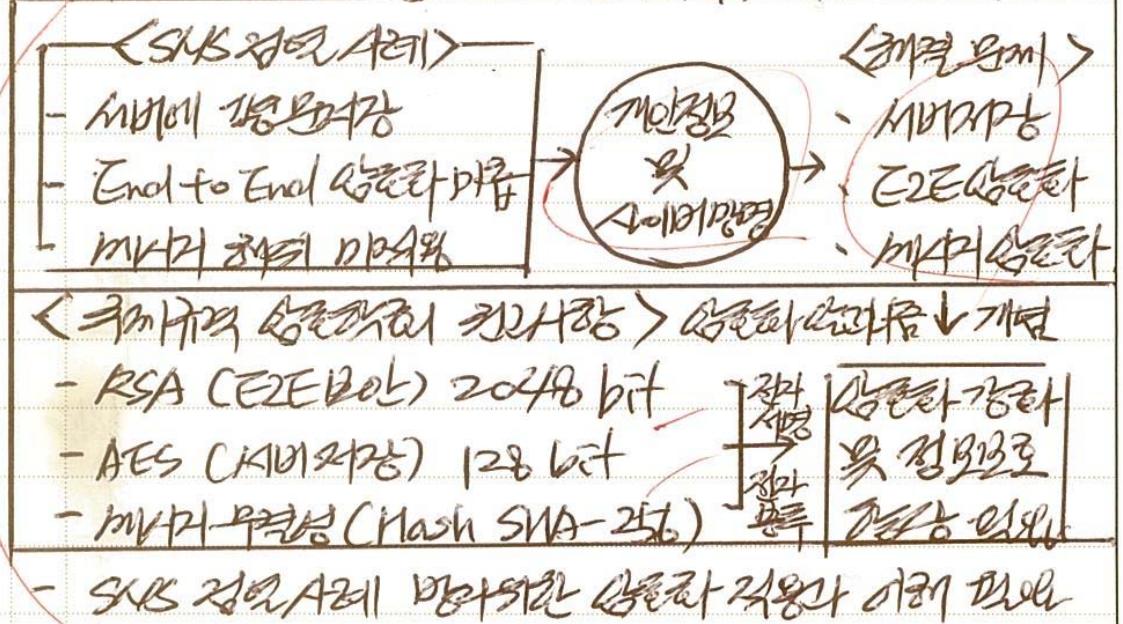
v. 허여 암호화를 적용된 편집기 풍선의 암호화 향상.



※ 3) ① RSA ② SNA-2 ③ AES

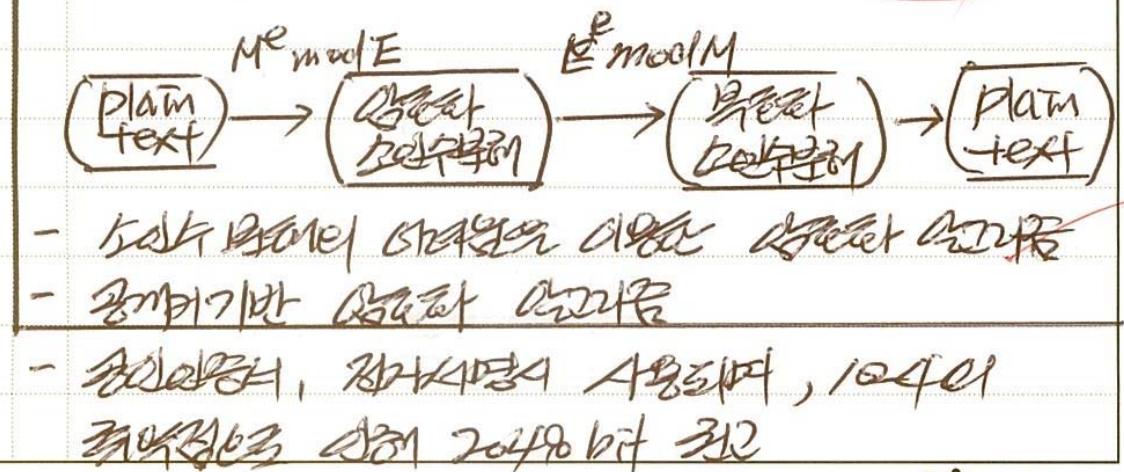
cf)

1. SNS 카드와 암호화 방식과 암호화 알고리즘 개요

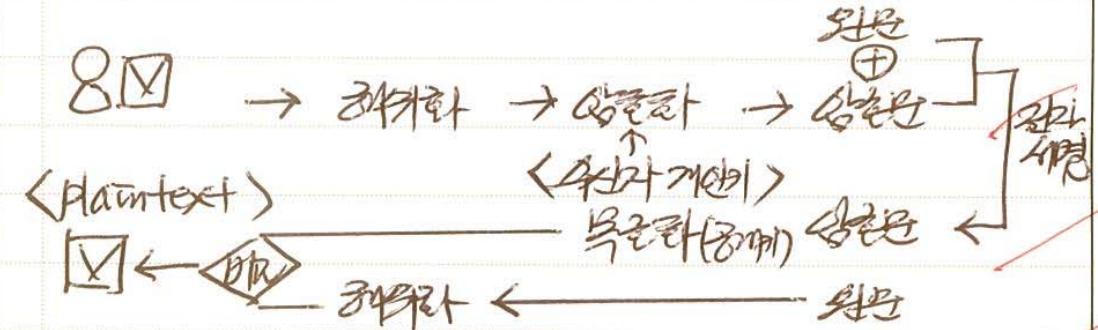


2. End-to-End 및 암호화 RSA

가. RSA (Rivest, Shamir, Adleman) ~~설명~~



1. RSA를 이용한 End-to-End Bat-AES (전화번호)

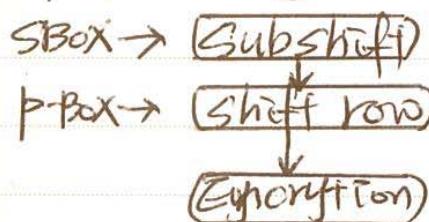


- RSA 자체로는 암호화만 가능하지 않고 키 교환

3. 2. GOST 암호화 AES (Advanced Encryption Standard)

가. AES의 기본 원리 살펴보기

(SPN) Byte Round (key) **<Spec>**



- Block 128 / 192

- Round 8 / 10 / 12

- Key 128 / 192 bit

- AES는 원래 128bit를 처리함.

4. AES 암호화 세부 내용

개념	설명	ID	J
SPN	- Round 이용, 페어링 풀기 비교적 암호화에서 처리하기	P-Box	S-BOX
혼란	- Confusion 혼란 처리	Confusion	
교체	- Substitution 교체 처리 SPN의 핵심 기법	Substitution (교체)	DES 원리

토픽	블록 암호화
키워드	평문, 블록단위로, 각 블록마다 암호화 과정 수행, 고정된 크기의 블록 단위 암호문 생성 ECB(Electronic Code Book, 전자코드북), CBC(Cipher-Block Chaining), CFB(Cipher FeedBack, 암호피드백), OFB(Output FeedBack, 출력 피드백), CTR(Counter, 카운터)
암기법	이씨씨오씨

출제문제

회차	과목	교시	문제
110	컴시응	4.1	1. 대칭 암호화와 비대칭(공개키) 암호화를 각각 설명하고, 비교하시오.
108	컴시응	4.6	6. 아래 암호화 기법을 설명하시오. 가. 블록(Block) 및 스트림(Stream) 암호화 기법 나. 워터마크(Watermark)
모의_2016.06	관리	2교시	암호화 알고리즘에 대하여 다음을 설명하시오. 가. 암호화 알고리즘의 원리와 특징에 대해 설명하시오. 나. 대칭(symmetric)키 알고리즘과 비대칭(asymmetric)키 알고리즘을 비교하시오. 다. 블록 암호화(block cipher)와 스트림 암호화(stream cipher)를 비교하시오.
모의_2015.10	관리	1교시	9. 블록 암호화 모드의 CBC와 CTR개념을 설명하시오.
모의_2010.08	관리	2교시	3. 정보보안의 기본적인 기술로 암호화 알고리즘의 원리를 이해하는 것은 중요한 요소이다. 다음 질문에 답하시오. 가) 암호화 알고리즘의 개념을 설명하시오. 나) 대칭키/비대칭키 알고리즘 비교 설명하시오. 다) 민관겸용 블록 암호화 알고리즘 ARIA 상세 설명하시오.

[목차]

- I. 블록단위 암호화 방식, 블록 암호화의 개요
 - 가. 블록 암호화(Block Cipher)의 정의
 - 나. 블록 암호화의 특징
- II. 블록 암호화 알고리즘의 개념도 및 운영 방식
 - 가. 블록 암호화의 개념도
 - 나. 블록 암호화의 운영 방식
- III. 블록 암호화 알고리즘의 유형 상세
 - 가. ECB mode
 - 나. CTR mode
 - 다. CBC mode
 - 라. OFB mode
 - 마. CFB mode

I. 블록단위 암호화 방식, 블록 암호화의 개요

가. 블록 암호화(Block Cipher)의 정의

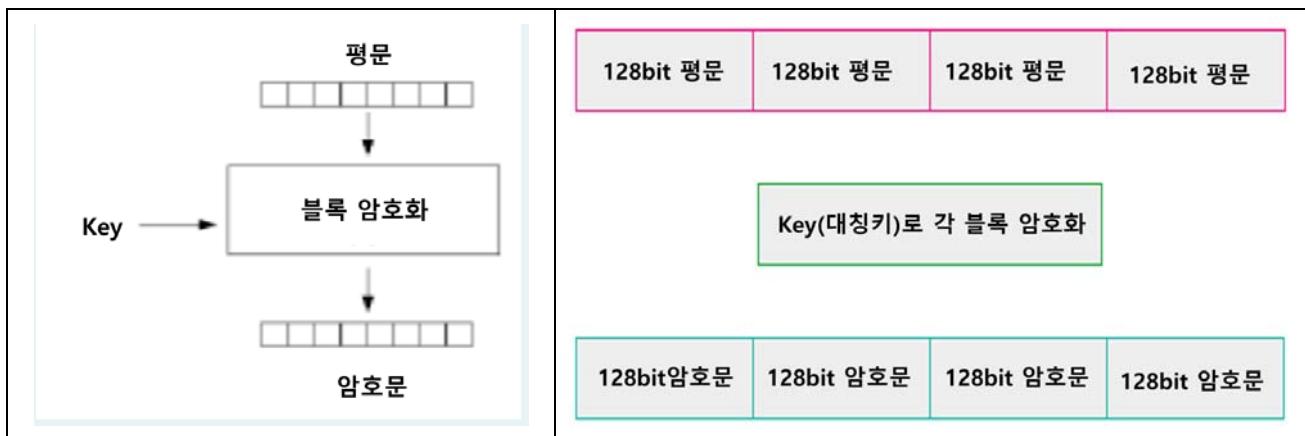
- 평문을 일정 블록단위로 나누어 각 블록마다 암호화 과정 수행, 고정된 크기의 블록 단위 암호문 생성

나. 블록 암호화의 특징

구분	내용
장점	<ul style="list-style-type: none"> - 평문에 혼돈성을 주어 해독 어렵게 함 - 완성된 암호문에 내용 추가 및 변경이 어려움
단점	<ul style="list-style-type: none"> - 암호화 속도가 상대적으로 느림 - 암호화 시 에러의 파급 효과 큼

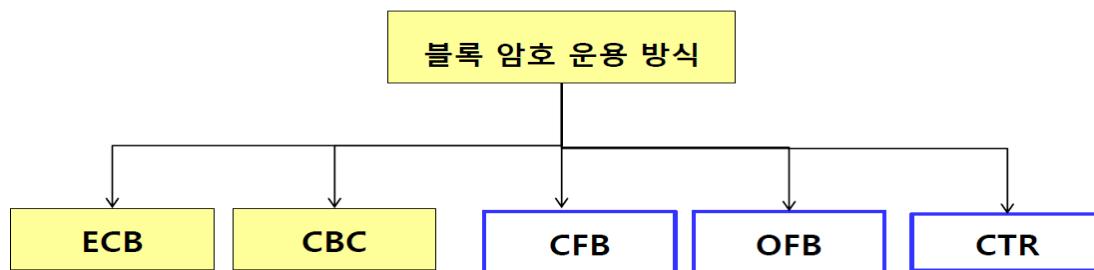
II. 블록 암호화 알고리즘 개념도 및 운용 방식

가. 블록 암호화 개념도



- 블록 암호화는 대칭키 알고리즘에 속하며, 128Bit 암호화 가정 시, 평문을 128Bit로 나눈 다음에 생성

나. 블록 암호화 알고리즘의 운용 방식



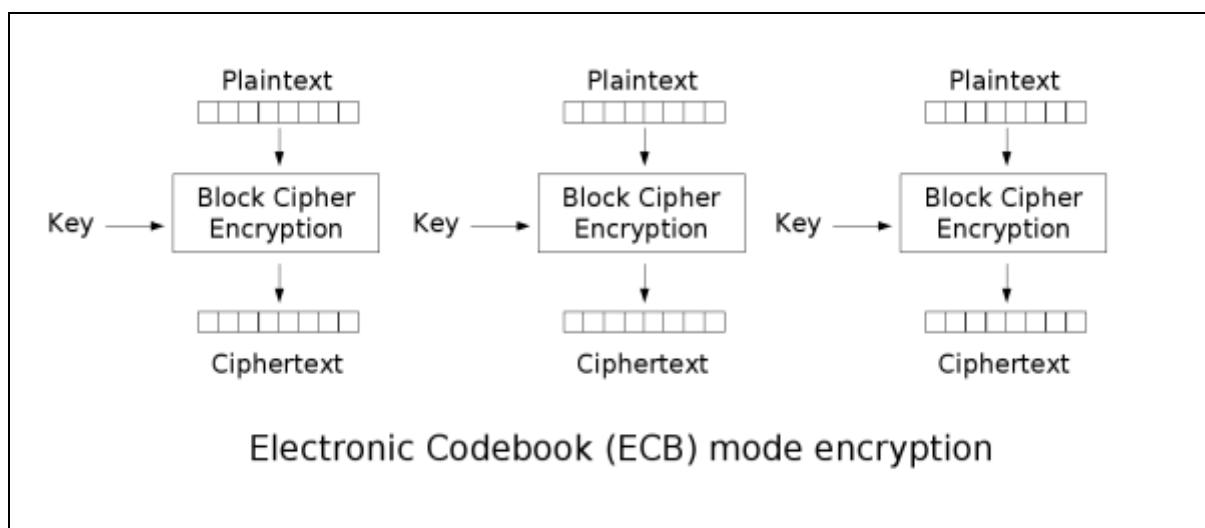
운용 모드	모드	설명
각 블록 독립적	ECB	<ul style="list-style-type: none"> - Electronic Code Block(전자코드북) - 하나의 키로 평문블록 암호화를 병렬진행
	CTR	<ul style="list-style-type: none"> - Counter(카운터) - 카운터를 이용, 평문블록을 스트림화하여 암호화 병렬 진행
이전 블록 암호화가 다음 블록에 영향	CBC	<ul style="list-style-type: none"> - Cipher-Block Chain(암호블록체인) - 초기화 백터와 평문블록의 XOR 결과를 암호화, 암호문 블록을 다음 블록의 백터로 사용
	OFB	- Output Feedback(출력피드백)

	- 초기화 벡터를 암호화하여 사용, 암호화와 복호화 구조가 동일
CFB	- Cipher Feedback(암호피드백) - 초기화 벡터를 암호화하여 사용, 암호블록을 다음 평문블록에 암호화에 사용

III. 블록 암호화 알고리즘의 유형 상세

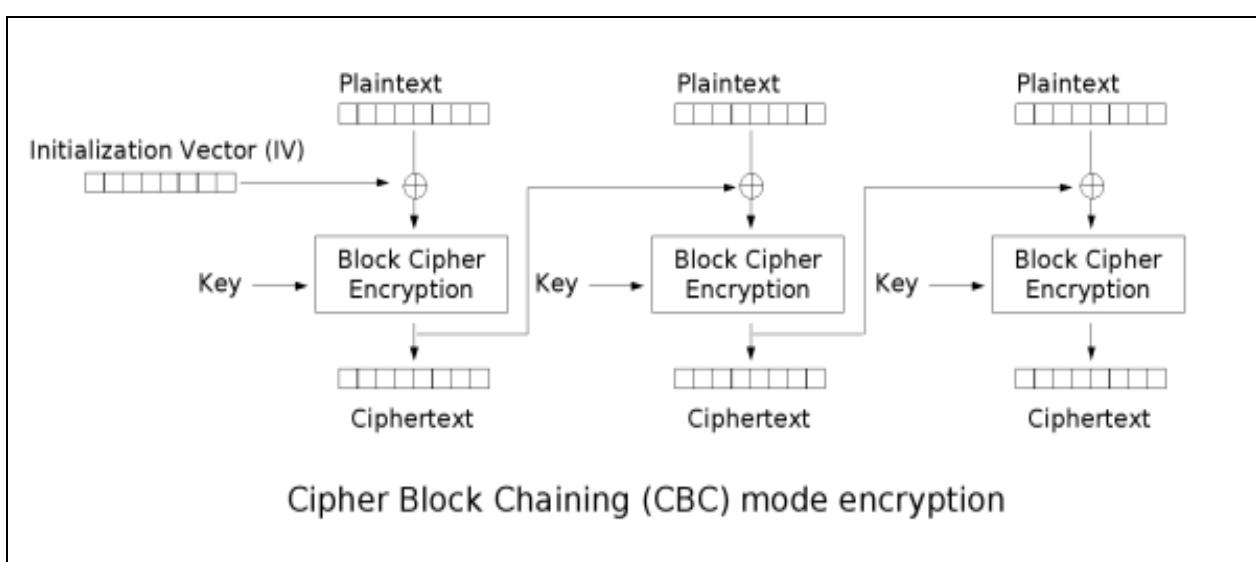
가. ECB (Electronic Code Block) Mode

- 가장 단순한 모드로 블록단위로 순차적으로 암호화하는 구조
- 한개의 블록만 해독되면 나머지 블록도 해독 되는 단점 (Brute-Force Attack, Dictionary Attack)
- 암호문이 블록의 배수가 됨 → 복호화 후 평문 알기 위해서 Padding 해야 함
- 각 블록이 독립적으로 동작, 한 블록에서 에러 난다고 해도 다른 블록에 영향을 주지 않음 → 해당 블록까지만 에러 전파



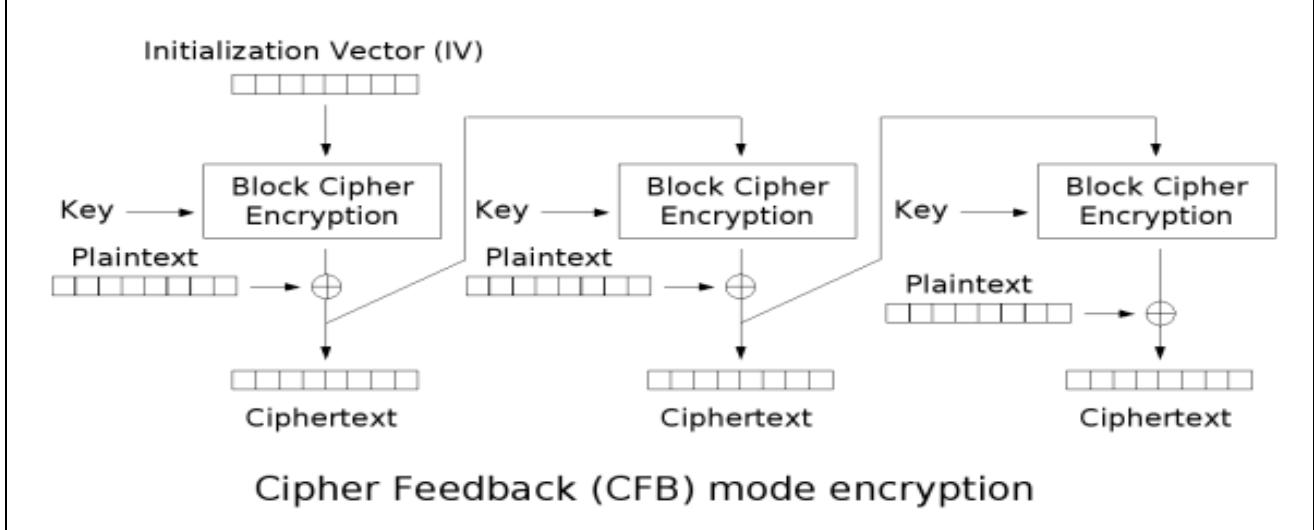
나. CBC(Cipher Block Chaining) Mode

- 블록 암호화 운영 모드 중 보안성 가장 높은 암호화 방법 → 가장 많이 사용
- 평문 각 블록은 XOR연산 통해 이전 암호문과 연산
- 첫번째 암호문에 대해서는 IV(Initial Vector)가 암호문 대신 사용, 이 때, IV는 제 2의 키 될 수 있음
- 암호문이 블록의 배수 → 복호화 후 평문 얻기 위해서 Padding
- 암호화가 병렬처리 아닌 순차적으로 수행
- 깨진 암호문의 해당블록과 다음블록의 평문까지 영향
- 무결성 검증에 사용되는 MAC 값 생성하기 위해 주로 사용



다. CFB(Cipher FeedBack) Mode

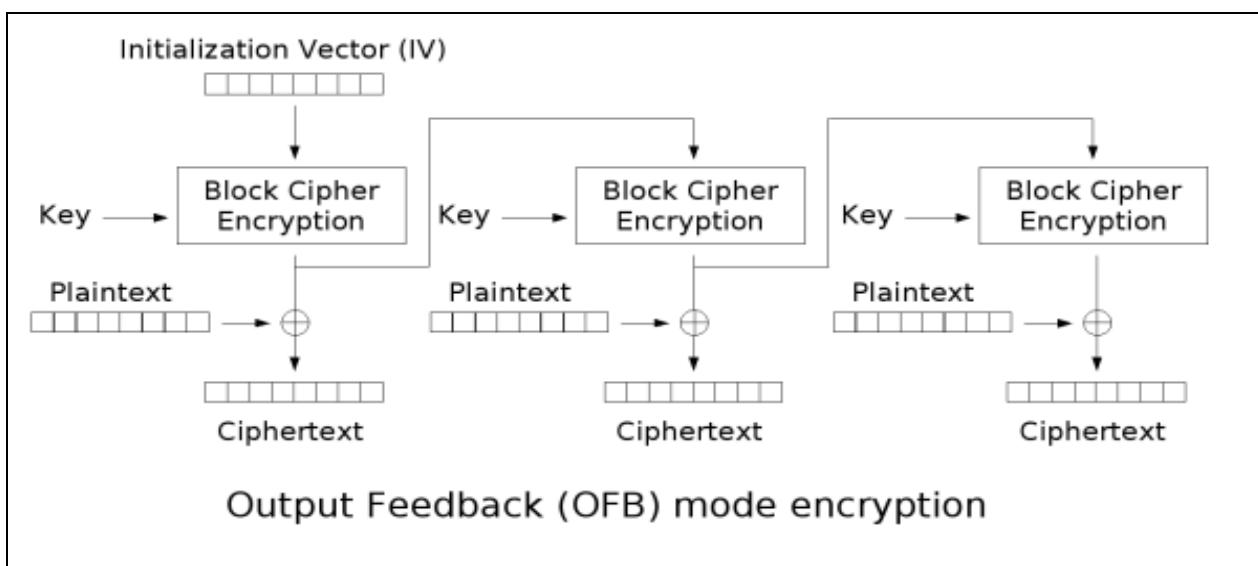
- 블록 암호화를 스트림 암호화처럼 구성해 평문과 암호문 길이 동일 (패딩 필요 없음)
- 최초 키생성 버퍼로 IV 사용되며, IV는 제2의 키 될 수 있음
- 스트림 기본단위를 Bit단위로 설정 가능, Bit단위에 따라 CFB8~CFB128로 쓰임
- 암호화, 복호화 모두 암호화로만 처리 가능
- CBC모드와 같이 암호화는 순차적, 복호화는 병렬적 처리



- CBC모드와 마찬가지로 한 암호문 블록 에러는 해당 평문블록과 다음 평문블록의 총 2개 블록에 전파

라. OFB(Output FeedBack) Mode

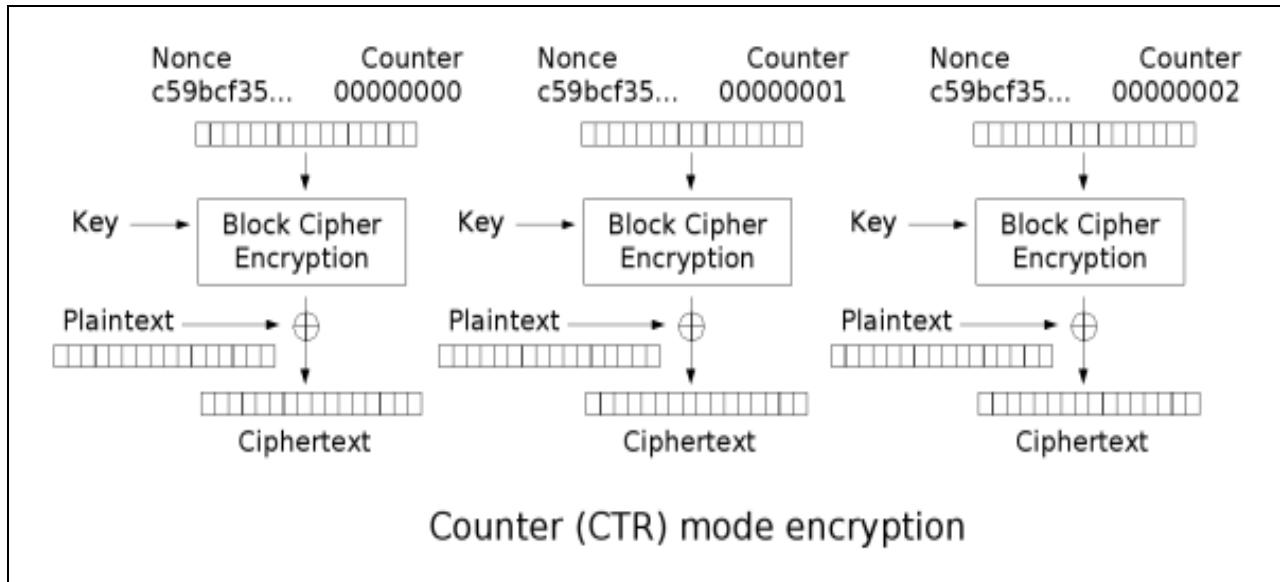
- 스트림 암호화처럼 블록 암호화 구성 → 평문과 암호문 길이가 동일 (패딩 필요 없음)
- 암호화 함수는 키 생성에만 사용
- 암호화 방법과 복호화 방법 동일 → 암호문을 한번 더 암호화하면 평문 (복호화 시에 암호화)
- IV가 최초 키생성 버퍼로 사용, IV는 제2의 키 될 수 있음
- 스트림 기본 단위를 Bit단위로 설정 가능, Bit단위에 따라 OFB8~OFB128로 쓰임
- 키스트림이 평문과 암호문에 의존하지 않음 → 암호화된 블록에서 발생되는 에러는 다음 블록에 영향없음



- 대응되는 한 블록에만 영향 미치므로, 영상이나 음성과 같은 digitized analog신호에 많이 사용됨

¶. CTR (CounTeR) Mode

- 블록을 암호화할 때마다 1씩 증가하는 카운터를 암호화하여 키스트림 제작 → 카운터를 암호화한 비트열과 평문블록과의 XOR 결과가 암호문 블록
- CTR모드는 OFB와 같은 스트림 암호의 일종
- CTR모드의 암/복호화는 완전히 같은 구조이므로 구현 간단 (OFB와 같은 스트림 암호의 특징)
- CTR모드에서는 블록 순서 임의 암/복호화 가능 (비표와 블록번호로부터 카운터 구할 수 있음)
- 블록을 임의 순서로 처리 가능 → 병렬처리 가능



- 각 블록이 병렬처리 되므로 같은 블록 내에서만 이루어짐

[추가]

Summary of Modes

Mode	공식	암호문
ECB	$Y_i = F(PlainText_i, Key)$	Y_i
CBC	$Y_i = PlainText_i \text{ XOR } Ciphertext_{i-1}$	$F(Y, key); Ciphertext_0 = IV$
PCBC	$Y_i = PlainText_i \text{ XOR } (Ciphertext_{i-1} \text{ XOR } PlainText_{i-1})$	$F(Y, key); Ciphertext_0 = IV$
CFB	$Y_i = Ciphertext_{i-1}$	$\text{Plaintext XOR } F(Y, key); Ciphertext_0 = IV$
OFB	$Y_i = F(Key, I_{i-1}); Y_0 = IV$	$\text{Plaintext XOR } Y_i$
CTR	$Y_i = F(Key, IV + g(i)); IV = token();$	$\text{Plaintext XOR } Y_i$

Table 1. Comparison between different modes of operation

Evaluation criteria	ECB	CBC	CTR	CCM	CC
Chain dependency	No	Yes	No	No	Yes
Error propagation	No	One block	No	No	One block
Authentication code	No	Yes	No	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes	Yes
Number of passes	One	One	One	Two	Two
Parallelism	Yes	No	Yes	No	Yes
implementing nonce	No	No	Could be	Yes	No, but could be in the counter
Message size	Any	Any	Any	Fixed	Any
Block cipher algorithm	Any	Any	Any	only with 128-bit block size algorithms	Any

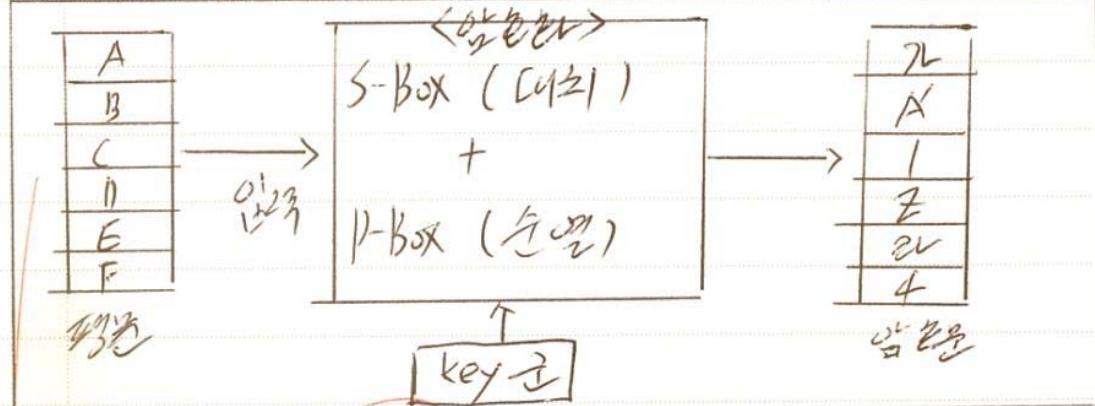
Table 4.1 Basic Block Cipher Modes

Mode	How It Works	Usage
Electronic Code Book (ECB)	In ECB mode, each block is encrypted independently, allowing randomly accessed files to be encrypted and still accessed without having to process the file in a linear encryption fashion.	Very short messages (less than 64 bits in length), such as transmission of a DES key.
Cipher Block Chaining (CBC)	In CBC mode, the result of encrypting one block of data is fed back into the process to encrypt the next block of data.	Authentication
Cipher Feedback (CFB)	In CFB mode, each bit produced in the keystream is the result of a predetermined number of fixed ciphertext bits.	Authentication
Output Feedback (OFB)	In OFB mode, the keystream is generated independently of the message	Authentication
Counter (CTR)	In CTR mode, a counter—a 64-bit random data block —is used as the first initialization vector.	Used in high-speed applications such as IPsec and Asynchronous Transfer Mode (ATM)

- 최근에는 S-Box 기반과 ECC (160bit) 기반 증가 추세.

III. 흐름 암호화와 스트림 암호화

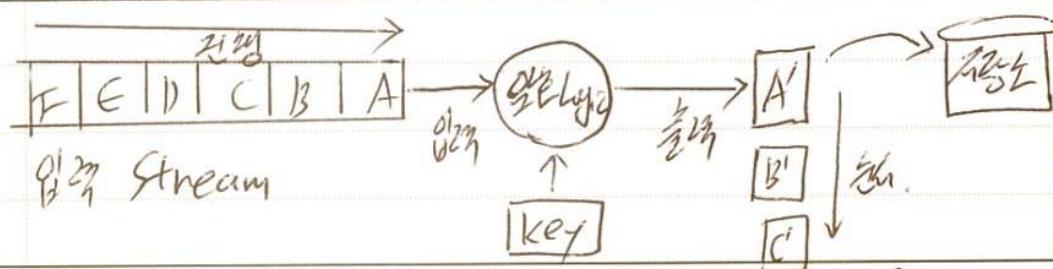
A. 흐름 암호화의 원리



개념	- Block 단위로 입출력을 받아서 입력 Data를 Substitution, Permutation을 통해 출력을 만들고자.	
특징	- Complexity 증가	- 암호공개 복잡성이 증가.
예	- DES, AES, ARIA, HIGHT 비대칭키 방식	- RSA, ECC

- 대부분의 System에서는 Block 암호를 사용이 된다.

B. 스트림 암호화



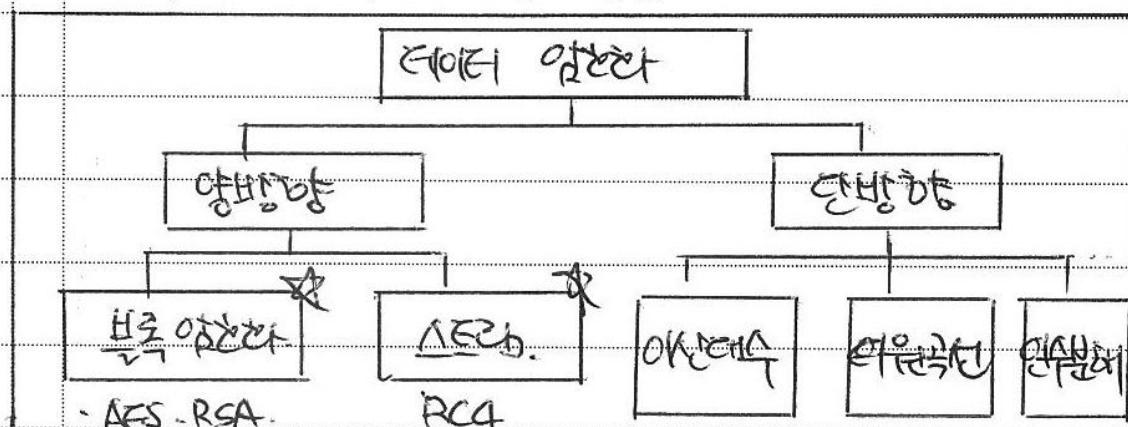
7417	- 원시 암호화를 위해 암호 Stream을 Bit, Byte, Word 단위로 암호화하는 방법.
특징	단계적 암호화 - 원시 암호화 단계
	Weak 암호화 - 중보 암호화로 암호화가 약함.
장단점	Bit Stream 암호화 - Bit 단위로 substitution 수행. Word 암호화 - Word 단위로 substitution 수행.
- 보통 암호화는 원시 암호화를 생략해 사용.	

11/29. 2

문 2). ② 볼록·스트리밍 ③ 암호화 응용프로그램 3가지 이상

답)

15
데이터 암호화의 기법 종류

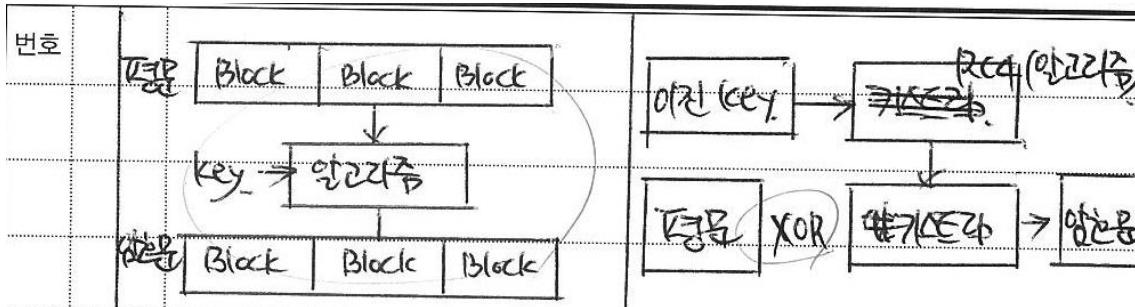


- 데이터 암호화의 기법에는 양방향과 단방향이라는
복록암호화와 스트리밍암호화가 대체적으

K. 볼록 및 스트리밍 암호화 기법.

가. 볼록 및 스트리밍 암호화 아키텍처.

볼록 암호화	스트리밍 암호화.
평문을 복록단위로 나누어	스트리밍 데이터를 블록
암호화 알고리즘 적용하는 기법	단위로 암호화하는 기법



- 블록 암호화는 평문·암호문을 블록으로 구분, 스트리밍 암호화
기법은 스트리밍 데이터를 블록 단위로 암호화 적용.

나 블록 및 스트리밍 암호화 기법 정리(10종)

구분	블록	스트리밍
단위.	Block	스트리밍(단위)
대표암호화	DES, 3DES, AES.	RC4.
수집	Block 단위의 구분 으로 스트리밍보다 느림.	시시각적 스트리밍 암호화로 빠른 수행
복잡성	간단	키스트리밍 추출로 복잡.
구현	P-Box S-Box 등에	XOR, OR 등의
방법.	직선 체인, 대체,	연산 이용.

- 가장 많이 이용되고 있는 블록 암호화는 운영 모드에 따라 ECB, CBC, CFB, OFB, CTR을 구분

다. 블록 암호화 - 운영모드 3가지 이상 정리

구분	암호화	복호화.
ECB.	key → P C	key → C P.

토픽	비밀키 암호화
키워드	공개키 암호화 대칭 암호화와 비대칭(공개키) 암호화
암기법	

출제문제

번호	문제	회차
1	1. 대칭 암호화와 비대칭(공개키) 암호화를 각각 설명하고, 비교하시오.	110.컴시응.4.1

[목차]

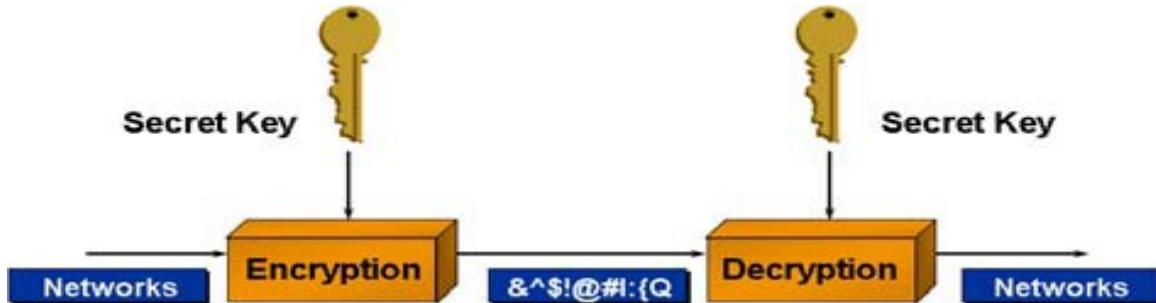
- I. 암호화 키와 복호화 키가 동일한, 비밀키 암호화의 개요
 - 가. 비밀키 암호화(Secret Key Encryption)의 정의
 - 나. 비밀키 암호화의 개념도
- II. 암호화 키와 복호화 키가 다른, 공개키 암호화의 개요
 - 가. 공개키 암호화(Public Key Encryption)의 정의
 - 나. 공개키 암호화의 개념도
- III. 비밀키 암호화와 공개키 암호화 비교

I. 암호화 키와 복호화 키 동일, 비밀키 암호화의 개요

가. 비밀키 암호화(Secret Key Encryption)의 정의

- 두 사용자가 동일한 비밀키 공유, 송신자는 전송 시 비밀키로 전송 메시지 암호화하고 수신자는 수신 메시지를 동일한 비밀키로 복호화하는 방법

나. 비밀키의 개념도



- 암호 알고리즘은 공개키에 비해 매우 효율적이고, 통신을 수행하는 두 주체는 상호 인증 가능

II. 암호화 키와 복호화 키가 다른, 공개키 암호화의 개요

가. 공개키 암호화(Public Key Encryption)의 정의

- 송신자는 전송 메시지를 수신자의 공개키로 암호화하여 전송, 수신자는 수신 메시지를 자신의 개인키로 복호화하는 방법

나. 공개키의 개념도



- 공개키로 암호화하면 개인키로만 복호화 가능

III. 비밀키 암호화와 공개키 암호화 비교

구분	비밀키 암호화(대칭키)	공개키 암호화(비대칭키)
키의 관계	암호키 = 복호키	암호키 ≠ 복호키
키의 수	2인 이상이 한 개의 동일한 비밀키 공유	전송 당사자간에 각각 키 쌍(개인키, 공개키) 공유
키의 종류	비밀키(Secret Key)	- 공개키(Public Key) - 개인키(Private Key)
키의 관리	복잡(거래 당사자 전부 관리)	인증기관 통해 전송 당사자별 개인키 발급 (상대적 단순)
부인방지 여부	대칭키로 인하여 부인방지 불가	키의 이원화로 부인방지 가능
속도	비트 단위 암호화로 상대적으로 빠른 속도 제공	큰 소수 찾거나, 곡률 방정식 등 연산으로 속도 느림

용도	개인파일암호화, 특정그룹 내의 파일 등의 통신에 사용	다수의 사용자에 주로 사용
일고리즘	AES, SEED, DES	RSA, ECC
장점	<ul style="list-style-type: none"> - 구현 용이, 변형 가능 - 키의 분배가 용이함 - 사용자의 증가에 따라 관리할 키의 개수가 상대적으로 적음 - 키 변화의 빈도가 적음 - 여러 가지 분야에서 응용이 가능함 	<ul style="list-style-type: none"> - 암호해독 어려움, 전자서명 - 암호화/복호화 속도가 빠름 - 키 길이가 짧음 - 구현 빠름 - 대칭키로 인해 부인방지 불가
단점	<ul style="list-style-type: none"> - 상대적으로 쉽게 해독가능, 키관리 어려움 - 암/복호화 속도 느림 - 키 길이가 길 	<ul style="list-style-type: none"> - 복호화 시간이 상대적으로 오래 걸림 - 사용자 증가에 따라 관리해야 할 키 수가 상대적으로 많음 - 키 변화 빈도 많음

=====

(참조)

I. 비밀키 암호화와 공개키 암호화의 개요

가. 비밀키 암호화 와 공개키 암호화의 정의

비밀키(대칭키) 암호화	공개키(비대칭키) 암호화
두 사용자가 동일한 비밀키를 공유하고 있는 상태에서 전송하고자 하는 데이터를 공유한 키로 암호화 하여 수신자에게 전송하면 수신자는 동일한 키로 복호화 데이터를 복원	송신자는 수신자의 공개키에 해당하는 정보를 사용하여 데이터를 암호화하여 네트워크를 통해 전송하고 수신자는 자신의 공개키에 해당하는 비밀키로 암호화된 데이터 복호화 평문을 복원

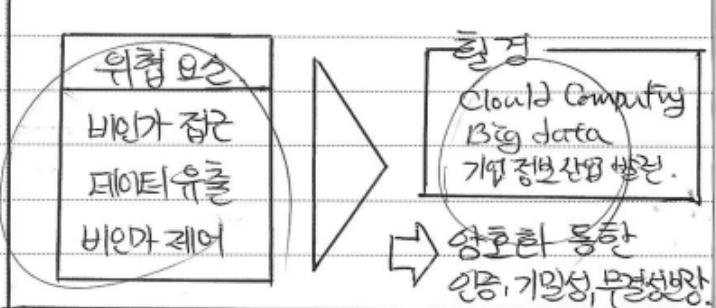
나. 비밀키 암호화와 공개키 암호화의 특징

비밀키(대칭키) 암호화	공개키(비대칭키) 암호화
<ul style="list-style-type: none"> -n명의 사용자로 구성된 네트워크에서 안전한 통신이 수행되기 위해서는 시스템 전체적으로 $n(n-1)/2$개의 키가 요구 -사용자가 보유해야 하는 키의 개수도 n-1개 -공개키에 비해 매우 효율적이고 통신을 수행하는 두 주체는 상호인증이 가능 	<ul style="list-style-type: none"> -다른 유저와 키를 공유하지 않더라도 암호를 통한 안전한 통신을 한다는 장점 존재

- 번호 2) 암호화 알고리즘 설명.
- 암호화 알고리즘 원리 틀리 설명
 - 대칭키 · 비대칭키 비교
 - 블록 암호화, 스트리밍 암호화 비교 설명

답)

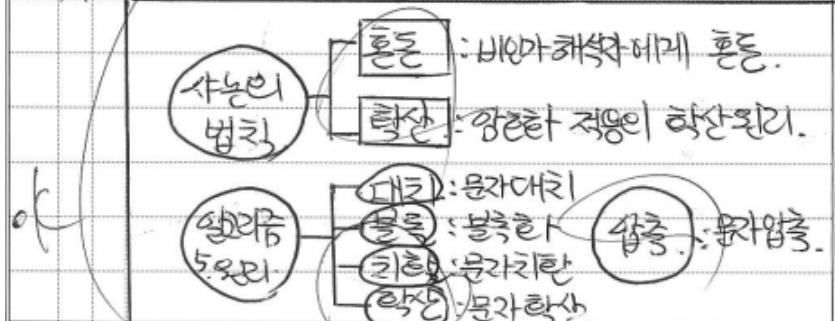
I. 암호화 적용의 필요성.



- 최근 스마트 사태, Big brother와 위협 대응 가능.

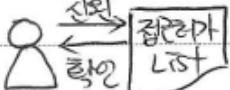
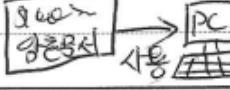
II. 암호화 알고리즘 원리 및 특징 설명.

A. 암호화 알고리즘의 원리.



- 번호 - 샤논의 법칙에 의거, 대칭, 불록, 치환, 확산, 압축
5가지 원리 기반으로 암호화 구현.

4. 암호화 알고리즘의 특징.

특징	개념	설명.
인증		사용자의 인증 가능.
기밀성		문서나 파일의 기밀성 보장.
무결성		데이터의 정연(정연) 보장.
부인방지		송신자, 문서 전자화 부인 불허 가능.
가용성.		사용 가능성 보장 특징.

- 암호알고리즘 적용시에선 인증, 기밀성, 무결성
부인방지, 가용성 보장의 특징을 제외.

III 대칭키 알고리즘과 비대칭키 알고리즘 비교 설명

가. 대칭키 알고리즘, 비대칭키 알고리즘 개념비교

종류	대칭키	비 대칭키
개념비교	암호화 키와 복호화 키가 같음	암호화 키와 복호화 키 별도 존재

번호	개념도.	$\boxed{\text{암호화}} = \boxed{\text{복호화}}$	$\boxed{\text{암호화}} \neq \boxed{\text{복호화}}$
----	------	---	--

- 대칭키, 비대칭키 알고리즘은 암·복호화 키의 동일 여부에 따라 알고리즘 개별 구현.

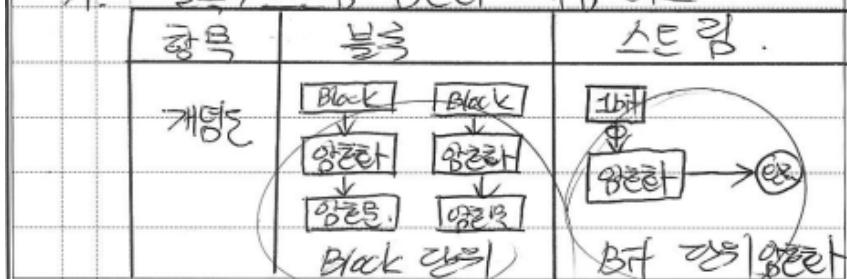
나. 대칭키·비대칭키 알고리즘 상세 비교.

항목	대칭키	비 대칭키
키의	비밀키	공개키, 개인키
부인방지	불가	가능.
구현	쉬움	복잡
기용도	$n : m$	$1 : m$
종류	블록암호, SPN, 퍼미, RSA, ECC	
예시	AES, DES, RSA	PKI, 흔연증

- 구현 복잡도, 키의 부인 방지 기능의 차이 존재.

IV. 블록 암호화와 스트림암호화 비교.

가. 블록/스트림 암호화 개념 비교



번호	개념비교	블록단위로 나누어 암호화	比特 단위 스트림으로 암호화하는 기법.
----	------	------------------	--------------------------

- 암호화 단위 따라 블록, 스트림으로 구분함.

나. 블록·스트림 암호화 상세 비교

항목	블록	스트림.
단위	Blocks 단위	bite 단위
암호화 단위	높음	낮음.
구현	다른 복잡	쉬움.
종류	ECB, CBC, 퍼미팅	Bit Encryption

V 암호화 강건성 위한 발전동향.

측면-	종류	설명
암호화 방식	캐스트레칭 salt 양자난수생성	문자열산출함수 Hash 이중 Hash 이용 아주난수 양자난수
양자 기술	양자컴퓨터 양자통신	양자컴퓨팅 빠른 대응 양자통신, 대칭암호화
페어워런	Homomorphic	DB 쿼리상태 사용 가능

파악한 좋은 방식 개발, 양자의 검인 양자컴퓨팅
대응 필요, Snowden사태, Big brother 대응.

"은"

토픽	스트림 암호화(stream cipher)
키워드	스트림 암호(stream cipher), 대칭키 암호의 구조 유사난수를 1 비트 생성하고, 암호화하는 값과 XOR 처리 이진수열을 이용하여 정보 암호화, 암호화 키와 복호화 키는 동일 bit 단위, RC4(전송 계층 보안(TLS)이나 WEP 등의 여러 프로토콜에 사용), SEA 무선통신 환경에서 사용
암기법	

출제문제

회차	과목	교시	문제
110	컴시응	4.1	1. 대칭 암호화와 비대칭(공개키) 암호화를 각각 설명하고, 비교하시오.
108	컴시응	4.6	6. 아래 암호화 기법을 설명하시오. 가. 블록(Block) 및 스트림(Stream) 암호화 기법 나. 워터마크(Watermark)
모의_2016.06	관리	2교시	암호화 알고리즘에 대하여 다음을 설명하시오. 가. 암호화 알고리즘의 원리와 특징에 대해 설명하시오. 나. 대칭(symmetric)키 알고리즘과 비대칭(asymmetric)키 알고리즘을 비교하시오. 다. 블록 암호화(block cipher)와 스트림 암호화(stream cipher)를 비교하시오.

[목차]

I. 순차적 처리의 대칭키 암호화 알고리즘, 스트림 암호화의 개요

- 가. 스트림 암호화(Stream Encryption)의 정의
- 나. 스트림 암호화의 특성

II. 스트림 암호화의 개념도 및 종류

- 가. 스트림 암호화의 개념도
- 나. 스트림 암호화의 종류

III. 스트림 암호화의 대표적 알고리즘

IV. 스트림 암호화와 블록 암호화의 비교

=====

I. 이진수열을 이용한 대칭키 알고리즘, 스트림 암호화의 개요

가. 스트림 암호화(stream cipher)의 정의

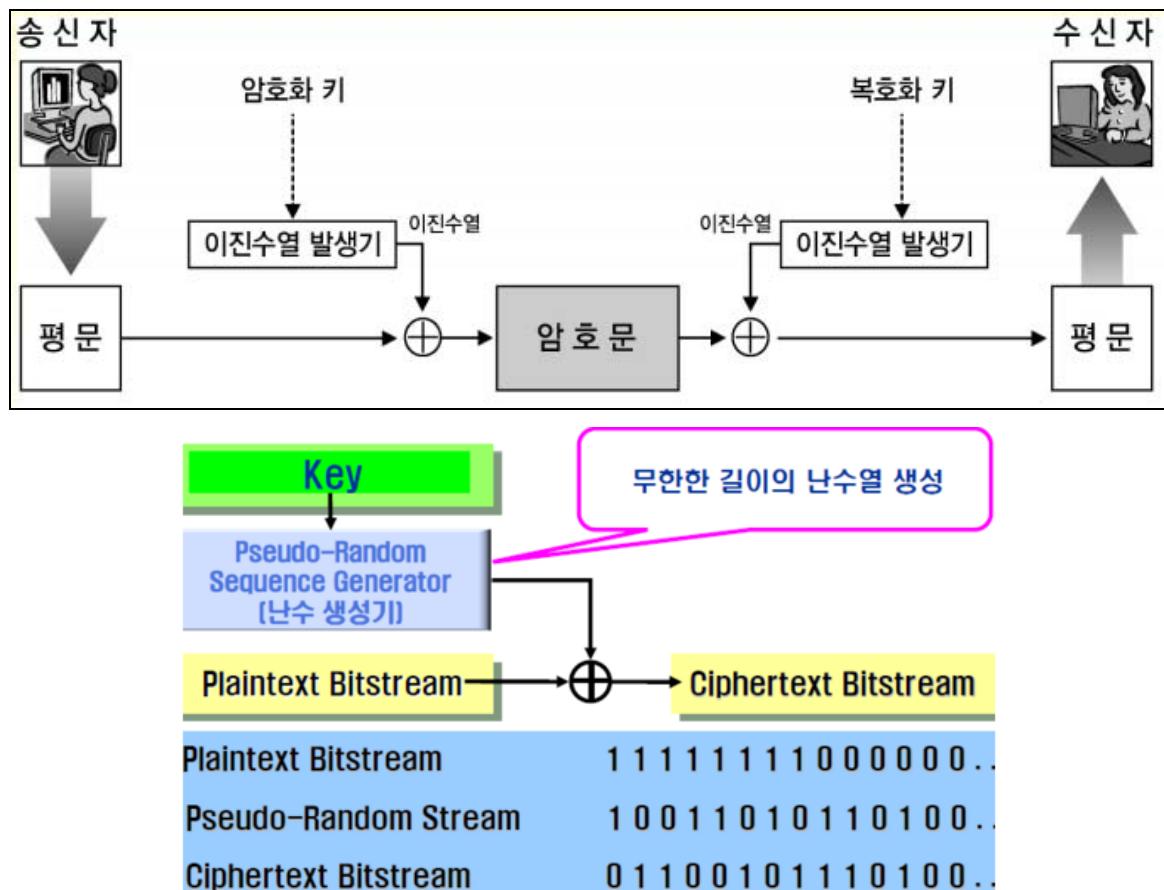
- 한 번에 1비트 혹은 1바이트의 디지털 데이터(스트림)를 암호화하는 방식
- 평문과 같은 길이의 키 스트림을 생성하여 평문과 키 이진 수열을 비트단위로 배타적 논리합(XOR) 이진 연산으로 결합하여 암호문을 생성하는 방식
- 평문(Plain Text)을 키스트림(key stream)이라는 의사랜덤 이진수열과 병합(주로 bit단위로 XOR)하는 대칭 키 알고리즘

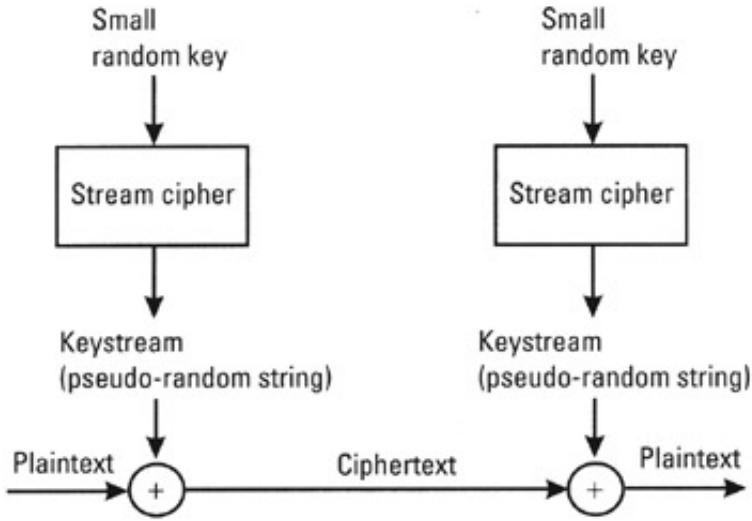
나. 스트림 암호화의 특징

특징	설명
빠른 수행속도	- 볼록암호화 대비 하드웨어 구현 용이, 수행속도 빠름
에러 전파현상 없음	- 1비트의 오류가 이웃 비트 오류 유발하지 않음
무선통신환경 적합	- 빠른 암복호화로 무선환경에 적합함

II. 스트림 암호화의 개념도 및 종류

가. 스트림 암호화의 개념도





- 이진수열을 이용하여 정보 암호화, 암호화 키와 복호화 키는 동일

나. 스트림 암호화의 종류

종류	내용	기술
동기식 스트림 암호화	<ul style="list-style-type: none"> - 키 스트림은 평문, 암호문, 이전 키 스트림에 독립적 - 암호화와 복호화에 상호 동기 필요 - 암호문 전송 시, 특정 비트 변조가 다른 비트 복호화에 영향 주지 않음 	RC4 OTP(One Time Pad)
자기 동기 스트림 암호화	<ul style="list-style-type: none"> - 키 스트림은 이전 평문이나 암호문에 종속적 - 암호문 전송 도중 변조 시, 후속 암호문 복호화에 사용 되지 않아 오류 파급 제한적 - 키스트림과 평문의 함수관계로 암호문 생성되므로 변조되어도 자기 동기화 가능 	CFB (Cipher Feedback)

III. 스트림 암호화의 대표적 알고리즘

구분	RC4	SEA(Software-optimized Encryption Algorithm)
개념	- Rivest가 설계, 바이트 단위로 연산하는 키 크기가 가변 스트림 암호	- Rdgaway와 Coppersmith에 의해 1993년 32비트 컴퓨터 고속 스트림 암호로 설계
알고리즘	<ul style="list-style-type: none"> - 임의순열(Random Permutation) 사용 - 암호 주기가 10보다 큼 - 출력 바이트마다 8~16개 기계 연산 수행 	<ul style="list-style-type: none"> - 초기화 단계: SH 이용하여 대량 테이블 집합 초기화 - 키 스트림 생성하는 동안 look-up 테이블 사용하여 출력 바이트 생성
장점	- 소프트웨어로 매우 빠르게 수행	- 출력 바이트 생성 시, 5개 명령만 사용하여 매우 빠른 성능

IV. 스트림 암호화와 블록 암호화 비교

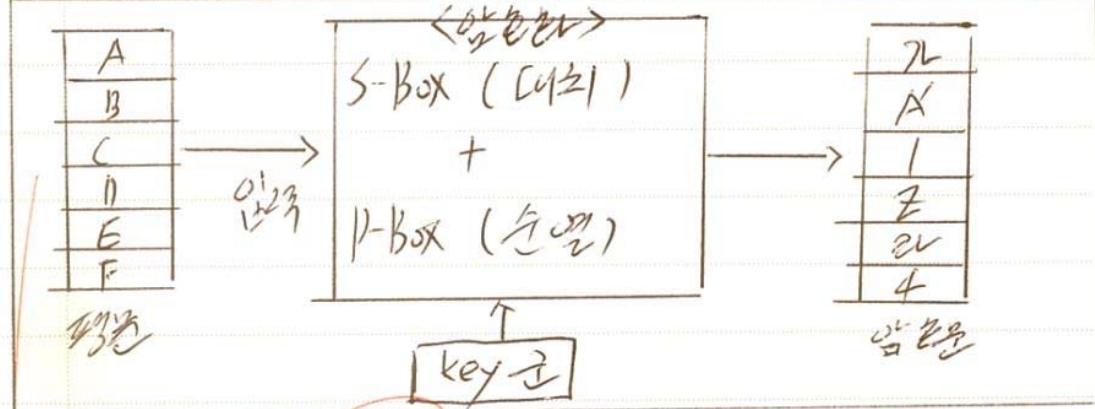
구분	스트림 암호화	블록 암호화
암호화 과정	평문 각 문자를 순서대로 즉시 암호화 스트림으로 만듦	평문 자체를 블록 단위로 배열, 순차적으로 암호화

알고리즘 예	<ul style="list-style-type: none"> - 단순 알파벳 암호화 알고리즘 - 복합 알파벳 암호화 알고리즘 	<ul style="list-style-type: none"> - 세로 방향으로 자리 옮김 알고리즘 - 모르스 부호 응용 알고리즘
장점	<ul style="list-style-type: none"> - 암호화 속도가 상대적으로 빠름 - 애러 파급 효과가 적음 	<ul style="list-style-type: none"> - 평문에 혼돈성 주어 해독 어렵게 함 - 완성된 암호문에 내용 추가 및 변경 어려움
단점	<ul style="list-style-type: none"> - 평문 특성이 암호문에도 그대로 반영 - 악의적 공격자에 의해 내용 첨가 및 변경 용이 	<ul style="list-style-type: none"> - 암호화 속도가 상대적으로 느림 - 암호화시 애러 파급 효과 큼

- 최근에는 S-Box 기반과 ECC (160bit) 기반 증가 추세.

III. 흐름 암호화와 스트림 암호화

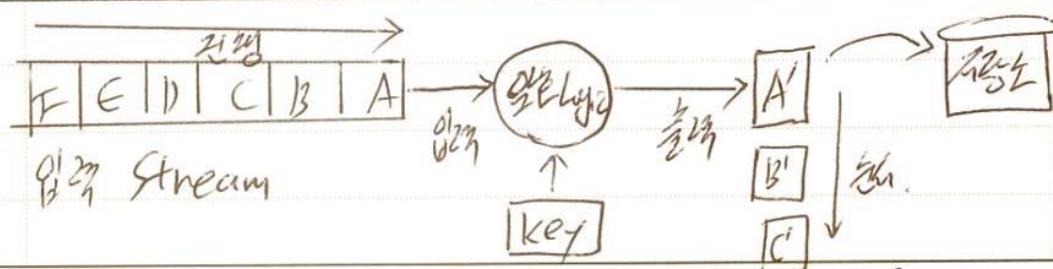
A. 흐름 암호화의 원리



개념	- Block 단위로 입출력을 받아서 입력 Data를 Substitution, Permutation을 통해 출력을 만들고자.	
특징	- Complexity 증가	- 암호공격 복잡성이 증가.
예	- DES, AES, ARIA, HIGHT 비대칭키 방식	- RSA, ECC

- 대부분의 System에서는 Block 암호화 사용이多い.

B. 스트림 암호화



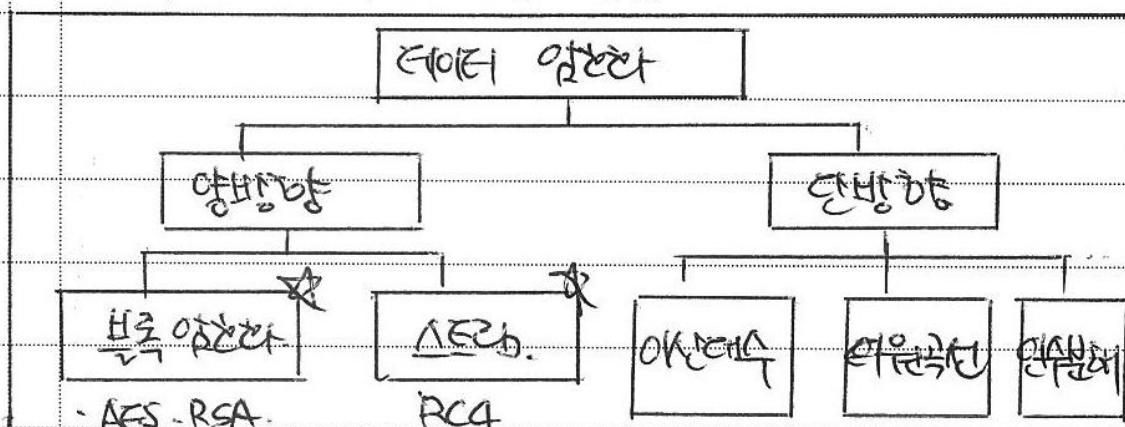
7417	- 원시 암호화를 위해 암호 Stream을 Bit, Byte, Word 단위로 암호화하는 방법.
특징	단계적 암호화 - 원시 암호화 단계
	Weak 암호화 - 중보 암호화로 암호화가 약함.
장단점	Bit Stream 암호화 - Bit 단위로 substitution 수행. Word 암호화 - Word 단위로 substitution 수행.
- 보통 암호화는 원시 암호화를 생략해 사용.	

11/29. 2

문 2). ② 볼록·스트리밍 ③ 암호화 응용프로그램 3가지 이상

답)

15
데이터 암호화의 기법 종류



- 데이터 암호화의 기법에는 양방향과 단방향이라는
복록암호화와 스트리밍암호화가 대체적으

K. 볼록 및 스트리밍 암호화 기법.

가. 볼록 및 스트리밍 암호화 아키텍처.

볼록 암호화

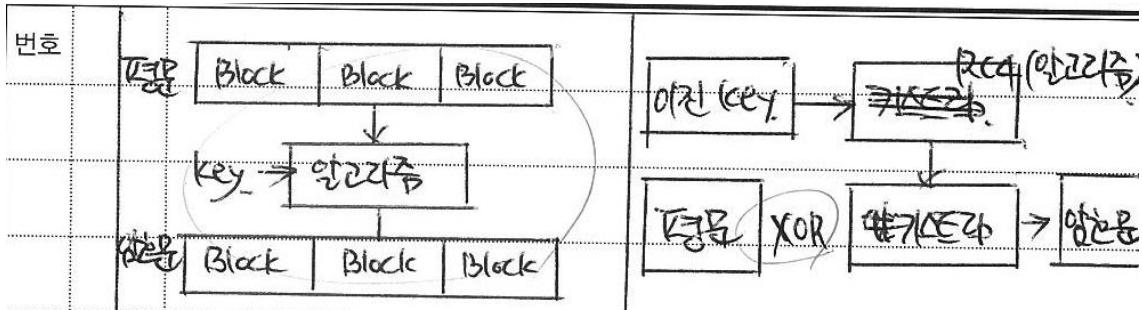
스트리밍 암호화.

평문을 복록단위로 나누어

스트리밍 라이터를 통해

암호화 알고리즘 적용하는 기법

단위로 암호화하는 기법



- 블록 암호화는 평문·암호문을 블록으로 구분, 스트리밍 암호화
기법은 스트리밍 데이터를 블록 단위로 암호화 적용.

나 블록 및 스트리밍 암호화 기법 정리(10종)

구분	블록	스트리밍
단위.	Block	스트리밍(단위)
대표암호화	DES, 3DES, AES.	RC4.
수집	Block 단위의 구분 으로 스트리밍보다 느림.	시시각적 스트리밍 암호화로 빠른 수행
복잡성	간단	키스트리밍 추출로 복잡.
구현	P-Box S-Box 등에	XOR, OR 등의
방법.	직선 체인, 대체,	연산 이용.

- 가장 많이 이용되고 있는 블록 암호화는 운영 모드에 따라 ECB, CBC, CFB, OFB, CTR을 구분

다. 블록 암호화 - 운영모드 3가지 이상 정리

구분	암호화	복호화.
ECB.	key → P C 암호화	key → C P 암호화

토픽이름	암호학적 해시 함수
분류	정보 보안 > 암호화 > 암호학적 해시 함수
키워드	임의 길이 데이터를 고정된 길이의 데이터로 맵핑 구성원칙 – 압축성(Compression), 효율성(Efficiency), 단방향성 (One-Wayness), 충돌 회피성(Collision Resistance), 제1역상저항성(Preimage Resistance), 제2역상저항성(Second Preimage Resistance), 충돌저항성(Collision Resistance) 구성요소 – 해시함수, 해시키, 해시 테이블, 버킷, 슬롯, 직접파일, 충돌, 동거자, 오버플로우 적용 알고리즘 – 나눗셈법, 중간 제곱 함수법, 폴딩법(이동/경계폴딩), 진수 변환법, 자릿수 분석법, 무작위방법 해쉬함수 이용 암호화 - MD5(Message Digest), SHA-1(Secure Hash Algorithm), SHA-2, HAVAL, Tiger
암기법	

기출문제

번호	문제	회차
1	11. 정보보호를 위한 해시함수(Hash Function) 종류에 대하여 설명하시오	105.정보관리.1.11
2	4. 정적해싱(Static Hashing) 과정에서 발생하는 오버플로우(Overflow)를 처리하기 위한 전형적인 기법 2가지를 제시하고, 성능 관점에서 비교하여 설명하시오.	104.정보관리.4.4
3	3. 해쉬 테이블(Hash Table)의 개념과 장단점, 활용분야 및 충돌 해결(Collision Resolution)의 여러 가지 기법에 대하여 설명하시오.	98.컴시응.4.3
4	10. Hashing에서의 overflow와 overflow 해결방안에 대하여 설명하시오.	합숙_2017.08.Day4
5	6. 단순 해쉬함수를 이용하여 패스워드 암호화 시 취약점과 개선방안을 제시하시오	합숙_2015.07.Day3
6	10. 암호화 해시 함수의 안전성 강화를 위한 슬트(Salt)와 키 스트레칭(Key Stretching)을 설명하시오	합숙_2015.07.Day5

I. 해시 키 검색을 이용한 해시 암호화 알고리즘의 개요

가. 해싱(Hashing)의 정의

- 해싱은 키 값에서 레코드가 저장되어 있는 주소를 직접 계산한 후 산출된 주소로 바로 접근이 가능하게 하는 방법
- 해싱은 하나의 문자열을 원래의 것을 상징하는 더 짧은 길이의 값이나 키로 변환하는 기술

나. 해싱이 사용되는 분야

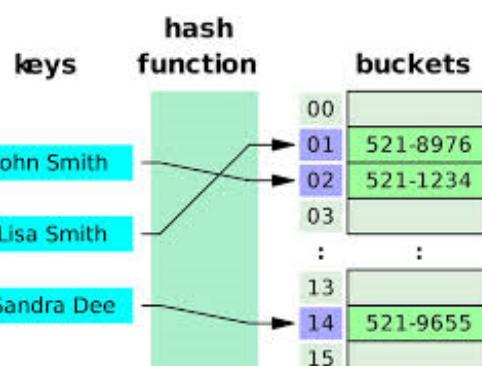
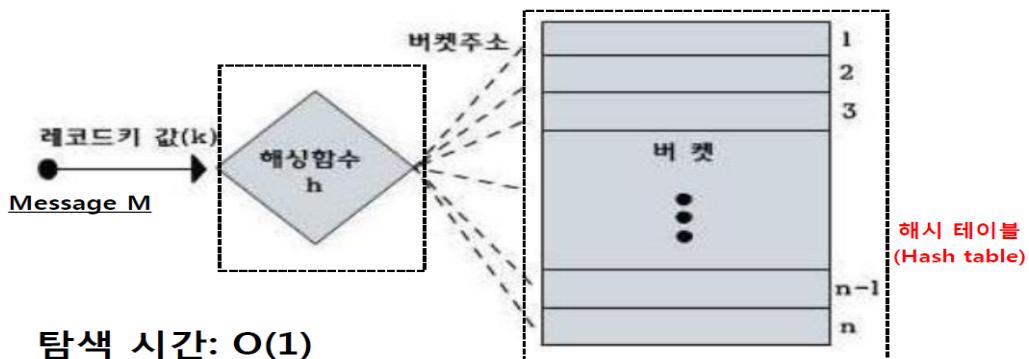
분야	내용
보안 분야	- 데이터의 위, 변조를 막기 위해 전자서명이나 보안 알고리즘에 사용
자료구조 분야	- 기억 공간에 저장된 정보를 보다 빠르게 검색하기 위해 절대번지나 상대번지가 아닌 해시 테이블을 생성하는 방식

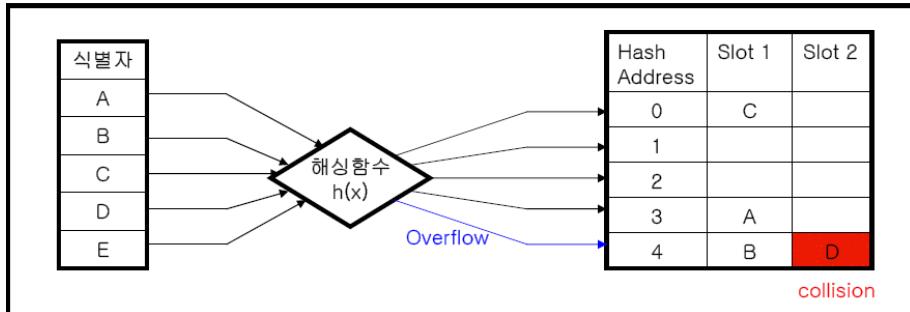
다. 해쉬 함수 구성 원칙

구분	내용
압축성 (Compression)	다양한 가변 길이의 입력에 고정된 크기의 결과값을 출력해야 함
효율성 (Efficiency)	어떤 입력값에 대해서도 해쉬값을 구하는 데 많은 자원과 노력이 소요 되지 않고 계산 속도가 빨라야 함
단방향성 (One-Wayness)	입력을 모르는 해쉬값 y 가 주어졌을 때, $H(x')=y$ 를 만족하는 x 를 찾는 것은 계산적으로 어려워야 한다.(제 1 역상 저항성) 설명) 해쉬 결과값으로부터 입력값을 계산하는 것은 불가능 해야 함
충돌 회피성 (Collision Resistance)	<ul style="list-style-type: none"> - 약한 충돌 회피성 (Weak Collision Resistance) <ul style="list-style-type: none"> <u>x 가 주어졌을 때</u> $H(x')=H(x)$ 인 $x'(\neq x)$ 를 찾는 것은 계산적으로 어려워야 한다. (제2역상 저항성) 설명) 입력값과 해쉬값을 알고 있을 때 동일한 해쉬값을 가지는 다른 입력값을 찾는 것은 불가능 해야 함 - 강한충돌 회피성 (Strong Collision Resistance) <ul style="list-style-type: none"> $H(x)=H(x')$ 인 서로 다른 임의의 두 입력 x 와 x' 를 찾는 것은 계산적으로 어려워야 한다. (충돌 저항성) 설명) 동일한 해쉬값을 가지는 서로 다른 메시지 쌍을 찾는 것은 불가능 해야 함

II. 해싱의 개념도 및 해싱의 적용 기술과 유형

가. 해싱의 개념도





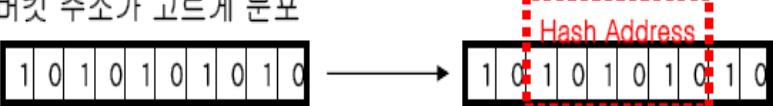
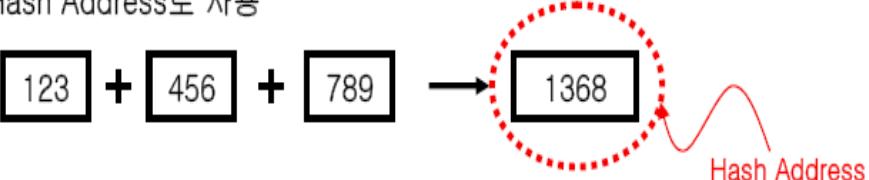
나. 해싱의 구성요소

용어	주요 개념
해싱함수 (Hashing Function)	<ul style="list-style-type: none"> - 키 값으로부터 레코드의 물리적 주소로 사상시키는 사상 함수 - 데이터 무결성 검증, 변조여부 파악을 위해 임의 길이 메시지를 고정길이 메시지(Message digest)로 변환 시 사용하는 단방향 함수(One-way Function)
해시 키 (Hash Key)	- 해싱 함수가 레코드 주소를 계산하기 위해 사용하는 레코드의 키 값을 말함
해시 테이블 (Hash Table)	<ul style="list-style-type: none"> - 해싱 함수에 의해 계산된 주소 - 키 연산에 의해 직접 접근이 가능한 구조(배열)의 기억장소
버켓 (Bucket)	<ul style="list-style-type: none"> - 하나의 주소를 가지면서 하나 이상의 레코드를 저장할 수 있는 파일의 한 구역 - 크기는 같은 주소에 포함될 수 있는 레코드 수 - 여러 개의 슬롯(slot)으로 구성,
슬롯(slot)	- 한 개의 레코드를 저장 할 수 있는 공간
직접파일 (Direct File)	<ul style="list-style-type: none"> - 해싱 방법을 기초로 하여 만들어진 파일 - 레코드를 식별하기 위한 키 값과 저장 장치에 저장되어 있는 레코드 사이의 사상(Mapping) 관계가 성립 되어야 함
충돌	- 서로 다른 레코드들이 같은 주소로 변환되는 경우임
동거자	- Synonyms, 해시 함수가 같은 주소로 변환시킨 모든 레코드
오버플로우	<ul style="list-style-type: none"> - 더 이상 빈자리가 없는 과잉 상태 - Bucket에 레코드들이 가득 찬 상태

다. 해시 알고리즘에 적용되는 기술

기술 구분	내용
제산함수 (Division)	<ul style="list-style-type: none"> - 나머지를 구하는 MOD 연산자 이용하여 주소 값을 취하는 방식 - 나누고자 하는 값, 즉 제수는 해싱 테이블의 크기를 나타냄 - 적재율은 70 ~ 80%가 적당 <p>내용</p> <p>$h(key) = key \% M$ (M : 버킷의 크기, 소수)</p> <p>정수인 탐색키(입력값)를 버킷의 크기로 나눈 나머지를 해시 주소로 사용</p> <p>[정리] %를 적용한 함수는 mod 함수이다.</p> <p>방법, 예제</p> <p>해시 주소의 고른 분포 보장 힘들 → M은 소수 (Prime Number)로 선택</p> <p>[정리] prime number(= 소수) 의 의미는, 양의 약수가 1과 자기 자신 뿐인 1보다 큰 자연수</p>

중간제곱함수 (Mid Square)	<ul style="list-style-type: none"> - 키 값의 중간 N자리를 뽑아서 제곱한 후 상대 번지로 사용 - 제곱한 결과를 주소 공간의 크기에 맞도록 조정 <p>레코드 키 값을 제곱한 후 결과값의 중간 위치의 비트들을 선택하여 해시테이블의 홈 주소로 결정</p> <p>예) $h(265) = 70225$의 중간값 = 022 위 265를 제곱함. 제곱한 중간값인 022의 비트값을 아래와 같이 표현하면, 비트로 표현이 가능하다. 중간 4비트 혹은 6비트를 선택한다.</p> <p>The diagram shows a sequence of 10 binary digits: 1 0 1 0 1 0 1 0 1 0. A red dotted box highlights the middle 6 bits: 0 1 0 1 0 1. An arrow points from this box to a second row of 10 binary digits: 1 0 1 0 1 0 1 0 1 0, where the same 6 bits are also highlighted with a red dotted box. Above the second row, the text "Hash Address" is written.</p>	옆의 사례로 대체함.								
중첩함수 (Folding)	<ul style="list-style-type: none"> - 키 값을 여러 방식으로 접어 값을 합산한 후 버켓(Bucket) 주소로 활용 <p><u>키값(입력값)을 레코드의 키를 마지막 부분을 제외한 모든 부분의 길이가 동일하게 여러 부분으로 나누고, 이들 부분을 모두 더하거나 배타적 논리합(XOR)을 취하여, 해쉬 테이블의 주소로 이용하는 방법.</u></p> <p>The diagram shows three boxes labeled 123, 456, and 789. An arrow points from these boxes to a fourth box labeled 1368, which is circled in red. A red arrow points from the number 1368 to the text "Hash Address".</p> <p>다시, 이것이 2개로 분류됨</p> <p>1) 이동 폴딩(Shift Folding): 수를 더함</p> <table border="1"> <tr> <td>특정 셀크:</td> <td>1 2 3 2 0 3 2 4 1 1 1 2 2 0</td> </tr> <tr> <td>이동 폴딩</td> <td>$1 2 3 + 2 0 3 + 2 4 1 + 1 1 2 + 2 0 = 6 9 9$</td> </tr> </table> <p>2) 경계 폴딩(Boundary Folding): 이웃한 부분의 수를 뒤집어서 더함</p> <table border="1"> <tr> <td>경계 폴딩</td> <td>$1 2 3 + 3 0 2 + 2 4 1 + 2 1 1 + 2 0 = 8 9 7$</td> </tr> <tr> <td></td> <td>1 2 3 2 0 2 2 4 1 2 1 1 2 0</td> </tr> </table>	특정 셀크:	1 2 3 2 0 3 2 4 1 1 1 2 2 0	이동 폴딩	$1 2 3 + 2 0 3 + 2 4 1 + 1 1 2 + 2 0 = 6 9 9$	경계 폴딩	$1 2 3 + 3 0 2 + 2 4 1 + 2 1 1 + 2 0 = 8 9 7$		1 2 3 2 0 2 2 4 1 2 1 1 2 0	<p>123456789012을 3개로 나눔</p> <p>1) 이동폴딩 : $123+456+789+012$</p> <p>2) 경계폴딩 : $123+654+789+210$</p>
특정 셀크:	1 2 3 2 0 3 2 4 1 1 1 2 2 0									
이동 폴딩	$1 2 3 + 2 0 3 + 2 4 1 + 1 1 2 + 2 0 = 6 9 9$									
경계 폴딩	$1 2 3 + 3 0 2 + 2 4 1 + 2 1 1 + 2 0 = 8 9 7$									
	1 2 3 2 0 2 2 4 1 2 1 1 2 0									
진수변환 (Radix Conversion)	<ul style="list-style-type: none"> - 주어진 키 값을 특정 진법으로 간주한 후 다른 진법으로 변환 값을 이용하는 기술임 <table border="1"> <tr> <td>기수변환법</td> <td>주어진 레코드 키를 특정한 진법의 수로 간주하고 키를 변환하여 홈 주소를 얻는 방법</td> </tr> <tr> <td></td> <td>예) 키의 항목이 10진수 [1234]로 되어 있을 경우에 7을 기수로 하여 변화시킬 때 상대주소는[466]이 된다.</td> </tr> </table> <p>$1*7^3 + 2*7^2 + 3*7^1 + 4*7^0$ (^는 승을 말함)</p>	기수변환법	주어진 레코드 키를 특정한 진법의 수로 간주하고 키를 변환하여 홈 주소를 얻는 방법		예) 키의 항목이 10진수 [1234]로 되어 있을 경우에 7을 기수로 하여 변화시킬 때 상대주소는[466]이 된다.					
기수변환법	주어진 레코드 키를 특정한 진법의 수로 간주하고 키를 변환하여 홈 주소를 얻는 방법									
	예) 키의 항목이 10진수 [1234]로 되어 있을 경우에 7을 기수로 하여 변화시킬 때 상대주소는[466]이 된다.									
기타	<ul style="list-style-type: none"> - 계수분석(Digit Analysis), 대수적 코딩(Algebraic Coding), 무작위방법((Pseudo-Random) 									

구 분	내 용
Mid-Square	<ul style="list-style-type: none"> - 키 값을 제곱한 후에 중간에 몇 비트를 취해서 해쉬 테이블의 버킷 주소를 생성 - 버킷 주소가 고르게 분포 
Division	<ul style="list-style-type: none"> - 키 값을 소수로 나누어 나머지를 Hash Address로 사용 - 현재로서는 가장 좋은 방식
Folding	<ul style="list-style-type: none"> - 키 값을 동일한 길이의 여러 부분으로 분할해 분할된 부분을 더해서 Hash Address로 사용 

라. 해시 함수를 적용한 암호화 기술

구분	설명	활용
MD5 (Message Digest)	<ul style="list-style-type: none"> - 128비트 암호화 해시 함수 (결과값이 16개 문자열) - 1991년 MIT 로널드라이 베스트 - MD4 대체목적 - 1996년 설계상 결함 발견 - 최근 보안관련 용도 사용 되지 않음 	<ul style="list-style-type: none"> - 파일, 메시지의 무결성 검사 - 주로 상업적 용도
SHA-1 (Secure Hash Algorithm)	<ul style="list-style-type: none"> - 160비트 암호화 해시 함수 - 1993년 미국 NIST에 의해 개발 - 가장 많이 사용 되고 있음 - 인터넷 Default 해시 알고리즘 	<ul style="list-style-type: none"> - 전자 서명 - 주로 정부 기관
HAVAL	<ul style="list-style-type: none"> - MD5를 변형하여 만들어진 해시 함수 - 128비트에서 256비트 까지 다양한 크기의 해시 코드를 만들 수 있음 	<ul style="list-style-type: none"> - MD5의 단점 보완
Tiger	<ul style="list-style-type: none"> - 64비트 프로세서에 최적화 - 매우 빠른 threeh - 32비트에서도 빠르게 동작 	<ul style="list-style-type: none"> - 64비트 프로세서에서의 해시

마. 해시 함수의 유형

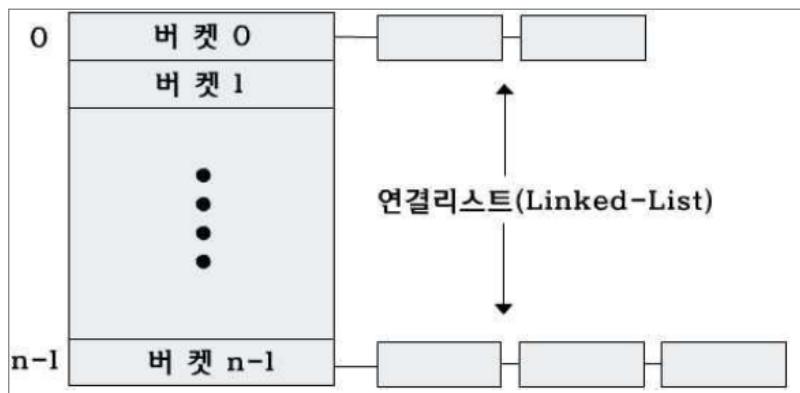
구분	설명
암호화 Hash 함수	<p>하나의 문자열을 원래의 것으로 상정하는 더 짧은 길이의 값이나 키로 변환하는 기법 전자서명을 암호화 및 복호화에 사용 의미</p> <p>즉, 암호화 해시 함수(cryptographic hash function)은 해시 함수의 일종으로, 해시 값으로부터 원래의 입력값과의 관계를 찾기 어려운 성질을 가지는 경우를 의미,</p> <p>이런 암호화 해시 함수의 성질이 역상저항성: 주어진 해시 값에 대해, 그 해시 값을 찾는 계산이 어려워여하는 제 1 역상 공격에 안전해야 한다.</p> <p>[참조]</p> <p>https://ko.wikipedia.org/wiki/%EC%95%94%ED%98%B8%ED%99%94_%ED%95%B4%EC%8B%9C_%ED%95%A8%EC%88%98</p> <p>역상저항성, 제 2 역상 저항성, 충돌 저항성에 안전해야 한다는 성질</p>
Disk에서의 Hash 함수	해시테이블이라는 자료구조는 데이터를 저장할 공간을 크게 확보한 뒤 해시함수라는 것을 이용하여 저장할 데이터에서 저장될 공간의 주소값을 계산해 데이터를 저장하는 방법을 의미함

유형	주요 개념	적용 사례
폐쇄 해싱 (Closed Hashing)	<ul style="list-style-type: none"> - 모든 레코드를 한 버켓에 저장시키고, 해싱함수로 버켓 내 주소를 계산하는 방식, - 정적 해싱 기법 	<ul style="list-style-type: none"> - 컴파일러, 어셈블러의 Symbol Table 구성
개방 해싱 (Open Hashing)	<ul style="list-style-type: none"> - 레코드의 증감에 적용하기 위해 동적으로 해싱 함수가 교정되도록 한 기법 - 동적 해싱 기법 	<ul style="list-style-type: none"> - 데이터베이스 시스템

III. 정적 해싱(Static Hashing) 기법

가. 정적 해싱(Static Hashing) 기법의 개념

- 버켓 주소 집합의 크기를 고정시켜 처리하는 해싱 기법임



나. 정적 해싱 기법의 특징

- 현재의 파일 크기에 근거하여 해싱 함수 선택
- 미래의 특정 시점의 파일 크기를 예상하여 해싱 함수 선택
- 파일의 크기가 커짐에 따라 주기적으로 해싱 구조를 재구성 해야 함

다. 정적 해싱의 문제점 및 해결방안

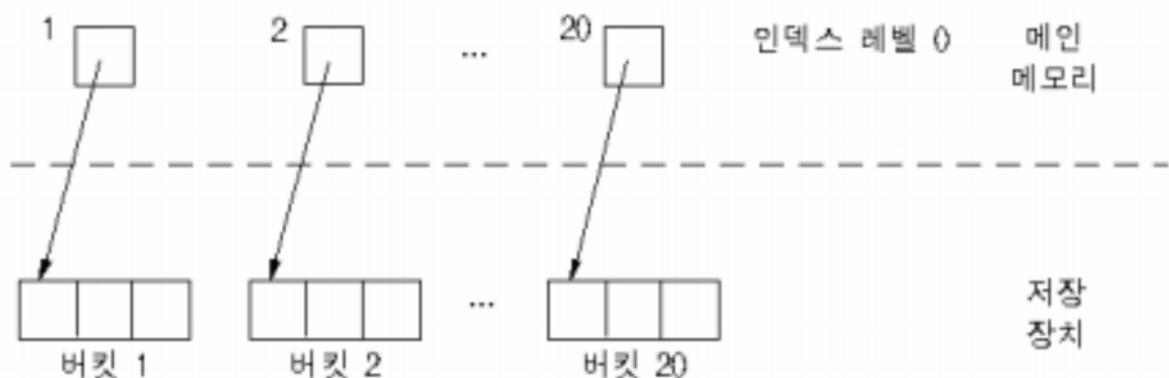
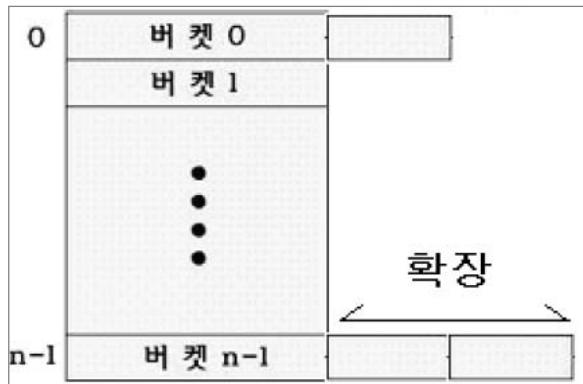
구 분	문제점	내 용
문제점	Collision	- 복수개의 키 값이 동일 Hash Address 사용
	Overflow	- 빈 버켓이 없는 상태에 Hash Address가 다시 지정된 상태
해결	선형 검색법	- 충돌이 일어난 그 위치에서 테이블 순으로 차례대로 검색하여

방안		첫 번째 빈 버켓 공간에 레코드 키를 저장하여 충돌을 해결함
	랜덤 검색법	- 충돌을 유발할 레코드 키를 저장할 수 있는 공간을 찾을 때까지, 난수를 적용하여 해시케이블의 흄 주소를 다음 주소로 선택하여 해결
	체인 이용법	- 충돌이 발생한 레코드들을 linked list로 연결하는 방법으로 해시 테이블 자체는 포인터를 배열로 만들고, 같은 버켓에 할당되는 레코드들은 체인으로 연결

IV. 동적 해싱(Dynamic Hashing) 기법

가. 동적 해싱 기법의 개념

- 데이터베이스가 확장 또는 축소되는데 이에 맞추어 해싱 함수를 동적으로 변경 시키는 해싱 기법
(Overflow 발생 시 2배수 확장)
- 키 값을 사용하여 이진 트리를 동적으로 변화시킴



나. 확장 해싱(Extendible Hashing)의 개념

- 동적 해싱의 한 형태이며 트리의 깊이가 2인 특별한 경우
- 해싱 구조의 재구성이 한번에 한 개의 버켓에서만 발생하므로, 상대적 부하경감

다. 확장 해싱의 장단점

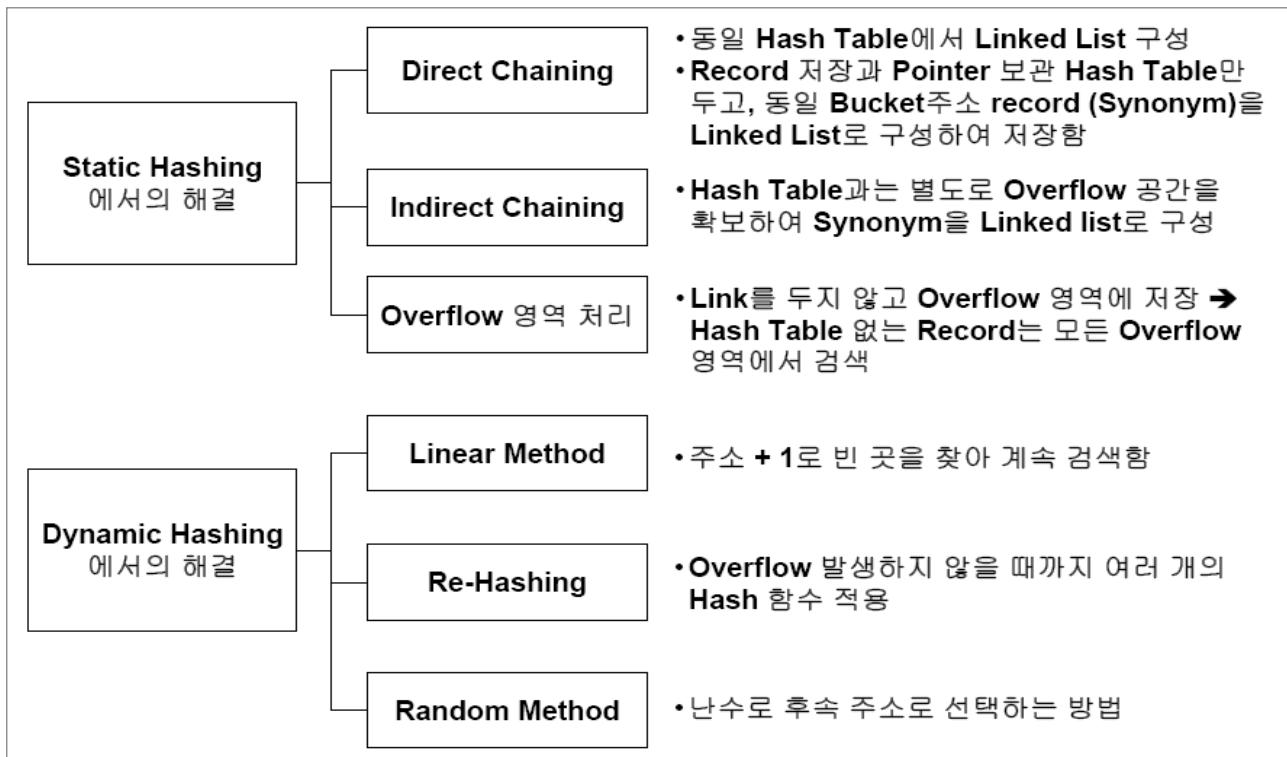
구 분	주요 내용
장점	<ul style="list-style-type: none"> - 파일의 크기가 크더라도 레코드를 접근하기 위해 디스크 접근이 두 번을 넘기지 않음 - 따라서, 파일의 크기가 증가하여도 성능이 나빠지지 않음 - 버켓 주소 테이블의 크기가 작으므로 저장 공간이 절약
단점	<ul style="list-style-type: none"> - 버켓 주소 테이블을 생성해야 하는 부담이 있음 - 각각의 버켓 주소가 실제의 버켓을 포인트하고 있으므로, 데이터의 숫자가 적으면 오히려 디스크의 낭비일 수 있음 - 버켓을 버켓 주소를 통해 간접적으로 검색하므로 추가적인 검색이 필요함

V. 충돌 해결 전략 및 해결 방안

가. Collision 해결 전략

방법	주요 내용
Bucket 해싱	<ul style="list-style-type: none"> - 버켓 : 하나의 주소를 가지면서 하나 이상의 레코드를 저장할 수 있는 파일의 한 구역 - 테이블 엔트리에 몇 개의 키 값이 들어가도록 공간을 만들어 놓음, - 충돌시 동일 버켓에 쌓아 놓음 - 버켓의 오버플로우 발생 가능, I/O증가로 인한 성능저하, 메모리 낭비
Open Addressing	<ul style="list-style-type: none"> - 충돌이 발생할 경우 다음 가용 공간에 저장 - 영역을 찾을 때까지 계속 수행하는 단순한 방법 - 별도 포인터나 데이터 스트럭처 사용하지 않음
Closed Addressing	<ul style="list-style-type: none"> - 같은 해시 값을 가지는 레코드들을 리스트로 만들어 관리 - 충돌을 쉽게 다룰 수 있음 - linked list를 통해 second clustering이라는 데이터 치우침 현상 방지 - 데이터 영역이 동적으로 할당되므로 - 테이블의 크기에 관계없이 다양한 레코드 관리가 가능함

나. Collision 해결 방안



VI. 해싱의 장단점 종합

구분	주요 내용
장점	<ul style="list-style-type: none"> - ISAM보다 상당히 빠른 검색속도를 지님 - 데이터에 대한 입력이나 삭제가 용이 - 검색시간이 데이터의 양과 무관하게 일정하게 유지
단점	<ul style="list-style-type: none"> - 연속적인 데이터 검색에는 비효율적 - 디스크 공간이 비효율적으로 사용됨 - 디스크 공간을 늘리고 재구조화하게 되면 재 검색을 위한 상당시간 소요됨

7(11) Hash 암호화 악용

6.5

I. 3가지 기밀성 확보, Hash 기반 암호화 악용 가능성

가. Hash 기반 암호화 악용

- 가변길이 암호를 고정길이 키의 길이로 축약하는
암호화 암호화 기법에 기반한 악용

나. Hash 기반 암호화 악용

1차 구조화된	2차 구조화된	예상치 험성
$y = f(x)$ 일 때 y값을 찾는 x를 찾는	$y = f(x)$ 일 때 $x = ?$ 일 때 y를 찾는	학수 많 Y를 이용 x가 찾을 수 있는 여러 가능

II. Hash 암호 악용 예방 방법

가. password 이용하는 Hash 암호 경우

방법	설명	방법 가능
PBDFI2	key stretching 시 시킨, 유도 Derived key 활용 해석	key - stretching
Bcrypt	Blowfish 암호 악용 기본의 pw 암호 해석 가능	(key를 암호화) salt
SCrypt	key 풀리기 Round 수를 증가 변경 가능 Hash 악용	(예로 풀리기 난수)

나. 무결성 기밀성 기반의 Hash 암호 악용

악용	설명	기본 가능
MD5	Message Digest 기반의	脆弱 Message

	HAS-160	341 페터슨 Hash Function KCDSA # 7 3회 Hash 160bit 512bit 128bit (128bit)
	SHA1(2)	Standard Hash Algorithm 93 SPN 구조 Confusion & Diffusion 512 (256, ~512 bit)
	RC4	128 ~ 512 bit key 64bit Hash algo. 암호화 알고리즘 512 "128"

토픽	암호화(Encryption), 암호화 원리
키워드	암호화(Encryption), 평문(Plain text), 암호화된 문장(Cipher text) 대체, 블록화, 치환, 압축, 혼돈과 확산, 확장
암기법	CIA 인부, 대블치아호화

출제문제

회차	과목	교시	문제
모의_2016.04	응용	3 교시	암호 알고리즘 설계의 기본원칙인 확산과 혼돈의 개념과 블록 암호의 구성 요소에 대하여 설명하시오.
모의_2014.01	응용	3 교시	암호알고리즘 설계의 기본원칙인 확산과 혼돈의 개념과 블록암호화에서의 Feistel 구조에 대해 설명하시오.

[목차]

I. 평문을 암호화된 문장으로 대체 및 전치환하는 방법, 암호화의 개요

- 가. 암호화(Encryption)의 정의
- 나. 암호화의 필요성
- 다. 암호화의 특성 (CIA, 기밀성, 완전성, 유통성)
- 라. 암호화 알고리즘의 원리 (대블치아호화)

II. 암호화 개념도 및 분류(유형)

- 가. 암호화 개념도
- 나. 암호화 구성요소 (평암~ 복키 알시)

III. 암호화 분류

- 가. 암호화 유형 분류 (정키기)
- 나. 암호화 정보단위에 따른 분류

I. 평문을 암호화된 문장으로 대체 및 전치환하는 방법, 암호화의 개요

가. 암호화(Encryption)의 정의

- 암호키와 알고리즘 이용하여 평문(Plain text)을 재구성, 쉽게 해독되지 않는 암호화된 문장(Cipher text)으로 변환하여, 데이터 무결성 및 기밀성 확보하는 기술
- 복호화: 암호화의 역과정으로 불명확한 메시지로부터 본래의 메시지로 환원하는 과정

나. 암호화의 필요성

특징	설명
보안 대책	정보 시스템이 요구하는 정보 보안 수준에 따라 효율적/계층적 보안 대책 제공
거래 신뢰성	암호화 기술 이용하여 전자화폐, 전자송금, 전자지갑 등에서 전자상거래 신뢰성/비밀성 제공
보안 위협 예방	외부 침입자(Intruder)에 의한 보안 위협 예방 효과
기밀성	정보 시스템의 기밀성을 위해 암호화 기술 이용

다. 암호화의 특성 (CIA 원칙)

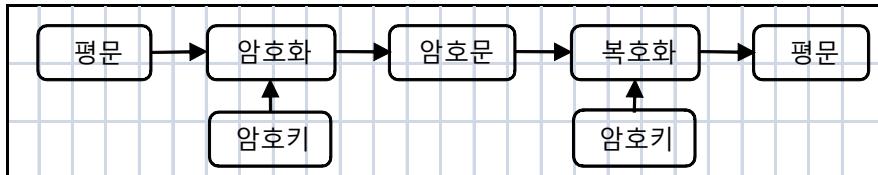
특성	기능	적용기술
기밀성 (Confidentiality)	송/수신자 이외는 송신내용 인지불가	암/복호화
무결성 (Integrity)	정보의 조작 및 변경 여부 확인	해쉬함수
가용성 (Availability)	요구사항에 대한 서비스 제공	암호/인증
인증 (Authentication)	PKI 사용자에 대한 신원 확인 기능	인증서
부인봉쇄 (Non-repudiation)	송수신자의 송수신 사실 부인 봉쇄	전자서명

라. 암호화 알고리즘의 원리 (대블치아호화)

특성	내용
대체(Substitution)	글자끼리 매치 시켜 놓은 표 등을 이용하여 대체 ex) 1→a
블록화(Blocking)	열과 행을 바꾸어 표현한 후 블록 구성
치환(Transposition)	문자열의 위치를 서로 바꾸어 표현 후 블록 구성
압축(Compaction)	문자열에서 일부 문자를 삭제하여 압축문과 삭제문을 분리
혼돈과 확산 (Confusion & Diffusion)	혼돈과 확산을 동시에 적용하여 해독이 어려운 암호화 구현
확장(Expansion)	무의미한 문자를 삽입하여 문자열을 확장

II. 암호화 개념도 및 분류(유형)

가. 암호화 개념도



- 침해자는 암호키가 없기 때문에 암호문을 파악할 수 없고, 암호키는 대칭키와 비대칭키 방식을 사용

나. 암호화 구성요소 (평암~ 복키 알시)

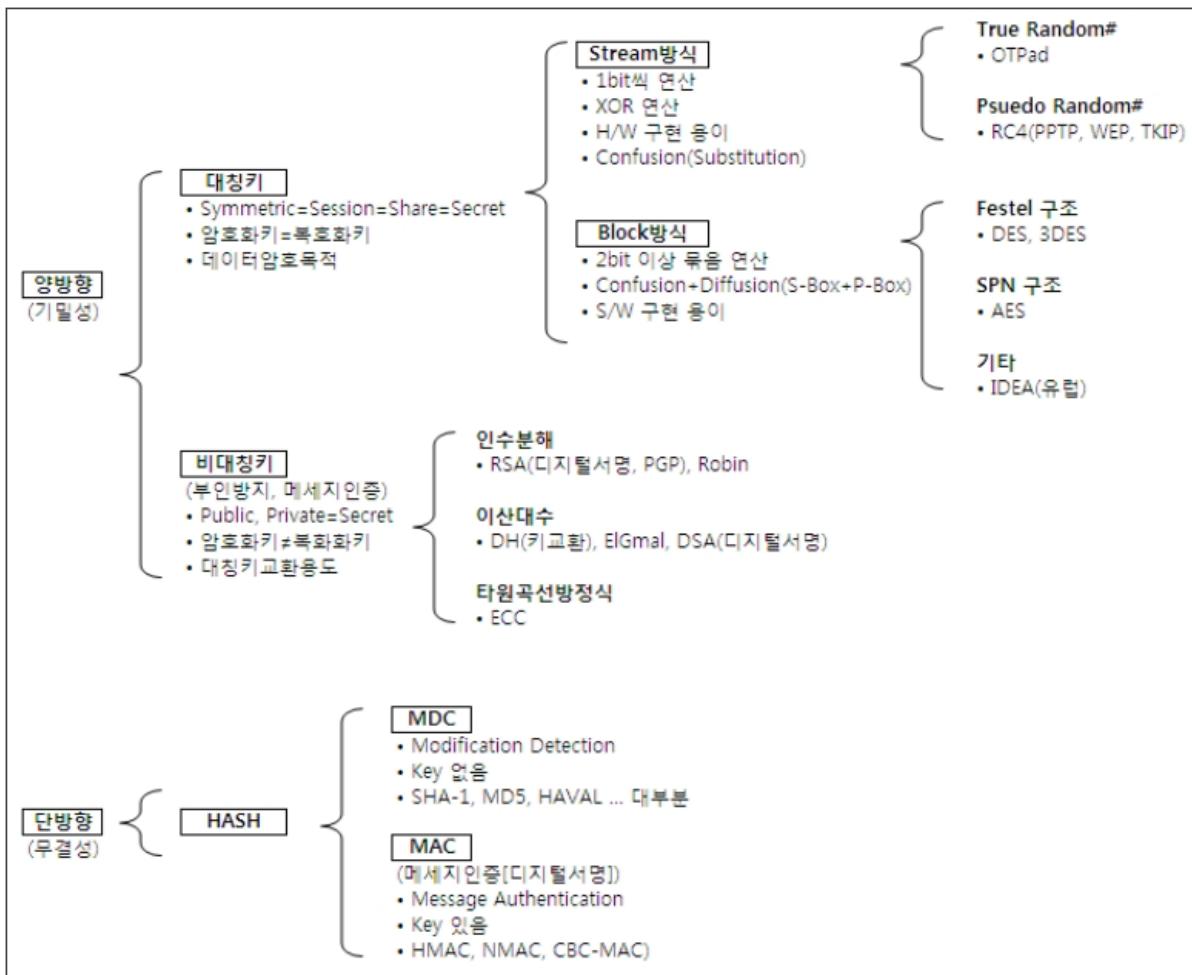
구성요소	내용
평문 (Plain-text)	암호화 하고자 하는 문장

암호문 (Cipher-text)	평문을 암호화 알고리즘과 키를 이용하여 암호화한 문장
암호화 (Encryption)	평문을 암호화 키를 이용하여 암호문으로 변환시키는 과정
복호화 (Decryption)	복호화 키를 이용하여 원래의 평문으로 변환시키는 과정
키 (Key)	암호화 알고리즘의 매개변수
암호 알고리즘 (Encryption Algorithm)	암호화와 복호화에 이용되는 알고리즘
암호 시스템 (Cryptosystem)	암호화 기술과 복호화 기술의 통칭

III. 암호화 분류

가. 암호화 유형 분류 (정기기)

분류	암호화	내용
정보단위	스트림 암호화	<ul style="list-style-type: none"> - 한번에 1 비트 혹은 1 바이트의 디지털 데이터를(스트림) 암호화하는 방식 - 암호화 속도가 상대적으로 빠름 - 암호화 시 에러 파급 효과가 적음
	블록 암호화	<ul style="list-style-type: none"> - 평문 블록을 단위 블록으로 나누어 암호화 블록을 생성하는 방식 - 평문 나누므로 혼돈성을 주어 해독을 어렵게 함 - 완성된 암호문에 내용 추가 및 변경이 어려움
Key형태	비밀키 암호화	<ul style="list-style-type: none"> - 송신자와 수신자가 공유한 비밀키로 암호화 복호화 하는 방식 - 구현 용이. 빠른 암호화 - Key 분배 시 노출 가능성
	공개키 암호화	<ul style="list-style-type: none"> - 송신자와 수신자가 각각 공개키-비밀키 한쌍을 보유. 상대방의 공개키로 암호화한 정보를 전송하면 공개키에 해당하는 비밀키로 복원하는 방식 - 암호해독 어려움, 키 분배의 용이, 전자서명
암호화기술 (7)	SPN	<ul style="list-style-type: none"> - Substitution-Permutation Network (대체순열구조) - 전치와 치환을 이용, 관용 암호 방식(암/복호화에 동일한 키 사용하는 방식) 문제 해결 - 128 비트를 4X4 행렬로 나타내어 행렬을 이용한 암호화 - 적용 알고리즘: AES, ARIA
	Feistel (피스텔)	<ul style="list-style-type: none"> - N 비트의 블록을 N/2 쪽 둘로 나누고, R 번의 라운드 만큼 반복된 연산 - 라운드 함수를 반복적 적용, 이전 블록 암호문과 평문을 XOR (Exclusive-OR) 한 형태 - 적용 알고리즘: DES, SEED
	인수분해	<ul style="list-style-type: none"> - 두 큰 소수 p 와 q 의 곱셈은 쉬우나 n 으로부터 p 와 q 를 추출하기 어려운 점 이용 - 적용 알고리즘: RSA
	타원곡선	<ul style="list-style-type: none"> - PKI 기반의 RSA 의 문제점인 속도와 안정성을 해결하기 위해서 타원 기반의 안정성과 효율성을 기반으로 생성된 알고리즘, 적용 알고리즘: ECC
	이산대수	<ul style="list-style-type: none"> - 이산대수의 계산은 어렵지만, 그 역함수/지수함수의 - 계산은 빠르게 수행하는 특징을 이용, 적용 알고리즘: Diffie-Hellman, DSA
	해시 알고리즘	<ul style="list-style-type: none"> - 임의의 길이를 가지고 있는 메시지를 받아들여 고정된 길이의 출력 값으로 바꾸어주는 알고리즘 - 단방향: 원래의 입력값을 찾아내기 불가능, 역상 저항성 - 적용 알고리즘: MD-5, SHA-1, SHA-2
	LEA	<ul style="list-style-type: none"> - LEA(Lightweight Low-power Encryption Algorithm) - 2012년 국가보안기술연구소가 개발한 128 비트 경량 고속 국산 블록화 알고리즘



나. 암호화 정보 단위에 따른 분류

구분	블록 암호화 (Block Cipher)	스트림 암호화(Stream Cipher)
개념도	 	
개념	평문을 일정한 블록단위로 나누어서 각 블록마다 암호화 과정 수행, 고정된 크기의 블록단위의 암호문 생성	평문과 같은 길이의 키 스트림 생성하여 평문과 키 이진 수열을 비트 혹은 바이트 단위로 XOR 이진연산으로 결합하여 암호문 생성
장점	기밀성, 해쉬함수 다양	암호속도가 빠름, 에러 전파현상 없음
사례	DES, AES, SEED, ARIA	LFSR, SEAL, RC4
단위	블록 단위	비트 단위

다. 암호화 기술에 따른 분류

암호화 기술	내용	적용 알고리즘
SPN	<ul style="list-style-type: none"> - Substitution-Permutation Network (대체-치환 망구조) - 전치/치환 이용하여 관용 암호방식 (암/복호화에 동일한 키를 사용하는 방식)의 문제 해결 - 128 비트를 4X4 행렬로 나타내어 행렬을 이용한 암호화 	<ul style="list-style-type: none"> - AES (Advanced Encryption Standard), - ARIA(Academy, Research Institute, Agency)
Feistel (피스텔)	<ul style="list-style-type: none"> - N 비트 블록을 N/2씩 둘로 나누고, R번의 라운드만큼 반복된 연산 - 라운드 함수를 반복적으로 적용, 이전 블록 암호문과 평문을 XOR (Exclusive-OR) 한 형태 	<ul style="list-style-type: none"> - DES(Data Encryption Standard) - SEED(KISA에서 만든 알고리즘, 한국에서만 사용)
인수분해	<ul style="list-style-type: none"> - 두 큰 소수 p 와 q 의 곱셈은 쉬우나 n으로 부터 p 와 q 를 추출하기 어려운 점 이용 	RSA(Rivest Shamir Adleman)
타원곡선 (이산대수)	<ul style="list-style-type: none"> - PKI(Public Key Infrastructure) 기반의 RSA 의 문제점인 속도와 안정성 해결하기 위해 타원곡선기반의 안정성/효율성 기반으로 생성된 알고리즘 	ECC, 타원곡선암호 (Elliptic Curved Cryptosystem)
이산대수	<ul style="list-style-type: none"> - Discrete logarithm problem - 이산대수의 계산은 어렵지만, 그 역함수/지수함수의 계산은 빠르게 수행하는 특징을 이용 	<ul style="list-style-type: none"> - Diffie-Hellman(디피헬만) - DSA(Digital Signature Algorithm)
해시 알고리즘	<ul style="list-style-type: none"> - 임의 길이의 메시지를 받아들여 고정된 길이의 출력값으로 바꾸어 주는 알고리즘 - 단방향 : 원래 입력값 찾아내기 불가능 	<ul style="list-style-type: none"> - MD-5(Message Digest), - - SHA-1 - SHA-2(Secure Hash Algorithm)

[참고] ECC(Elliptic Curve Cryptosystem, 타원곡선암호)

- 타원 곡선 시스템을 이용한 공개키 암호 방식
- 해독방법은 아직 발견되지 않았으며, 짧은 키 사이즈로 높은 안전성 확보되고, 또한 서명할 때의 계산을 고속으로 할 수 있는 것이 특징
- 스마트카드(IC카드) 등의 정보처리능력이 높지 않은 기기에서 이용하기에 적합한 암호화 방식

I. 주요 암호화 알고리즘 비교 및 활용/선정기준

가. 주요 암호 기술

암호기술	내용
DES	<ul style="list-style-type: none"> - Data Encryption Standard - 64bit 블록, 56bit 키, 대칭키 - 16라운드 Festel 구조, 라운드 함수는 SPN 구조 - 1997년까지 미국 표준
AES	<ul style="list-style-type: none"> - Advance Encryption Standard - 128bit 블록, 128, 192, 256 bit 가변키 - 10, 12, 14회 라운드

RSA	<ul style="list-style-type: none"> - Rivest-Shamir-Adlman - 큰 두 소수의 곱 $n=pq$의 인수분해 문제 - n이 1024bit 이상 안전, 2048bit 이상 권장
ECC	<ul style="list-style-type: none"> - Elliptic Curve Cryptosystem - RSA보다 키 길이 작다(160) - 모바일 환경에 적합 - 한국(ECKCDSA) 2001년 TTA 표준
SEED	<ul style="list-style-type: none"> - 한국 정보보호센터 KISA(Korea Information Security Agency)가 1988년도에 개발한 128bit 대칭형 키 블록 알고리즘 - 안정성, 신뢰성이 우수하며 3-DES보다 처리속도 고속 - IPSec을 위한 SEED 암호사용 표준, IETF(Internet Engineering Task Force)의 RFC 표준

나. 주요 암호화 알고리즘 비교

구분	DES	3DES	AES	SEED	ARIA
평문블록크기	64	64	128	128	28
키 크기	56	168	128/192/256	128/192/256	128/192/256
암호문 블록크기	64	64	128	128	128
전체구조	Feistel	Feistel	SPN	Feistel	ISPN
라운드수	16	48	10/12/14	16	12/14/16
개발기관	미국 표준 기술 연구소(NIST)		정보보호진흥원		국가보안기술연구소

다. 암호화 알고리즘 활용분야 및 알고리즘 선정기준

구분	내용
활용분야	<ul style="list-style-type: none"> - 개인 식별 및 인증, 전자서명, 키분배 - 전자화폐, 전자결재, 전자선거
선정기준	<ul style="list-style-type: none"> - 암호화 강건성: 보호하려는 데이터의 성격에 따라 암호화 알고리즘 선정 - 성능: 암호화를 적용하려는 시스템 및 단말에 요구되는 성능을 만족을 하는지 검토

[블록 암호화의 원리]

I. 블록 암호화의 원리, 혼돈과 확산의 개요

가. 혼돈과 확산의 정의

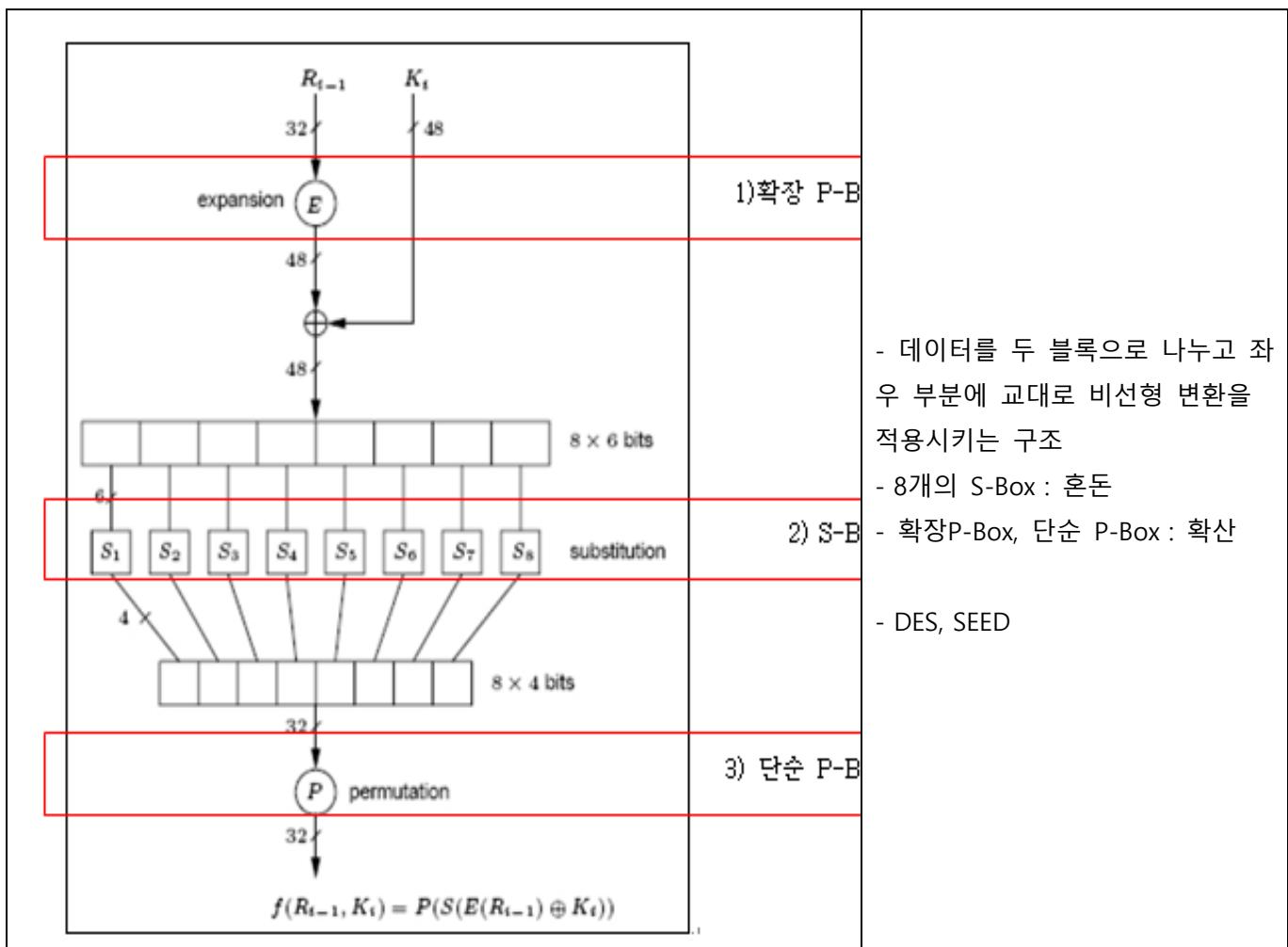
혼돈 (Substitution)	- 암호문과 암호키 관계를 은닉, 암호문 이용하여 암호키 찾는 공격 방지 기법 - 키의 단일비트가 변하면 암호문 대부분 비트가 변할 수 있음
확산 (Permutation)	- 암호문과 평문사이 관계를 은닉, 암호문에 대한 통계 테스트 통해 평문 유추하는 공격 방지 기법 - 평문의 단일 비트가 변하면 암호문에 특정 비트나 모든 비트가 변할 수 있음

나. 혼돈과 확산의 상세 설명

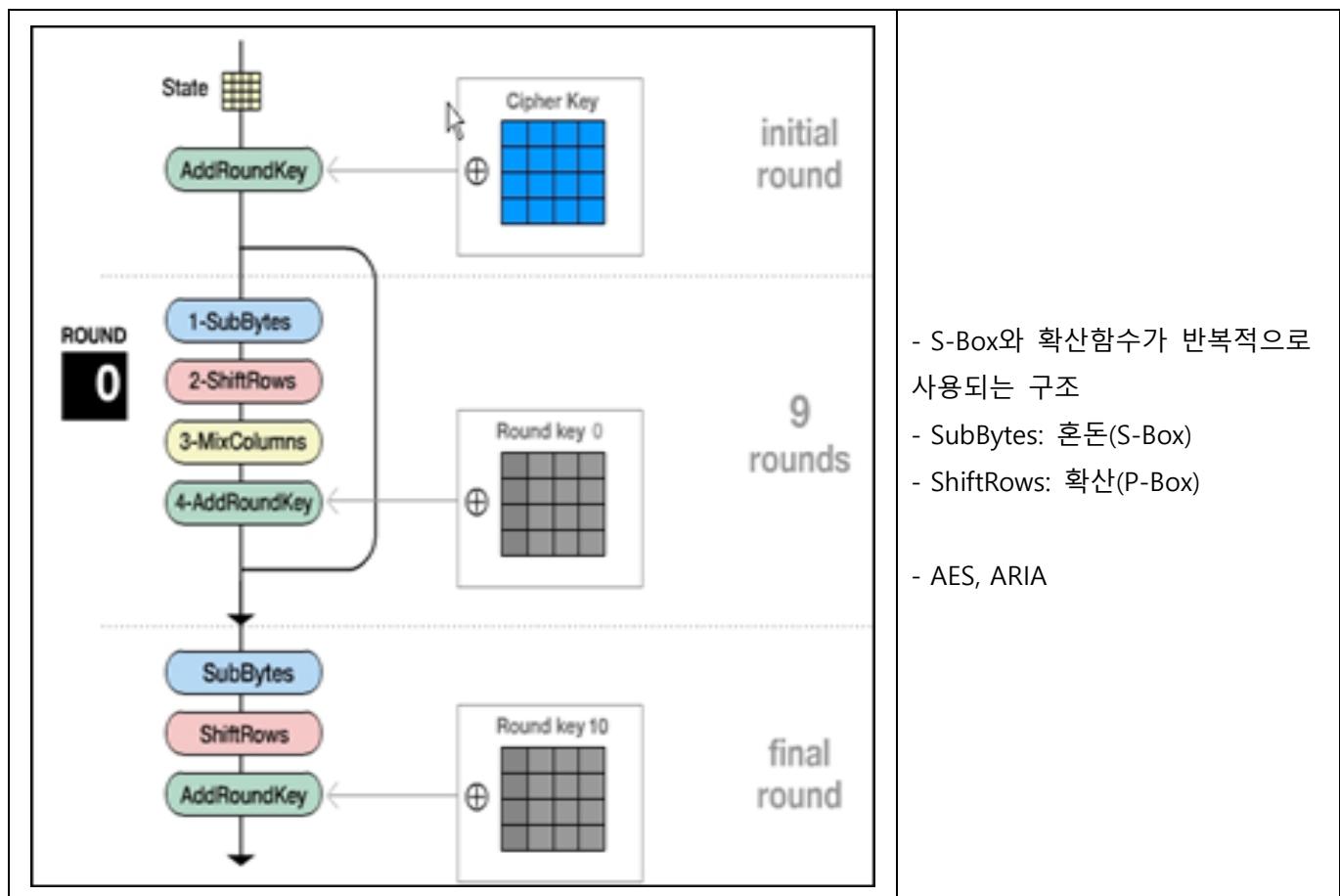
구분	내용	기법
혼돈이론	- 대체(Substitution)형 암호 - 혼돈의 특성을 이용 - 평문의 특정 비트를 임의의 특정 값으로 대체	S-Box(Substitution)
확산이론	- 전치(Transposition)형 암호 - 확산의 특성을 이용 - 평문의 각 비트의 재배열	P-Box(Permutation)

II. 혼돈과 확산을 적용한 블록암호화의 사례

가. Feistel 구조



나. SPN 구조



- S-Box와 확산함수가 반복적으로 사용되는 구조
- SubBytes: 혼돈(S-Box)
- ShiftRows: 확산(P-Box)
- AES, ARIA

- 현대 블록암호화는 P-Box와 S-Box를 결합하여 혼돈과 확산을 동시 적용
- 반복 암호시스템(*Integrated Cryptosystem*)
 - : 암호학적으로 취약한 라운드 함수를 중첩하여 좀 더 안전한 암호 만드는 방식
 - : 혼돈과 확산을 반복함으로서 통계적 성질을 제거한 안전한 블록암호 구성

번호 1) 암호화 알고리즘의 개념, 대칭키/비대칭키
암호화 알고리즘 비교, 복호암호화 방식 알아보자.

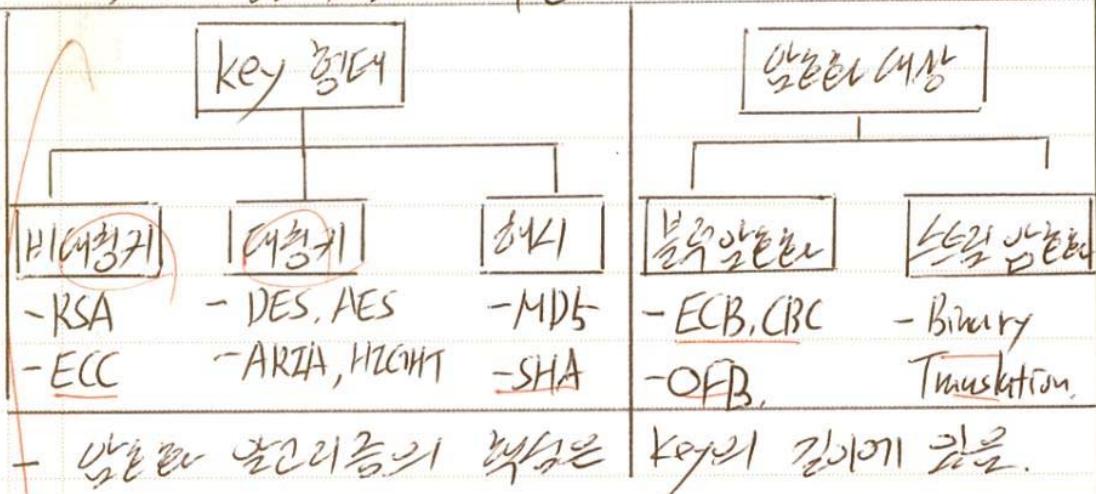
(1)

I. Plain Text to Cipher Text, 암호화 알고리즘의 개념

가. 암호화 알고리즘의 정의.

- 텍스트(Plain Text) 형태의 입력에 의해 외부의 비밀한 사용자가 복호할 수 있도록 암호문(Cipher Text) 형태로 변환하는 알고리즘.

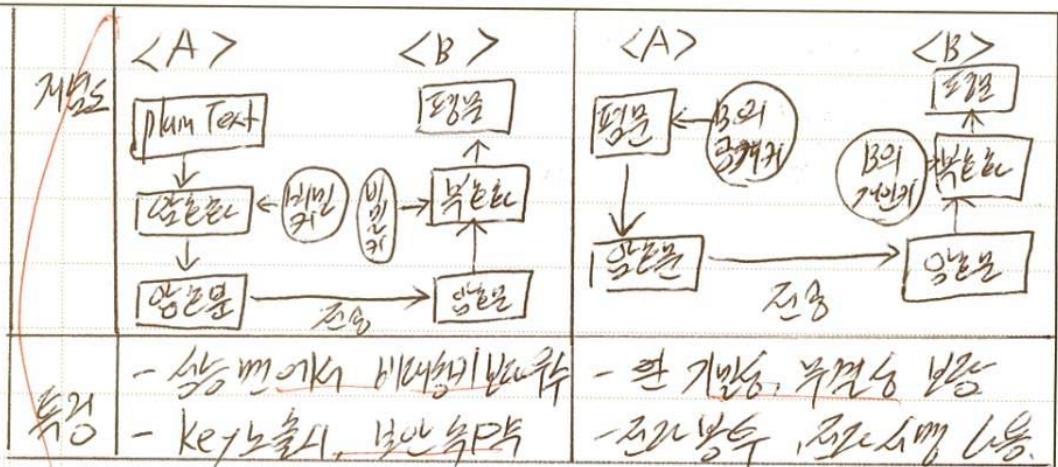
나. 암호화 알고리즘의 구분.



II. 대칭키 / 비대칭키 알고리즘 비교.

가. 대칭키 / 비대칭키 알고리즘의 개념 비교.

구분	대칭키 알고리즘	비대칭키 알고리즘
개념	- 비밀키를 공유하여 키를 통한 암복호화 구현	- 공개키/개인키를 통해 기밀성/무결성 기반 알고리즘.



II. 대칭기 / 비대칭기 알고리즘의 개념 비교

구분	대칭기 기법	비 대칭기 기법.
대통령 기법.	<Feistel 기법> 	<RSA 기법> $C = P^e \text{ Mod } N$ ← e * d 의 $P = C^d \text{ Mod } N$ ← d * e 의 $e: 32비트, d: 256비트$
Advanced 기법	<SISA 기법> 	<ECC 기법>

토픽이름	양자암호
분류	정보 보안 > 암호화 > 양자암호
키워드	일회용 난수표(one-time pad), 데이터+암호키 이분화 통신 특성 - 양자 복제 불가능, 비밀키 분배의 안전성, 일부 발췌 불가 구성 - 양자키분배(QKD), 암호장비 양자암호통신(Quantum Cryptography Communication) 양자키분배 (QKD, Quantum Key Distribution) Quantum Channel
암기법	

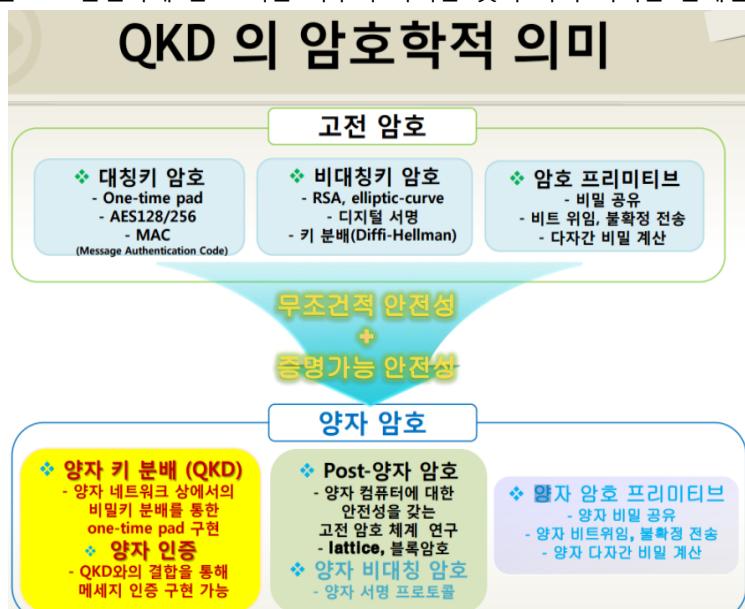
기출문제

번호	문제	회차
1	양자 알고리즘이 현대 암호에 미치는 영향에 대해서 'Shor 알고리즘'과 'Grover 알고리즘' 중심으로 설명하시오.	컴시응, 113, 4
2	양자암호통신(Quantum Cryptography Communication)에 대해 설명하시오.	모의 2015.04 응용, 1교시, 9
4	양자컴퓨팅(Quantum Computing)에 대해 설명하시오.	합숙 3일차 2017.01.16(월)
5	양자암호통신(Quantum Cryptography Communication)에 대하여 설명하시오	합숙 4일차 2016.01.26(화)

I. 양자역학 기반의 양자정보체계를 활용한 암호체계, 양자암호

가. 양자암호(Quantum Cryptography)

- 양자암호는 안전한 통신을 위한 암호체계이며(1984년 C. H. Bennett과 G. Brassard가 제안하였으며), 기준에 있던 대부분의 암호체계가 대부분 수학적 복잡성에 기반하는데 비해, 양자암호는 **자연현상에 기반**하고 있는 특징을 띠며, 암호에 사용되는 **원타임 패드**를 생성하는 이상적인 방법 (다른 말로 **양자 키 분배**(Quantum Key Distribution)체계라고도 한다.)
- 양자암호통신은 자연의 근본원리인 양자역학의 법칙에 의해서 도청 및 감청이 절대적으로 불가능한 새로운 개념의 차세대 통신보안 기술로서 양자정보과학 중에서도 가장 기초적이고 기술성숙도가 높은 기술이며 점점 심각해지는 통신네트워크의 보안문제를 해결할 중요한 대안기술이다.
- 일회용 난수표(one-time pad)를 송신자와 수신자가 미리 안전하게 나누어 가진 후 이것을 암호 키로 사용하여 비밀 통신을 하는 원리적으로 안전성이 증명된 대칭암호체계이다.
(두 사용자 사이에 실시간으로 안전하게 암호 키를 나누어 가지는 것이 극히 어려운 문제임)



나. 양자(Quantum)의 고유한 특성.

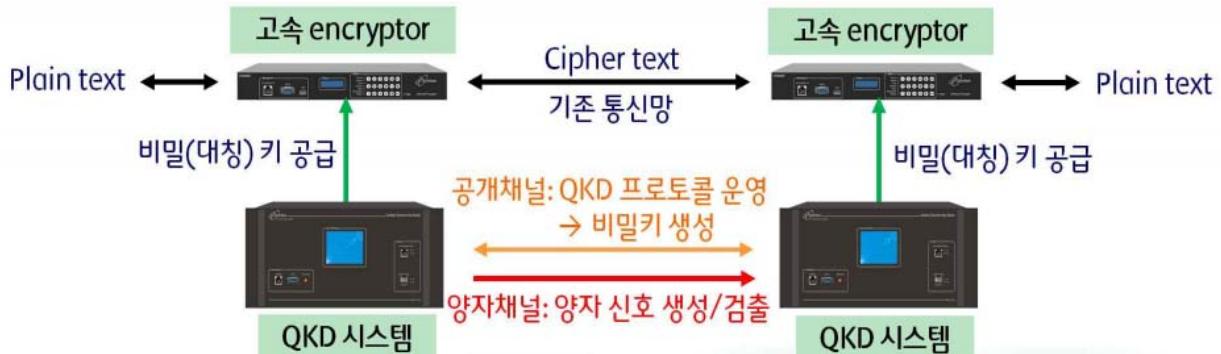
- 양자증첩이란 여러 상태가 확률적으로 하나의 양자에 동시에 존재하고 측정하기 전까지 정확한 양자상태를 알 수 없다는 특성이다.
- 양자얽힘은 둘 이상의 양자가 가지는 비고전적 상관관계로 두 양자가 서로 멀리 떨어져 있어도 존재하는 특성
- 불확정성은 서로 다른 물리량이 동시에 정확하게 측정이 불가능한 특성이다.



- 여러 상태를 동시에 갖고 있고 이를 동시에 정확하게 측정할 수 없기 때문에 양자는 복제 불가능하다.
- **복제 불가능성**에 기반하여 양자암호는 비밀키 분배의 안전성을 보장받는다.
- 양자의 종류에는 광자, 전자, 이온, 원자 등 여러 가지가 있지만
양자암호통신에서는 빛의 최소단위인 **광자를** 이용한다.

II. 양자암호 통신의 구조

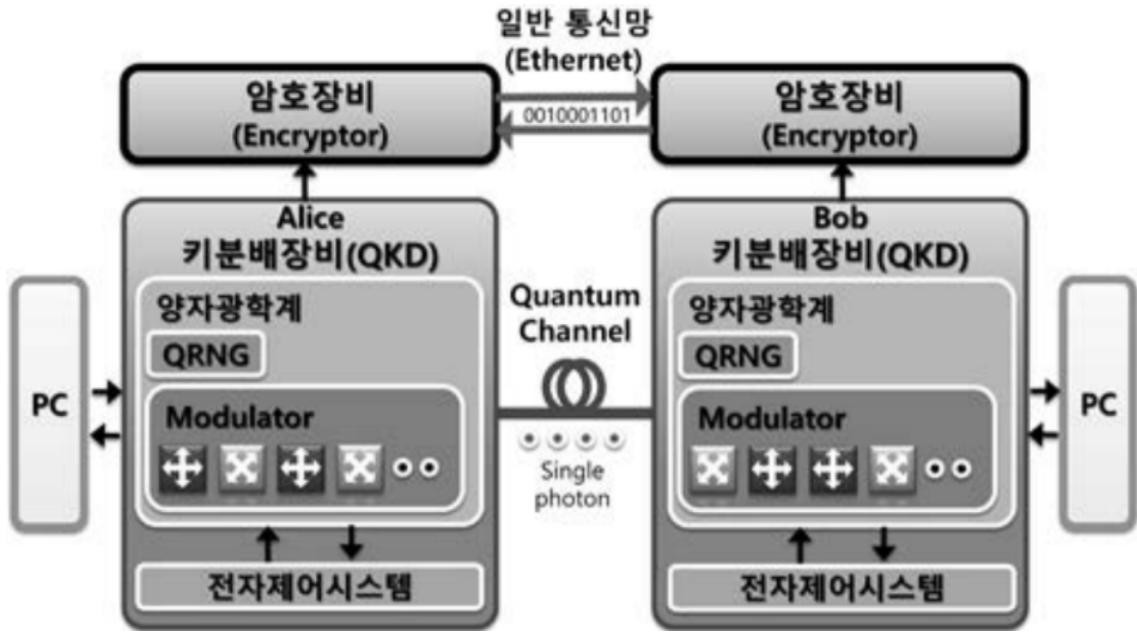
가. 양자 암호 통신의 구성도



도청불가 원리



<그림2> QKD 시스템 구성도



- 양자암호 통신은 크게 두 부분으로 구성되는데 양자의 특성을 이용하여 비밀키를 송/수신자가 안전하게 나누어 갖는 양자키분배 (QKD, Quantum Key Distribution)와 나누어진 비밀키를 이용하여 암호통신을 하기 위한 데이터 암호화/복호화를 수행하는 암호장비로 구성된다.
- 흔히 양자암호라 하면 양자키 분배만을 지칭하기도 한다.

나. 양자암호통신(Quantum Cryptography Communication)

- 양자암호통신은 멀리 떨어져 있는 두 사람이 통신상에서 암호 비밀키를 안전하게 나누어 갖고 이를 이용해 암호 통신을 수행하는 것이다.
- 양자암호통신은 '단일양자의 복제불가능성'과 '양자측정의 비가역성' 등과 같은 양자역학의 근본적인 원리를 이용하여 공간적으로 멀리 떨어진 두 사용자 사이에 이러한 비밀 암호 키(일회용 난수표)를 실시간으로 절대적으로 안전하게 분배하는 방법으로서 '양자암호(Quantum Cryptography)' 혹은 '양자 키 분배(Quantum Key Distribution)' 기술로 알려져 있다

다. 양자 암호 통신의 특징

- 중간에 도청자가 난입할 경우 그 존재가 드러나며, 신호가 왜곡되어 도청자가 정확한 정보를 얻을 수 없는 보안성을 띠고 있다.
- 양자키 분배에서는 하나의 정보를 하나의 광자에 실어 보내기 때문에 일부만 발췌한다는 것이 원천적으로 불가능
- 양자의 종류에는 광자, 전자, 이온, 원자 등 여러 가지가 있지만 양자암호통신에서는 빛의 최소단위인 광자를 이용한다.

라. 양자암호통신의 도입 필요성

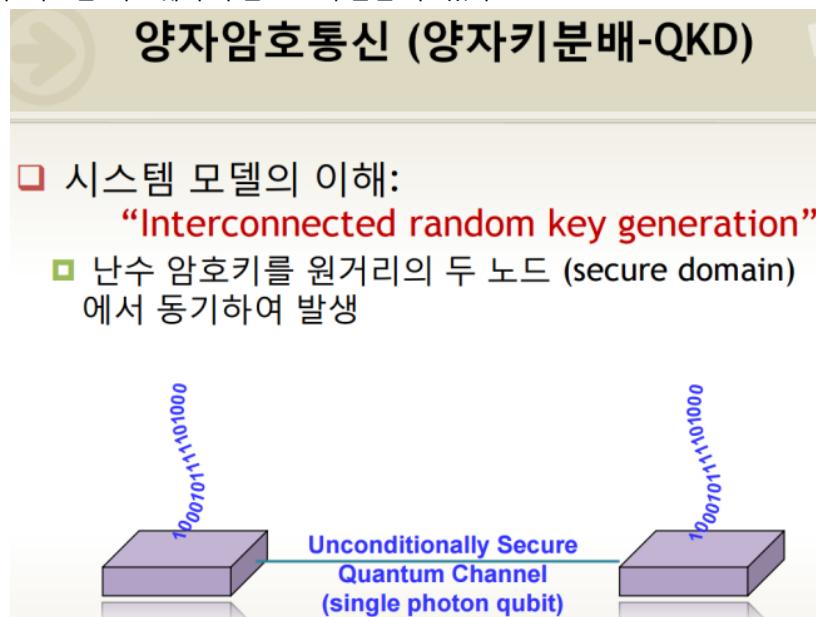
구분	설명
관리적 이유	<p>국가안보보안망, 국가행정전산망, 금융권/의료권 정보보호 필요</p> <ul style="list-style-type: none"> - 군사, 기관, 기업, 금융 등의 네트워크가 일반 개인 네트워크와 유무선으로 연결되어 있음 - 다양한 경로를 통해 중요 정보들이 누출될 가능성이 높음 - 모든 고전 정보들은 근본적으로 가독성을 지님 - 정보보호를 위해서는 암호화가 필수적이며 - 결국, 비밀키의 생성, 분배, 관리가 정보보호의 가장 중요한 요소임 - 국가적 자국 솔루션 확보 절대적 <p>Ex) 광통신 백본망의 도청</p> <p>단순한 도청코드 삽입으로 중요한 정보를 인터넷을 통한 유출가능</p> <p>미국 NSA 스노든-적성국은 물론 우방국의 대규모 도감청</p> <p>정보보호에 있어서는 우방국이 없음</p>
기술적 이유	<p>기존 암호체계 취약성, 차세대 컴퓨터의 급격한 발전</p> <ul style="list-style-type: none"> - 정보 매체의 물리적 특성을 고려한 차세대 컴퓨팅 기술의 발전 - 양자 컴퓨터는 10~15년 내에 가시적 개발 성과가 예상됨

	<ul style="list-style-type: none"> - 소인수 분해, 이산로그 기반 암호의 안전성은 모두 파괴됨 - RSA(소인수분해), Diffie-Hellman(이산로그)과 같은 대부분의 공개키 알고리즘은 양자 알고리즘에 의해 안전성이 파괴됨. - 양자암호 또는 post-양자암호와 같은 차세대 컴퓨팅기술에 대해 안전성을 보장할 수 있는 기법을 개발해야 함. - 대체 암호 기술 개발 불가피 <p>무조건적 안전성을 보장하는 양자 암호 통신</p> <ul style="list-style-type: none"> - 대칭키를 깨는 알고리즘은 알려지지 않음 -> QKD를 통한 완벽한 대칭키 암호체계 구축 - QKD를 이용한 안전성이 보장된 암호 통신 가능 - 유무선 네트워크 상에서의 비밀키 생성/분배가 가능
--	---

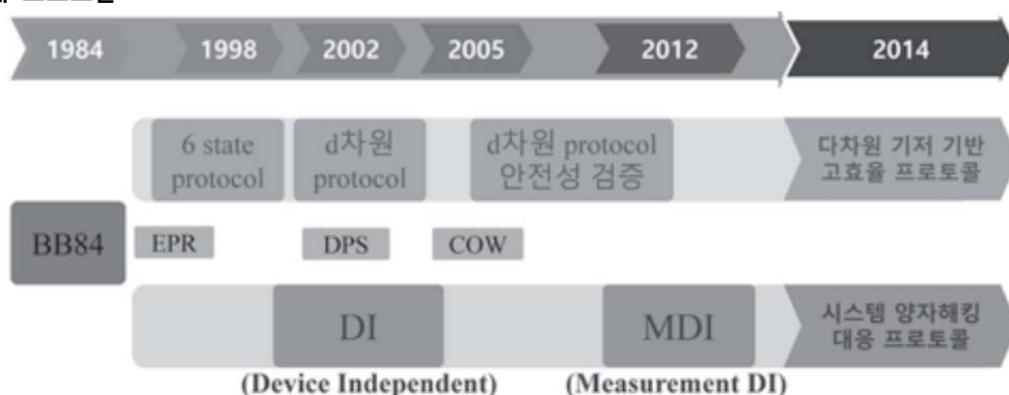
III. 양자암호 주요 기술

가. 양자키 분배

- 양자암호통신을 이용한 안전한 보안통신의 핵심 기술은 비밀키를 실시간으로 통신상에서 안전하게 분배하는 기술이다.
- 비밀키를 양자의 특성을 이용하여 안전하게 분배하는 것을 양자키 분배라 하는데 크게 프로토콜 부분과 시스템 하드웨어 부분으로 구분할 수 있다.



나. 양자키 분배 프로토콜



❖BB84: The protocol that presented by Charles Bennett & Gilles Brassard

❖EPR: The protocol that presented by Einstein, Podolsky and Rosen

❖DPS: Differential Phase Shift protocol

❖COW: Coherent One-Way protocol

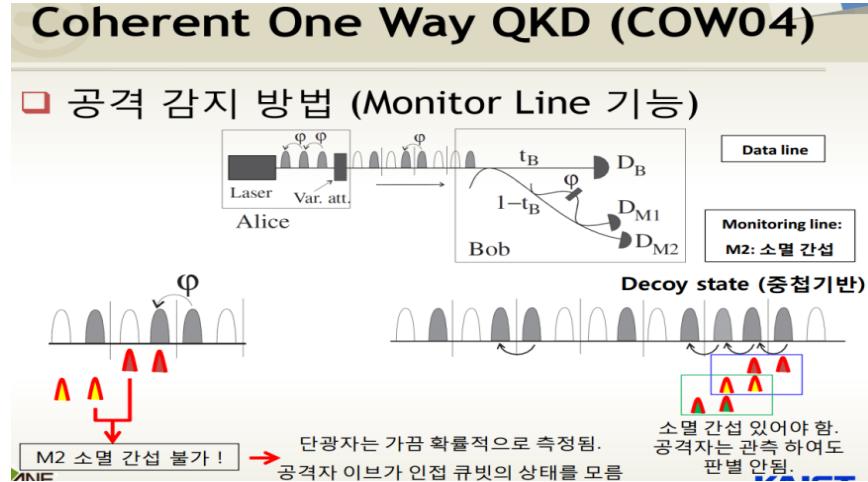
그림 5. 고효율 프로토콜의 발전 방향

- 양자키 분배 프로토콜은 1984년 BB84 프로토콜이 처음 제안된 이후로 다양한 프로토콜이 제안되어 왔다.
- 그림에 나타난 것처럼 다차원 기저 기반 고효율 프로토콜과 시스템 양자해킹 대응 프로토콜이 제시되고 있다.
- 그러나 아직까지도 BB84 프로토콜은 안전성 면과 구현가능성 면에서 가장 강력한 프로토콜로 대부분의 실제 시스템에 채용되고 있다.

다. 양자키 분배 시스템 하드웨어로 구현하는 방법

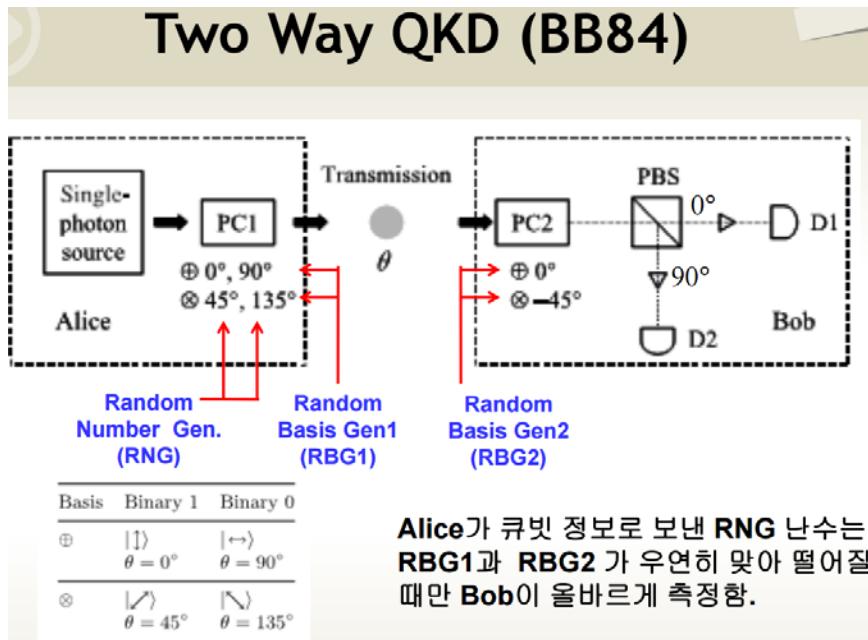
- One way 방식

- 고속 동작의 장점이 있지만 환경변화에 따른 시스템 동작의 안정성 측면에서 단점을 갖는다.



- Two way 방식(Plug and play 방식)

- 비밀키 분배 속도에서는 단점이 있을지라도 시스템의 안정적인 동작에는 매우 유리한 방법이다.



IV. BB84 프로토콜 동작 순서 및 시스템 구조

가. BB84 프로토콜 동작 순서

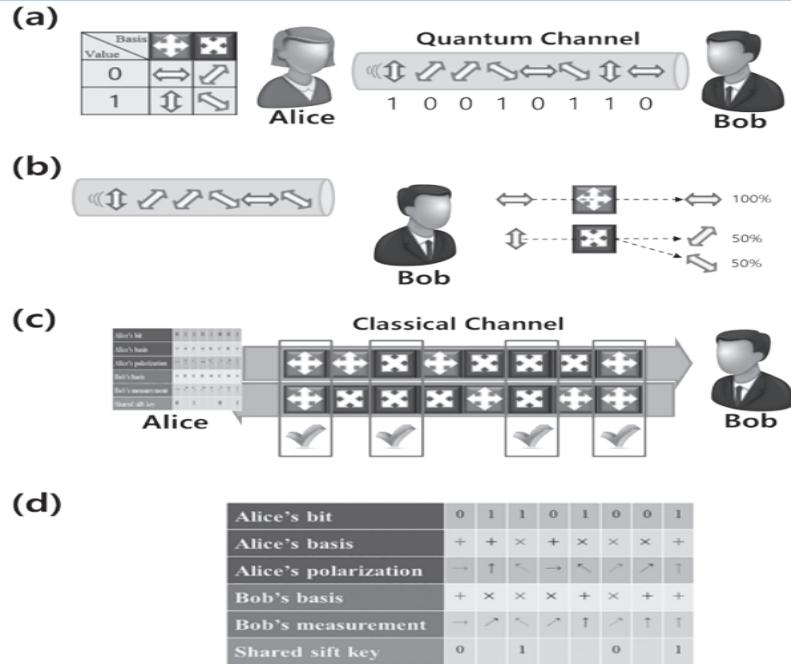
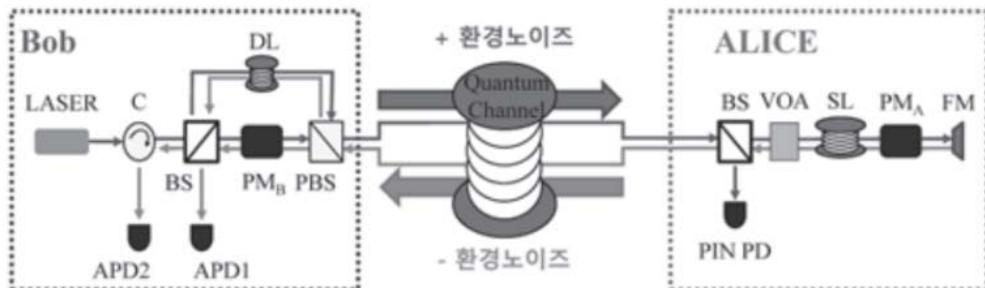


그림 6. BB84 프로토콜

- 양자의 한 종류인 단일광자를 이용하여 양자키 분배를 구현하고 단일광자의 편광을 비밀키 전송을 위한 변조 수단으로 사용한다고 할 때 (a)와 같이 송신자 Alice는 랜덤한 편광을 가진 단일광자를 수신자 Bob에게 전송
- Alice와 Bob은 수직·수평기저에서 편광 $0^\circ, 90^\circ$ 를 각각 Bit 0과 1로 약속하고, 대각기저에서는 편광 $45^\circ, 135^\circ$ 를 각각 Bit 0과 1로 약속했다고 가정한다.
- Bob은 (b)와 같이 도달한 모든 단일광자에 대해 편광 기저를 랜덤하게 선택하여 측정을 수행한다. 이때 단일광자의 편광과 편광 기저가 일치하는 경우, 100%의 확률로 편광상태를 정확하게 측정하게 된다. 만약 단일광자의 편광과 편광 기저가 다른 경우, 50%의 확률로 측정오류가 발생하게 된다.
- 이후 Alice와 Bob은 (c)와 같이 각자의 기저정보를 기준 통신망을 이용하여 공유한다.
- 최종적으로 (d)와 같이 Alice와 Bob의 편광 기저가 같은 경우에 측정된 결과만 비밀키 생성에 이용하는 것으로 프로토콜을 완성한다.

나. BB84 프로토콜 시스템 구조



C: optical circulator, BS : beamsplitter, DL: delay line, SL : storage line,
PM : phase modulator, PBS : polarizing beamsplitter,
PIN PD : multi photon detector, VOA : variable optical attenuator,
APD1 and APD2 : single photon detectors, FM : Faraday mirror,

그림 7. Plug and play QKD system

- 그림에서와 같이 먼저 수신부(Bob)에서 생성한 빛 신호가 송신부(Alice)에 도착하고 송신부에서는 비밀키 정보를 변조한 후 이를 단일광자 수준으로 빛 세기를 약화시켜 다시 수신부로 재전송한다. 이 과정에서 빛 신호는 환경 노이즈의 영향을 반대로 두 번 받기 때문에 자동 노이즈 보상이 이루어지게 된다. 따라서 비밀키 분배 속도에서는 단점이 있을지라도 시스템의 안정적인 동작에는 매우 유리한 방법이다.

V. 양자암호통신 기술의 국내 적용 사례 및 기술동향

가. 해외

- 현재 전세계적으로 양자암호에 대한 활발한 연구 활동이 이루어지고 있다.
해외 기술 선진국에서는 80년대부터 본격적인 연구가 시작되어 90년대 연구용 시제품이 개발되었고
2000년대 이후부터는 테스트 베드를 구축하여 실환경 성능 검증을 하고 이를 통한 상용화 단계에 도달했다.
특히 표1에 보여지는 양자정보통신 (양자암호통신, 양자컴퓨터, 양자소자 등을 포함) 기술정책을 통해
국가전략기술로서 양자 기술을 집중육성하고 이를 활용한 선진 양자암호통신 기술 확보에 주력하고 있다.

나. 국내

- 이에 반해 국내 양자정보통신 기술은 90년대부터 2000년대 중반까지 학계를 중심으로
양자기술 원천연구가 이루어졌고 2010년까지 출연(연) 중심의 양자암호통신 기초연구가 진행되었다.
2011년 SKT Quantum Lab.의 설립과 2012년 출연(연)최초의 양자기술 전문 연구센터인
KIST 나노양자정보 연구센터의 개소 및 퀀텀 포럼 창립 등 연구 여건이 개선되고는 있으나
아직까지는 선진국과의 기술격차를 좁히지 못하고 있다.
2013년 KIST가 세계 양자암호 학회인 Qcrypt에서 순수 국내 기술로 개발한
양자키 분배 시스템을 전시 및 발표하는 성과를 내었고
정부에서도 양자 기술의 체계적인 발전을 위한 중장기 전략을 기획하는 등
양자정보통신 분야 기술 선진국으로 도약하기 위한 기반이 다져지고 있다.

표 1. 해외의 양자암호기술동향

구분	주요 정책 동향
유럽	<ul style="list-style-type: none">• Qurope(Quantum Europe) 프로그램을 통해 유럽 양자정보통신 연구개발 로드맵을 제시하고 일관된 연구 수행• EU는 미래기술(FET, Future Emerging Technologies) 사업에 Quantum Simulation을 선정, 525억 투자• 영국은 2013년 Autumn Statement를 통해 양자기술 산업화에 2015년부터 5년간 4,800억 투자 발표
미국	<ul style="list-style-type: none">• 2008년 국가양자정보과학비전(A Federal Vision for Quantum Information Science) 발표 후 NSF, IARPA, DARPA 등을 통해 年1조 투자
러시아	<ul style="list-style-type: none">• 2010년 Russian Quantum Center를 설립하고 양자광학, 양자재료, 양자정보처리, 양자기술 등에 집중 투자
캐나다	<ul style="list-style-type: none">• 캘거리大, 워터루大, 토론토大 등에 양자정보통신학과를 설치, 미래 ICT 선도를 위한 인재 집중 양성• 워터루大 Quantum–Nano Center를 설립, 年500억 투자
중국	<ul style="list-style-type: none">• 中과학기술부(MOST)는 2012년부터 5년간 양자기술, 나노기술 등에 2,900억 투자
일본	<ul style="list-style-type: none">• FIRST 프로그램을 통해 양자정보처리(Quantum Information Processing)에 4년간 430억원 지원• Riken, CREST 등을 통해 양자정보통신에 年 220억원 지원• NICT는 2040년까지 기밀성이 보장된 사회를 위한 양자로드맵에 따른 기술 개발을 진행 중
싱가포르	<ul style="list-style-type: none">• 싱가포르국립대학을 통해 양자기술에 年1,300억 투자

VI. 양자키 분배 시스템 취약점

가. 광자분리공격

- 광자분리공격(Photon Number Splitting Attack, PNS Attack)은

현재 존재하는 단일광자 생성기(Single photon generator)의 불완정성을 이용하여 파괴하는 방법이다.
일반적으로 신호를 생성하면 하나의 광자만 생성되지 않고 수개의 광자가 동시에 생성되어 전송된다.
통신회선 중간에 반투명거울(Beam Splitter)을 설치하여 광신호의 일부를 분리해 낸 다음
측정하여 전송되는 신호가 무엇인지 알아내는 공격방법이다.

나. 맨-인더-미들-어택

- 맨-인더-미들-어택(Man-in-the-middle attack, MITM Attack)은 중간에 공격자가 중계소 행세를 하며
송신자와 수신자를 교란하는 방법이다.
송신자와 공격자 사이에 다른 키를 서로 공유하고,
공격자와 수신자 사이에 다른 키를 공유하며 중간에서 오가는 신호를 도청하는 방법이다.

다. 서비스 거부 공격

- 서비스 거부 공격(Denial of Service, DoS)은 통신선상에 과부하를 주어서
정상적인 통신을 하지 못하거나 하기 힘들게 만드는 것을 뜻한다.
제일 대표적인 서비스 거부 공격으로는 케이블의 물리적 절단이 있다.
그 외에도 퍼블릭 채널을 대상으로 하는 고전적인 서비스 거부 공격 등이 가능하다.

양자 암호 기술의 현재

	Commercial	Lab(2010)	Lab(2013)
System Clock	1MHz ~ 10MHz	500MHz ~ 2GHz	Over 2GHz
Protocols	Decoy QKD + Phase encoding Entanglement distribution	Decoy QKD DPS SARG04 Entanglement distribution	Entanglement Swapping + Quantum memory + Quantum error correction
Stability	More than 1~5 years	1 minute ~ 36 hours	A few seconds
QBER	2~4%	2~4%	2~4%
Distance	~ 50km (Metropolitan)	50km ~ 150 km (between cities)	Over 200km
Key Rate	1~100 kbps (OTP for 음성통신)	10Mbps (OTP for 음성통신)	

양자 암호 기술의 미래

● 양자 중계 기술

- 1000km 이상의 거리에서 QKD 구현
- 라우팅 기술을 통한 true network 구현

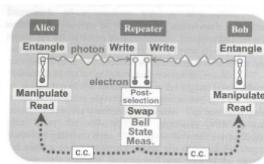


Fig. 1: Necessary functions for building a quantum repeater.

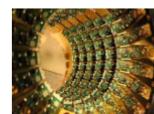
● 고효율/고속도 단일 광자 검출 기술

- QKD 시스템 key rate 향상
- QKD 시스템 clock speed 향상



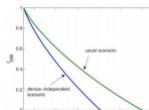
● 장시간 양자 메모리

- 현재 최고 lifetime : 수초 이내
- but, 급격한 성능 향상이 예상됨



● 안전성 증명 기법

- device-independent proof
- 부채널 공격에 대한 안전성 증명



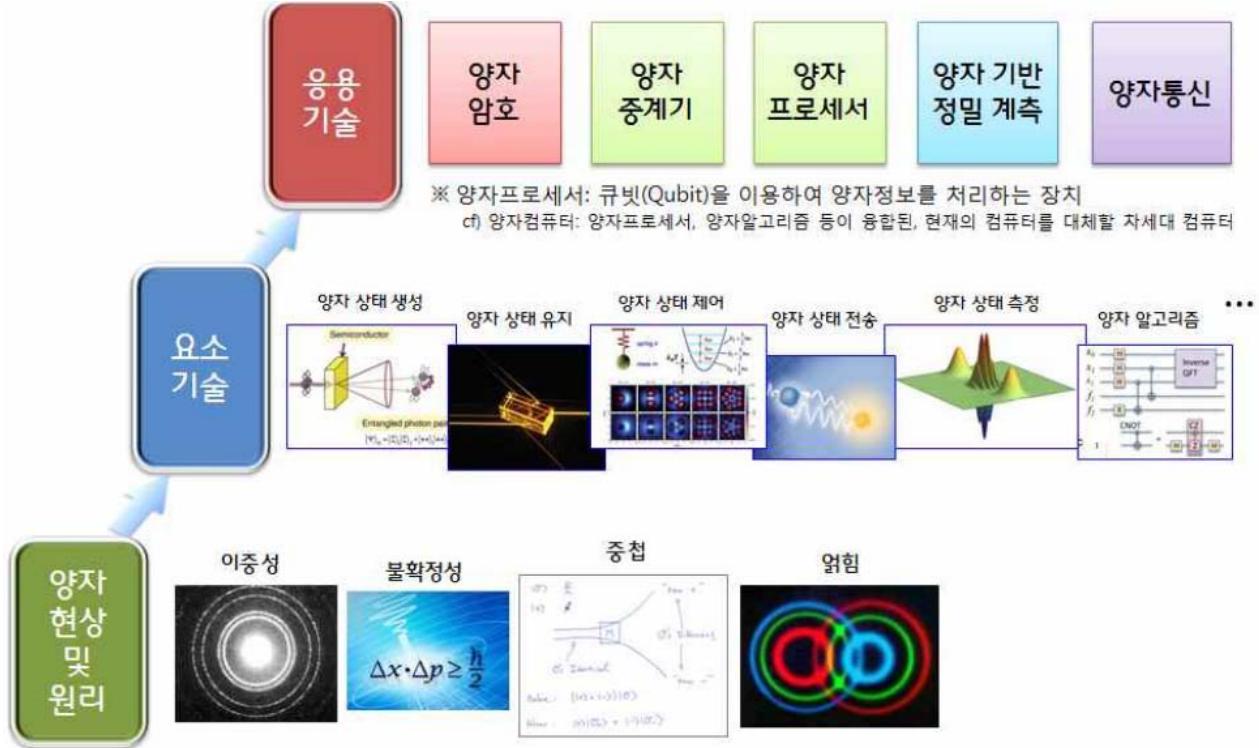
양자 암호 세계 연구 동향



국방정보보호컨퍼런스

10

[참고] 양자암호통신 시스템 구현을 위한 요소 기술



<그림9> 양자 응용 기술

- 양자암호통신 기술은 양자적 현상에 기반한 다양한 요소기술이 융합되어 개발되는 응용기술의 한 분야라고 할 수 있으며, 이러한 응용 기술에는 양자암호통신을 포함 하여 양자중계기, 양자프로세서 및 양자컴퓨터, 양자기반 정밀계측, 양자기반 초고속 통신 등이 있다.
- 이상과 같이 분류한 각각의 응용 기술은 서로 독립적인 기술이라기 보다는 다양한 요소기술을 공유하거나 상호보완적으로 활용되며,
- 양자의 이중성 불 확정성, 중첩 및 얹힘현상 등 양자역학적 원리와 현상에 바탕을 두고 있는 다양한 요소기술을 개념적으로 분류하면 양자 상태의 생성, 유지(저장), 제어, 전송, 측정을 위한 기술 및 양자알고리즘으로 나눌 수 있다.

<표2> 양자정보통신 기술 분류표

양자 암호 기술	양자 암호 프로토콜 개발 및 안전성 모델링 순수 난수 생성 (True Random Number Generation) 양자 신호 후처리 기술 고속 암호화 기술 양자 암호 응용 보안 서비스
양자 송수신 시스템	단일 광자 생성 및 검출 기술 양자 얹힘 생성 및 검출 기술 단일 광자 검출 소자 제작 기술 간섭계 제작 및 안정화 기술 연속변수(Continuous variable) 기반 양자 송수신 기술 자유공간 양자키분배 기술
양자 전송 제어 기술	양자 스위칭 기술 양자 가입자망 구현 기술 양자 네트워크 제어 및 관리 기술
양자 중계 기술	Ion trap 기반 양자 중계 기술 고순도 양자 얹힘 유지 (양자 메모리) 기술 양자 원격 전송 (Quantum teleportation) 초장거리 양자 중계 시스템 구현 기술 양자 정보 인터페이싱
양자 프로세서	양자 상태 생성 및 검출 양자 게이트 구현 기술 양자 프로세서 제어 프로그래밍 기술
양자 알고리즘	양자 계산 알고리즘 개발 및 최적화 양자 오류 수정
양자 정밀 계측 (Quantum Metrology)	양자 시계 (Quantum clock) 리소그래피 (Lithography) 초정밀 센싱 LIDAR (Light Detection And Ranging) 양자 이미징 (Quantum imaging) 양자 OCT (Optical Coherence Tomography)
양자 정보 응용 기술	Quantum simulator Quantum gaming Quantum auction

- 양자암호통신에서 요구되는 기술들을 절대적인 기준에 의해 서 분류하는 것은 무리가 있지만, 위에서처럼 비교적 큰 개념으로 보면, 양자 암호기술, 양자송수신기술, 양자전송네트워크기술, 양자인터넷기술, 양자중계기술, 양자프로세서구현기술, 양자알고리즘 등으로 분류할 수 있다
- 양자암호기술은 양자상태 송수신을 통하여 절대적인 안전성 확보, 비밀키 기반 고속암호화 및 이를 응용하는 기술을 포함하며, 양자암호 프로토콜 개발 및 안전성 모델링 기술, 순수 난수 생성(True random number generation) 기술, 양자신호 후처리 기술, 고속 암호화 기술, 양자암호 응용 보안서비스
- 양자송수신기술은 양자 상태의 중첩, 불확정성의 원리, 양자 복제 불가능성 등의 양자 역학적 특성을 이용하여 양자정보생성 및 검출하는 기술을 의미하며, 단일 광자 광원 기술, 양자 얹힘 생성 기술, 단일 광자 검출 기술, 연속변수 기반 양자 송수신 기술 등
- 양자전송네트워크기술은 양자기반의 점대점 통신을 다수의 양자 네트워크 통신으로 확장하기 위한 기술과 통신 채널을 유선 및 무선으로 확장하기 위한 기술을 의미하며, 양자 스위칭 및 라우팅 기술, 유선 양자 전송기술, 무선/자유공간 양자 전송 기술, 양자 가입자망 구현 기술, 양자 네트워크 제어 및 관리 기술 양자상태 멀티캐스팅 기술 등을 포함한다.
- 양자인터넷기술은 양자 상태의 저장 및 변환을 위한 기술을 포함하며, 기능성 양자노드 기술, 양자메모리 기술, 확정적 단일광자 생성 기술, 확정적 양자 얹힘 생성/제어/전송 기술, 이종 양자상태간 인터페이싱 기술, 양자파장 변환 기술, 비고전광 저장 및 재생 기술 등이 이에 해당한다.
- 양자중계기술은 물리적으로 한계가 있는 양자상태의 전송거리를 장거리로 확장하는 기술이며, 반도체 기반 양자 중계기술, 이온 포획 기반 양자 중계기술, 양자 메모리 기술, 양자 원격전송 기술, 장거리양자중계시스템 구현
- 양자프로세서구현기술은 양자비트(Qubit) 기반의 양자상태의 제어 및 양자 알고리즘 구현 등에 의한 정보처리 기술이며, 양자비트 구현 기술, 양자게이트 구현 기술, 양자프로세서 제어 프로그래밍(컴파일러) 기술 등을 포함한다.
- 양자알고리즘기술은 고전역학에 기반한 방법으로는 효율적인 계산이 불가능한 복잡한 문제를 양자역학적 원리를 이용하여 단시간 내에 처리하는 양자 계산 알고리즘과 계산 및 통신 과정의 오류를 수정하는 오류 수정 코딩을 포함하는 기술이며, 양자 알고리즘 기술, 양자 정보 분석 기술, 양자 오류 정정
- 이상 열거한 기술 외에도 단일광자, 얹힘광자의 양자적 상관관계 등을 이용하여 고전 계측기술로는 불가능한 초정밀 또는 초고감도 계측을 가능하게 하는 양자계측 기술에 포함되는 양자시계(Quantum clock) 기술, 양자 리소그래피(Lithography) 및 이미징 기술, 양자 트랜지스터, 양자 OCT(Optical coherence tomography) 기술 등과 양자역학의 원리에 의해 구현된 양자암호, 양자알고리즘, 양자상태 제어 등을 응용 및 확장하는 양자정보응용기술에 포함되는 양자 시뮬레이터 기술, 양자 gaming, 양자 auction, 양자 암호 응용 보안서비스 기술 등은 양자암호통신 기술의 발전과 밀접한 관계를 가지고 있다.

문 13) 양자암호 통신

답)

1. 양자 ~~부이~~ 이용한 암호화 통신. 양자암호 통신.

가. 양자 암호 통신의 장단

- 양자의 ~~암호~~ ~~교인~~ 특성을 이용 양자키를.

서버하고 이를 이용 비밀키를 대신 사용하여 비밀

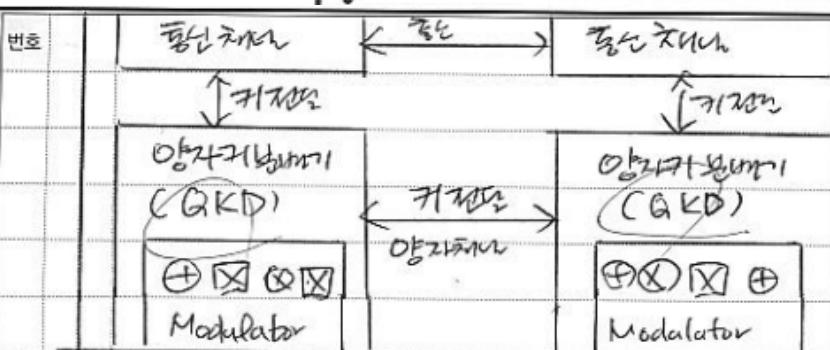
통신하는 암호화 통신 가능

나. 양자 암호 통신의 주요 원리.

① 양자역학	② 양자암호	③ 기본 암호화 원리
.	: 키교환	자료.

2. 양자암호로 통신의 원리 및 주요 기능

가. 양자암호로 통신의 원리



- 양자기장비에 의해 키교환

나. 양자 암호 통신의 주요 기능

구분	기능	제공 기능
양자	암호	전자간 암호화, 양자기장비
역학	교인	학률비판은 0, 1 상태.
Hw	QKD Modulator	양자기 사용하고 배포 제작 및 허용 양자기 것을

"설"

번호지 1) 양자 암호통신, 양자 성질, 구현도, 분야별
1쪽

1. 불확적성이 원리, 양자 암호통신 기초

정의	양자의 특성을 이용하여 기존 통신에 보안을 강화한 양자 역학 기반통신 기술		
이유	54 등장	개인정보보호	Legacy 보안 문제
“양자 암호통신과 전송 신뢰성 보장”			

2. 양자의 정질 설명

가	양자의 자연 법칙으로 설명		
개연	광자, 전자, 이온, 원자 등과 같은 자기 현상을 구현하는 물체의 회선 단위		
주요성질	“불확정성”, “양자증립”, “양자암호”		

3. 양자의 성질 상세 설명

성질	설명	특징
불확정성	입자의 상태는 뻔한	복잡
양자증립	0과 1의 동시성	보안성
양자암호	거리의 상관관계	신뢰성
- 양자의 성질을 이용한 양자 암호통신 구현		

2쪽

번호지 2) 양자 암호통신 구현도 설명
2쪽

가 양자 암호통신 구현도

〈송신부〉 ① public channel → 〈수신부〉

- ① public channel : 라이터 전송 및 보안

- ② OKD (Quantum Key Distribution) : 키 분배

나 양자 암호통신 구현 구현요소

항목	설명	핵심 기능
OKD	• 키 분배 처리 • 양자 단위 키 분배 가능	• 신호 고환 • 신뢰성 보장
BB84	• 양자 단위 키 분배 • 전송 프로토콜 가능	• 토글화 • 응수인 기능
현장/원자	• 전송 위치, 양자기기 • 전송 최단 단위	• 흐름을 • 신뢰성 보장
PKI/PKM (폐밀)	• 라이터 단위 기준 • 전송 라이터 고관	• 공공망 이용 • 별별 수령

	양자기 분배 방식 설명									
가)	양자기 분배 방식 개념도,									
(토)	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td></td><td>X</td><td>+</td></tr> <tr> <td>수직</td><td>0</td><td>1</td></tr> <tr> <td>수평</td><td>1</td><td>0</td></tr> </table> ↗ "수직/수평가지." ↗ $\frac{\text{수직}}{\text{수평}}$ 대각가지 		X	+	수직	0	1	수평	1	0
	X	+								
수직	0	1								
수평	1	0								
-	수직 수평 가지와 (90° , 360°) 대각 (45° , 135°)									
2)	양자기 분배 방식 상식 설명,									
	$0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1$ 송신: / / - - \ \ / Alice 수신: \ / - - / \ / Bob $/ \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1$									
	→ 송수신 키 분배. 수평/수직 가지가 다른 ① ② ③ ④ 같은 지역인 키 구성									
-	양자 키 (key) 분배에 의한 송수신 가능 "길"									