<2002 ICU 한국정보통신교육원 지원 -
무선인터넷 및 통신 s/w 전문인력 양성사업:
유·무선인터넷 통합기술과정 -제3강의>

유•무선 인터넷 보안

동서대학교
인터넷공학부 정보네트워크전공
이 훈 재
http://cg.dongseo.ac.kr/~hjlee
E-mail=hjlee@dongseo.ac.kr

목 차

제1부. 정보보안 소개[1-4][8]
1. 정보보안 개요
2. A5와 LILI 스트림 암호
3. DES, IDEA와 AES 블록 암호
4. RSA와 ECC 공개키 암호

제2부. 유무선 인터넷보안[5-7]
5. 인터넷 보안[5]
6. 무선 인터넷 보안

References

1. B. Schneier, ***Applid Cryptography (2nd Ed.),*** John Wiley & Sons, Inc., 1995.
2. A. Menezes, ***Handbook of Applied Cryptography***, CRC Press, 1997.
3. D. Stinson, ***Cryptography – Theory and Practice (2nd Ed.),*** CRC Press, 2002.
4. William Stalling, ***Cryptography and Network Security (2nd Ed.)***, Prentice-Hall, Inc., 1999
5. 박창섭, ***암호이론과 보안***, 대영사, 1999
6. 최용락외, ***컴퓨터 통신 보안***, 도서출판 그린, 2001
7. 이만영외, ***전자상거래 보안기술***, 생능출판사, 1999.
8. 한국정보보호진흥원(KISA) 홈페이지 http://www.kisa.or,kr

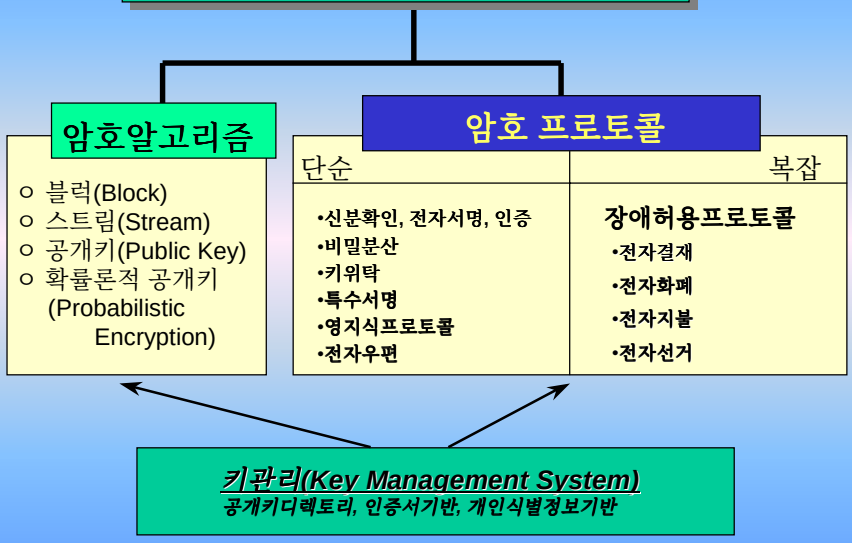
1. 정보보안 개요

암호의 역사

- 기원전 이집트 상형문자, 시저 암호
- 1800. Vigenere cipher
- 1918. Vernam cipher = one-time pad
- 1917. Rotor Machine
- 1920. Enigma Machine, Hegelin Machine
- 1948. C.E.Shannon, “Secrecy System 이론” 정립
- 1970. Europe, “Stream Cipher” 설계/응용
- 1970. Fiestel, “LUCIFER”
- 1975. IBM, “DES”
- 1976. Diffie & Hellman, “Public-Key Cryptosystems”
- 1978. Rivest, Shamir & Adleman, “RSA”
- 1980-90 A5, RC4, skipjack, AES(Rijndael), ECC 등

1. 정보보안 개요

암호학 (Cryptology) 연구 범위



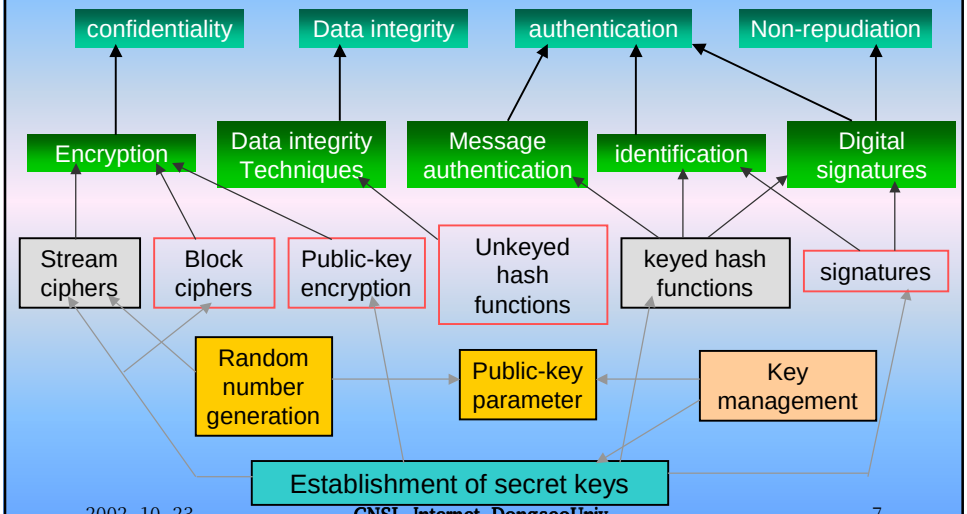
1. 정보보안 개요

암호 프로토콜 응용 서비스 예

기밀성(confidentiality)	1. 소극적 공격으로 부터 전송자료를 보호 2. 트래픽 흐름분석에 대한 보호
인증(authentication)	통신의 신뢰성을 갖도록 보증함(송.수신 인증 등)
무결성(data integrity)	메시지 자체의 신뢰성을 보증함
부인 봉쇄(notorization)	송신자와 수신자의 메시지 송.수신 사실을 부정하지 못하도록 함
접근제어 (access control)	1. 시스템내의 자료의 액세스를 제어 2. 통신링크를 통한 원격 액세스 제어
가용성(availability)	정당한 사용자의 시스템 사용 요구시 사용할 수 있어야 함

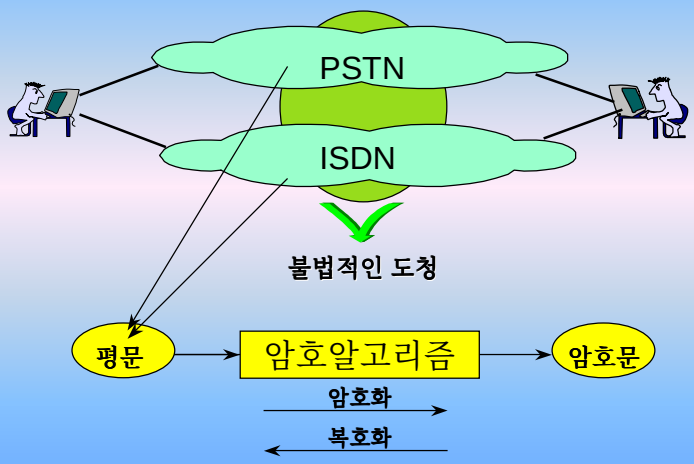
1. 정보보안 개요

암호학 (Cryptology) 연구 범위



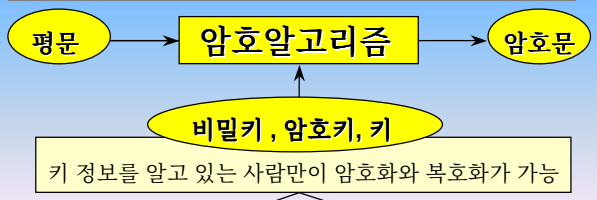
1. 정보보안 개요

암호 알고리즘 (Encryption)



1. 정보보안 개요

암호 알고리즘 (Encryption)



키 정보를 알고 있는 사람만이 암호화와 복호화가 가능

관용키(CONVENTIONAL)
=비밀키(Secret-key)
=대칭키(Symmetric-key)

암호화키 = 복호화키

- 블록암호: **DES** , SKIPJACK , **IDEA , AES, SEED**
- 스트림암호: **A5, LILI**, f8, RC4

공개키(PUBLIC KEY)
=비대칭키(Asymmetric-key)

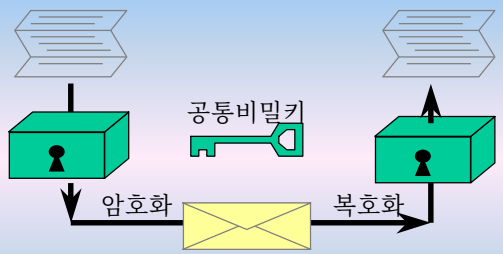
암호화키 ≠ 복호화키

RSA , ElGamal, **ECC**

1. 정보보안 개요

대칭키 암호 (Symmetric)

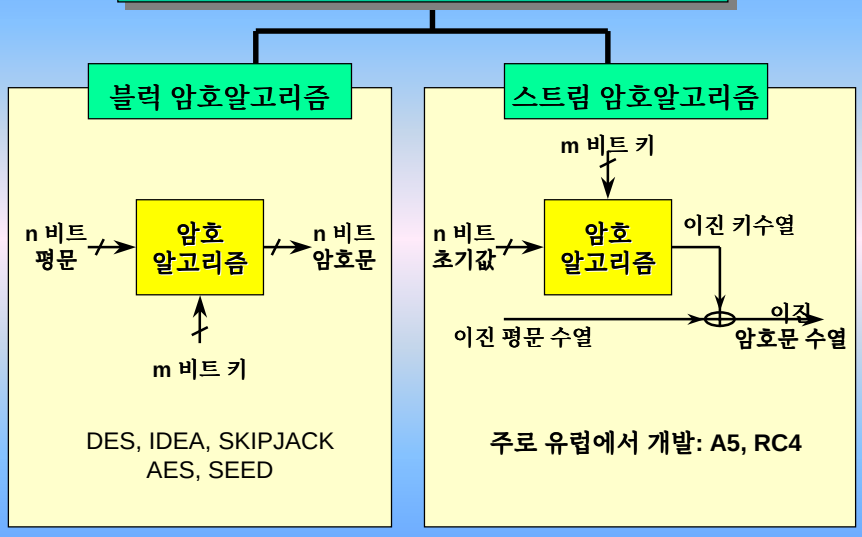
대칭키 암호시스템(관용암호, 비밀키 암호)



- 특징 : 암호화키와 복호화키가 동일
- 장점 : 암호화 및 복호화 속도가 빠름
- 단점 : 키관리의 어려움. 키분배의 문제. 다양한 응용의 어려움
- 사례 : DES, FEAL, IDEA, Skipjack, AES, SEED 등

1. 정보보안 개요

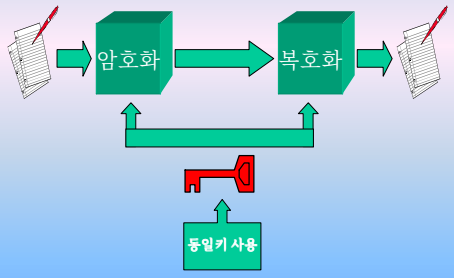
대칭키 암호 알고리즘 형태



1. 정보보안 개요

대칭키 암호 특징

- Confusion(Substitution), Diffusion(Transposition)으로 구성



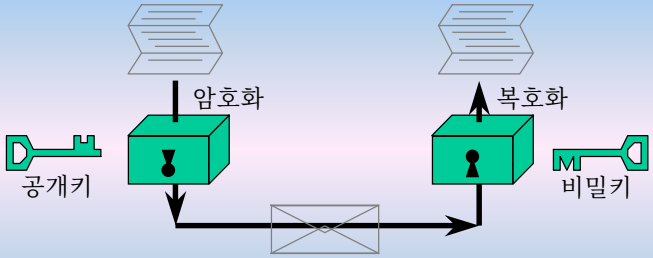
대칭키 알고리즘의 특징

암호키와의 관계	암호키=복호키
암호화키	비밀
복호화키	비밀
비밀키의 전송	필요
비밀키의 관리	문제점
암호화의 속도	빠르다

1. 정보보안 개요

비대칭키 암호 (Asymmetric)

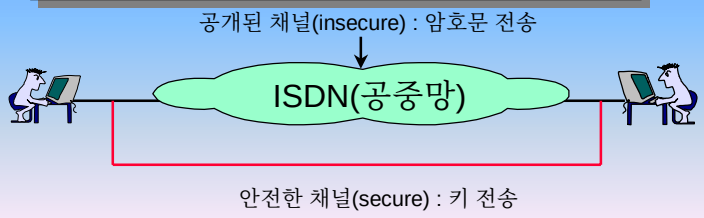
비대칭형 암호시스템(공개키 암호)



- 특징 : 복호화키(=비밀키)와 암호화키(=공개키)가 다름
- 장점 : 키관리가 용이. 다양한 응용이 가능. 안전성이 뛰어남
- 단점 : 암호화 및 복호화 속도가 느림
- 사례 : RSA 등

1. 정보보안 개요

비대칭키 암호 (Asymmetric)

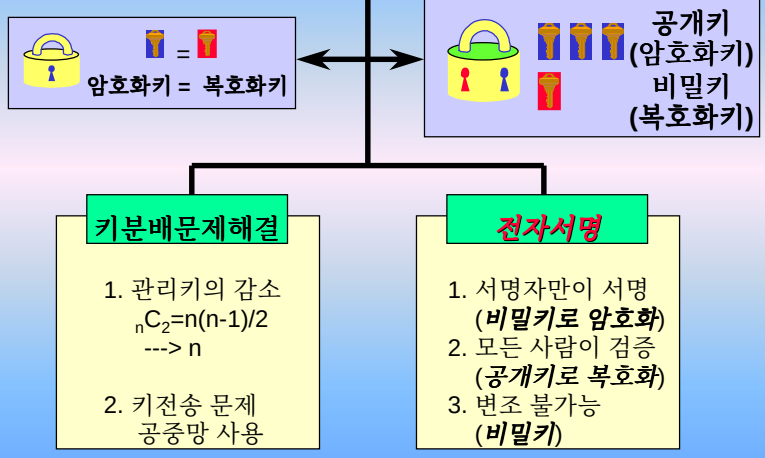


키분배문제

키 전송을 위한 안전한 채널이 필요
(현실적으로 어떻게 안전한 채널을 구성하는가?)
---> 1. 인편 : 시간 문제 , 2. 복잡한 키관리

1. 정보보안 개요

공개키 암호 개념 및 응용



키분배문제해결

1. 관리키의 감소
   ${}_nC_2 = n(n-1)/2$
   ---> n
2. 키전송 문제
   공중망 사용

전자서명

1. 서명자만이 서명
   (***비밀키로 암호화***)
2. 모든 사람이 검증
   (***공개키로 복호화***)
3. 변조 불가능
   (***비밀키***)

1. 정보보안 개요

공개키 암호와 서명

RSA	
Composite $n = p \cdot q$	Factorization problem
1024bits	Most Popular

KCDSA	
Prime p	Discrete logarithm problem
1024bits	국내표준

Elliptic curve family	
Elliptic curve group over F_p	ECDL problem
160bits	최근 활발한 연구

1. 정보보안 개요

해쉬 함수 (Hash Function)

임의의 길이를 가지는 문서

해쉬함수

고정된 길이를 가지는 문서

Dyejsmldmnf
mdfnmd,sdd
fnfnfnlkfekkfe
ekfkjefjefelfee

해 쉬 함 수

- 특징: 일방향(one -way) 함수, 메시지 압축
- 용도: 디지털서명, 메시지 무결성
- 알고리즘: SHA -1, MD5 등

1. 정보보안 개요

해쉬 함수 (Hash Function)

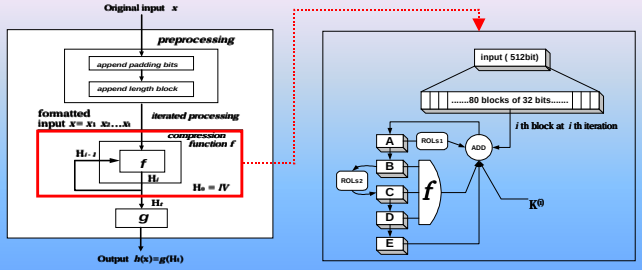
➢HAS(Hash Algorithm Standard) -160

✓1998년 TTA에 의해 국내 암호학적 해쉬함수의 표준으로 제정

✓임의의 메시지블록을 160비트 해쉬코드로 변형

✓SHA와 유사(메시지확장의 차이)

❑ **HAS-160의 구조**



1. 정보보안 개요

암호 알고리즘에 따른 안전한 키 길이

❑ 암호키의 크기를 연도별로 요약.

출처) A.K. Lenstra & E.R.Verheul, “Selecting Cryptographic Key Sizes” , PKC2000, Jan, 2000

연도	대칭키	RSA/DH	Subgroup	Elliptic Curve	MIPS Year	H/W cost
2000	70	952	125	132	7.13×10^{9}	1.39×10^{8}
2005	74	1149	131	147	1.02×10^{11}	1.96×10^{8}
2010	78	1369	138	160	1.45×10^{12}	2.77×10^{8}
2020	86	1881	151	188	2.94×10^{14}	5.55×10^{8}

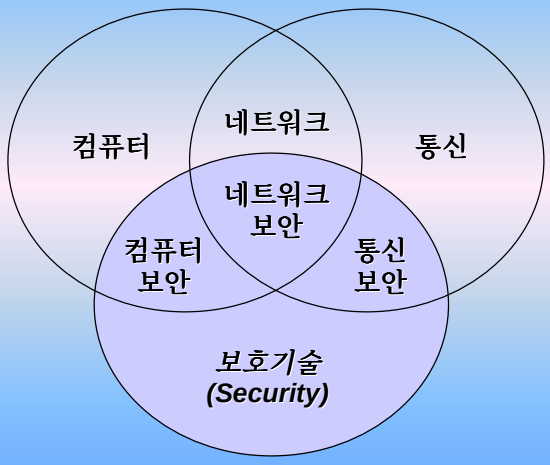
1. 정보보안 개요

관용키 시스템과 공개키 시스템의 비교

	관용키 방식 (대칭키)	공개키 방식 (비대칭키)
암호키의 관계	암호키=복호키	암호키≠복호키
암호화 키	비밀	공개
복호화 키	비밀	비밀
비밀키의 전송	필요	불필요
비밀키의 보호 유지수	많음	적다
안전한 인증	곤란	용이함
암호화 속도	빠르다	늦다

1. 정보보안 개요

정보보호와 암호기술



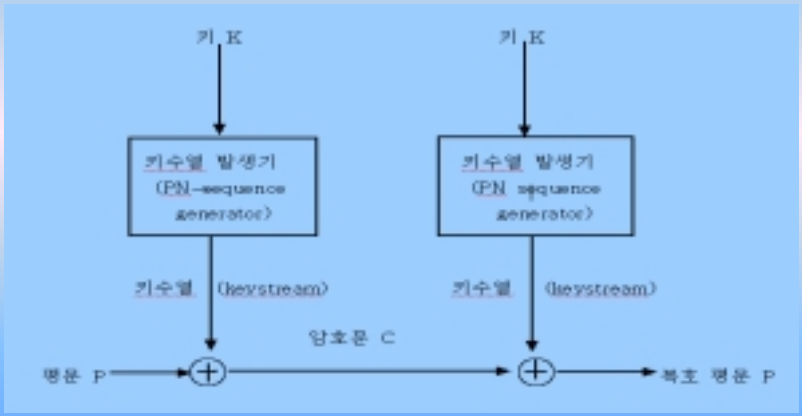
2. A5와 LILI 스트림 암호

스트림 암호의 정의

이진화된 평문과 이진 키 수열의 배타적 논리합(XOR) 연산을 실행하여 암호문을 생성하는 알고리즘을 말하며, 이 때 출력 키 수열에 대한 특성과 발생방법이 안전도에 직접적인 영향을 미친다.

2. A5와 LILI 스트림 암호

스트림 암호의 정의



2. A5와 LILI 스트림 암호

스트림 암호 특징

- 에러 확산이 없음.
- 비도 수준에 대한 수학적 정량화가 가능.
- 하드웨어 구현이 용이.
- 통신 지연이 없음.
- 고속 통신이 가능함.
- 키수열 발생기에 대한 암호학적 안전성
- 통신 채널 환경에 적합한 키 수열 동기 방식 성능(통신 신뢰성)
- 암호화 속도 등에 대한 성능 분석

2. A5와 LILI 스트림 암호

스트림 암호 비도(안전성) 요구사항

- Beker, Siegenthaler와 Golic 제시

① 주기(Period): 출력 키 수열은 주기에 대한 최소값이 보장되어야 한다.

② 랜덤 특성(Randomness): 출력 키 수열은 좋은 랜덤 특성을 갖어야 한다.

② 선형 복잡도(Liner complexity): 출력 키 수열은 큰 선형 복잡도를 갖어야 한다.

④ 상관 면역도(Correlation immunity): 출력 키 수열은 높은 상관 면역도를 갖는다.

⑤ 키 수열 사이클 수(Keystream cycle): 출력 키 수열은 1개 이상의 키 수열 사이클에서 발생되어야 한다

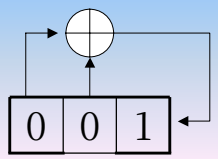
2. A5와 LILI 스트림 암호

LFSR 기반의 스트림 암호

- 선형 귀환 쉬프트 레지스터(LFSR,liner feedback shift register)란?
  - 선형 궤한 쉬프트 레지스터(LFSR)은 순서 이진 비트 생성을 위한 기계이다. 레지스터는 대부분 비밀키인 초기 벡터에 의해 결정되는 기억소자의 나열로 구성된다. 레지스터의 동작은 시계와 각 시간이 넘어가는 순간에 규칙적을 동작한다. 레지스터의 기억소자의 내용은 하나씩 오른쪽으로 이동한다. 그리고 기억소자 내용의 작은부분의 XOR는 가장 왼편의 소자에서 이루어진다. 출력의 한비트는 일반적으로 이 위의 과정동안 얻어 진다.

2. A5와 LILI 스트림 암호

LFSR 의 동작원리



0 0 1
0 1 0 = (0 ⊕ 0)
1 0 1 = (0 ⊕ 1)
0 1 1 = (1 0)
1 1 1 = (0 1)
1 1 0 = (1 1)
1 0 0 = (1 1)
0 0 1 = (1 0)
0 1 0 = (0 0)
1 0 1 = (0 1)
0 1 1 = (1 0)
1 1 1 = (0 1)
1 1 0 = (1 1)
1 0 0 = (1 1)

주기 = 2^{3-1}
= 7

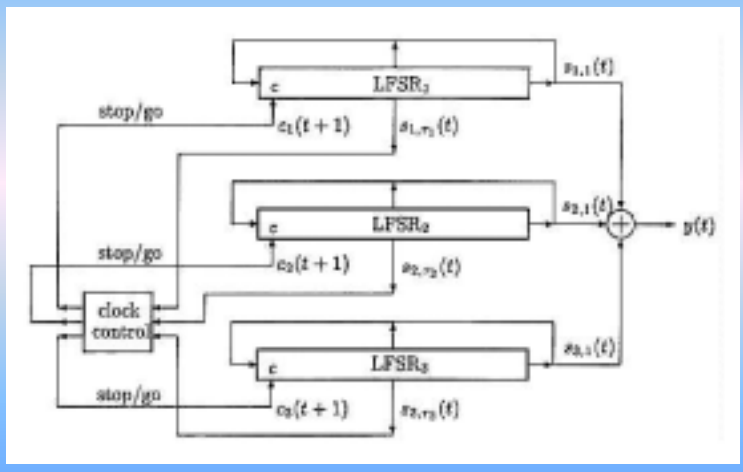
2. A5와 LILI 스트림 암호

A5 스트림 암호 (A5 Stream cipher)

- A5 스트림 암호
  - 유럽 GSM 무선 데이터 보호 표준
- 구성
  - 3개의 레지스트(각각의 길이 19, 22, 23)
  - Clock Control
  - 4개의 XOR 게이트
  - Majority Function

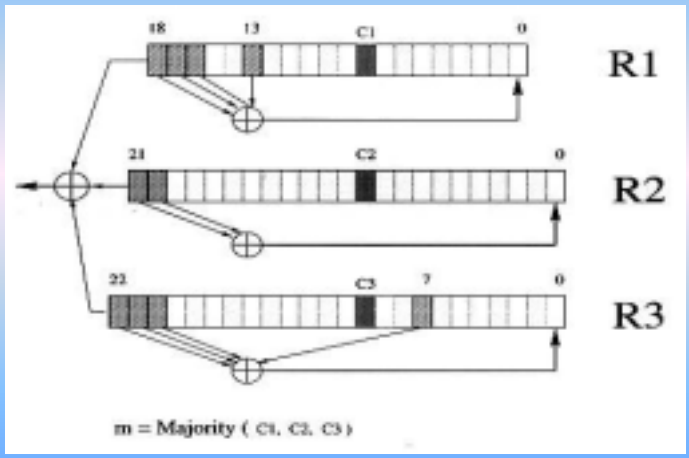
2. A5와 LILI 스트림 암호

A5 스트림 암호



2. A5와 LILI 스트림 암호

A5 스트림 암호

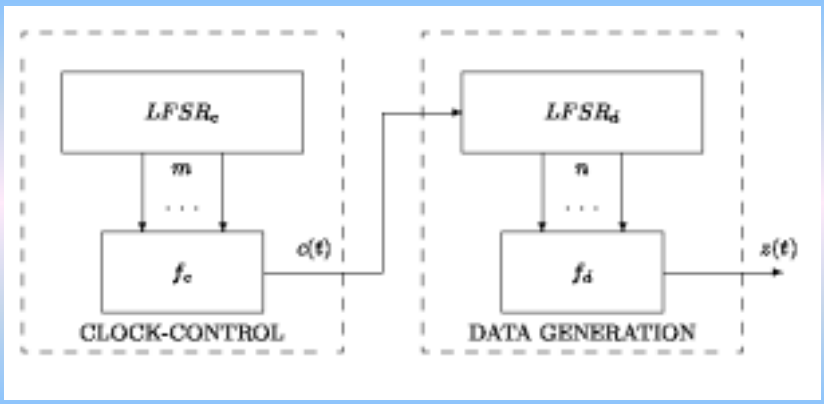


2. A5와 LILI -II 스트림 암호

- LILI -II Stream Cipher
  - ACISP'2002 proposed
  - Hoonjae Lee (Dongseo Univ.)
  - Sangjae Moon(Kyungpook Nat'l Univ.)
  - A. Clark, E.Dawson, J. Fuller, J.Golic, W. Millan and L. Simpson (QUT -ISRC, Austallia)
  - 255 -bit key size (internal memory)
  - Strong to Time -Memory Tradeoff Attack

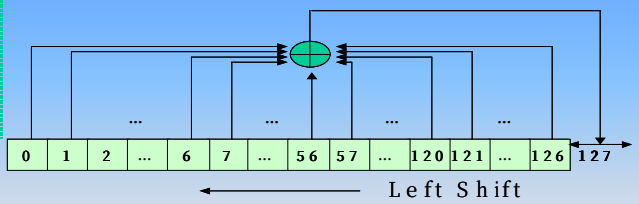
2. A5와 LILI -II 스트림 암호

- LILI -II Keystream Generator



2. A5와 LILI-II 스트림암호

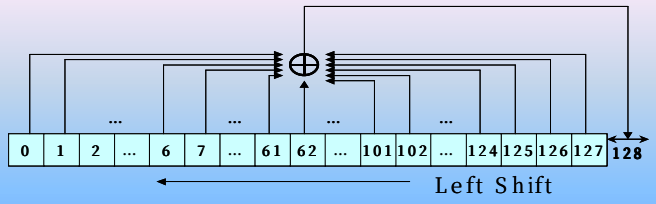
(1) LFSRc (127)



(2) Clock-Controlled Function fc

fc(x0,x126) = 2(x0) + x126 + 1

(3) LFSRd (128)



(4) Data Generation Function fd

LFSRd positions (0,1,3,7,12,20,30,44,65,80,96,122)

2. A5와 LILI-II 스트림 암호

- Primitive Polynomial of $LFSR_c$

$$x^{128}+x^{126}+x^{125}+x^{124}+x^{123}+x^{122}+x^{119}+x^{117}+x^{115}+x^{111}+x^{108}$$
$$+x^{106}+x^{105}+x^{104}+x^{103}+x^{102}+x^{96}+x^{94}+x^{90}+x^{87}+x^{83}+x^{81}$$
$$+x^{80}+x^{79}+x^{77}+x^{74}+x^{73}+x^{72}+x^{71}+x^{70}+x^{67}+x^{66}+x^{65}+x^{61}$$
$$+x^{60}+x^{58}+x^{57}+x^{56}+x^{55}+x^{53}+x^{52}+x^{51}+x^{50}+x^{49}+x^{47}+x^{44}$$
$$+x^{43}+x^{40}+x^{39}+x^{36}+x^{35}+x^{30}+x^{29}+x^{25}+x^{23}+x^{18}+x^{17}+x^{16}$$
$$+x^{15}+x^{14}+x^{11}+x^{9}+x^{8}+x^{7}+x^{6}+x^{1}+1$$

- Clock-Controlled Function f_c

$$f_c(x_0, x_{126}) = 2(x_0) + x_{126} + 1.$$

2. A5와 LILI -II 스트림 암호

- Primitive Polynomial of $LFSR_d$

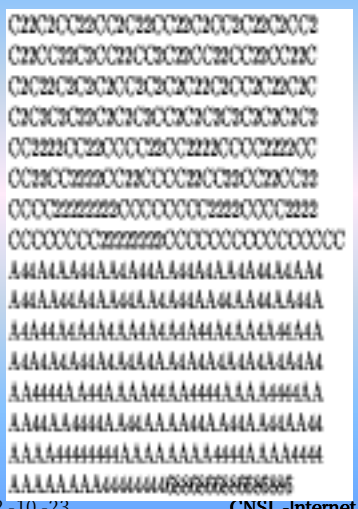
$$x^{127}+x^{121}+x^{120}+x^{114}+x^{107}+x^{106}+x^{103}+x^{101}+x^{97}+x^{96}+x^{94}$$
$$+x^{92}+x^{89}+x^{87}+x^{84}+x^{83}+x^{81}+x^{76}+x^{75}+x^{74}+x^{72}+x^{69}+x^{68}$$
$$+x^{65}+x^{64}+x^{62}+x^{59}+x^{57}+x^{56}+x^{54}+x^{52}+x^{50}+x^{48}+x^{46}+x^{45}$$
$$+x^{43}+x^{40}+x^{39}+x^{37}+x^{36}+x^{35}+x^{30}+x^{29}+x^{28}+x^{27}+x^{25}+x^{23}$$
$$+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{14}+x^{10}+x^{8}+x^{7}+x^{6}+x^{4}+x^{3}+x^{2}+x+1$$

- Data Generation Function f_d

$LFSR_d$ positions {0, 1, 3, 7, 12, 20, 30, 44, 65, 80, 96, 122}

2. A5와 LILI -II 스트림 암호

- $LFSR_d$ and f_d



2. A5와 LILI -II 스트림 암호

❑ Cryptographic Properties

The Boolean Function has 12 inputs and these properties:
Balanced, CI(1), Order=10, Nonlinearity=1992, No Linear Structures.

3. DES, IDEA와 AES 블록 암호

DES의 역사

- 1973년 다음 전제 조건을 전제로 표준 알고리즘을 공모
  1. 표준 암호 알고리즘은 높은 수준의 안전성을 보장할 수 있어야 한다.
  2. 표준 암호 알고리즘은 사양의 정의가 완전하여 간단히 이해할 수 있어야 한다.
  3. 표준 암호 알고리즘이 제공하는 안전성 알고리즘의 비밀성에 의존되어서는 안 된다.
  4. 표준 암호 알고리즘은 사용자나 제작자가 모두 사용 가능해야 한다.
  5. 표준 알고리즘의 응용이 다양해야 한다.
  6. 표준 암호 알고리즘은 전자 장치로써 제품화가 간단하고 또한, 사용이 간단해야 한다.
  7. 알고리즘의 타당성 검증에 협력해야 한다.
- 1974년 8월 2차 공모
  Water Tuchman과 Carl Meyer가 lucifer cipher를 개량한 암호 알고리즘이 위의 조건이 만족되어 표준 암호 알고리즘으로 검토되기 시작
- 1977년 1월 15일 정식 등록
- DES는 5년마다 안전성을 검토
- ANSI의 표준으로 지정되어 순수 민간용으로 사용하고 있음

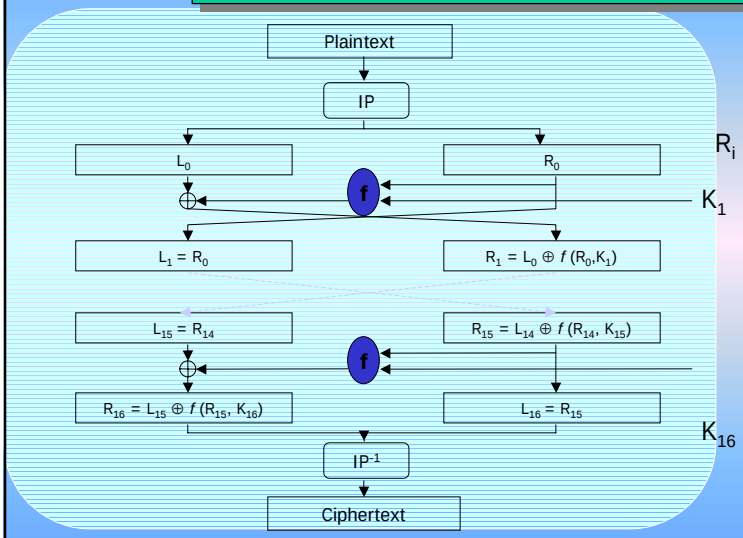
3. DES, IDEA와 AES 블록 암호

DES의 기본 개념

- DES는 64비트의 키를 적용하여 64비트의 평문을 64비트의 암호문으로 암호화 시키는 대칭형 블록 암호기법
- 대체(substitution)과 치환(permutation)이라는 2개의 기본적인 암호화 함수가 반복적으로 16회 적용
  1. 혼돈(confusion) : 평문 1비트의 변화가 암호문에 어떤 변화를 초래할지를 예측할 수 없는 성질
  2. 확산(diffusion) : 평문을 구성하는 각각의 비트들의 정보가 여러 개의 암호문 비트들에 분산되어야 한다는 성질
- DES에서는 대체는 체계적으로 어떤 비트들의 유형을 다른 비트들로 전환함으로써 혼돈 성질을 제공하고, 반면에 치환은 비트들의 순서를 재배열함으로써 효과를 띄게 한다.

3. DES, IDEA와 AES 블록 암호

DES 내부 구조



$L_i = R_i\text{-}1$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

3. DES, IDEA와 AES 블록 암호

DES 내부 구조

❑ IP(Initial Permutation)

평 문

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	19	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}

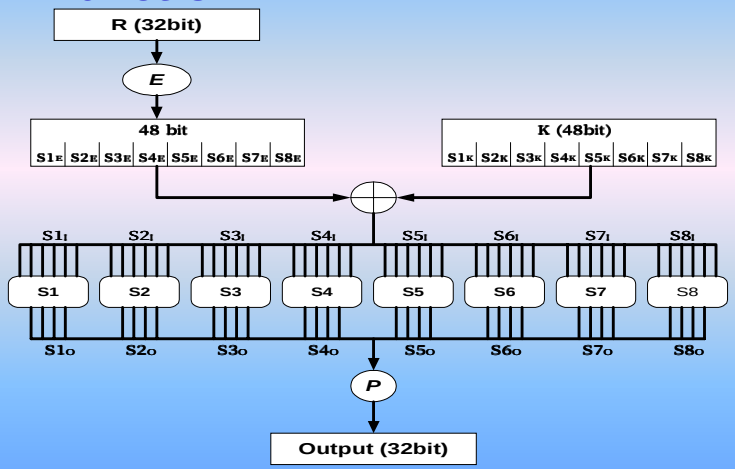
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

- IP
  58번째 비트 -> 1번째 비트 / 50번째 비트 -> 2번째 비트
- IP^{-1}
  1번째 비트 -> 58번째 비트 / 2번째 비트 -> 50번째 비트

3. DES, IDEA와 AES 블록 암호

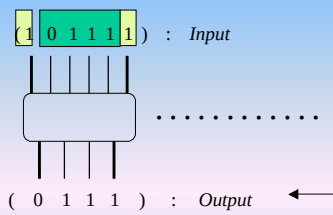
DES 내부 구조

❑ *f* Function



3. DES, IDEA와 AES 블록 암호

DES S-BOX 원리



$11_{(2)}$ =3rd ROW

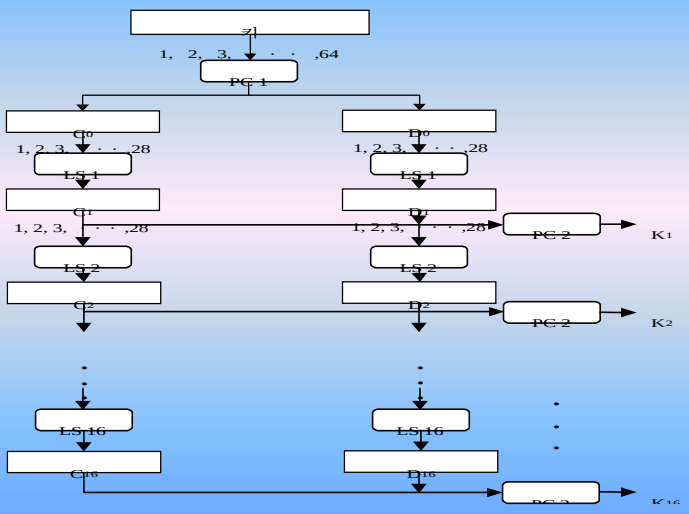
$0111_{(2)}$ = 7TH COLUMN

S1 box

ROW	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

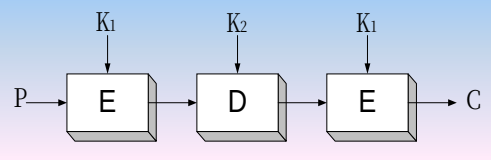
3. DES, IDEA와 AES 블록 암호

DES 키 스케쥴링



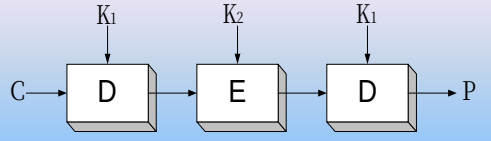
3. DES, IDEA와 AES 블록 암호

- T -DES(Triple DES with two keys)



$C = E_{K_1}[D_{K_2}[E_{K_1}[P]]]$

Encryption



$P = D_{K_1}[E_{K_2}[D_{K_1}[C]]]$

Decryptipn

Multiple Encryption

3. DES, IDEA와 AES 블록 암호

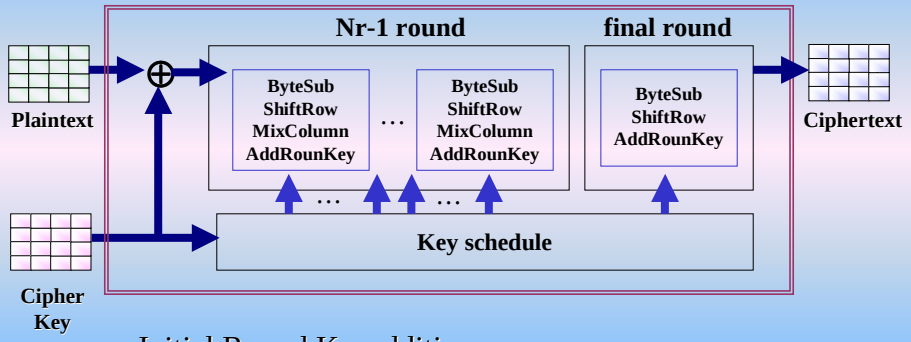
- AES 개발 배경
  - **1977**년 - **DES** (미연방 표준)
  - **1996**년 - **DES**의 효과적인 공격법 제안
    - ✓**DC : 2^{47}**
    - ✓**LC : 2^{43}**
  - 1997년 – NIST 알고리즘 공모
  - 2000년 10월 – Rijndael 채택
  - 2001년 8월 – FIPS 공식 문서로 발표

3. DES, IDEA와 AES 블록 암호

- Rijndael의 특징
  - 가변 길이 Key Length : 16,24,32 bytes
  - 가변 길이 Block Size : 16,24,32 bytes
  - 디자인의 간결성
  - 알려진 모든 공격에 안전
  - 다양한 플랫폼에서 speed 와 compact
  - SP-Network 구조
  - 블록 전체가 라운드마다 대치와 치환을 반복수행
  - 블록 code 응용
  - Operation over GF(2^8) extension field

3. DES, IDEA와 AES 블록 암호

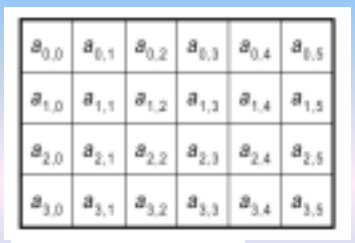
- Cipher의 구성



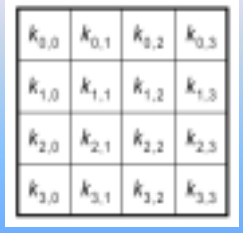
Initial Round Keyaddition
Nr-1 Rounds
final round

3. DES, IDEA와 AES 블록 암호

❑ Rijndael의 Key, Block 크기



가변적 Block Size :
16 byte(128 bit)
24 byte(192 bit)
32 byte(256 bit)

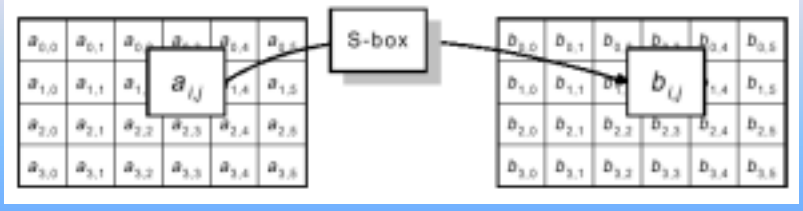


가변적 Key Size :
16 byte(128 bit)
24 byte(192 bit)
32 byte(256 bit)

3. DES, IDEA와 AES 블록 암호

❑ Rijndael의 SubBytes – Round Step 1

✓ S-box(substitution table) 적용
- 높은 비선형성(non-linearity)
- 1-byte(State) 단위 연산
- GF(2^8)상의 연산
- 역함수
- Affine (over GF(2)) transformation 적용



3. DES, IDEA와 AES 블록 암호

- Rijndael의 S-box

x \ 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

3. DES, IDEA와 AES 블록 암호

- IDEA(International Data Encryption Algorithm)
  - Xuejia Lai , James Massey at Swiss Federal Institute of Technology
  - DES vs. IDEA
    - DES : 64bit data block, 56bit key size, 16 round
    - IDEA : 64bit data block, 128bit key size, 8 round
  - Cryptographic Strength
    - Block length : 64bit, long enough to deter statistical analysis.
    - Key length : 128bit, long enough to prevent exhaustive key searches
    - Confusion : complicate the determination of how the statistics of the ciphertext depend on the statistics of the plaintext
    - Diffusion : each plaintext bit should influence every ciphertext bit, and each key bit should influence every ciphertext bit.

3. DES, IDEA와 AES 블록 암호

❑ Implementation

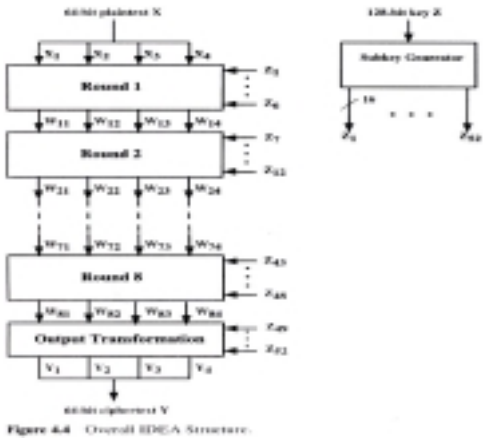
- IDEA : facilitate both S/W and H/W implementation
- S/W implementation
  - ➢ Use 16bit subblocks
  - ➢ Use simple operations

- H/W implementation
  - ➢ Similarity of encryption and decryption
  - ➢ Regular structure

3. DES, IDEA와 AES 블록 암호

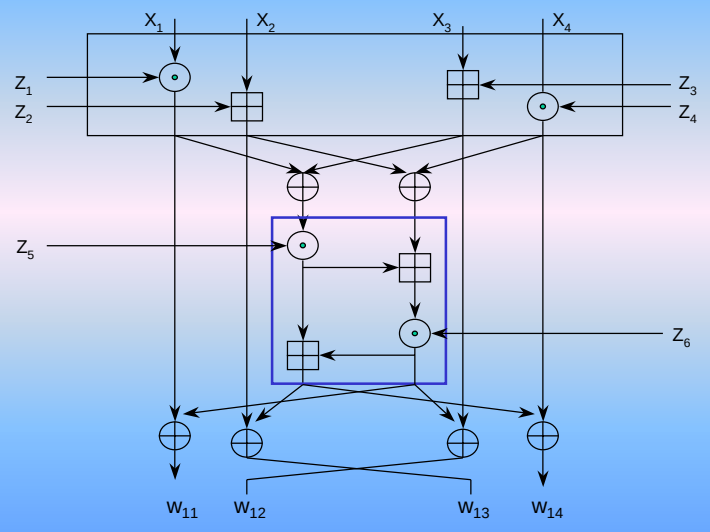
❑ Encryption

- 8 -round
  (6 x 8 = 48 subkeys)
- output transformation
  (4 subkeys)
- Key generation
  (16 -bit, 52 subkeys)



3. DES, IDEA와 AES 블록 암호

❑ Single Iteration of IDEA



3. DES, IDEA와 AES 블록 암호

❑ Conf.& Diff.➔ MA(multiplication/Addition)

- three operations: two 16bit inputs, two 16bit keys → two 16bit outputs
- ⊕ : XOR
- ⊞ : Addition of integers mod(2^{16})
- ⊙ : Multiplication mod(2^{16} + 1)

0000000000000000
⊙ 1000000000000000
= 1000000000000001
2^{16} x 2^{15} mod (2^{16} + 1)

- Effectiveness: complete diffusion

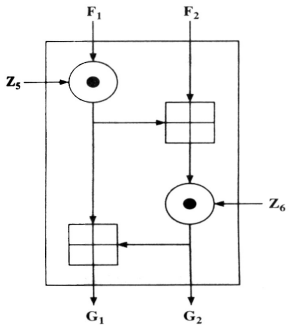


Figure 4.3 Multiplication/Addition (MA) Structure.

3. DES, IDEA와 AES 블록 암호

❑ Subkey generations : 16 -bit, 52 subkeys

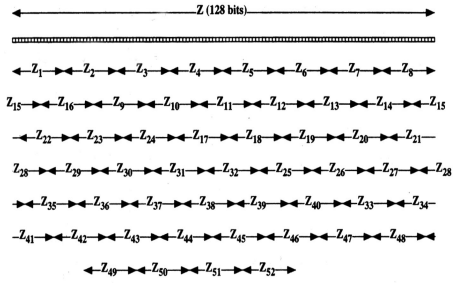


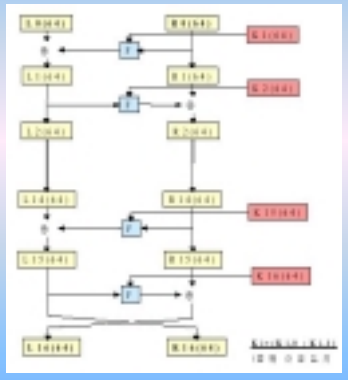
Figure 4.7 IDEA Subkeys.

- 128bit key → 16 -bit 52 subkeys generated
- circular left shift of 25 -bit position:

Z1 = Z[1 .... 16]
Z7 = Z[97 .... 112]
Z13 = Z[90 .... 105]
Z19 = Z[83 .... 98]
Z25 = Z[76 .... 91]
Z37 = Z[37 .... 52]
Z43 = Z[30 .... 45]

3. DES, IDEA와 AES 블록 암호

SEED



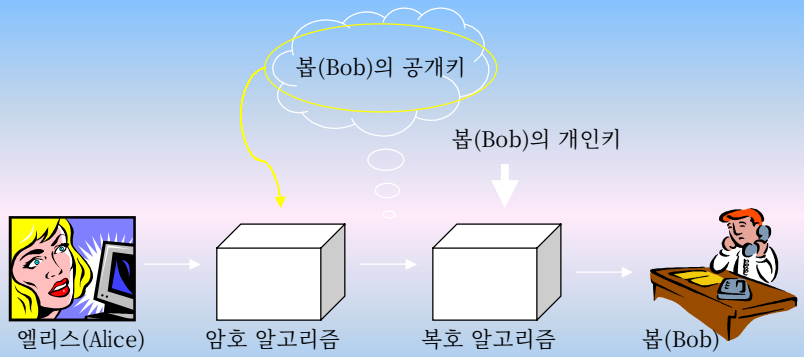
SEED 전체 구조도

- 국내 전자상거래의 활용 가능한 안전한 대칭키 암호알고리즘의 한국표준으로 개발되어 채택
- 구조
  전체 16round로 128비트 평문 블록을 128비트 비밀키를 이용해 암호화하는 DES와 유사한 feistal구조

  F함수의 비선형성 그 안전도를 의존
- 특징
  암복호 블록과 키 길이를 DES의 2배인 128비트로 하고 F함수의 비선형성을 높여서 안전도를 강화

4. RSA와 ECC 공개키 암호

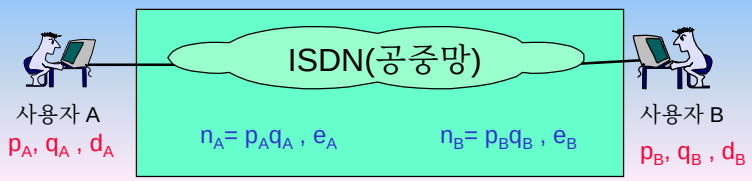
RSA 공개키 암호



공개키 암호 시스템

4. RSA와 ECC 공개키 암호

RSA



사용자 A가 사용자 B에게 평문 M을 전송할 경우

- 사용자 A : B의 공개키 e_B를 **획득**
  $M^{eB} \bmod n_B = C$를 계산하여 전송
- 사용자 B는 자신의 비밀키 d_B로 다음을 계산
  $C^{dB} \bmod n_B = M^{eBdB} \bmod n_B = M$

4. RSA와 ECC 공개키 암호

RSA

- RSA 알고리즘의 기본구조
  - 1단계 : 두 개의 큰 소수 p와 q를 선정
  - 2단계 : n=pq, $\phi(n)$ =(p -1)(q -1)
  - 3단계 : $\phi(n)$과 서로소인 임의의 정수 e 선택
  - 4단계 : ed=1(mod$\phi(n)$)을 만족하는 d를 유클리드 호제법 등으로 계산하여 비밀 열쇠로 한다

    비밀 열쇠 – d

    공개 자물쇠 – n , e

    암호화 단계 – $C = M^e \pmod n$

    복호화 단계 – $C^d = M^{ed} = M \pmod n$

4. RSA와 ECC 공개키 암호

RSA

- RSA의 특징
  - 키 관리가 간단
  - 키 사이즈가 크다
  - 연산시간이 길다
  - 디지털 서명과 인증에 관한 문제해결에 가장 적합
  - E -mail, 전자상거래, 자료보안 등에 이용
  - 1999년 미국 PATENT 만료

4. RSA와 ECC 공개키 암호

RSA

- Euler's theorem

$$M^{\phi(n)} \bmod n = 1$$

- ✓ $\phi(n)$: the number of positive integers less than n and relatively prime to n.

4. RSA와 ECC 공개키 암호

- Trap -door one -way function property
  - ✓ select a public key e and a private key d such that
  - ✓ Y = $f_k(X)$ easy.
  - ✓ X = $f_k^{-1}(Y)$ easy, if k and Y are known.

$$ed \bmod \phi(n) = 1$$

$$M^e \bmod n = C$$

$$C^d \bmod n$$

$$= (M^e)^d \bmod n$$

$$= M^{k\phi(n)+1} \bmod n$$

$$= M \bmod n$$

$$(ed \bmod \phi(n) = 1 \Leftrightarrow ed = k\phi(n)+1)$$

  - ✓ X = $f_k^{-1}(Y)$ infeasible, if Y is known but k is not known.

$$M^e \bmod n \xrightarrow{infeasible} M \text{ or } d$$

4. RSA와 ECC 공개키 암호

RSA

- Key Generation
  - ✓Select primes. p, q p and q are
  - ✓Calculate $n = p \times q$
  - ✓Calculate $\phi(n) = (p-1)(q-1)$ $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
  - ✓Select integer e
  - ✓Calculate d $d = e^{-1} \bmod \phi(n)$
  - ✓Public key KU = $\{e, n\}$
  - ✓Private key KR = $\{d, n\}$

4. RSA와 ECC 공개키 암호

RSA

- Encryption
  - ✓ Plaintext $M < n$
  - ✓ Ciphertext $C = M^e \pmod n$
- Decryption
  - ✓ Ciphertext C
  - ✓ Plaintext $M = C^d \pmod n$
- Example

$p = 7$ and $q = 17$ $n = p \times q = 7 \times 17 = 119$

$\phi(n) = (p-1)(q-1) = 96$

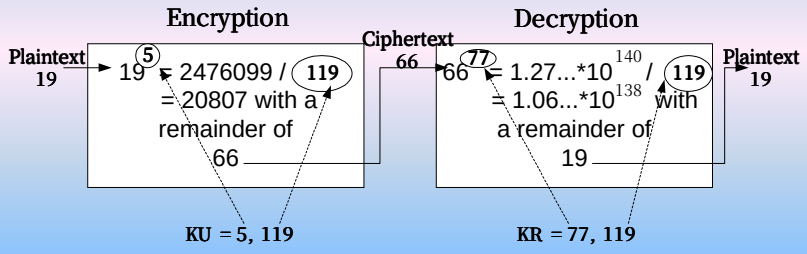
$e = 5$ $\gcd(96,5) = 1$

$5d = 1 \bmod 96 \Rightarrow d = 77$

4. RSA와 ECC 공개키 암호

RSA

➢Example of RSA Algorithm.



4. RSA와 ECC 공개키 암호

RSA

❑Computational Aspects

➢Encryption and Decryption

✓Modular multiplication

$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

✓Methods of modular exponentiation

$$x^{16} \bmod n = x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \bmod n$$

: 15 modular multiplications

$$x^{16} \bmod n = x^{10000_2} \bmod n = (((x^2)^2)^2)^2 \bmod n$$

: 4 modular multiplications

4. RSA와 ECC 공개키 암호

RSA

- Key Generation
  - ✓Determine prime number
    1. Pick an odd integer n at random
    2. Perform the probablistic primality test, such as Miller-Rabin. If n fails the test, reject the value n and go to step1. Else accept n.
  - ✓Calculate multiplicative inverse
    : using extended Euclid's algorithm.

4. RSA와 ECC 공개키 암호

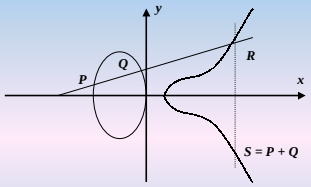
RSA

- The Security of RSA
  - Brute force
    trying all possible private keys.
  - Mathematical attacks
    factoring the product of two primes.
    A key size in the range of 1024 to 2048 bits seems reasonable.
  - Timing attacks
    These depend on the running time of the decryption algorithm.

4. RSA와 ECC 공개키 암호

ECC(Eliptic Curve Cryptosystems)

- Elliptic Curve Group (타원곡선 군)



첫째, 무한대 점은 O으로 표기하며 타원곡선 위의 임의의 점 P에 대해서 $P + O = P$가 성립된다. 즉 무한대 점은 덧셈상의 항등원(identity)이 된다.

둘째는 타원곡선상의 임의의 점 P에 대해서 $P + Q = O$을 만족하는 점 Q가 존재하는데

$Q = -P$로 나타내며 뺄셈 $R-S$는 $R + (-S)$로 정의된다. 점 $-P$는 점 P의 x축에 대한 대칭점이 되기 때문에 점 P의 좌표가 (x, y)이면 점 $-P$의 좌표는 $(x, -y)$가 된다.

셋째, 타원곡선상의 임의의 점 P와 Q에 대해서 $P + Q = Q + P$가 성립한다.

넷째, 타원곡선상의 임의의 점 P, Q와 R에 대해서 $P + (Q + R) = (P + Q) + R$이 성립한다.

4. RSA와 ECC 공개키 암호

- 유한체(finite Field) 상에서의 타원곡선

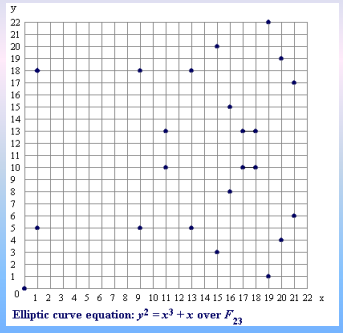
p가 소수일 때 유한 체 $GF(p)$상에서의 타원곡선(elliptic curve)은 $a, b \in GF(p)$의 경우에 방정식 $y^2 \bmod p = x^3 + ax + b \bmod p$를 만족하는 (x, y) 점들의 집합과 무한대 점 O을 의미한다. 물론, $x, y \in GF(p)$

$a = 1$ and $b = 0$일 때, 타원곡선 $y^2 = x^3 + x$.
점 (9,5)은 위의 식을 만족 because :

$$y^2 \bmod p = x^3 + x \bmod p$$
$$5^2 \bmod 23 = 9^3 + 9 \bmod 23$$
$$25 \bmod 23 = 738 \bmod 23$$
$$2 = 2$$

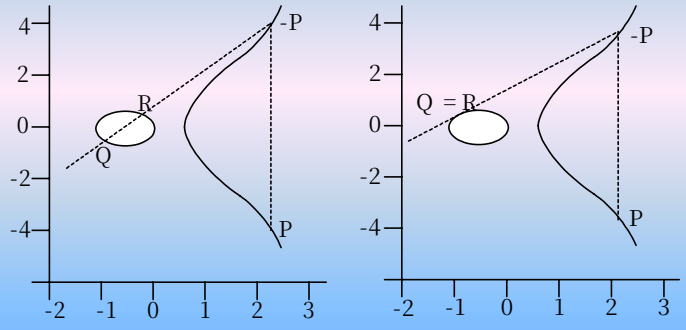
The 23 points which satisfy this equation are:

(0,0) (1,5) (1,18) (9,5) (9,18) (11,10) (11,13) (13,5) (13,18) (15,3) (15,20) (16,8) (16,15) (17,10) (17,13) (18,10) (18,13) (19,1) (19,22) (20,4) (20,19) (21,6) (21,17)



4. RSA와 ECC 공개키 암호

- Elliptic Curves
  - $y^2 + axy + by = x^3 + cx^2 + dx + e$ and the point at infinity O

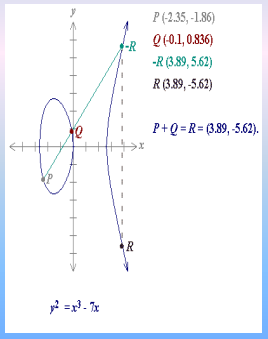


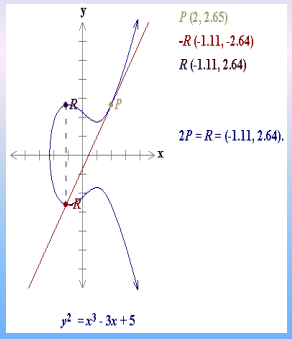
Elliptic Curves and Point Addition.

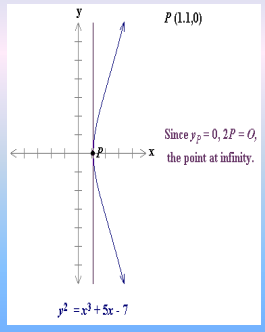
4. RSA와 ECC 공개키 암호

- Elliptic Curve 예

실수(real number)상에서의 타원곡선(elliptic curve)은 *a*와 *b*가 고정된 실수일 경우에 방정식 $y^2 = x^3 + ax + b$을 만족하는 (x, y) 점들의 집합을 의미한다.

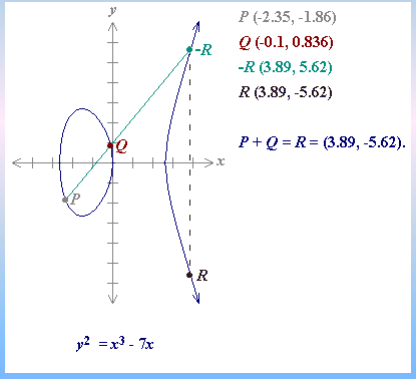






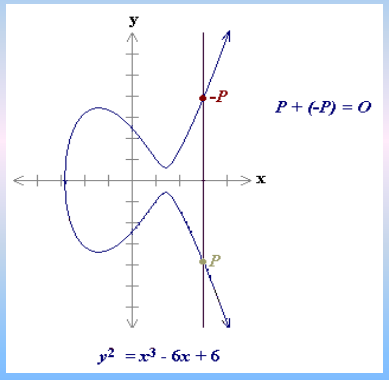
4. RSA와 ECC 공개키 암호

❑ **Addition of point *P* and point *Q***



4. RSA와 ECC 공개키 암호

❑ **Addition of *P* and *–P***



By definition, $P + (-P) = \boldsymbol{O}$.

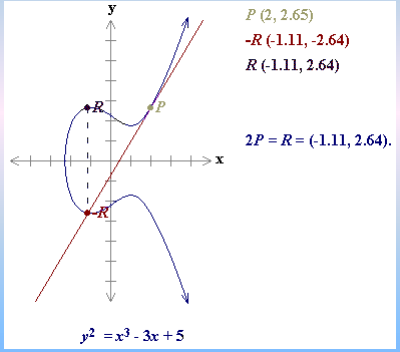
As a result of this equation,
$P + \boldsymbol{O} = P$ in the elliptic curve group .

O = the additive identity of the elliptic curve group;

All elliptic curves have an additive identity.

4. RSA와 ECC 공개키 암호

❑ **Doubling the point *P***



***P* = (*x*, *y*)**

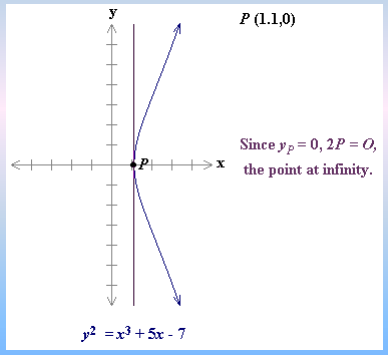
If $y \neq 0$, then *P* 에서의 접선은 정확히 타원곡선의 다른 한 점과 교차.

the law for doubling a point on an elliptic curve group **:**

P* + *P* = 2*P* = *R

4. RSA와 ECC 공개키 암호

❑ **Doubling the point *P* if *y* = 0**



By definition, 2*P* = *O* for such a point *P*.

To find 3*P* in this situation, one can add 2*P* + *P*. Then, *P* + *O* = *P*

Thus 3*P* = *P*.
3*P* = *P*, 4*P* = O, 5*P* = *P*, 6*P* = O, 7*P* = *P*, …

4. RSA와 ECC 공개키 암호

- Ex) Elliptic Curves over Finite Fields
  - $E_p(a,b)$: the elliptic group of points from (0, 0) to (p, p) that satisfying the equation together with the point at infinity O.

$$y^2 = x^3 + ax + b \pmod{p}$$

  - $E_{23}(1,1)$: $y^2 = x^3 + x + 1 \pmod{23}$

(0,1)	(0,22)	(1,7)	(1,16)	(3,10)
(3,13)	(4,0)	(5,4)	(5,19)	(6,4)
(6,19)	(7,11)	(7,12)	(9,7)	(9,16)
(11,3)	(11,20)	(12,4)	(12,19)	(13,7)
(13,16)	(17,3)	(17,20)	(18,3)	(18,20)
(19,5)	(19,18)	and the point at infinity		

4. RSA와 ECC 공개키 암호

- The rules for addition
  - ✓$P + O = P$: O serves as the additive identity.
  - ✓$P = (x, y)$, $-P = (x, -y)$
  - ✓$P = (x_1, y_1)$ and $Q = (x_2, y_2)$, then $P + Q = (x_3, y_3)$

$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p}$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod{p}$$
$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \dfrac{3x_1 + a}{2y_1} & \text{if } P = Q \end{cases}$$

  - ✓$2P = P + P$, $3P = P + P + P$, . . .

4. RSA와 ECC 공개키 암호

✓Example

- If $P = (3, 10)$ and $Q = (9, 7)$, then

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} = 11 \bmod 23$$

$$x_3 = 11^2 - 3 - 9 = 109 \equiv 17 \bmod 23$$

$$y_3 = 11(3-(-6)) - 10 = 89 \equiv 20 \bmod 23$$

=> $P + Q = (17, 20)$

4. RSA와 ECC 공개키 암호

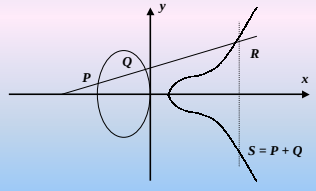
❑ **EC $y^2=x^3+ax+b$에서 Addition S=P+Q**

(x_1, y_1), (x_2, y_2), (x_3, y_3)을 점 $P, Q, S = P + Q$의 좌표. 점 $P + Q = S$ 좌표 (x_3, y_3)을 x_1, y_1, x_2, y_2로 표현.

$y = \alpha x + \beta$를 점 P와 Q를 지나는 선의 방정식,
$\alpha = (y_2 - y_1) / (x_2 - x_1)$, $\beta = y_1 - \alpha x_1$.

만약, $(\alpha x + \beta)^2 = x^3 + ax + b$이면 점 P와 Q를 지나는 선 위의 점 $(x, \alpha x + \beta)$는 타원곡선상의 점이 된다.

3차 방정식 $x^3 - (\alpha x + \beta)^2 + ax + b$의 각각의 근(root)에 대하여 한 개의 교차점이 존재하게 된다.
$(x_1, \alpha x_1 + \beta)$와 $(x_2, \alpha x_2 + \beta)$는 타원곡선상의 두 점 P와 Q이기 때문에 x_1과 x_2가 3차 방정식의 근.



$$x_1 + x_2 + x_3 = \alpha^2$$

결국 나머지 근은 $x_3 = \alpha^2 - x_1 - x_2$이 되고 점 $P + Q$의 좌표 (x_3, y_3)

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \qquad y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$$

4. RSA와 ECC 공개키 암호

❑ Addition S=P+Q

$P + Q$에서 $P = Q$가 되면 α는 점 P에서의 미분 값이 되기 때문에

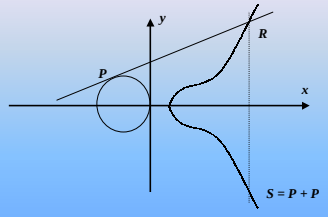
$y^2 = x^3 + ax + b$을 음함수 미분하면

$2yy' = 3x^2 + a$가 되고 점 $P = (x_1, y_1)$에서의 기울기는 $\alpha = (3x_1^2 + a) / 2y_1$이 된다.

점 $P + Q = S$의 좌표 (x_3, y_3)을 x_1, y_1, x_2, y_2를 통해서 표현하면 다음과 같다.

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)$$



4. RSA와 ECC 공개키 암호

❑ 타원곡선 이산대수 문제

- $GF(p)$, where p is a prime(소수)
- 타원곡선상의 점 P의 위수(order) t : $tP = 0$을 만족하는 가장 작은 정수 t
- $GF(p)$상에서 정의된 타원곡선상의 점 Q, 위수가 t 인 점 P,
  $Q = xP$를 만족하는 정수 $x \in [0, t-1]$를 구하는 문제

$P, 2P = P + P, 3P = P + P + P, \ldots$를 연속적으로 계산

$y^2 \bmod 23 = x^3 + 9x + 17 \bmod 23,$

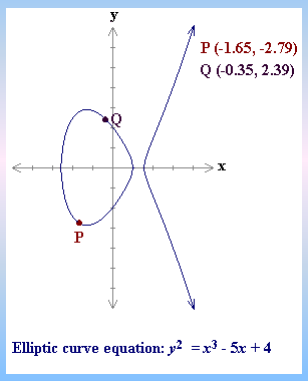
What is the discrete logarithm x of $Q = (4,5)$ to the base $P = (16,5)$? $Q = xP$

$P = (16,5)$ $2P = (20,20)$ $3P = (14,14)$ $4P = (19,20)$ $5P = (13,10)$
$6P = (7,3)$ $7P = (8,7)$ $8P = (12,17)$ $9P = (4,5)$

Since $9P = (4,5) = Q$, the discrete logarithm of Q to the base P is $x = 9$.

4. RSA와 ECC 공개키 암호

❑ 타원곡선 이산대수 문제



What is the discrete logarithm of Q(-0.35,2.39) to the base P(-1.65,-2.79) in the elliptic curve group $y^2 = x^3 - 5x + 4$ over real numbers?

4. RSA와 ECC 공개키 암호

❑ **ECC 타원곡선 공개키 암호**

- Exponential ←→ Multiplication
- Multiplication ←→ Addition

ElGamal 공개키 암호	타원곡선 공개키 암호
공개키 : $\{ g, p, y = g^x \bmod p \}$ 개인키 : $\{ x \}$ 암호화 : $[c_1, c_2] = [g^{x'} \bmod p, y^{x'} m \bmod p]$ 복호화 : $c_2 c_1^{-x} \bmod p$ Where x'=random	$\{ G, p, Y = xG \}$ $\{ x \}$ $[C_1, C_2] = [x'G, x'Y + M]$ $C_2 - xC_1$

[예] $p = 11$, $a = 1$, $b = 6$인 경우에 $GF(p)$상에서 타원곡선 $y^2 = x^3 + x^2 + 6$이 정의되고 타원곡선상의 점들은 다음과 같다.

(2, 4) (2, 7) (3, 5) (3, 6) (5, 2) (5, 9)
(7, 2) (7, 9) (8, 3) (8, 8) (10, 2) (10, 9)

수신자의 개인키 $x = 7$, 공개키 $G = (2, 7)$, $Y = 7(2, 7) = (7, 2)$가 주어졌을 때, 송신자는 임의의 난수 $x = 3$을 선정하여 평문 $M = (10, 9)$을 암호문 $C_1 = 3(2, 7) = (8, 3)$, $C_2 = 3(7, 2) + (10, 9) = (10, 2)$로 전환한다.

4. RSA와 ECC 공개키 암호

- ECC: 반복 2배수 -덧셈 (Double and Addtion)

• $2P = P + P$

• $100P = 2(2(P + 2(2(2(P + 2P))))$

100(D) = 1 | 1 0 0 1 0 0 (B) ← key

where, "1"=double & addition, "0"=double

- RSA: 반복 (Square and Multiplicaiton)

• $M^2 = M \times M$

• $M^{100(D)} \Rightarrow 1 \mid 1\ 0\ 0\ 1\ 0\ 0(B) \leftarrow key$

where, "1"=square & multiple, "0"=square

$$x^{16} \bmod n = x^{10000_2} \bmod n = (((x^2)^2)^2)^2 \bmod n$$

4. RSA와 ECC 공개키 암호

- Cryptography with Elliptic Curves
  - Elliptic curve discrete logarithm problem
    - ✓ $aG = P$ for any point P, a generator point G in $E_p(a, b)$.
      => find integer a.
  - Analog of Diffie -Hellman Key Exchange

Generate	*random* $n_A < n$		
Calculate	$P_A = n_A G$	$\xrightarrow{P_A}$	*Generate* *random* $n_B < n$
		$\xleftarrow{P_B}$	*Calculate* $P_B = n_B G$
Calculate	$K = n_A P_B$		*Calculate* $K = n_B P_A$
	$= n_A n_B G$		$= n_B n_A G$

4. RSA와 ECC 공개키 암호

- Elliptic Curve Encryption/Decryption
  1. Encoding the plaintext message m to a point P_m.
  2. Encryption : $C_m = \{kG, P_m + kP_B\}$ where k is random number.
  3. Decryption : $C_m - n_B(kG) = P_m + kP_B - k(n_BG) = P_m$
  4. Decoding the point P_m to the plaintext message m.

- Security of Elliptic Curve Cryptography
  - Smaller key size for same security.
  - For example, the 160 -bit key size of ECC offer equal security for 1024 -bit key size of RSA.

4. RSA와 ECC 공개키 암호

- 타원곡선 이산대수와 소인수 분해에 소요되는 계산량

1–mips 컴퓨터가 1초에 40,000번의 타원곡선 덧셈을 수행할 수가 있다고 가정.

1–mips 컴퓨터는 1년 동안에 $(40{,}000)(60\times60\times24\times365) \approx 2^{40}$번의 타원곡선 덧셈을 수행.

왼쪽 표는 여러 개의 t값에 대해서 *Pollard*의 *rho* 알고리즘을 적용 할 때, 한 개의 타원곡선 이산대수를 계산하기 위해 소요되는 계산량을 나타낸다. $\sqrt{\pi t/2}$

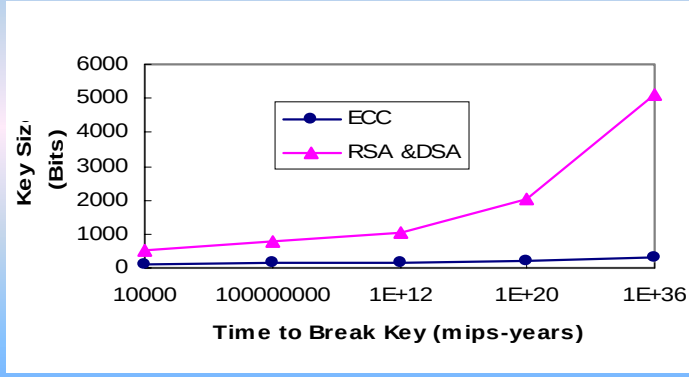
예를 들면 1,000–mips 컴퓨터 10,000대를 이용하여 $t = 2^{160}$인 경우의 타원곡선 이산대수를 구하기 위해서는 96,000–year가 소요된다

p(bits)	t (bits)	$\sqrt{\pi t/2}$	mips–year
163	160	2^{80}	9.6×10^{11}
191	186	2^{93}	7.9×10^{15}
239	234	2^{117}	1.6×10^{23}
359	354	2^{177}	1.5×10^{41}
431	426	2^{213}	1.0×10^{52}

n (bits)	mips–year
512	3×10^{4}
768	2×10^{8}
1024	3×10^{11}
1280	1×10^{14}
1536	3×10^{16}
2048	3×10^{20}

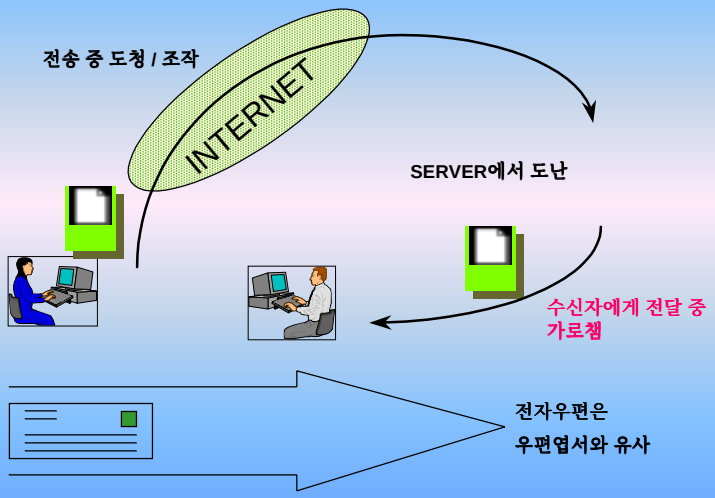
4. RSA와 ECC 공개키 암호

❑ ECC, RSA, DSA 안전성 비교분석



5. 인터넷 보안

❑ 전자우편 보안



5. 인터넷 보안

❑ 전자우편 보안 서비스

- ❑ 메시지 기밀성
- ❑ 송신자에 대한 실체인증
- ❑ 메시지 무결성
- ❑ 부인봉쇄

- ❑ **PEM** (Privacy Enhanced Mail)
- ❑ **PGP (Pretty Good Privacy)**
- ❑ **S/MIME(Secure/Multipurpose Internet Mail Extensions) , by RSA 사**
- ❑ **MOSS(MIME Object Security Service)**

5. 인터넷 보안

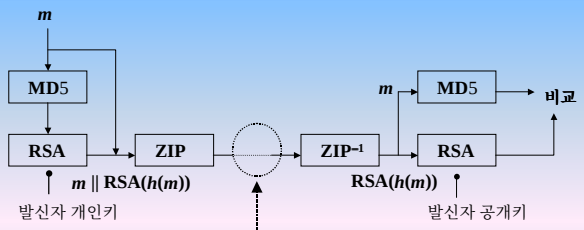
❑ PGP

- ❑ Phil Zimmerman
- ❑ 전세계적으로 다양한 기종에서 실행되는 공개 소프트웨어
- ❑ 공개적인 검토 작업을 통해서 대단히 안전하다고 할 수 있는 알고리즘을 기반
  - ➢ 공개키 암호 **RSA**, 대칭형 암호 **IDEA**, 해쉬 함수 **MD5**
- ❑ 파일과 메시지를 암호화하는 표준화된 방법

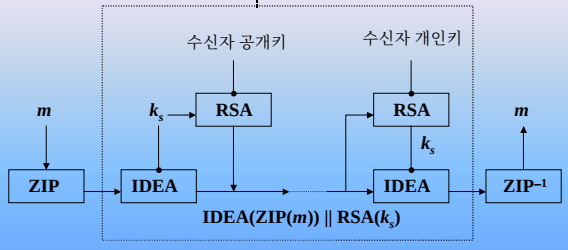
기능	알고리즘
메시지 암호화	**RSA, IDEA**
디지털 서명	**RSA, MD5**
압축	**ZIP**
전자우편 호환성	**기수-64 변환**

5. 인터넷 보안

- PGP 디지털 서명 메커니즘

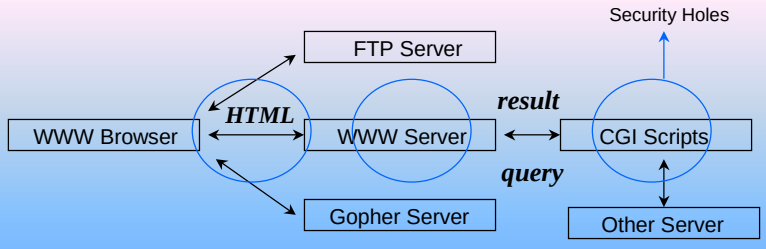


- PGP 기밀성 메커니즘



5. 인터넷 보안

- WWW 보안
  - Browser (Explorer, Netscape) Server (NCSA HTTP, httpd)
  - URL (Uniform Resource Locator)
  - HTML (HyperText Manipulation Language)
  - CGI (Common Gateway Interface) - e.g. form processing

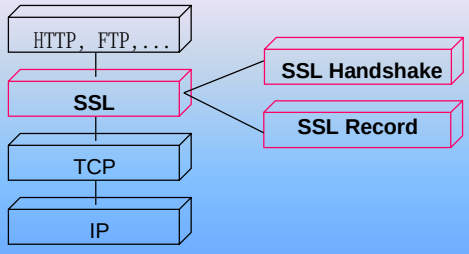


5. 인터넷 보안

- WWW 보안 요구사항
  - Client / Server 상호인증
  - 교환되는 메시지 / 문서의 무결성
  - 기밀성
- WWW 보안 프로토콜
  - 채널보안 기법
    - SSL (Secure Socket Layer)
    - PCT (Privacy Communication Technology)
  - 메시지 보안기법
    - S-HTTP

5. 인터넷 보안

- SSL (secure socket layer)
  - Netscape Communications
  - Privacy, Data Integerity, Server [Client] Authentication,
  - RSA, Diffie-Hellman, Fortezza for Key Exchange
  - DES, 3DES, IDEA, RC2, RC4[stream cipher] for Data Encryption
  - MD5, SHA for Hash Function (MAC)

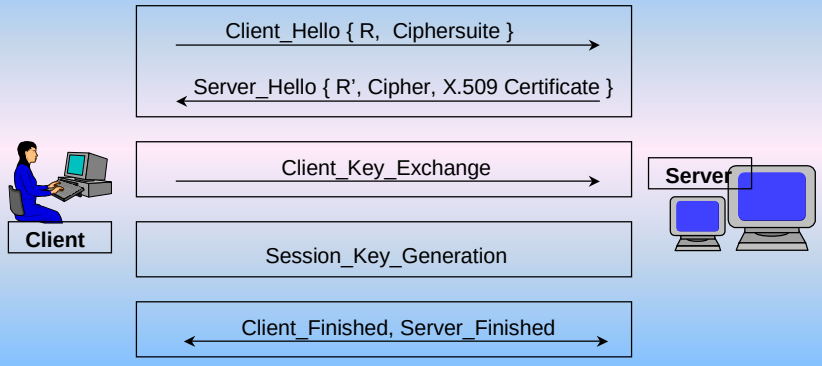


Algorithm Negotiation,
Key Exchange,
Authentication

Data Encapsulation
for data protection

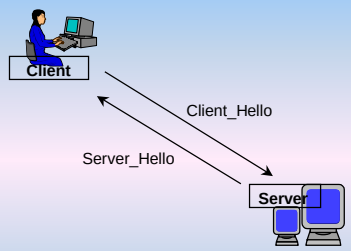
5. 인터넷 보안

- **SSL Handshake Protocol**



5. 인터넷 보안

- **SSL Client Hello Phase**
  - client SSL version
  - 28-byte random number R
  - session ID
  - cipher_suites
  - compression methods



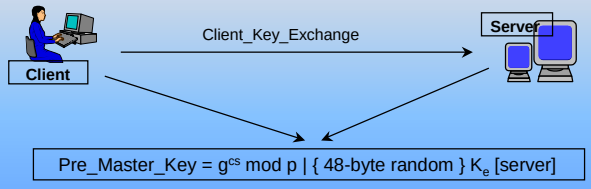
- **SSL Server Hello Phase**
  - server SSL version
  - 28-byte random number R'
  - session ID -> If a new session, server's certificate
  - cipher_suite { key exchange algorithm }
  - compression method

5. 인터넷 보안

SSL Client Key Exchange

- Key Exchange Algorithm's Parameter in Certificate
  - RSA : public exponent k_e, modulus n
  - Diffie-Hellman : g, modulus p, g^s mod p
- From *Pre_Master_Key* To *Mater-Key* [MD5, SHA, R, R']

Master_Key = MD5 (Pre_Master_Key || SHA ('A' || Pre_Master_Key || R || R')) ||
MD5 (Pre_Master_Key || SHA ('BB'|| Pre_Master_Key || R || R'))||
MD5 (Pre_Master_Key || SHA ('CCC'|| Pre_Master_Key || R | R'))



5. 인터넷 보안

SSL Session Key Generation

- Keys for data encryption and data integrity

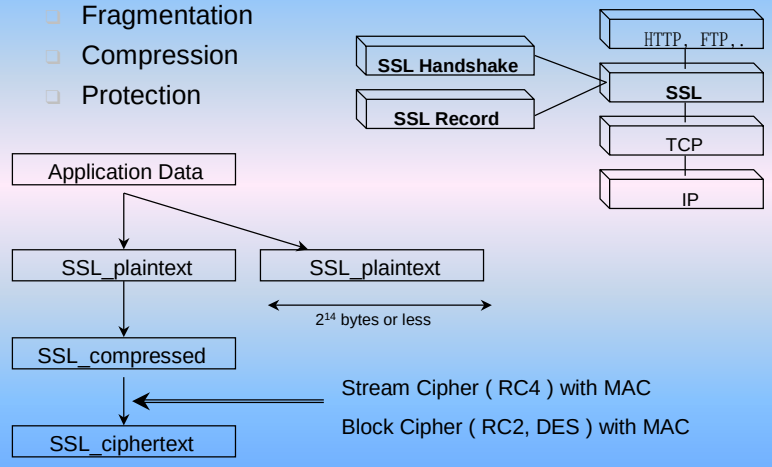
Key_Block = MD5 (Master_Key || SHA ('A' || Master_Key || R || R')) ||
MD5 (Master_Key || SHA ('BB' || Master_Key || R || R')) ||
MD5 (Master_Key || SHA ('CCC' || Master_Key || R || R')) || .....

SSL Client-Server Finished

- Key Exchange, Authentication 확인
- Negotiated Algorithm, Parameter
- All Handshaked Messages
- Sender's value { client[0x434C4E54], server[0x53525652] }

5. 인터넷 보안

- **SSL Record Protocol**
  - Fragmentation
  - Compression
  - Protection



5. 인터넷 보안

- **Change cipher spec 프로토콜**
  - Change cipher spec 메시지는 이후의 레코드에 대해 cipherspec에 정의된 알고리즘과 키를 이용해 보호될 수 있도록 수신측에 알리기 위해 사용된다.
  - 클라이언트는 키 교환메시지와 인증서 확인 메시지를 전송한 후에 보냄
  - 서버는 클라이언트로부터 받은 키 교환 메시지를 성공적으로 처리한 후에 보냄

- **Alert 프로토콜**
  - SSL 레코드 계층에서 제공되는 컨텐츠 타입 중 하나
  - 각종 오류에 대한 메시지와 설명을 전송하는데 이용

  (압축 및 암호화 오류, MAC 오류, 인증서 오류, 프로토콜 실패 등)

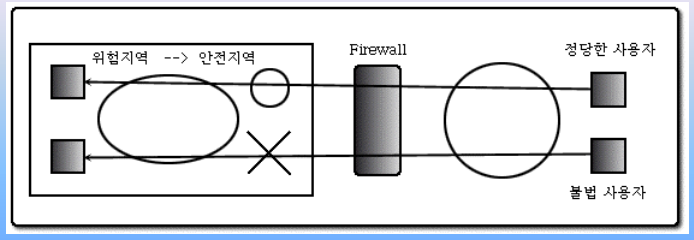
5. 인터넷 보안

❑ 방화벽 종류 및 특징

➢ *방화벽의 기능 (정보보호 서비스)*

•방화벽이란:

- 불법 트래픽/ 정당하지 않은 사용자 접근 방지
- 합법 트래픽/ 정당한 사용자 투명한 접근 허용



5. 인터넷 보안

❑ 방화벽 종류 및 특징

➢ *방화벽 기능 (정보보호 서비스)*

A. 인증(Authentication) : 메시지 인증, 사용자 인증 기능; [예] One-Time Password

B. 접근제어(Access Control) : 네트워크 자원에 대하여 자격을 검사하여 접근 통제

C. 트래픽 암호(Traffic Enciphering) : 트래픽 데이터에 대한 암호화 기능 (DES, RSA, IDEA 등)

D. 트래픽 로그(Traffic Log) : 네트워크에 접근하는 모든 트래픽에 대한 로그 파일 기록

E. 감사 추적 기능(Audit)

5. 인터넷 보안

- ***방화벽 분류***

A. Packet Filtering Firewall

- 스크리닝 라우터 (Screening Router)

- 베스천 호스트 (Bestion Host)

B. Circuit Level Firewall

- 서킷 게이트웨이 (Circuit Gateway)

C. Application Level Firewall

- 프록시 서버 호스트 (Proxy Server Host)

- 듀얼-홈드 게이트웨이 (Dual-Homed Gateway)

5. 인터넷 보안

- ***방화벽 분류***

D. Hybrid Firewall

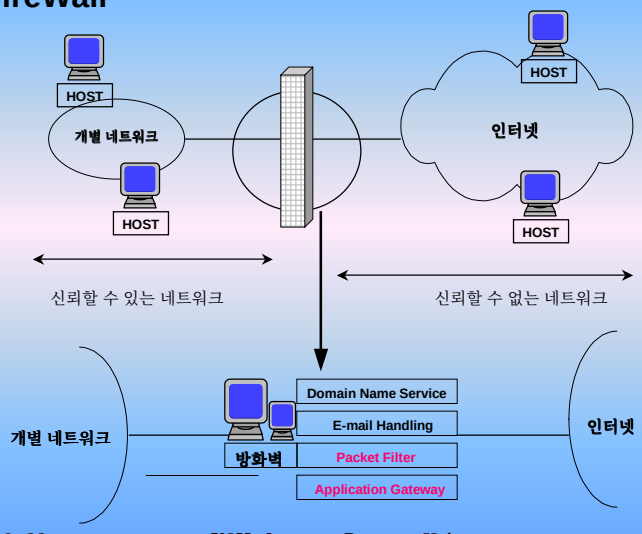
- 스크린드 호스트 (Screened Host)

- 스크린드 서브넷 (Screened Subnet)

E. Stateful Inspection Firewall

5. 인터넷 보안

- FireWall



5. 인터넷 보안

- 소스 라우팅(Source routing)
  - 스크리닝 라우터는 소스 라우팅 옵션이 켜져있는 모든 패킷은 쉽게 막을 수 있다.
- 어드레스 필터링
  - 소스 어드레스를 확인함으로써 모르는 호스트로부터 오는 침입자를 막을 수 있다.

[표 3.4] 어드레스 필터링

Rule	Direction	Source Address	Destination Address	Action
1	Inbound	158.104.96.105	158.104.1.1	Permit
2	Outbound	158.104.1.1	158.104.*.*	Permit
3	Inbound	199.237.36.3	158.104.1.1	Drop
default	********	* * * *	* * * *	Drop

5. 인터넷 보안

❑(3)소스와 목적지 포트들의 필터링

[표 3.5] 소스와 목적지 포트를 기술할 수 있을 때의 패킷 필터링

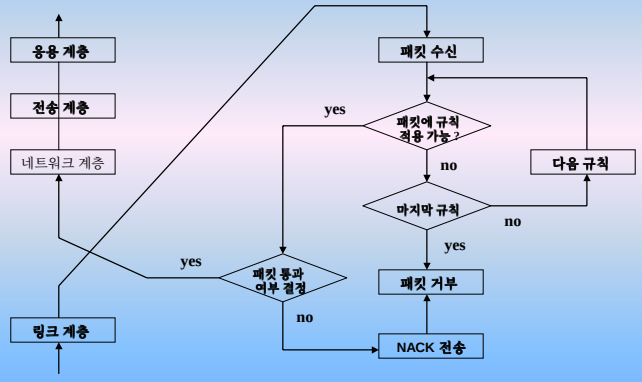
Rule	Source		Destination		Protocol	Action
	Address	Port	Address	Port		
1	199.237.36.3 (external host)	5555	158.104.96.105 (internal host)	6666	TCP	Permit

[표 3.6] 목적지 포트만을 기술할 때의 패킷 필터링

Rule	Source		Destination		Protocol	Action
	Address	Port	Address	Port		
1	158.104.96.105	****	199.237.36.3	6666	TCP	Permit
2	199.237.36.3	****	158.104.96.105	5555	TCP	Permit

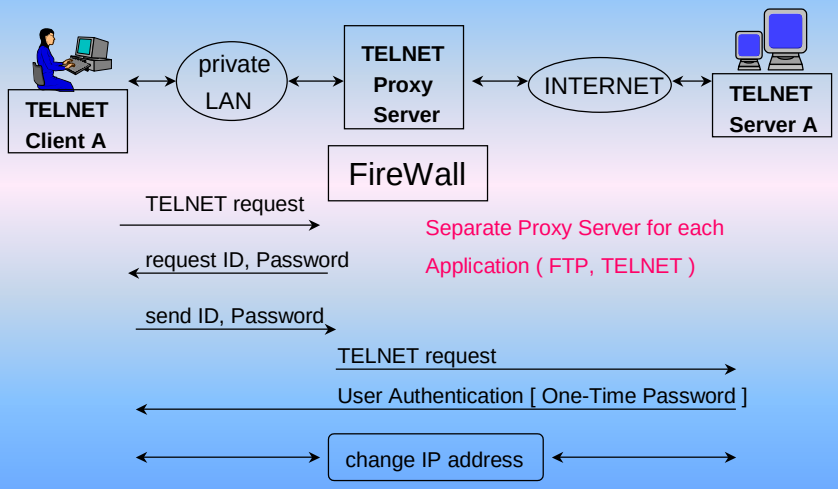
5. 인터넷 보안

❑ **Packet Filter Operations**



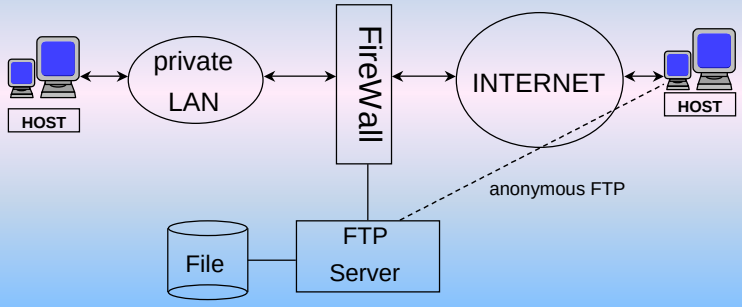
5. 인터넷 보안

- **Proxy Server**



5. 인터넷 보안

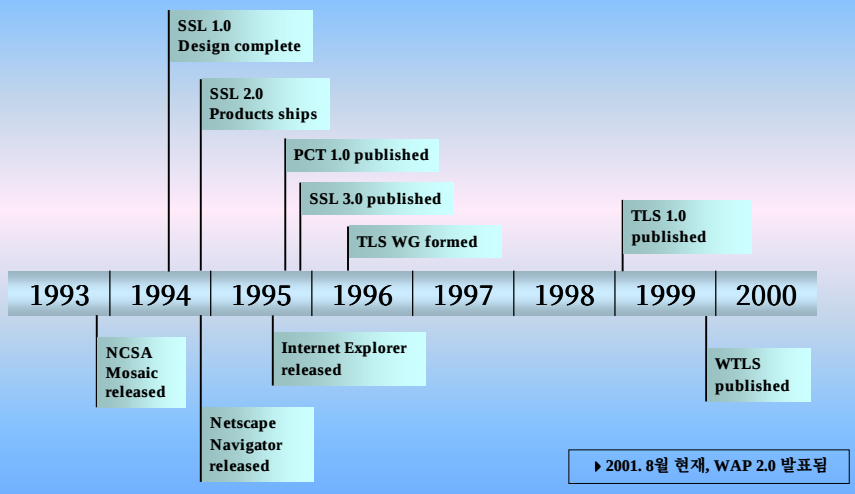
- **Externalized FTP Server**



6. 무선인터넷 보안

- History & TLS
- Handshake Protocol
- Other protocols
- WAP
- WTLS Protocols

6. 무선인터넷 보안



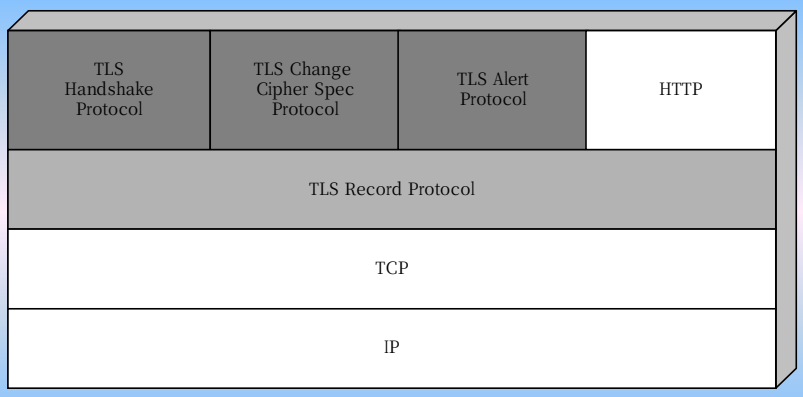
6. 무선인터넷 보안

- TLS(Transport Layer Security)의 개요
  - TLS는 Netscape社에서 개발한 SSL(Secure Socket Layer)의 표준화 버전이다. – IETF RFC2246 – 1999
  - 서버와 클라이언트 사이의 통신과정에서 비밀성(privacy)과 데이터 무결성(integrity)을 제공한다.
  - 네트워크 계층의 암호화 방식이기 때문에 HTTP뿐 아니라 NNTP, FTP등에서도 사용할 수 있다.
  - 표준화 홈페이지

    http://www.ietf.org/html.charters/tls -charter.html

6. 무선인터넷 보안

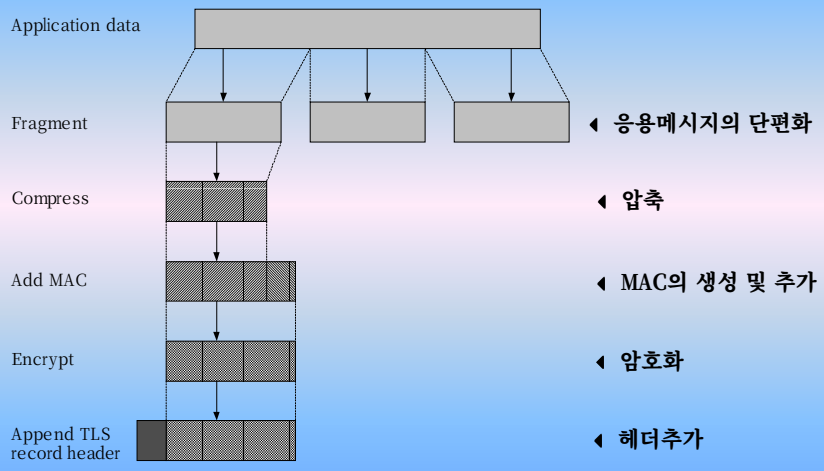
TLS Architecture



※ TLS는 두 개의 계층, 네 개의 프로토콜로 이뤄져 있다.

6. 무선인터넷 보안

❑ TLS Record Protocol



6. 무선인터넷 보안

❑ Handshake Protocol

(1) Handshake protocol의 기능 및 절차

- 서버와 클라이언트간의 상호 인증을 수행한다.
- 실질적 보안 프로토콜인 Record protocol에서 사용될 암호 알고리듬, 키 등을 협상한다.
- Handshake protocol은 크게 4단계의 절차를 가진다.
  - ✓ Phase 1. Establish Security Capabilities
  - ✓ Phase 2. Server Authentication and Key Exchange
  - ✓ Phase 3. Client Authentication and Key Exchange
  - ✓ Phase 4. Finish

6. 무선인터넷 보안

❑ Other protocols

(1) Change Cipher Spec 프로토콜

- ➢ 현재의 연결에서 사용할 Cipher Suite을 갱신하기 위해 사용된다.

(2) Alert 프로토콜

- ➢ TLS 프로토콜 사용시 발생하는 경고 메시지를 peer 개체에게 전송하기 위해서 사용된다.
- ➢ 발생하는 경고메시지의 종류
  - ✓메시지의 부적절함이나 전송상태의 오류
  - ✓MAC의 부정확/복호시의 오류
  - ✓인증서에 관련된 오류
  - ✓암호 스펙의 협상과정에서의 오류 등

6. 무선인터넷 보안

❑ WAP (Wireless Application Protocol)

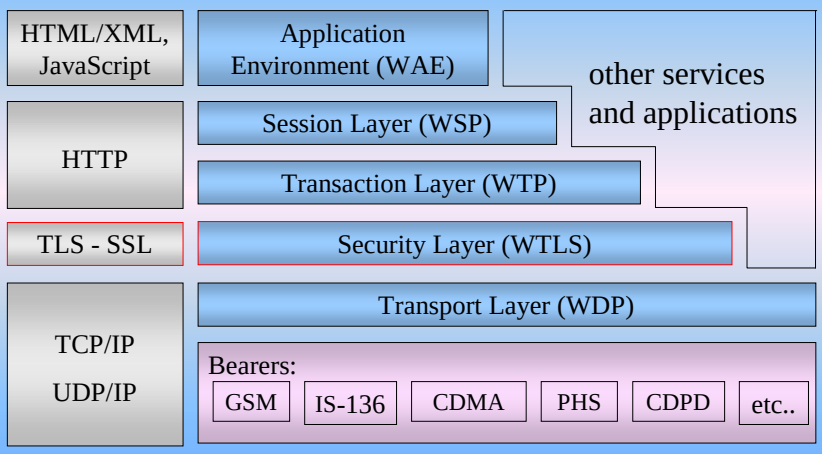
(1) 무선 통신 환경에서의 어플리케이션을 개발하기 위해 산업 규격을 제정하는 WAP Forum의 연구 결과

(2) 네트워크 기술, 무선 데이터 기술, 인터넷 기술 등의 빠른 발전으로 생겨난 기술

(3) 휴대용 단말기 하나만으로 무선 인터넷에 접속(양방향통신)할 수 있도록 브라우저 개발 및 표준 언어의 개발의 필요성 대두로 WAP이 탄생

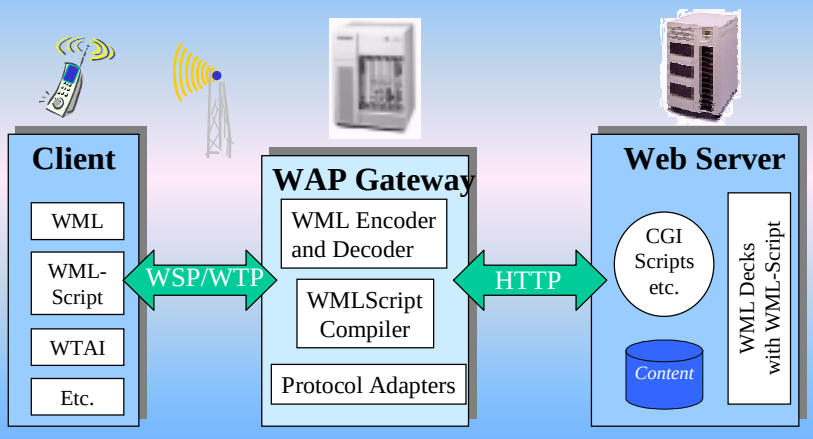
6. 무선인터넷 보안

❑ WAP Architecture



6. 무선인터넷 보안

❑ WAP programming model



6. 무선인터넷 보안

❑ WAP Gateway

(1) Gateway와 WAP 브라우저 사이에 보안제공을 위해 WTLS사용

- ➢ 무선환경에 적합하도록 SSL(TLS) 에 비해 datagram support, optimized handshake, dynamic key refresh 지원

(2) SSL과 WTLS 보안 프로토콜 사이의 상호 변환

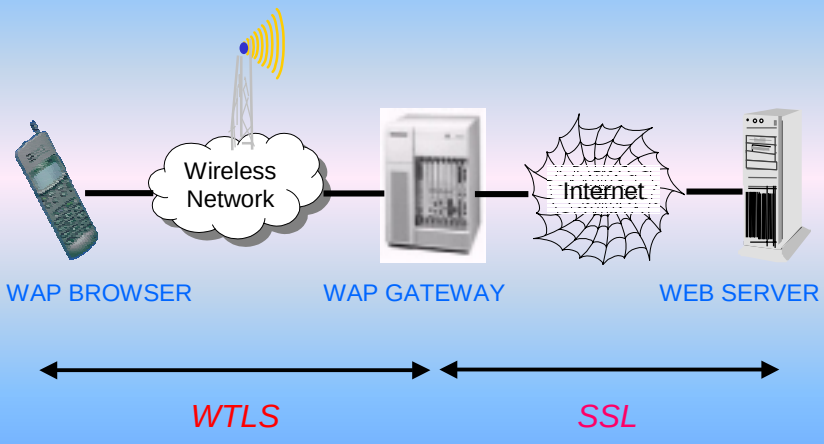
- ➢ 유선에서 SSL-encrypted message를 무선 네트웍에서의 WAP WTLS 로 변환

(3) Secondary media에서 decrypted contents가 저장되어서는 안 된다.

(4) Gateway를 인증된 사람만이 접근 할 수 있도록 해야 한다.

6. 무선인터넷 보안

❑ Security in a WAP environment



6. 무선인터넷 보안

❑ WTLS (Wireless Transport Layer Security)

(1) SSL, TLS와 같은 인터넷 보안 프로토콜에 기초한 안전한 접속을 위한 framework 규정

(2) Confidentiality, Authentication, Integrity 같은 보안 서비스 제공

(3) node -to -node security 제공

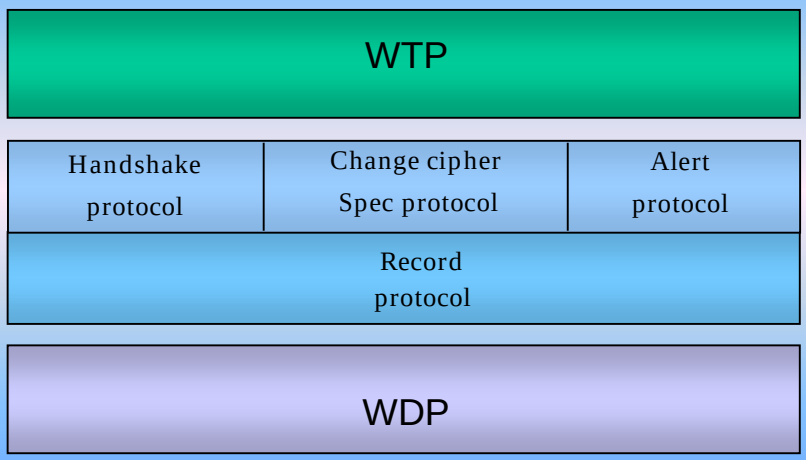
(4) 무선 환경에 적합하도록 대역폭, 메모리, 소요 전력을 고려한 효율적인 프로토콜

(5) SSL보다 protocol overhead를 최소화하고 데이터 압축을 더 많이 함

(6) 무선 환경에 적합한 security algorithm을 포함

6. 무선인터넷 보안

❑ Architecture of WTLS



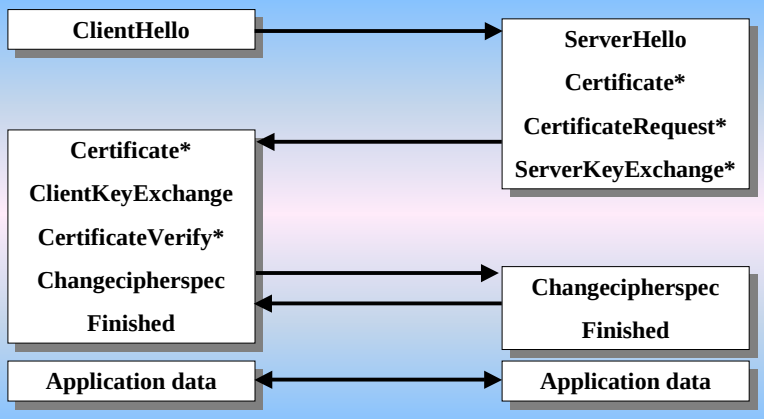
6. 무선인터넷 보안

❑ WTLS Protocols

Handshake protocol	서버와 클라이언트 간의 인증 수행 사용할 암호 알고리즘 및 키 분배
Change cipher spec protocol	설정된 세션 정보와 연결 정보를 사용한다는 것을 상대방에게 알린다
Alert protocol	오류 메시지 전송 (암호, 압축, MAC 오류, 인증서 실패, etc)
Record protocol	전송되는 메시지의 기밀성과 무결성 제공

6. 무선인터넷 보안

❑ WTLS Full Handshake Protocol



❖ TLS와 달리 인증서의 형식으로 X.509형식 뿐 아니라, WTLS 인증서, X9.68 인증서 중 하나를 선택해서 사용 가능

6. 무선인터넷 보안

❑ Abbreviated/Optimized Handshake

(1) Abbreviated Handshake Protocol

- 새로운 세션을 시작하지 않고 이전 세션 정보를 이용해 세션을 재사용 할 경우
- 인증서를 위한 정보들이 교환되지 않고, 암호 파라메터들도 처음부터 재 생성되지 않는다.

(2) Optimized Handshake Protocol

- 서버나 다른 저장소에 저장되어 있는 클라이언트 인증서를 통해 클라이언트를 인증하고자 할 경우

6. 무선인터넷 보안

❑ WTLS Record Protocol

(1) TLS와의 차이점

- TLS 에서 이루어지는 데이터 fragmentation(단편화)는 WTLS 에서 이루어지지 않음
  (하위 계층인 WDP/UDP 계층에서 단편화가 이루어 짐)