충남대학교
CHUNGNAM NATIONAL UNIVERSITY

블록암호 (2)

2022년 9월 28일 수요일

정보보호

충남대학교 정보보호연구실 허강준

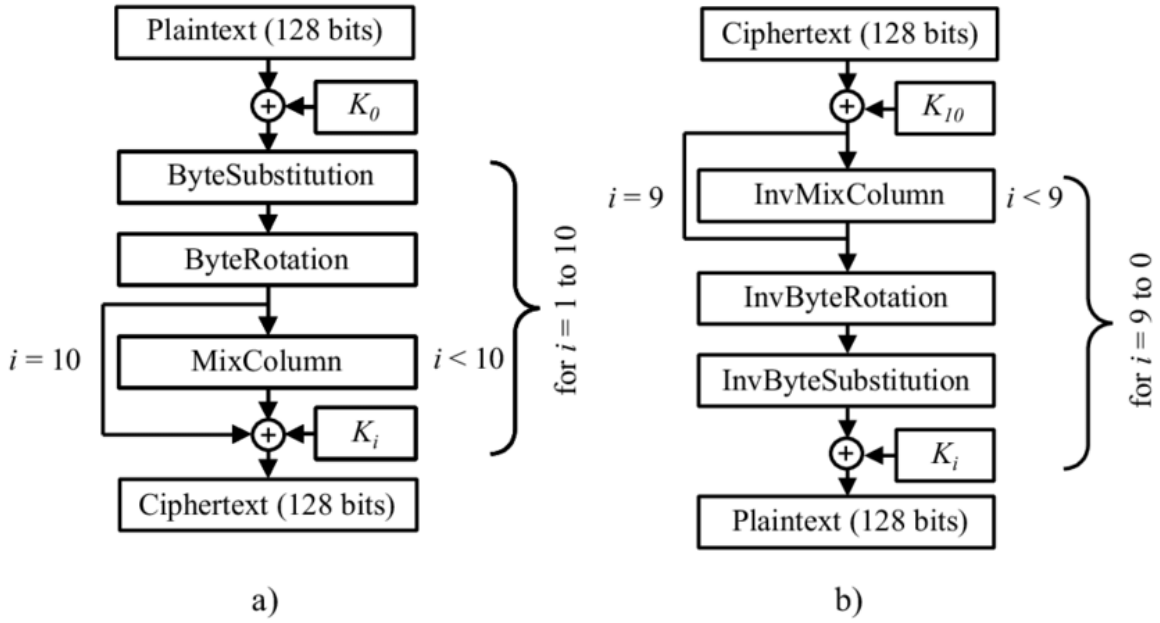
AES (Advanced Encryption Standard)

- AES (Advanced Encryption Standard)
  - DES를 대체하기 위한 차세대 암호 표준
  - 2001년 선정 (NIST-FIPS-197, ISO/IEC 18033-3)
  - 당시 경쟁자들
    - Rijndael → 최종 선정
    - MARS, RC6, Serpent, Twofish

https://dblp.org/db/conf/aes/index.html

AES (Advanced Encryption Standard)

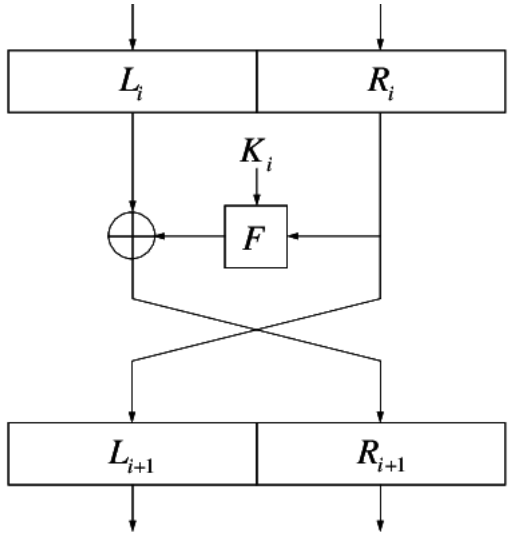
- Rijndael 암호
  - Joan Daemen, Vincent Rijmen
  - 128비트 블록 크기, 128/192/256 비트 키 길이
  - SPN (Substitution-Permutation Network) 구조

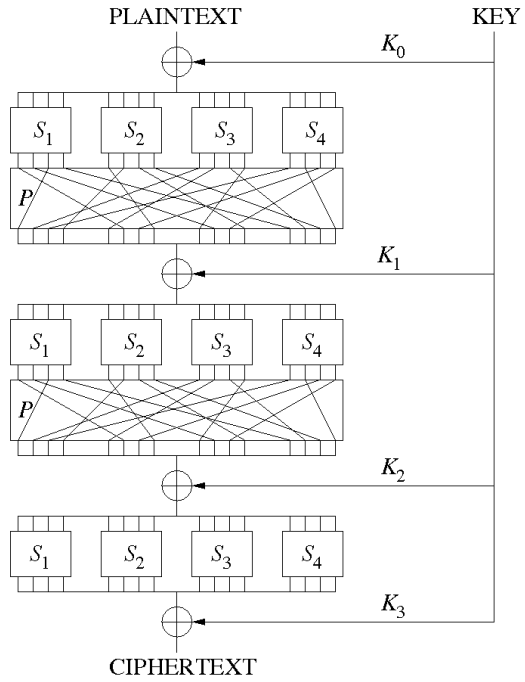


AES

Feistel vs SPN

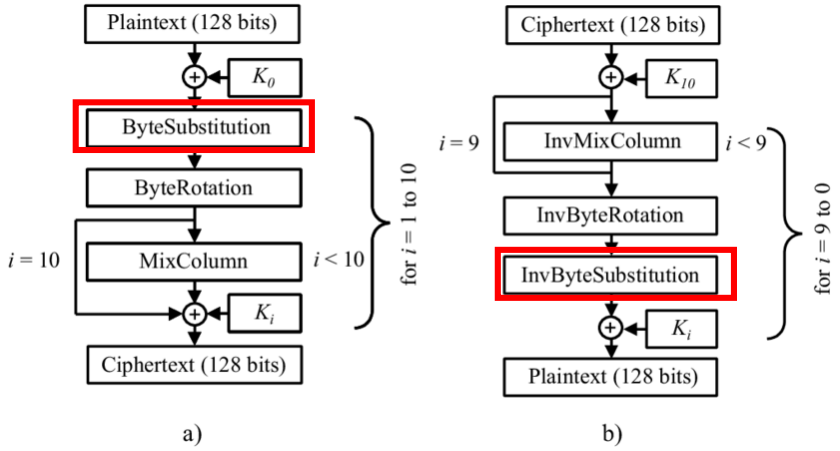
- 블록암호를 이루는 알고리즘들…
  - Feistel Network
  - SPN (Substitution-Permutation Network)





Feistel vs SPN

- AES의 S-Box



AES S-box

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

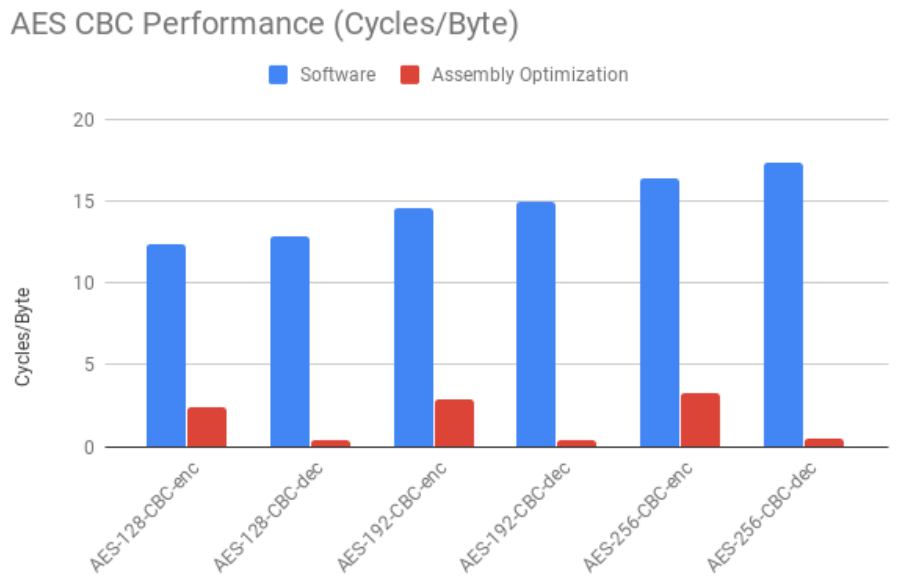
The column is determined by the least significant nibble, and the row by the most significant nibble. For example, the value $9a_{16}$ is converted into $b8_{16}$.

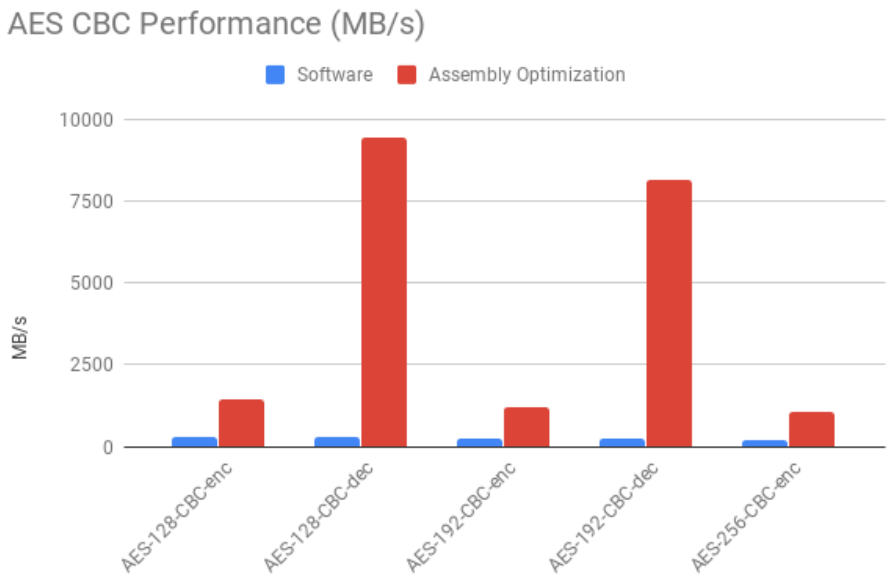
Inverse S-box

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

AES-NI?

- AES-NI (New Instructions)
  - CPU 자체에 탑재된 하드웨어 AES 명령어 → 굉장히 빠름!
  - 여러 CPU에서 지원
    - Intel: Sandy Bridge 이후부터 지원 (e.g. i5-2500)
    - AMD: Bulldozer 이후부터 지원





https://www.wolfssl.com/intels-extended-instructions-accelerate-aes-performance-amd-processors/

과제

- 블록암호를 이용한 암호 통신기 완성하기
- 이미 구현된 것들
  - 네트워크 코드 (소켓 등…)
  - 서버 (암호화 잘 되고 있는지…)

- 구현 해야 하는 것들
  - 입력 처리기 뒷단 → 메세지 송/수신 전에 해야하는 암호화 처리
  - AES 암복호화 코드 (직접구현 x, 라이브러리 사용!)
  - pyCryptodome: `pip install pycryptodome`

과제

- pyCryptodome를 이용한 AES-128 암호화 (ECB 모드)

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad

BLOCK_SIZE = 16

text = pad(b'This is a plaintext', BLOCK_SIZE)
key = b'16byte-key-here!'
cipher = AES.new(key, AES.MODE_ECB)

ciphertext = cipher.encrypt(text)
print(ciphertext)
```

- pad가 없으면?

ValueError: Data must be aligned to block boundary in ECB mode

과제

- pyCryptodome를 이용한 AES-128 암호화 (ECB 모드)

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad

# 암호화 전단계 생략…

ciphertext = cipher.encrypt(text) # 암호화 된 결과

plaintext = cipher.decrypt(ciphertext)
print( unpad(plaintext, BLOCK_SIZE) ) # This is a plaintext
```

- unpad가 없으면?

b'This is a plaintext\r\r\r\r\r\r\r\r\r\r\r\r\r'

이후 일정

주차	실습 주제	과제	날짜
1	오리엔테이션 & 썰풀기	과제를 위한 GitHub 설정	9/7
2	카이사르&비즈네르 암호	ENIGMA	9/14
3	XOR과 블록암호	Simplified DES 구현하기	9/21
4	여러가지 블록암호	블록암호를 이용하여 암호통신기 완성하기	9/28
5	블록암호 운용모드	S-DES-CBC, S-DES-ECB 구현하기	10/5
6	RSA	RSA 구현하기, 저강도 RSA 크랙하기	10/12
7	해시	암호통신기에 무결성 검증 기능 추가하기	10/19
8	중 간 고 사 (10/24)		공강
9	메세지 인증코드(MAC)	HMAC 구현하기	11/2
10	디지털 서명	사설인증서 생성 및 프로그램 코드 서명	11/9
11	하이브리드 암호	하이브리드 기반 암호 통신기	11/16
12	난수	시드값 추측을 이용한 암호문 크랙	11/23
13	블록체인과 머클 트리	머클트리 구현하기	11/30
14	TLS와 PGP(GPG)	GPG를 이용하여 암호 메일 보내기	12/7
15	기 말 고 사 (12/12)		종강

질문?

- 없으면 자리에서 일어나셔도 좋습니다 :)
- 대학원 입학 문의는 언제나 환영
  - 블록체인, Web 3, 해킹 관심있거나 유경험자 우대

입학문의

- 류재철 교수님 (jcryou [at] cnu.ac.kr)
- 허강준 조교 (knowledge [at] o.cnu.ac.kr)