충남대학교
CHUNGNAM NATIONAL UNIVERSITY

중간고사 해설

2022년 11월 1일 수요일

정보보호

충남대학교 정보보호연구실 허강준

1번

1. 다음과 같은 암호문을 복호화하여 평문을 제시하시오. (3점)

10 ㅜ 8 2 ㅏ 5 3 ㅐ 14 ㅏ 1 1 ㅛ

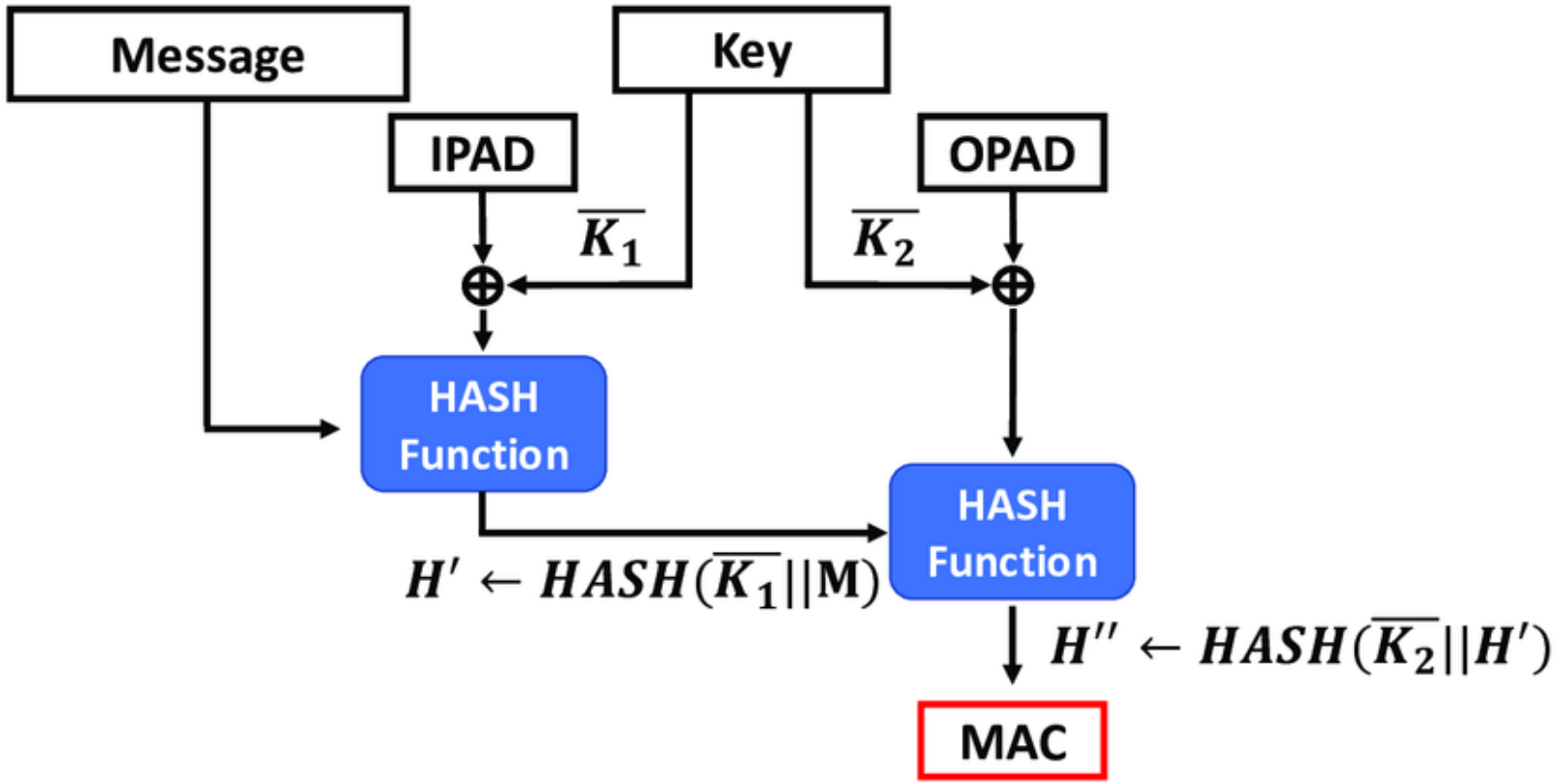
1	2	3	4	5	6	7	8	9	10	11	12	13	14
ㄱ	ㄴ	ㄷ	ㄹ	ㅁ	ㅂ	ㅅ	ㅇ	ㅈ	ㅊ	ㅋ	ㅌ	ㅍ	ㅎ

ㅊ ㅜ ㅇ ㄴ ㅏ ㅁ ㄷ ㅐ ㅎ ㅏ ㄱ ㄱ ㅛ

충남대학교

2. 다음 질문에 답하시오.

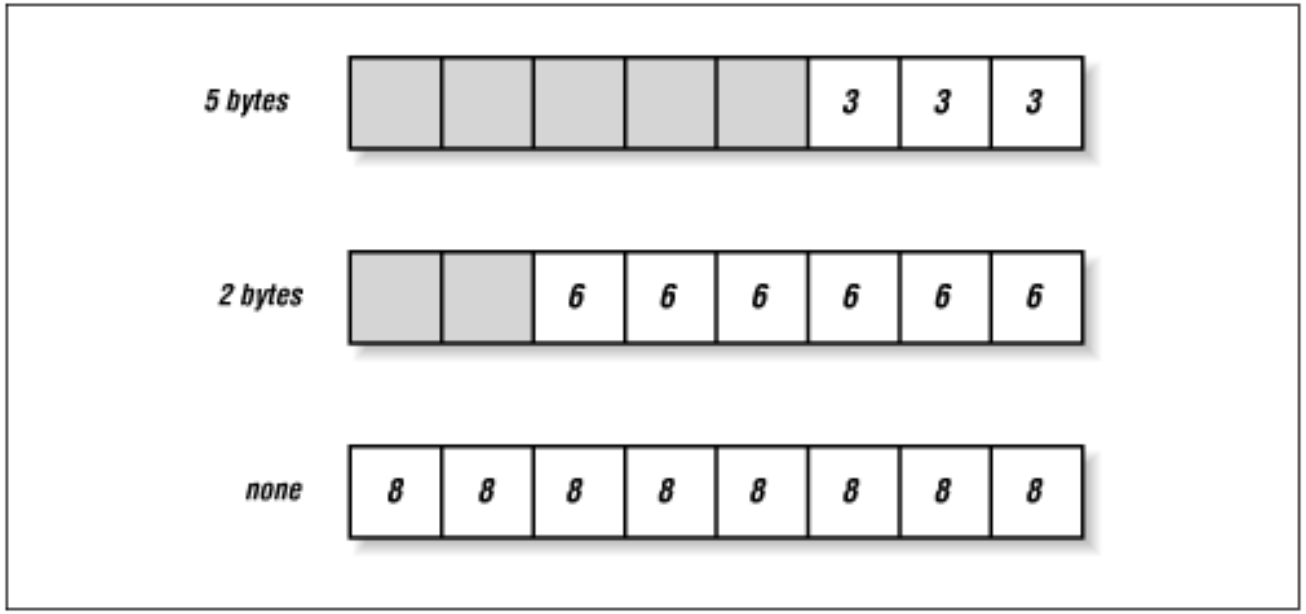
(가) MAC(Message Authentication Code) 개념을 설명하시오. (3점)



2. 다음 질문에 답하시오.

(나) MAC을 이용한 교통카드 동작과정을 제시하고 설명하시오. (4점)

3. 블록암호를 사용할 때 Padding의 용도에 대해 설명하고 이와 관련된 표준에 대해 설명하시오. (5점)



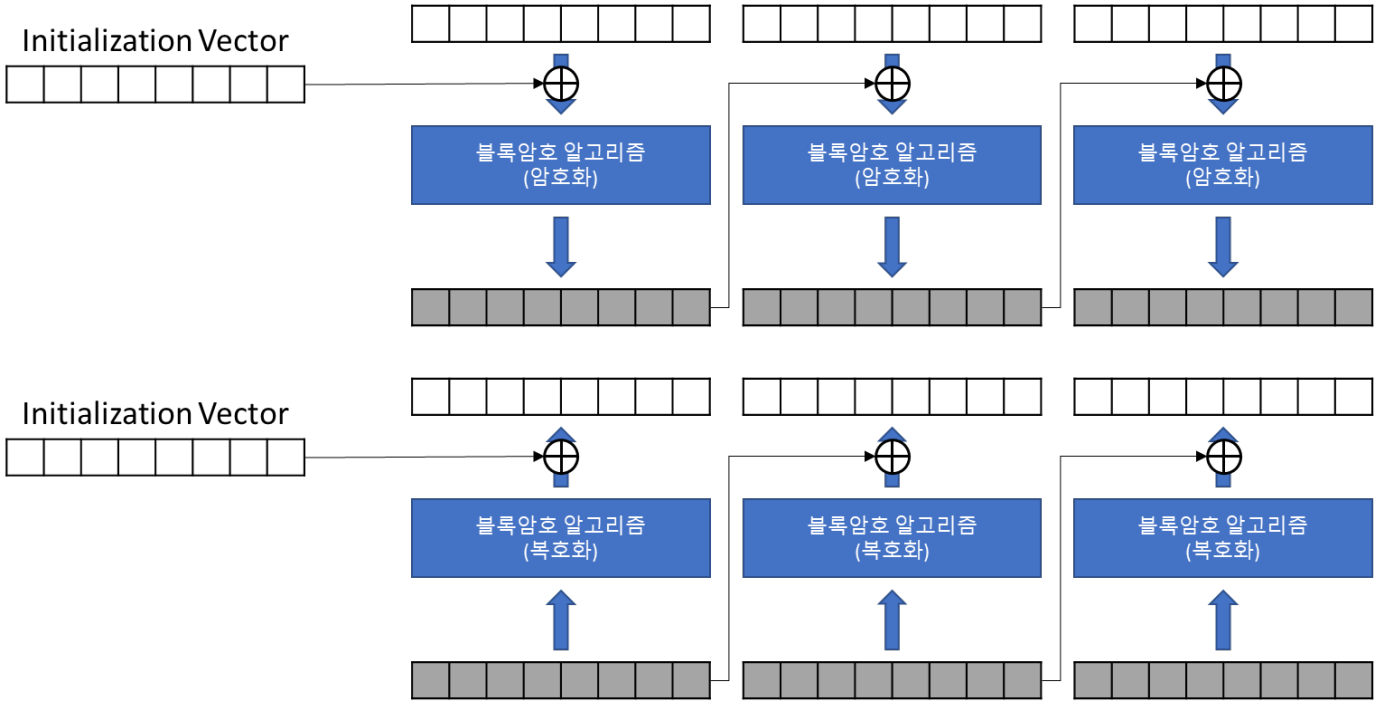
PKCS #5, PKCS #7

4. One Time-Pad(OTP) 작동 원리와 한계를 설명하시오. (5점)

평문:	10110011 11110000 00001111 11101110 11111111
암호키:	10000001 11111111 11110000 11001100 00001111
암호문:	00110010 00001111 11111111 00100010 11110000
암호키:	10000001 11111111 11110000 11001100 00001111
평문:	10110011 11110000 00001111 11101110 11111111

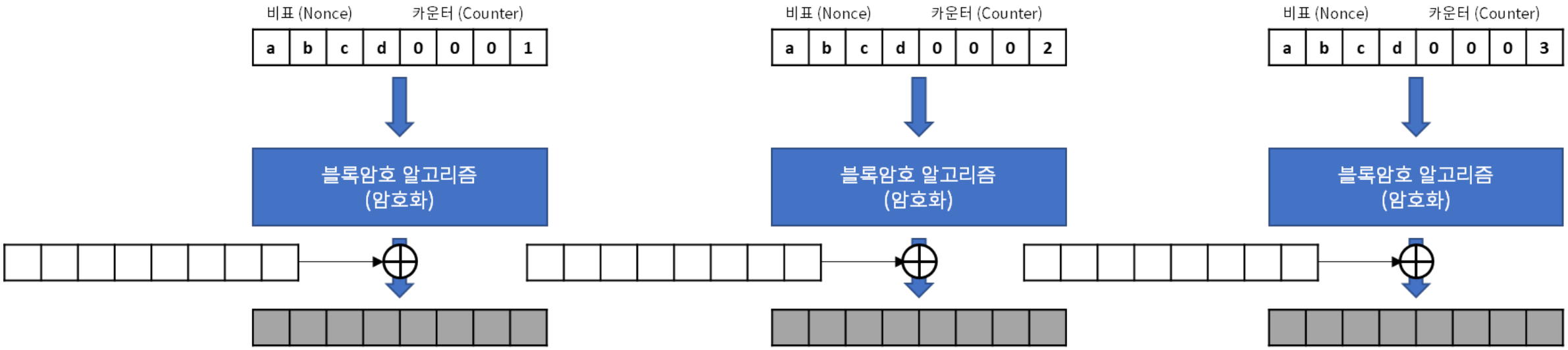
5. 관용암호방식의 운용모드와 관련하여 다음에 답하시오.

(가) CBC, CFB, OFB에서는 IV(Initialization Vector)를 사용한다. IV 용도에 대해 설명하시오. (2점)



5. 관용암호방식의 운용모드와 관련하여 다음에 답하시오.

(나) CTR은 암복화 과정에서 병렬처리 및 사전처리가 가능하다고 한다. 어떻게 가능한지 설명하시오. (3점)



6. 어떤 사람의 개인키가 유출되었다. 이를 활용하여 17을 암,복호화를 진행하고 식을 보이시오. (5점)

```
RSAPrivateKey ::= SEQEUNCE {
  version                 1,
  modulus                 33,
  publicExponent          7,
  privateExponent         3,
  prime1                  3,
  prime2                  11,
  exponent1               0,
  exponent2               3,
}
```

$N = 3 \times 11 = modulus$

$p = 17^3 \ mod \ 33$
$= 4913 \ mod \ 33$
$= 29$

$c = 29^7 \ mod \ 33$
$= 17249876309 \ mod \ 33$
$= 17$

$c = 17^7 \ mod \ 33$
$= 410338673 \ mod \ 33$
$= 8$

$p = 8^3 \ mod \ 33$
$= 512 \ mod \ 33$
$= 17$

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)