Korea Communications Standard

방송통신표준

KCS.KO-12.0166

제정일: 2013년 12월 31일

64 비트 블록 암호 HIGHT 운영 모드

Modes of Operation for the 64-bit Block Cipher HIGHT

미래창조과학부

국립전파연구원

방송통신표준

KCS.KO-12.0166 제정일: 2013년 12월 31일

64 비트 블록 암호 HIGHT 운영 모드

Modes of Operation for the 64-bit Block Cipher HIGHT

미래창조과학부

국립전파연구원

서 문

1. 표준의 목적

본 표준은 정보처리시스템 및 정보통신망 환경에 사용되는 64 비트 블록 암호 알고리즘 표준 HIGHT(HIGh security and lightweigHT)의 운영 모드 전자 코드 북(ECB, Electronic Code Book), 암호 블록 연결(CBC, Cipher Block Chaining), 암호 피드백(CFB, Ciper FeedBack), 출력 피드백(OFB, Output FeedBack), 카운터(CTR)에 대해 규정한다.

2. 주요 내용 요약

64 비트 블록 암호 알고리즘 HIGHT에 대한 운전자 코드 북(ECB, Electronic Code Book), 암호 블록 연결(CBC, Cipher Block Chaining), 암호 피드백(CFB, Ciper FeedBack), 출력 피드백(OFB, Output FeedBack), 카운터(CTR)운영 모드의 암·복호화 과정을 규정하고 있으며, 구현 적합성을 확인하기 위한 참조 구현값이 부록에 명시되어 있다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

본 표준은 RFID 등과 같이 초고속, 초경량, 저전력을 요구하는 유비쿼터스 컴퓨팅 환경에서의 기밀성 기능을 제공하는 정보 보호 시스템 및 암호 제품에 다양하게 활용되어 국내 정보통신망의 안전성·신뢰성을 제고할 수 있다

4. 참조 표준(권고)

4.1. 국외 표준(권고)

- NIST SP 800-38A, 'Recommendation for Block Cipher Modes of Operation - Methods and Techniques', 2001.
- ISO/IEC 10116, 'Information technology — Security techniques — Modes of operation for an n-bit block cipher', 2006.

4.2. 국내 표준

- TTAS.KO-12.0040/R1, '64비트 블록암호 HIGHT', 2008.12.

5. 참조 표준(권고)과의 비교

5.1. 참조 표준(권고)과의 관련성

본 표준은 'NIST SP 800-38A'와 'ISO/IEC 10116' 표준에서 ECB, CBC, CFB, OFB, CTR 운영 모드에 대한 기본적인 개념 및 설계 기준만을 참조하고 있다.

5.2. 참조한 표준(권고)과 본 표준의 비교표

KCS.KO-12.0166	참조 표준			비고
	NIST SP 800-38A	ISO/IEC 10116	TTAS.KO-12.0040/R1	
1. 개요	-	-	-	추가
2. 표준의 구성 및 범위	-	-	-	추가
3. 용어 정의 및 약어	-	-	-	추가
4. 운영 모드	6. BLOCK CIPHER MODES OF OPERATION	6. Electronic Codebook(ECB) mode 7. Cipher Block Chaining(CBC) mode 8. Cipher Feedback(CFB) mode 9. Output Feedback(OFB) mode 10. Counter (CTR) mode	5. 운영 모드	수정
부록 I. 덧붙이기(패딩) 방법	APPENDIX A: PADDING	-	부록 I. 덧붙이기 방법	수정
부록 II. 참조 구현값	APPENDIX F: EXAMPLE VECTORS FOR MODES OF OPERATION OF THE AES	Annex D. Examples for the Modes of Operation	부록 II. 참조구현값	수정
부록 III. 관련 문헌	-	-	-	추가

6. 지식 재산권 관련 사항

본 표준의 ‘지적 재산권 확약서’ 제출 현황은 국립전파연구원 웹사이트에서 확인할 수 있다.

※본 표준을 이용하는 자는 이용함에 있어 지식 재산권이 포함되어 있을 수 있으므로, 확인 후 이용한다.

※본 표준과 관련하여 접수된 확약서 이외에도 지식 재산권이 존재할 수 있다.

7. 시험 인증 관련 사항

7.1. 시험 인증 대상 여부

해당 사항 없음.

7.2. 시험 표준 제정 현황

해당 사항 없음.

8. 표준의 이력 정보

8.1. 표준의 이력

판 수	제정·개정일	제정·개정 내역
제1판	2013.12.31.	제정 KCS,KO-12.0166

8.2. 주요 개정 사항

해당 사항 없음.

Preface

1. Purpose of Standard

This Standard provides specifications of the recommended ECB, CBC, CFB, OFB and CTR modes of operation for the 64-bit block cipher HIGHT in the information processing systems and communication environments.

2. Summary of Contents

This standard explains the structure of ECB, CBC, CFB, OFB and CTR modes of operation for 64-bit block cipher HIGHT.

3. Applicable Fields of Industry and its Effect

This standard facilitates to implement ECB, CBC, CFB, OFB and CTR modes of operation for 64-bit block cipher HIGHT that has been applied to many cryptographic applications to provide Ubiquitous environment.

4. Reference Standards(Recommendations)

4.1. International Standards(Recommendations)

- NIST SP 800-38A, “Recommendation for Block Cipher Modes of Operation - Methods and Techniques”, 2001.
- ISO/IEC 10116, “Information technology — Security techniques — Modes of operation for an n-bit block cipher”, 2006.

4.2. Domestic Standards

- TTAS.KO-12.0040/R1, “64-bit Block Cipher HIGHT”, 2008.12.

5. Comparison between Reference Standards(Recommendations) and this Standard

5.1. Relevance of this Standard with Reference Standards(Recommendations)

This standard refers to the basic concept and design principle of ECB, CBC, CFB, OFB and CTR modes of operation in NIST SP 800-38A and ISO/IEC 10116.

5.2. A Comparative Table of Reference Standard(Recommendation) and this Standard

KCS.KO-12.0166	Reference Standards			Remarks
	NIST SP 800-38A	ISO/IEC 10116	TTAS.KO-12.0040/R1	
1. Introduction	-	-	-	Added
2. Constitution and Scope	-	-	-	Added
3. Terms Definition and Abbreviations, Symbols	-	-	-	Added
4. Mode of Operation	6. BLOCK CIPHER MODES OF OPERATION	6. Electronic Codebook(ECB) mode 7. Cipher Block Chaining(CBC) mode 8. Cipher Feedback(CFB) mode 9. Output Feedback(OFB) mode 10. Counter (CTR) mode	5. Mode of Operation	Modified
Appendix Ⅰ. Padding Method	APPENDIX A: PADDING	-	Appendix Ⅰ. Padding Method	Modified
Appendix Ⅱ. Test Vectors	APPENDIX F: EXAMPLE VECTORS FOR MODES OF OPERATION OF THE AES	Annex D. Examples for the Modes of Operation	Appendix Ⅱ. Test Vectors	Modified
Appendix Ⅲ. Related Documents	-	-	-	Added

6. Statement of Intellectual Property Rights

"Written Confirmation of Intellectual Property Rights" for this standard can be referenced to the website of the National Radio Research Agency.

Those using this standard must confirm that whether intellectual property rights are included in this standard.

Other intellectual property rights may exist in relation to written confirmation received for this standard.

7. Statement of Testing and Certification

7.1. Object of Testing and Certification

None

7.2. Standards of Testing and Certification

None

8. History of Standard

8.1. Change History

Edition	Issued date	History
The 1st edition	2013.12.31.	Established KCS.KO-12.0166

8.2. Revisions Related Details

None

목 차

Contents

64 비트 블록 암호 HIGHT 운영 모드
(Modes of Operation for the 64-bit Block Cipher HIGHT)

1. 개요

본 표준은 64 비트 블록 암호 HIGHT를 이용하여 64 비트 블록보다 큰 길이의 데이터를 암호화·복호화할 때, 해당 데이터를 블록 단위로 분할하여 암호화·복호화하는 운영 모드 전자 코드 북(ECB, Electronic Code Book), 암호 블록 연결(CBC, Cipher Block Chaining), 암호 피드백(CFB, Ciper FeedBack), 출력 피드백(OFB, Output FeedBack), 카운터(CTR)에 대해 규정한다.

2. 표준의 구성 및 범위

본 표준에서는 HIGHT의 운영 모드로 전자 코드 북(ECB, Electronic Code Book), 암호 블록 연결(CBC, Cipher Block Chaining), 암호 피드백(CFB, Ciper FeedBack), 출력 피드백(OFB, Output FeedBack), 카운터(CTR) 모드를 규정하고, 각 운영 모드의 암호화·복호화 과정의 상세 명세와 운영 모드를 사용하기 위한 매개변수값을 규정한다. 부가적으로, 운영 모드 사용에 필요한 덧붙이기 방법과 표준 적합성 테스트를 위한 참조 구현값은 부록에서 기술한다.

3. 용어 정의 및 약어

3.1. 용어 정의

평문	암호화 대상 또는 암호문을 복호화한 원래의 데이터
평문 데이터	평문 블록들의 집합
암호문	평문을 암호 알고리즘을 이용하여 변환한 데이터
암호문 데이터	암호문 블록들의 집합
암호화	평문을 암호문으로 변환하는 과정
복호화	암호문을 평문으로 변환하는 과정
비밀 키	평문 또는 암호문의 암·복호화에 사용되는 비밀정보
평문 블록	운영 모드에 사용되는 블록 크기의 평문
암호문 블록	운영 모드에 사용되는 블록 크기의 암호문

3.2. 약어

CBC	Cipher Block Chaining
CFB	Cipher FeedBack
ECB	Electronic Codebook
OFB	Output FeedBack

3.3. 기호

K	비밀 키
P	평문 데이터
C	암호문 데이터
IV	초기값
ctr	초기 카운터 블록
P_i	i 번째 단계의 평문 블록
C_i	i 번째 단계의 암호문 블록
I_i	i 번째 단계의 HIGHT의 입력 블록
O_i	i 번째 단계의 HIGHT의 출력 블록
$E_K(\cdot)$	비밀 키 K 를 이용한 HIGHT 암호화 함수
$D_K(\cdot)$	비밀 키 K 를 이용한 HIGHT 복호화 함수
$X \mid\mid Y$	X 와 Y의 연접 연산
$X \oplus Y$	X 와 Y의 배타적 논리합 연산
$X \bmod Y$	X 를 Y 로 나눈 나머지
$LSB_s(X)$	X 의 하위 s 비트 예) $LSB_3(10100011) = 011$
$MSB_s(X)$	X의 상위 s 비트 예) $MSB_3(10100011) = 101$

4. 운영 모드

4.1. ECB 모드

ECB 모드는 평문 블록을 암호문 블록으로 독립적으로 암호화하는 운영 모드이다.

4.1.1. ECB 모드 암호화

ECB 모드의 암호화 과정은 평문 블록(P_i)을 입력 블록(I_i)으로 설정하고, 이를 암호화한 출력 블록(O_i)을 암호문 블록(C_i)으로 설정한다.

○ ECB 모드 암호화 의사 코드

```
o 입력 : P={P1,…,Pn}, K
o 출력 : C={C1,…,Cn}
o 처리 과정
   for i = 1 to n
        Ii = Pi
        Oi = EK(Ii)
        Ci = Oi
```

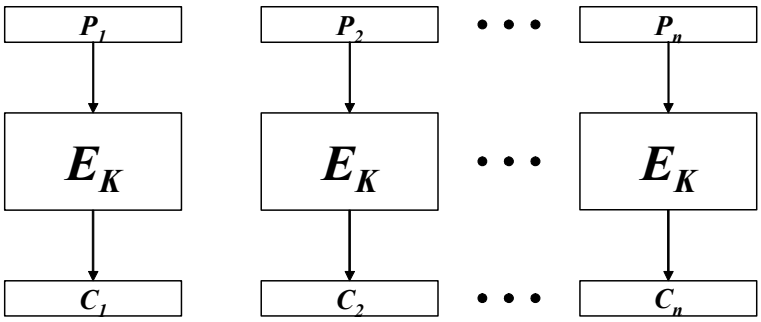

그림 4.2 ECB 모드 암호화

4.1.2. ECB 모드 복호화

ECB 모드의 복호화 과정은 암호문 블록(C_i)를 입력 블록(I_i)으로 설정하고, 이를 복호화한 출력 블록(O_i)을 평문 블록(P_i)으로 설정한다.

○ ECB 모드 복호화 의사 코드

```
o 입력 : C={C1,…,Cn}, K
o 출력 : P={P1,…,Pn}
o 처리 과정
   for i=1 to n
        Ii = Ci
        Oi = DK(Ii)
        Pi = Oi
```

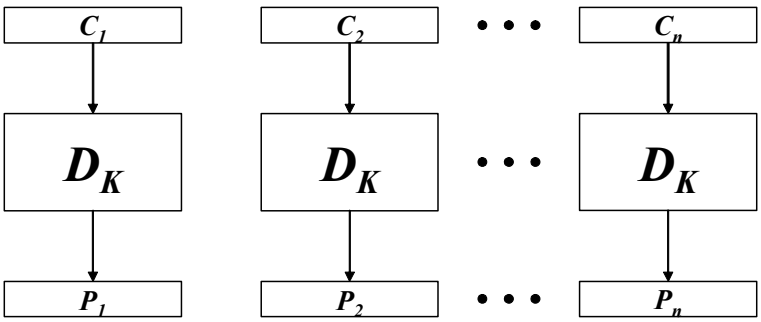

그림 4.3 ECB 모드 복호화

4.2. CBC 모드

CBC 모드는 동일한 평문 블록과 암호문 블록 쌍이 발생하지 않도록 전 단계의 암호화·복호화한 결과가 현 단계에 영향을 주는 운영 모드이다.

4.2.1. CBC 모드 암호화

CBC 모드의 암호화 과정은 현 단계의 평문 블록(P_i)과 전 단계의 암호문 블록(C_{i-1})을 배타적 논리합(exclusive OR) 연산한 결과를 현 단계의 입력 블록(I_i)으로 설정하고, 이를 암호화한 출력 블록(O_i)을 현 단계의 암호문 블록(C_i)으로 설정한다.

○ CBC 모드 암호화 의사 코드

```
o 입력 : P={P1,…,Pn}, K, IV
o 출력 : C={C1,…,Cn}
o 처리 과정
   C0 = IV
   for i=1 to n
        Ii = Pi ⊕ Ci-1
        Oi = EK(Ii)
        Ci = Oi
```

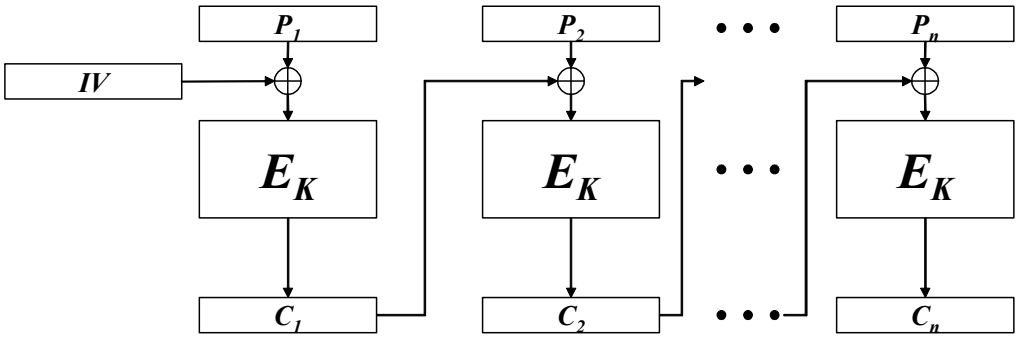

그림 4.4 CBC 모드 암호화

4.2.2. CBC 모드 복호화

CBC 모드의 복호화 과정은 현 단계의 암호문 블록(C_i)을 입력 블록(I_i)으로 설정하고, 이를 복호화한 출력 블록(O_i)을 전 단계의 입력 블록(I_{i-1})인 암호문 블록(C_{i-1})과 배타적 논리합 연산한 결과를 현 단계의 평문 블록(P_i)으로 한다.

○ CBC 모드 복호화 의사 코드

```
o 입력 : C={C1,…,Cn}, K, IV
o 출력 : P={P1,…,Pn}
o 처리 과정
   C0 = IV
   for i=1 to n
        Ii = Ci
        Oi = DK(Ii)
        Pi = Ci-1 ⊕ Oi
```

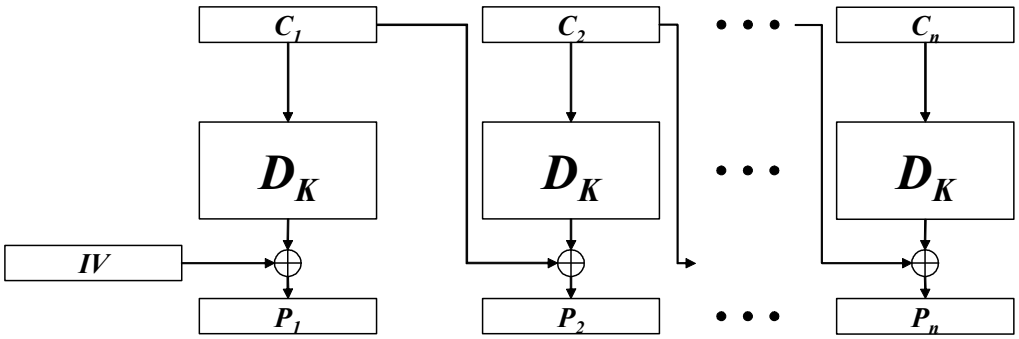

그림 4.5 CBC 모드 복호화

4.3. CFB 모드

CFB 모드에서는 평문 데이터를 s 비트 평문 블록으로 분할하여 암호화·복호화를 수행하는 운영 모드이다. 단. 본 표준에서는 매개변수 s 를 1, 8, 16, 32, 64로 제한하고, 매개변수 s 에 따라 “CFB-s 모드”로 표기한다.

4.3.1. CFB 모드 암호화

CFB-s 모드의 암호화 과정은 입력 블록(I_i)을 암호화한 출력 블록(O_i)의 상위 s 비트($MSB_s(O_i)$)를 평문 블록(P_i) s 비트와 배타적 논리합 연산을 수행함으로 암호문 블록(C_i) s 비트를 생성한다. 다음 단계의 입력 블록(I_{i+1})은 현 단계의 입력 블록의 하위 64-s 비트($LSB_{64-s}(I_i)$)와 현 단계의 암호문 블록(C_i) s비트와 연접 결합함으로 64 비트 블록을 생성한다.

○ CFB-s 모드 암호화 의사 코드

o 입력 : P={P_1,…,P_n}, K, IV, s
o 출력 : C={C_1,…,C_n}
o 처리 과정
$I_1 = IV$
for i=1 to n
$O_i = E_K(I_i)$
$C_i = P_i \oplus MSB_s(O_i)$
$I_{i+1} = LSB_{64-s}(I_i) \,||\, C_i$

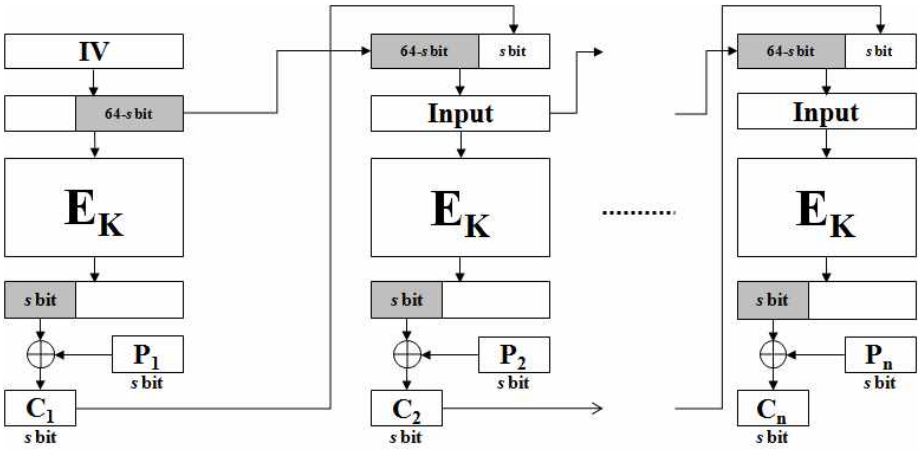

그림 4.6 CFB-s 모드 암호화

4.3.2. CFB 모드 복호화

CFB-s 모드의 복호화 과정은 입력 블록(I_i)을 암호화한 출력 블록(O_i)의 상위 s비트($MSB_s(O_i)$)를 암호문 블록(C_i) s비트와 배타적 논리합 연산을 수행함으로 평문 블록(P_i) s비트를 생성한다. 다음 단계의 입력 블록(I_{i+1})은 현 단계의 입력 블록의 하위 64-s 비트($LSB_{64-s}(I_i)$)와 현 단계의 암호문 블록(C_i) s 비트와 연접 결합함으로 64 비트 블록을 생성한다.

○ CFB-s 모드 복호화 의사 코드

o 입력 : $C=\{C_1,\cdots,C_n\}$, K, IV, s
o 출력 : $P=\{P_1,\cdots,P_n\}$
o 처리 과정
$I_1 = IV$
for $i=1$ to n
$O_i = E_K(I_i)$
$P_i = C_i \oplus MSB_s(O_i)$
$I_{i+1} = LSB_{64-s}(I_i) \parallel C_i$

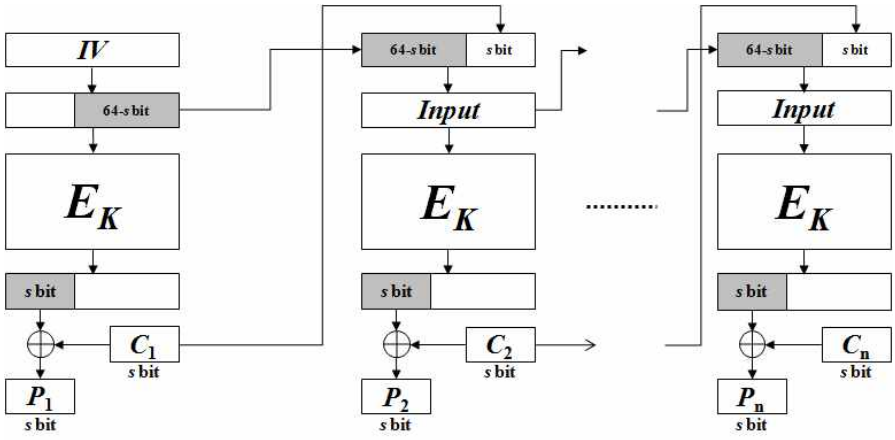

그림 4.7 CFB-*s* 모드 복호화

4.4. OFB 모드

OFB(Output FeedBack) 모드는 전 단계의 출력 블록을 현 단계의 입력 블록으로 사용하는 운영 모드이다.

4.4.1. OFB 모드 암호화

OFB 모드의 암호화 과정은 입력 블록(I_i)을 암호화한 출력 블록(O_i)과 평문 블록(P_i)를 배타적 논리합 연산을 수행함으로 암호문 블록(C_i)을 생성한다. 다음 단계의 입력 블록(I_{i+1})은 현 단계의 출력 블록(O_i)으로 설정한다.

○ OFB 모드 암호화 의사 코드

o 입력 : $P=\{P_1,\cdots,P_n\}$, K, IV
o 출력 : $C=\{C_1,\cdots,C_n\}$
o 처리 과정

$I_1 = IV$
for $i=1$ to n
$O_i = E_K(I_i)$
$C_i = P_i \oplus O_i$
$I_{i+1} = O_i$

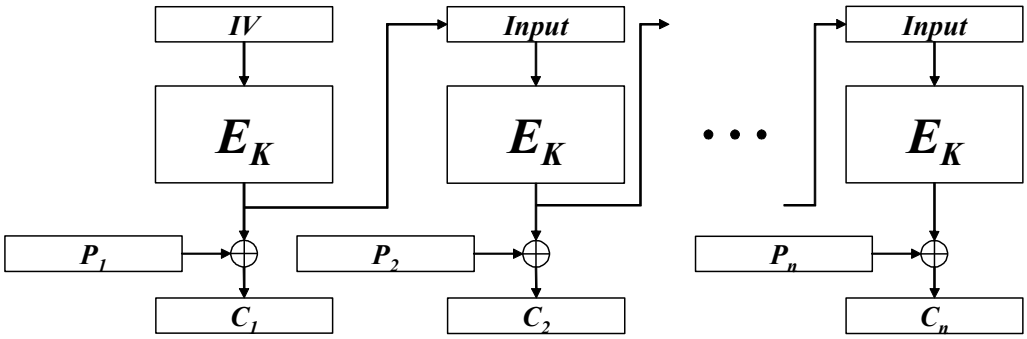

그림 4.8 OFB 모드 암호화

4.4.2. OFB 모드 복호화

OFB 모드의 복호화 과정은 입력 블록(I_i)을 암호화한 출력 블록(O_i)과 암호문 블록(C_i)을 배타적 논리합 연산을 수행함으로 평문 블록(P_i)을 생성한다. 다음 단계의 입력 블록(I_{i+1})은 현 단계의 출력 블록(O_i)으로 설정한다.

○ OFB 모드 복호화 의사 코드

o 입력 : $C=\{C_1,\cdots,C_n\}$, K, IV
o 출력 : $P=\{P_1,\cdots,P_n\}$
o 처리 과정
$I_1 = IV$
for $i=1$ to n
$O_i = E_K(I_i)$
$P_i = C_i \oplus O_i$
$I_{i+1} = O_i$

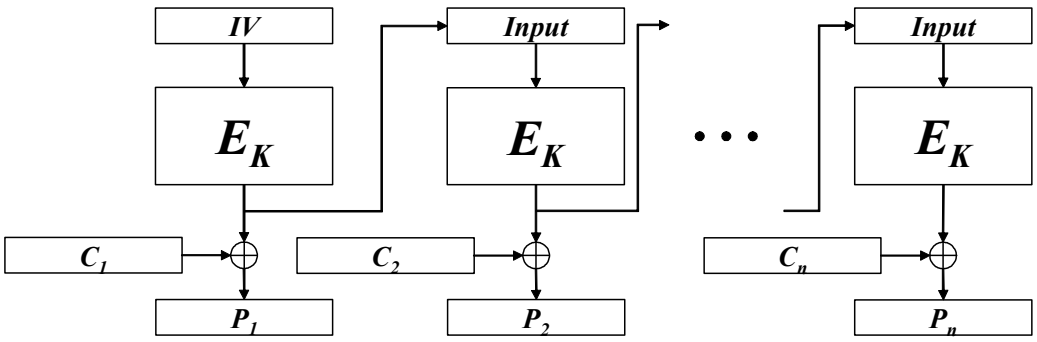

그림 4.9 OFB 모드 복호화

4.5. CTR 모드

CTR(Counter) 모드는 각 단계에 따라 증가되는 카운트 블록을 입력 블록으로 사용하는 운영 모드이다.

4.5.1. CTR 모드 암호화

CTR 모드의 암호화 과정은 카운터($ctr+(i-1)$)를 현 단계의 입력 블록(I_i)으로 하여 암호화한 출력 블록(O_i)을 평문 블록(P_i)과 배타적 논리합 연산을 수행함으로 암호문 블록(C_i)을 생성한다.

○ CTR 모드 암호화 의사 코드

o 입력 : $P=\{P_1,\cdots,P_n\}$, K, ctr
o 출력 : $C=\{C_1,\cdots,C_n\}$
o 처리 과정
for $i=1$ to n
$I_i = ctr+(i-1) \bmod 2^{64}$
$O_i = E_K(I_i)$
$C_i = P_i \oplus O_i$

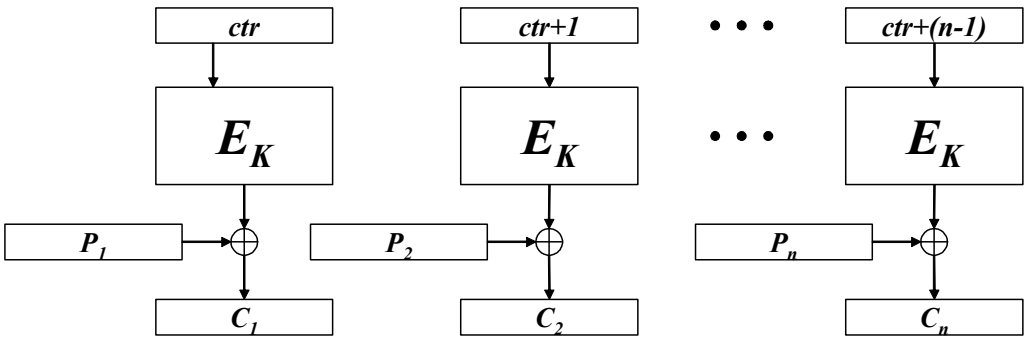

그림 4.10 CTR 모드 암호화

4.5.2. CTR 모드 복호화

CTR 모드의 복호화 과정은 카운터($ctr+(i-1)$)를 현 단계의 입력 블록(I_i)으로 하여 암호화한 출력 블록(O_i)을 암호문 블록(C_i)과 배타적 논리합 연산을 수행함으로 평문 블록(P_i)을 생성한다.

○ CTR 모드 복호화 의사 코드

o 입력 : $C=\{C_1,\cdots,C_n\}$, K, ctr
o 출력 : $P=\{P_1,\cdots,P_n\}$
o 처리 과정
for $i=1$ to n
$I_i = ctr+(i-1) \bmod 2^{64}$
$O_i = E_K(I_i)$
$P_i = C_i \oplus O_i$

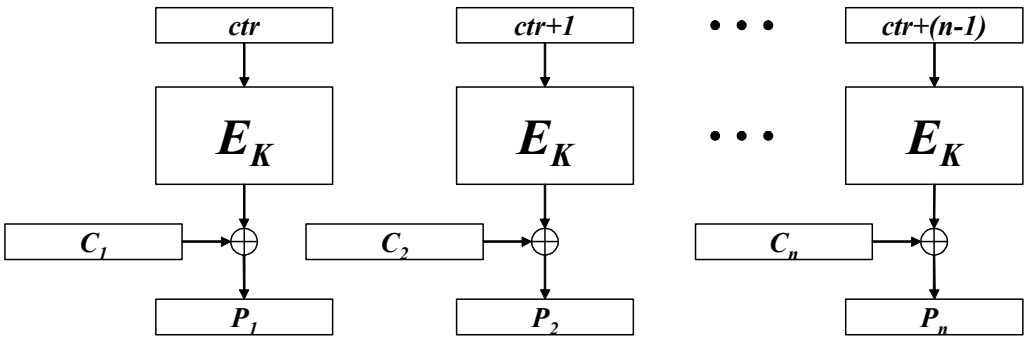

그림 4.11 CTR 모드 복호화

부 록 Ⅰ
덧붙이기(패딩) 방법

ECB, CBC 모드는 평문 블록을 암호화의 입력으로 사용하기 때문에, 평문 데이터의 길이가 64 비트의 양의 정수 배가 되도록 덧붙이기 방법이 적용되어야만 한다. 그러나, CFB-s, OFB, CTR 모드의 경우, 마지막 암호화 단계의 평문 블록이 64 비트(CFB-s 모드의 경우 s 비트)를 만족하지 못하고 m 비트가 남아있을 때, 마지막 출력 블록(On) 64 비트 중 상위 m 비트(MSBs(On))와 마지막 평문 블록 m 비트와 배타적 논리합 연산함으로 덧붙이기 방법을 적용하지 않을 수 있다.

본 덧붙이기 방법은 ISO/IEC 국제 표준 및 공개 키 암호 표준(PKCS, Public-Key Cryptography Standards)에서 사용되는 방법으로, 적용되는 시스템에 맞는 방법을 선택하여 사용함을 권고한다. 단, '덧붙이기 방법 1'의 경우, 복호화할 평문 데이터와 추가로 덧붙여진 값과의 구분이 모호할 수 있으므로 평문 데이터의 길이가 명확히 알려져 있는 경우에 사용함을 권고한다.

덧붙이기 방법의 사용 예는 16진법 바이트 단위로 표기된다.

Ⅰ.1. 덧붙이기 방법 1

평문 데이터의 길이가 (64×t+m) 비트 (0≤m<64, 0≤t)일 때, m이 0이 아닐 경우, 평문 데이터의 길이가 64 비트의 양의 정수배가 되도록 평문 데이터의 끝에 (64-m) 개의 '0' 비트를 덧붙인다.

예) 평문 데이터(48 비트) : 4F 52 49 54 48 4D
적용 결과(64 비트) : 4F 52 49 54 48 4D 00 00

평문 데이터(64 비트) : 53 45 45 44 41 4C 47 A8
적용 결과(64 비트) : 53 45 45 44 41 4C 47 A8

Ⅰ.2. 덧붙이기 방법 2

평문 데이터의 길이가 (64×t+m) 비트 (0≤m<64, 0≤t)일 때, m이 0이 아닐 경우, 평문 데이터의 길이가 64 비트의 양의 정수 배가 되도록 평문 데이터의 끝에 비트 '1'을 추가한 후 (64-m-1) 개의 '0' 비트를 덧붙인다. 또한, m이 0인 경우에는 덧붙이기 방법이 사용됨을 표기하기 위해, 추가적인 64 비트 '10…00' 블록을 추가한다.

예) 평문 데이터(48 비트) : 4F 52 49 54 48 4D
적용 결과(64 비트) : 4F 52 49 54 48 4D 80 00
평문 데이터(64 비트) : 53 45 45 44 41 4C 47 A8
적용 결과(128 비트): 53 45 45 44 41 4C 47 A8 80 00 00 00 00 00 00 00

Ⅰ.3. 덧붙이기 방법 3

본 덧붙이기 방법은 바이트 단위로만 적용이 되는 방법이다. 평문 데이터의 길이가 (8×t+m) 바이트 (0≤m<8, 0≤t)일 때, m이 0이 아닐 경우 평문 데이터의 길이가 8 바이트의 양의 정수배가 되도록 평문 데이터의 끝에 덧붙이기가 필요한 바이트 수 (8-m)을 덧붙인다. m이 0인 경우에는 덧붙이기 방법이 사용됨을 표기하기 위해, 추가적인 8 바이트 '08…08' 블록을 추가한다.

예) 평문 데이터(6 바이트) : 4F 52 49 54 48 4D
적용 결과(8 바이트) : 4F 52 49 54 48 4D 02 02

평문 데이터(8 바이트) : 53 45 45 44 41 4C 47 A8
적용 결과(16 바이트) : 53 45 45 44 41 4C 47 A8 08 08 08 08 08 08 08 08

부 록 II
참조 구현값

본 부록에서는 HIGHT 운영 모드 표준의 구현 적합성 실험을 위한 참조 구현값(Test Vectors)이 제공된다.

참조 구현값을 생성하기 위한 평문 데이터와 키, 초기값, 초기 카운트는 아래와 같다. 512 비트 입력 데이터 1과 데이터 2에 대한 참조 구현값은 암호화·복호화 연산에서 단계별 입력 블록(Ii), 출력 블록(Oi)의 구체적인 중간값(Intermediate Value)이 추가로 제공된다.

o 초기값

26 8d 66 a7 35 a8 1a 81

o 데이터 1

d7 6d 0d 18 32 7e c5 62
b1 5e 6b c3 65 ac 0c 0f
8d 41 e0 bb 93 85 68 ae
eb fd 92 ed 1a ff a0 96
39 4d 20 fc 52 77 dd fc
4d e8 b0 fc e1 eb 2b 93
d4 ae 40 ef 47 68 c6 13
b5 0b 89 42 f7 d4 b9 b3

o 데이터 2

6b c1 be e2 2e 40 9f 96
e9 3d 7e 11 73 93 17 2a
ae 2d 8a 57 1e 03 ac 9c
9e b7 6f ac 45 af 8e 51
30 c8 1c 46 a3 5c e4 11
e5 fb c1 19 1a 0a 52 ef
f6 9f 24 45 df 4f 9b 17
ad 2b 41 7b e6 6c 37 10

o 키1

88 E3 4F 8F 08 17 79 F1 E9 F3 94 37 0A D4 05 89

o 키2

2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

II.1. HIGHT ECB 운영 모드

II.1.1. HIGHT ECB 평문1, 키1 - 암호화

```
블록 #1
        평문 블록 1   :d76d0d18327ec562
        입력 블록 1   :d76d0d18327ec562
        출력 블록 1   :e4bc2e312277e4dd
        암호문 블록 1 :e4bc2e312277e4dd
블록 #2
        평문 블록 2   :b15e6bc365ac0c0f
        입력 블록 2   :b15e6bc365ac0c0f
        출력 블록 2   :a0147afbac9d2899
        암호문 블록 2 :a0147afbac9d2899
블록 #3
        평문 블록 3   :8d41e0bb938568ae
        입력 블록 3   :8d41e0bb938568ae
        출력 블록 3   :9d76e80678f9851c
        암호문 블록 3 :9d76e80678f9851c
블록 #4
        평문 블록 4   :ebfd92ed1affa096
        입력 블록 4   :ebfd92ed1affa096
        출력 블록 4   :274c1b4daf769baa
        암호문 블록 4 :274c1b4daf769baa
블록 #5
        평문 블록 5   :394d20fc5277ddfc
        입력 블록 5   :394d20fc5277ddfc
        출력 블록 5   :1c1d73234270f0b0
        암호문 블록 5 :1c1d73234270f0b0
블록 #6
        평문 블록 6   :4de8b0fce1eb2b93
        입력 블록 6   :4de8b0fce1eb2b93
        출력 블록 6   :095a1454e192addd
        암호문 블록 6 :095a1454e192addd
블록 #7
        평문 블록 7   :d4ae40ef4768c613
        입력 블록 7   :d4ae40ef4768c613
        출력 블록 7   :3c9e22a4ed615c31
        암호문 블록 7 :3c9e22a4ed615c31
블록 #8
        평문 블록 8   :b50b8942f7d4b9b3
        입력 블록 8   :b50b8942f7d4b9b3
```

출력 블록 8 :175e90fbe73a5508
암호문 블록 8 :175e90fbe73a5508

II.1.2. HIGHT ECB 평문1, 키1 - 복호화

블록 #1
암호문 블록 1 :e4bc2e312277e4dd
입력 블록 1 :e4bc2e312277e4dd
출력 블록 1 :d76d0d18327ec562
평문 블록 1 :d76d0d18327ec562
블록 #2
암호문 블록 2 :a0147afbac9d2899
입력 블록 2 :a0147afbac9d2899
출력 블록 2 :b15e6bc365ac0c0f
평문 블록 2 :b15e6bc365ac0c0f
블록 #3
암호문 블록 3 :9d76e80678f9851c
입력 블록 3 :9d76e80678f9851c
출력 블록 3 :8d41e0bb938568ae
평문 블록 3 :8d41e0bb938568ae
블록 #4
암호문 블록 4 :274c1b4daf769baa
입력 블록 4 :274c1b4daf769baa
출력 블록 4 :ebfd92ed1affa096
평문 블록 4 :ebfd92ed1affa096
블록 #5
암호문 블록 5 :1c1d73234270f0b0
입력 블록 5 :1c1d73234270f0b0
출력 블록 5 :394d20fc5277ddfc
평문 블록 5 :394d20fc5277ddfc
블록 #6
암호문 블록 6 :095a1454e192addd
입력 블록 6 :095a1454e192addd
출력 블록 6 :4de8b0fce1eb2b93
평문 블록 6 :4de8b0fce1eb2b93
블록 #7
암호문 블록 7 :3c9e22a4ed615c31
입력 블록 7 :3c9e22a4ed615c31
출력 블록 7 :d4ae40ef4768c613
평문 블록 7 :d4ae40ef4768c613
블록 #8
암호문 블록 8 :175e90fbe73a5508
입력 블록 8 :175e90fbe73a5508

출력 블록 8 :b50b8942f7d4b9b3
평문 블록 8 :b50b8942f7d4b9b3

II.1.3. HIGHT ECB 평문2, 키2 - 암호화

블록 #1
평문 블록 1 :6bc1bee22e409f96
입력 블록 1 :6bc1bee22e409f96
출력 블록 1 :9813d32ce7fd5abb
암호문 블록 1 :9813d32ce7fd5abb
블록 #2
평문 블록 2 :e93d7e117393172a
입력 블록 2 :e93d7e117393172a
출력 블록 2 :0113b32d34e6243f
암호문 블록 2 :0113b32d34e6243f
블록 #3
평문 블록 3 :ae2d8a571e03ac9c
입력 블록 3 :ae2d8a571e03ac9c
출력 블록 3 :95eba84588a70bc7
암호문 블록 3 :95eba84588a70bc7
블록 #4
평문 블록 4 :9eb76fac45af8e51
입력 블록 4 :9eb76fac45af8e51
출력 블록 4 :030bd8791a35625b
암호문 블록 4 :030bd8791a35625b
블록 #5
평문 블록 5 :30c81c46a35ce411
입력 블록 5 :30c81c46a35ce411
출력 블록 5 :dc873b5175d4bf97
암호문 블록 5 :dc873b5175d4bf97
블록 #6
평문 블록 6 :e5fbc1191a0a52ef
입력 블록 6 :e5fbc1191a0a52ef
출력 블록 6 :7a6551493ab263f2
암호문 블록 6 :7a6551493ab263f2
블록 #7
평문 블록 7 :f69f2445df4f9b17
입력 블록 7 :f69f2445df4f9b17
출력 블록 7 :6d20c1ee2c6c31a3
암호문 블록 7 :6d20c1ee2c6c31a3
블록 #8
평문 블록 8 :ad2b417be66c3710

입력 블록 8 :ad2b417be66c3710
출력 블록 8 :12f6cee2fe4759a5
암호문 블록 8 :12f6cee2fe4759a5

II.1.4. HIGHT ECB 평문2, 키2 - 복호화

블록 #1
암호문 블록 1 :9813d32ce7fd5abb
입력 블록 1 :9813d32ce7fd5abb
출력 블록 1 :6bc1bee22e409f96
평문 블록 1 :6bc1bee22e409f96
블록 #2
암호문 블록 2 :0113b32d34e6243f
입력 블록 2 :0113b32d34e6243f
출력 블록 2 :e93d7e117393172a
평문 블록 2 :e93d7e117393172a
블록 #3
암호문 블록 3 :95eba84588a70bc7
입력 블록 3 :95eba84588a70bc7
출력 블록 3 :ae2d8a571e03ac9c
평문 블록 3 :ae2d8a571e03ac9c
블록 #4
암호문 블록 4 :030bd8791a35625b
입력 블록 4 :030bd8791a35625b
출력 블록 4 :9eb76fac45af8e51
평문 블록 4 :9eb76fac45af8e51
블록 #5
암호문 블록 5 :dc873b5175d4bf97
입력 블록 5 :dc873b5175d4bf97
출력 블록 5 :30c81c46a35ce411
평문 블록 5 :30c81c46a35ce411
블록 #6
암호문 블록 6 :7a6551493ab263f2
입력 블록 6 :7a6551493ab263f2
출력 블록 6 :e5fbc1191a0a52ef
평문 블록 6 :e5fbc1191a0a52ef
블록 #7
암호문 블록 7 :6d20c1ee2c6c31a3
입력 블록 7 :6d20c1ee2c6c31a3
출력 블록 7 :f69f2445df4f9b17
평문 블록 7 :f69f2445df4f9b17

블록 #8
암호문 블록 8 :12f6cee2fe4759a5
입력 블록 8 :12f6cee2fe4759a5
출력 블록 8 :ad2b417be66c3710
평문 블록 8 :ad2b417be66c3710

II.2. HIGHT CBC 운영 모드

II.2.1. HIGHT CBC 평문1, 키1 - 암호화

블록 #1
평문 블록 1 :d76d0d18327ec562
입력 블록 1 :f1e06bbf07d6dfe3
출력 블록 1 :9c8fa0a59f9e3631
암호문 블록 1 :9c8fa0a59f9e3631
블록 #2
평문 블록 2 :b15e6bc365ac0c0f
입력 블록 2 :2dd1cb66fa323a3e
출력 블록 2 :a6e7cbd3c42426b8
암호문 블록 2 :a6e7cbd3c42426b8
블록 #3
평문 블록 3 :8d41e0bb938568ae
입력 블록 3 :2ba62b6857a14e16
출력 블록 3 :1f120612a40e43ad
암호문 블록 3 :1f120612a40e43ad
블록 #4
평문 블록 4 :ebfd92ed1affa096
입력 블록 4 :f4ef94ffbef1e33b
출력 블록 4 :784f4226a3714463
암호문 블록 4 :784f4226a3714463
블록 #5
평문 블록 5 :394d20fc5277ddfc
입력 블록 5 :410262daf106999f
출력 블록 5 :da5fb1c3c0d828cf
암호문 블록 5 :da5fb1c3c0d828cf
블록 #6
평문 블록 6 :4de8b0fce1eb2b93
입력 블록 6 :97b7013f2133035c
출력 블록 6 :18e04803a1b79c43
암호문 블록 6 :18e04803a1b79c43

블록 #7
평문 블록 7 :d4ae40ef4768c613
입력 블록 7 :cc4e08ece6df5a50
출력 블록 7 :4cd58b74c585ed18
암호문 블록 7 :4cd58b74c585ed18
블록 #8
평문 블록 8 :b50b8942f7d4b9b3
입력 블록 8 :f9de0236325154ab
출력 블록 8 :d1ab55e04aabe765
암호문 블록 8 :d1ab55e04aabe765

II.2.2. HIGHT CBC 평문1, 키1 - 복호화

블록 #1
암호문 블록 1 :9c8fa0a59f9e3631
입력 블록 1 :9c8fa0a59f9e3631
출력 블록 1 :f1e06bbf07d6dfe3
평문 블록 1 :d76d0d18327ec562
블록 #2
암호문 블록 2 :a6e7cbd3c42426b8
입력 블록 2 :a6e7cbd3c42426b8
출력 블록 2 :2dd1cb66fa323a3e
평문 블록 2 :b15e6bc365ac0c0f
블록 #3
암호문 블록 3 :1f120612a40e43ad
입력 블록 3 :1f120612a40e43ad
출력 블록 3 :2ba62b6857a14e16
평문 블록 3 :8d41e0bb938568ae
블록 #4
암호문 블록 4 :784f4226a3714463
입력 블록 4 :784f4226a3714463
출력 블록 4 :f4ef94ffbef1e33b
평문 블록 4 :ebfd92ed1affa096
블록 #5
암호문 블록 5 :da5fb1c3c0d828cf
입력 블록 5 :da5fb1c3c0d828cf
출력 블록 5 :410262daf106999f
평문 블록 5 :394d20fc5277ddfc
블록 #6
암호문 블록 6 :18e04803a1b79c43
입력 블록 6 :18e04803a1b79c43
출력 블록 6 :97b7013f2133035c
평문 블록 6 :4de8b0fce1eb2b93

블록 #7
암호문 블록 7 :4cd58b74c585ed18
입력 블록 7 :4cd58b74c585ed18
출력 블록 7 :cc4e08ece6df5a50
평문 블록 7 :d4ae40ef4768c613
블록 #8
암호문 블록 8 :d1ab55e04aabe765
입력 블록 8 :d1ab55e04aabe765
출력 블록 8 :f9de0236325154ab
평문 블록 8 :b50b8942f7d4b9b3

II.2.3. HIGHT CBC 평문2, 키2 - 암호화

블록 #1
평문 블록 1 :6bc1bee22e409f96
입력 블록 1 :4d4cd8451be88517
출력 블록 1 :899ac010903a53fd
암호문 블록 1 :899ac010903a53fd
블록 #2
평문 블록 2 :e93d7e117393172a
입력 블록 2 :60a7be01e3a944d7
출력 블록 2 :ea8dab0376325e87
암호문 블록 2 :ea8dab0376325e87
블록 #3
평문 블록 3 :ae2d8a571e03ac9c
입력 블록 3 :44a021546831f21b
출력 블록 3 :25d3681e049f323f
암호문 블록 3 :25d3681e049f323f
블록 #4
평문 블록 4 :9eb76fac45af8e51
입력 블록 4 :bb6407b24130bc6e
출력 블록 4 :daacde164a02bb28
암호문 블록 4 :daacde164a02bb28
블록 #5
평문 블록 5 :30c81c46a35ce411
입력 블록 5 :ea64c250e95e5f39
출력 블록 5 :1a17e3d813d40b06
암호문 블록 5 :1a17e3d813d40b06
블록 #6
평문 블록 6 :e5fbc1191a0a52ef
입력 블록 6 :ffec22c109de59e9
출력 블록 6 :a0c9f415e060ad5f

암호문 블록 6 :a0c9f415e060ad5f
블록 #7
평문 블록 7 :f69f2445df4f9b17
입력 블록 7 :5656d0503f2f3648
출력 블록 7 :1733ef74ecdb7cb7
암호문 블록 7 :1733ef74ecdb7cb7
블록 #8
평문 블록 8 :ad2b417be66c3710
입력 블록 8 :ba18ae0f0ab74ba7
출력 블록 8 :dc01a65f5c8ae349
암호문 블록 8 :dc01a65f5c8ae349

II.2.4. HIGHT CBC 평문2, 키2 - 복호화

블록 #1
암호문 블록 1 :899ac010903a53fd
입력 블록 1 :899ac010903a53fd
출력 블록 1 :4d4cd8451be88517
평문 블록 1 :6bc1bee22e409f96
블록 #2
암호문 블록 2 :ea8dab0376325e87
입력 블록 2 :ea8dab0376325e87
출력 블록 2 :60a7be01e3a944d7
평문 블록 2 :e93d7e117393172a
블록 #3
암호문 블록 3 :25d3681e049f323f
입력 블록 3 :25d3681e049f323f
출력 블록 3 :44a021546831f21b
평문 블록 3 :ae2d8a571e03ac9c
블록 #4
암호문 블록 4 :daacde164a02bb28
입력 블록 4 :daacde164a02bb28
출력 블록 4 :bb6407b24130bc6e
평문 블록 4 :9eb76fac45af8e51
블록 #5
암호문 블록 5 :1a17e3d813d40b06
입력 블록 5 :1a17e3d813d40b06
출력 블록 5 :ea64c250e95e5f39
평문 블록 5 :30c81c46a35ce411
블록 #6
암호문 블록 6 :a0c9f415e060ad5f
입력 블록 6 :a0c9f415e060ad5f
출력 블록 6 :ffec22c109de59e9

평문 블록 6 :e5fbc1191a0a52ef
블록 #7
암호문 블록 7 :1733ef74ecdb7cb7
입력 블록 7 :1733ef74ecdb7cb7
출력 블록 7 :5656d0503f2f3648
평문 블록 7 :f69f2445df4f9b17
블록 #8
암호문 블록 8 :dc01a65f5c8ae349
입력 블록 8 :dc01a65f5c8ae349
출력 블록 8 :ba18ae0f0ab74ba7
평문 블록 8 :ad2b417be66c3710

II.3. HIGHT CFB 운영 모드

II.3.1. HIGHT CFB-1 평문1, 키1 - 암호화

블록 #1
입력 블록 1 :268d66a735a81a81
출력 블록 1 :106240c41a85aa0b
평문 블록 1 :1
암호문 블록 1 :1
블록 #2
입력 블록 2 :4d1acd4e6b503503
출력 블록 2 :62e69be939113ff0
평문 블록 2 :1
암호문 블록 2 :1
블록 #3
입력 블록 3 :9a359a9cd6a06a07
출력 블록 3 :a96b8f449e391205
평문 블록 3 :0
암호문 블록 3 :1
블록 #4
입력 블록 4 :346b3539ad40d40f
출력 블록 4 :be5574372cb38717
평문 블록 4 :1
암호문 블록 4 :0
블록 #5
입력 블록 5 :68d66a735a81a81e
출력 블록 5 :f4e0a8e0b0459eed
평문 블록 5 :0
암호문 블록 5 :1
블록 #6

입력 블록 6 :d1acd4e6b503503d
출력 블록 6 :6dc1e8b19afb28d7
평문 블록 6 :1
암호문 블록 6 :1
블록 #7
입력 블록 7 :a359a9cd6a06a07b
출력 블록 7 :33da261cf5184343
평문 블록 7 :1
암호문 블록 7 :1
블록 #8
입력 블록 8 :46b3539ad40d40f7
출력 블록 8 :b570627b15796b3c
평문 블록 8 :1
암호문 블록 8 :0
블록 #9
입력 블록 9 :8d66a735a81a81ee
출력 블록 9 :364cdf30feb2488d
평문 블록 9 :0
암호문 블록 9 :0
블록 #10
입력 블록 10 :1acd4e6b503503dc
출력 블록 10 :e18c09c6291bd445
평문 블록 10 :1
암호문 블록 10 :0
블록 #11
입력 블록 11 :359a9cd6a06a07b8
출력 블록 11 :9a6cf6080f104928
평문 블록 11 :1
암호문 블록 11 :0
블록 #12
입력 블록 12 :6b3539ad40d40f70
출력 블록 12 :b24a07321abd5787
평문 블록 12 :0
암호문 블록 12 :1
블록 #13
입력 블록 13 :d66a735a81a81ee1
출력 블록 13 :0cf4f361f8f50680
평문 블록 13 :1
암호문 블록 13 :1
블록 #14
입력 블록 14 :acd4e6b503503dc3
출력 블록 14 :0e54aa4014260d5d
평문 블록 14 :1

```
        암호문 블록 14 :1
블록 #15
        입력 블록 15   :59a9cd6a06a07b87
        출력 블록 15   :b54e09e08c9c1fb1
        평문 블록 15   :0
        암호문 블록 15 :1
블록 #16
        입력 블록 16   :b3539ad40d40f70f
        출력 블록 16   :f8a0ac13437e7187
        평문 블록 16   :1
        암호문 블록 16 :0
블록 #17
        입력 블록 17   :66a735a81a81ee1e
        출력 블록 17   :a86726eb39436be2
        평문 블록 17   :0
        암호문 블록 17 :1
블록 #18
        입력 블록 18   :cd4e6b503503dc3d
        출력 블록 18   :ea9eaf1ebf1821f5
        평문 블록 18   :0
        암호문 블록 18 :1
블록 #19
        입력 블록 19   :9a9cd6a06a07b87b
        출력 블록 19   :8253988edc6b3939
        평문 블록 19   :0
        암호문 블록 19 :1
블록 #20
        입력 블록 20   :3539ad40d40f70f7
        출력 블록 20   :4e4deb10938e7e2e
        평문 블록 20   :0
        암호문 블록 20 :0
블록 #21
        입력 블록 21   :6a735a81a81ee1ee
        출력 블록 21   :33e9db3de9aa6c1f
        평문 블록 21   :1
        암호문 블록 21 :1
블록 #22
        입력 블록 22   :d4e6b503503dc3dd
        출력 블록 22   :1488d6262ed198ea
        평문 블록 22   :1
        암호문 블록 22 :1
블록 #23
        입력 블록 23   :a9cd6a06a07b87bb
```

출력 블록 23 :9fabe8852430ae17
평문 블록 23 :0
암호문 블록 23 :1
블록 #24
입력 블록 24 :539ad40d40f70f77
출력 블록 24 :f2c646bcd82a4e1b
평문 블록 24 :1
암호문 블록 24 :0
블록 #25
입력 블록 25 :a735a81a81ee1eee
출력 블록 25 :e9e8370609a8760c
평문 블록 25 :0
암호문 블록 25 :1
블록 #26
입력 블록 26 :4e6b503503dc3ddd
출력 블록 26 :04bd0537e28a06cd
평문 블록 26 :0
암호문 블록 26 :0
블록 #27
입력 블록 27 :9cd6a06a07b87bba
출력 블록 27 :326a78cd8e55da3f
평문 블록 27 :0
암호문 블록 27 :0
블록 #28
입력 블록 28 :39ad40d40f70f774
출력 블록 28 :4affa93c1daaba4e
평문 블록 28 :1
암호문 블록 28 :1
블록 #29
입력 블록 29 :735a81a81ee1eee9
출력 블록 29 :eebc1c158a48a87d
평문 블록 29 :1
암호문 블록 29 :0
블록 #30
입력 블록 30 :e6b503503dc3ddd2
출력 블록 30 :556be0407019aca9
평문 블록 30 :0
암호문 블록 30 :0
블록 #31
입력 블록 31 :cd6a06a07b87bba4
출력 블록 31 :7374086f5f5fe8b6
평문 블록 31 :0
암호문 블록 31 :0

블록 #32
입력 블록 32 :9ad40d40f70f7748
출력 블록 32 :25d5aeebde4f0795
평문 블록 32 :0
암호문 블록 32 :0

II.3.2. HIGHT CFB-1 평문1, 키1 - 복호화

블록 #1
입력 블록 1 :268d66a735a81a81
출력 블록 1 :106240c41a85aa0b
암호문 블록 1 :1
평문 블록 1 :1
블록 #2
입력 블록 2 :4d1acd4e6b503503
출력 블록 2 :62e69be939113ff0
암호문 블록 2 :1
평문 블록 2 :1
블록 #3
입력 블록 3 :9a359a9cd6a06a07
출력 블록 3 :a96b8f449e391205
암호문 블록 3 :1
평문 블록 3 :0
블록 #4
입력 블록 4 :346b3539ad40d40f
출력 블록 4 :be5574372cb38717
암호문 블록 4 :0
평문 블록 4 :1
블록 #5
입력 블록 5 :68d66a735a81a81e
출력 블록 5 :f4e0a8e0b0459eed
암호문 블록 5 :1
평문 블록 5 :0
블록 #6
입력 블록 6 :d1acd4e6b503503d
출력 블록 6 :6dc1e8b19afb28d7
암호문 블록 6 :1
평문 블록 6 :1
블록 #7
입력 블록 7 :a359a9cd6a06a07b
출력 블록 7 :33da261cf5184343
암호문 블록 7 :1
평문 블록 7 :1

블록 #8
입력 블록 8 :46b3539ad40d40f7
출력 블록 8 :b570627b15796b3c
암호문 블록 8 :0
평문 블록 8 :1
블록 #9
입력 블록 9 :8d66a735a81a81ee
출력 블록 9 :364cdf30feb2488d
암호문 블록 9 :0
평문 블록 9 :0
블록 #10
입력 블록 10 :1acd4e6b503503dc
출력 블록 10 :e18c09c6291bd445
암호문 블록 10 :0
평문 블록 10 :1
블록 #11
입력 블록 11 :359a9cd6a06a07b8
출력 블록 11 :9a6cf6080f104928
암호문 블록 11 :0
평문 블록 11 :1
블록 #12
입력 블록 12 :6b3539ad40d40f70
출력 블록 12 :b24a07321abd5787
암호문 블록 12 :1
평문 블록 12 :0
블록 #13
입력 블록 13 :d66a735a81a81ee1
출력 블록 13 :0cf4f361f8f50680
암호문 블록 13 :1
평문 블록 13 :1
블록 #14
입력 블록 14 :acd4e6b503503dc3
출력 블록 14 :0e54aa4014260d5d
암호문 블록 14 :1
평문 블록 14 :1
블록 #15
입력 블록 15 :59a9cd6a06a07b87
출력 블록 15 :b54e09e08c9c1fb1
암호문 블록 15 :1
평문 블록 15 :0
블록 #16
입력 블록 16 :b3539ad40d40f70f
출력 블록 16 :f8a0ac13437e7187

암호문 블록 16 :0
평문 블록 16 :1
블록 #17
입력 블록 17 :66a735a81a81ee1e
출력 블록 17 :a86726eb39436be2
암호문 블록 17 :1
평문 블록 17 :0
블록 #18
입력 블록 18 :cd4e6b503503dc3d
출력 블록 18 :ea9eaf1ebf1821f5
암호문 블록 18 :1
평문 블록 18 :0
블록 #19
입력 블록 19 :9a9cd6a06a07b87b
출력 블록 19 :8253988edc6b3939
암호문 블록 19 :1
평문 블록 19 :0
블록 #20
입력 블록 20 :3539ad40d40f70f7
출력 블록 20 :4e4deb10938e7e2e
암호문 블록 20 :0
평문 블록 20 :0
블록 #21
입력 블록 21 :6a735a81a81ee1ee
출력 블록 21 :33e9db3de9aa6c1f
암호문 블록 21 :1
평문 블록 21 :1
블록 #22
입력 블록 22 :d4e6b503503dc3dd
출력 블록 22 :1488d6262ed198ea
암호문 블록 22 :1
평문 블록 22 :1
블록 #23
입력 블록 23 :a9cd6a06a07b87bb
출력 블록 23 :9fabe8852430ae17
암호문 블록 23 :1
평문 블록 23 :0
블록 #24
입력 블록 24 :539ad40d40f70f77
출력 블록 24 :f2c646bcd82a4e1b
암호문 블록 24 :0
평문 블록 24 :1
블록 #25

입력 블록 25 :a735a81a81ee1eee
출력 블록 25 :e9e8370609a8760c
암호문 블록 25 :1
평문 블록 25 :0
블록 #26
입력 블록 26 :4e6b503503dc3ddd
출력 블록 26 :04bd0537e28a06cd
암호문 블록 26 :0
평문 블록 26 :0
블록 #27
입력 블록 27 :9cd6a06a07b87bba
출력 블록 27 :326a78cd8e55da3f
암호문 블록 27 :0
평문 블록 27 :0
블록 #28
입력 블록 28 :39ad40d40f70f774
출력 블록 28 :4affa93c1daaba4e
암호문 블록 28 :1
평문 블록 28 :1
블록 #29
입력 블록 29 :735a81a81ee1eee9
출력 블록 29 :eebc1c158a48a87d
암호문 블록 29 :0
평문 블록 29 :1
블록 #30
입력 블록 30 :e6b503503dc3ddd2
출력 블록 30 :556be0407019aca9
암호문 블록 30 :0
평문 블록 30 :0
블록 #31
입력 블록 31 :cd6a06a07b87bba4
출력 블록 31 :7374086f5f5fe8b6
암호문 블록 31 :0
평문 블록 31 :0
블록 #32
입력 블록 32 :9ad40d40f70f7748
출력 블록 32 :25d5aeebde4f0795
암호문 블록 32 :0
평문 블록 32 :0

II.3.3. HIGHT CFB-1 평문2, 키2 - 암호화

```
블록 #1
        입력 블록 1   :268d66a735a81a81
        출력 블록 1   :96b71e0493e7e1fa
        평문 블록 1   :0
        암호문 블록 1 :1
블록 #2
        입력 블록 2   :4d1acd4e6b503503
        출력 블록 2   :5db869f99b5d4710
        평문 블록 2   :1
        암호문 블록 2 :1
블록 #3
        입력 블록 3   :9a359a9cd6a06a07
        출력 블록 3   :b16b31a06521a026
        평문 블록 3   :1
        암호문 블록 3 :0
블록 #4
        입력 블록 4   :346b3539ad40d40e
        출력 블록 4   :cc8401674b3c8f19
        평문 블록 4   :0
        암호문 블록 4 :1
블록 #5
        입력 블록 5   :68d66a735a81a81d
        출력 블록 5   :505b206c775cdc02
        평문 블록 5   :1
        암호문 블록 5 :1
블록 #6
        입력 블록 6   :d1acd4e6b503503b
        출력 블록 6   :262df63f927d4c52
        평문 블록 6   :0
        암호문 블록 6 :0
블록 #7
        입력 블록 7   :a359a9cd6a06a076
        출력 블록 7   :c0c61018045eddae
        평문 블록 7   :1
        암호문 블록 7 :0
블록 #8
        입력 블록 8   :46b3539ad40d40ec
        출력 블록 8   :0d548c4578b64521
        평문 블록 8   :1
        암호문 블록 8 :1
블록 #9
```

입력 블록 9 :8d66a735a81a81d9
출력 블록 9 :c24c22b881389d90
평문 블록 9 :1
암호문 블록 9 :0
블록 #10
입력 블록 10 :1acd4e6b503503b2
출력 블록 10 :bd8f5c9622050a01
평문 블록 10 :1
암호문 블록 10 :0
블록 #11
입력 블록 11 :359a9cd6a06a0764
출력 블록 11 :1dbf465031200928
평문 블록 11 :0
암호문 블록 11 :0
블록 #12
입력 블록 12 :6b3539ad40d40ec8
출력 블록 12 :2ff6f2b3b2684dcb
평문 블록 12 :0
암호문 블록 12 :0
블록 #13
입력 블록 13 :d66a735a81a81d90
출력 블록 13 :0498c599f4c09d6c
평문 블록 13 :0
암호문 블록 13 :0
블록 #14
입력 블록 14 :acd4e6b503503b20
출력 블록 14 :67555219f8500687
평문 블록 14 :0
암호문 블록 14 :0
블록 #15
입력 블록 15 :59a9cd6a06a07640
출력 블록 15 :3d7da8bb73d6332d
평문 블록 15 :0
암호문 블록 15 :0
블록 #16
입력 블록 16 :b3539ad40d40ec80
출력 블록 16 :883460a6a2cf119c
평문 블록 16 :1
암호문 블록 16 :0
블록 #17
입력 블록 17 :66a735a81a81d900
출력 블록 17 :2e5a87484e49e2ee
평문 블록 17 :1

```
        암호문 블록 17 :1
블록 #18
        입력 블록 18   :cd4e6b503503b201
        출력 블록 18   :ed0db3abe067750b
        평문 블록 18   :0
        암호문 블록 18 :1
블록 #19
        입력 블록 19   :9a9cd6a06a076403
        출력 블록 19   :5dee09be8c6eaa76
        평문 블록 19   :1
        암호문 블록 19 :1
블록 #20
        입력 블록 20   :3539ad40d40ec807
        출력 블록 20   :948f5e4b7aa3b014
        평문 블록 20   :1
        암호문 블록 20 :0
블록 #21
        입력 블록 21   :6a735a81a81d900e
        출력 블록 21   :7521702b5678446c
        평문 블록 21   :1
        암호문 블록 21 :1
블록 #22
        입력 블록 22   :d4e6b503503b201d
        출력 블록 22   :39ab43d2058ea74f
        평문 블록 22   :1
        암호문 블록 22 :1
블록 #23
        입력 블록 23   :a9cd6a06a076403b
        출력 블록 23   :7441a72e6ef10da0
        평문 블록 23   :1
        암호문 블록 23 :1
블록 #24
        입력 블록 24   :539ad40d40ec8077
        출력 블록 24   :57658c960c9470b0
        평문 블록 24   :0
        암호문 블록 24 :0
블록 #25
        입력 블록 25   :a735a81a81d900ee
        출력 블록 25   :34a2167b1e548885
        평문 블록 25   :1
        암호문 블록 25 :1
블록 #26
        입력 블록 26   :4e6b503503b201dd
```

출력 블록 26 :081d3ef07df54ffe
평문 블록 26 :1
암호문 블록 26 :1
블록 #27
입력 블록 27 :9cd6a06a076403bb
출력 블록 27 :f611d65874b08c06
평문 블록 27 :1
암호문 블록 27 :0
블록 #28
입력 블록 28 :39ad40d40ec80776
출력 블록 28 :61915ae5dfad5a2e
평문 블록 28 :0
암호문 블록 28 :0
블록 #29
입력 블록 29 :735a81a81d900eec
출력 블록 29 :5abb168261d45056
평문 블록 29 :0
암호문 블록 29 :0
블록 #30
입력 블록 30 :e6b503503b201dd8
출력 블록 30 :ff727b263c1b3eef
평문 블록 30 :0
암호문 블록 30 :1
블록 #31
입력 블록 31 :cd6a06a076403bb1
출력 블록 31 :c2abd7951498c987
평문 블록 31 :1
암호문 블록 31 :0
블록 #32
입력 블록 32 :9ad40d40ec807762
출력 블록 32 :07ec93f2349e18de
평문 블록 32 :0
암호문 블록 32 :0

II.3.4. HIGHT CFB-1 평문2, 키2 - 복호화

블록 #1
입력 블록 1 :268d66a735a81a81
출력 블록 1 :96b71e0493e7e1fa
암호문 블록 1 :1
평문 블록 1 :0
블록 #2

```
        입력 블록 2    :4d1acd4e6b503503
        출력 블록 2    :5db869f99b5d4710
        암호문 블록 2 :1
        평문 블록 2    :1
블록 #3
        입력 블록 3    :9a359a9cd6a06a07
        출력 블록 3    :b16b31a06521a026
        암호문 블록 3 :0
        평문 블록 3    :1
블록 #4
        입력 블록 4    :346b3539ad40d40e
        출력 블록 4    :cc8401674b3c8f19
        암호문 블록 4 :1
        평문 블록 4    :0
블록 #5
        입력 블록 5    :68d66a735a81a81d
        출력 블록 5    :505b206c775cdc02
        암호문 블록 5 :1
        평문 블록 5    :1
블록 #6
        입력 블록 6    :d1acd4e6b503503b
        출력 블록 6    :262df63f927d4c52
        암호문 블록 6 :0
        평문 블록 6    :0
블록 #7
        입력 블록 7    :a359a9cd6a06a076
        출력 블록 7    :c0c61018045eddae
        암호문 블록 7 :0
        평문 블록 7    :1
블록 #8
        입력 블록 8    :46b3539ad40d40ec
        출력 블록 8    :0d548c4578b64521
        암호문 블록 8 :1
        평문 블록 8    :1
블록 #9
        입력 블록 9    :8d66a735a81a81d9
        출력 블록 9    :c24c22b881389d90
        암호문 블록 9 :0
        평문 블록 9    :1
블록 #10
        입력 블록 10    :1acd4e6b503503b2
        출력 블록 10    :bd8f5c9622050a01
        암호문 블록 10 :0
```

```
        평문 블록 10    :1
블록 #11
        입력 블록 11    :359a9cd6a06a0764
        출력 블록 11    :1dbf465031200928
        암호문 블록 11 :0
        평문 블록 11    :0
블록 #12
        입력 블록 12    :6b3539ad40d40ec8
        출력 블록 12    :2ff6f2b3b2684dcb
        암호문 블록 12 :0
        평문 블록 12    :0
블록 #13
        입력 블록 13    :d66a735a81a81d90
        출력 블록 13    :0498c599f4c09d6c
        암호문 블록 13 :0
        평문 블록 13    :0
블록 #14
        입력 블록 14    :acd4e6b503503b20
        출력 블록 14    :67555219f8500687
        암호문 블록 14 :0
        평문 블록 14    :0
블록 #15
        입력 블록 15    :59a9cd6a06a07640
        출력 블록 15    :3d7da8bb73d6332d
        암호문 블록 15 :0
        평문 블록 15    :0
블록 #16
        입력 블록 16    :b3539ad40d40ec80
        출력 블록 16    :883460a6a2cf119c
        암호문 블록 16 :0
        평문 블록 16    :1
블록 #17
        입력 블록 17    :66a735a81a81d900
        출력 블록 17    :2e5a87484e49e2ee
        암호문 블록 17 :1
        평문 블록 17    :1
블록 #18
        입력 블록 18    :cd4e6b503503b201
        출력 블록 18    :ed0db3abe067750b
        암호문 블록 18 :1
        평문 블록 18    :0
블록 #19
        입력 블록 19    :9a9cd6a06a076403
```

출력 블록 19 :5dee09be8c6eaa76
암호문 블록 19 :1
평문 블록 19 :1
블록 #20
입력 블록 20 :3539ad40d40ec807
출력 블록 20 :948f5e4b7aa3b014
암호문 블록 20 :0
평문 블록 20 :1
블록 #21
입력 블록 21 :6a735a81a81d900e
출력 블록 21 :7521702b5678446c
암호문 블록 21 :1
평문 블록 21 :1
블록 #22
입력 블록 22 :d4e6b503503b201d
출력 블록 22 :39ab43d2058ea74f
암호문 블록 22 :1
평문 블록 22 :1
블록 #23
입력 블록 23 :a9cd6a06a076403b
출력 블록 23 :7441a72e6ef10da0
암호문 블록 23 :1
평문 블록 23 :1
블록 #24
입력 블록 24 :539ad40d40ec8077
출력 블록 24 :57658c960c9470b0
암호문 블록 24 :0
평문 블록 24 :0
블록 #25
입력 블록 25 :a735a81a81d900ee
출력 블록 25 :34a2167b1e548885
암호문 블록 25 :1
평문 블록 25 :1
블록 #26
입력 블록 26 :4e6b503503b201dd
출력 블록 26 :081d3ef07df54ffe
암호문 블록 26 :1
평문 블록 26 :1
블록 #27
입력 블록 27 :9cd6a06a076403bb
출력 블록 27 :f611d65874b08c06
암호문 블록 27 :0
평문 블록 27 :1

```
블록 #28
        입력 블록 28    :39ad40d40ec80776
        출력 블록 28    :61915ae5dfad5a2e
        암호문 블록 28 :0
        평문 블록 28    :0
블록 #29
        입력 블록 29    :735a81a81d900eec
        출력 블록 29    :5abb168261d45056
        암호문 블록 29 :0
        평문 블록 29    :0
블록 #30
        입력 블록 30    :e6b503503b201dd8
        출력 블록 30    :ff727b263c1b3eef
        암호문 블록 30 :1
        평문 블록 30    :0
블록 #31
        입력 블록 31    :cd6a06a076403bb1
        출력 블록 31    :c2abd7951498c987
        암호문 블록 31 :0
        평문 블록 31    :1
블록 #32
        입력 블록 32    :9ad40d40ec807762
        출력 블록 32    :07ec93f2349e18de
        암호문 블록 32 :0
        평문 블록 32    :0
```

II.3.5. HIGHT CFB-8 평문1, 키1 - 암호화

```
블록 #1
        입력 블록 1    :268d66a735a81a81
        출력 블록 1    :106240c41a85aa0b
        평문 블록 1    :d7
        암호문 블록 1 :c7
블록 #2
        입력 블록 2    :8d66a735a81a81c7
        출력 블록 2    :3631fcbaf1b9dc29
        평문 블록 2    :6d
        암호문 블록 2 :5b
블록 #3
        입력 블록 3    :66a735a81a81c75b
        출력 블록 3    :75e7ba5ce56af327
        평문 블록 3    :0d
```

암호문 블록 3 :78
블록 #4
입력 블록 4 :a735a81a81c75b78
출력 블록 4 :91c4862d22066e93
평문 블록 4 :18
암호문 블록 4 :89
블록 #5
입력 블록 5 :35a81a81c75b7889
출력 블록 5 :2e7acc08aa541fa5
평문 블록 5 :32
암호문 블록 5 :1c
블록 #6
입력 블록 6 :a81a81c75b78891c
출력 블록 6 :b917d9c0ed3c45ef
평문 블록 6 :7e
암호문 블록 6 :c7
블록 #7
입력 블록 7 :1a81c75b78891cc7
출력 블록 7 :fa77b0bbd5248abc
평문 블록 7 :c5
암호문 블록 7 :3f
블록 #8
입력 블록 8 :81c75b78891cc73f
출력 블록 8 :0a36065abbb6399c
평문 블록 8 :62
암호문 블록 8 :68
블록 #9
입력 블록 9 :c75b78891cc73f68
출력 블록 9 :f2851eb03884958e
평문 블록 9 :b1
암호문 블록 9 :43
블록 #10
입력 블록 10 :5b78891cc73f6843
출력 블록 10 :f0c22dcd817a9ad3
평문 블록 10 :5e
암호문 블록 10 :ae
블록 #11
입력 블록 11 :78891cc73f6843ae
출력 블록 11 :a6852ed06aff800a
평문 블록 11 :6b
암호문 블록 11 :cd
블록 #12
입력 블록 12 :891cc73f6843aecd

출력 블록 12 :0e5a844707c4057d
평문 블록 12 :c3
암호문 블록 12 :cd
블록 #13
입력 블록 13 :1cc73f6843aecdcd
출력 블록 13 :5bcec0e2256a7295
평문 블록 13 :65
암호문 블록 13 :3e
블록 #14
입력 블록 14 :c73f6843aecdcd3e
출력 블록 14 :7facf8da651ac408
평문 블록 14 :ac
암호문 블록 14 :d3
블록 #15
입력 블록 15 :3f6843aecdcd3ed3
출력 블록 15 :1a3523238c6dcad7
평문 블록 15 :0c
암호문 블록 15 :16
블록 #16
입력 블록 16 :6843aecdcd3ed316
출력 블록 16 :882dd8a5262e80fc
평문 블록 16 :0f
암호문 블록 16 :87
블록 #17
입력 블록 17 :43aecdcd3ed31687
출력 블록 17 :e8516bc3d6faead5
평문 블록 17 :8d
암호문 블록 17 :65
블록 #18
입력 블록 18 :aecdcd3ed3168765
출력 블록 18 :d6edd5ed737c563a
평문 블록 18 :41
암호문 블록 18 :97
블록 #19
입력 블록 19 :cdcd3ed316876597
출력 블록 19 :efa9898c07e988fb
평문 블록 19 :e0
암호문 블록 19 :0f
블록 #20
입력 블록 20 :cd3ed3168765970f
출력 블록 20 :5ab54977249b67bb
평문 블록 20 :bb
암호문 블록 20 :e1

블록 #21
입력 블록 21 :3ed3168765970fe1
출력 블록 21 :dedb6992472a8260
평문 블록 21 :93
암호문 블록 21 :4d
블록 #22
입력 블록 22 :d3168765970fe14d
출력 블록 22 :5b405bb9733dc092
평문 블록 22 :85
암호문 블록 22 :de
블록 #23
입력 블록 23 :168765970fe14dde
출력 블록 23 :1628daa1c7c74d37
평문 블록 23 :68
암호문 블록 23 :7e
블록 #24
입력 블록 24 :8765970fe14dde7e
출력 블록 24 :e2b0ee0ea9a6c1ba
평문 블록 24 :ae
암호문 블록 24 :4c
블록 #25
입력 블록 25 :65970fe14dde7e4c
출력 블록 25 :5f50f4f5b50a4585
평문 블록 25 :eb
암호문 블록 25 :b4
블록 #26
입력 블록 26 :970fe14dde7e4cb4
출력 블록 26 :6873fba41764e0d8
평문 블록 26 :fd
암호문 블록 26 :95
블록 #27
입력 블록 27 :0fe14dde7e4cb495
출력 블록 27 :b3a58d21794540d9
평문 블록 27 :92
암호문 블록 27 :21
블록 #28
입력 블록 28 :e14dde7e4cb49521
출력 블록 28 :6b714cac52833c1e
평문 블록 28 :ed
암호문 블록 28 :86
블록 #29
입력 블록 29 :4dde7e4cb4952186
출력 블록 29 :e809c0ef561ec09e

평문 블록 29 :1a
암호문 블록 29 :f2
블록 #30
입력 블록 30 :de7e4cb4952186f2
출력 블록 30 :be268810557603d5
평문 블록 30 :ff
암호문 블록 30 :41
블록 #31
입력 블록 31 :7e4cb4952186f241
출력 블록 31 :2a387e7d2d2964a3
평문 블록 31 :a0
암호문 블록 31 :8a
블록 #32
입력 블록 32 :4cb4952186f2418a
출력 블록 32 :087a8646d918186b
평문 블록 32 :96
암호문 블록 32 :9e

II.3.6. HIGHT CFB-8 평문1, 키1 - 복호화

블록 #1
입력 블록 1 :268d66a735a81a81
출력 블록 1 :106240c41a85aa0b
암호문 블록 1 :c7
평문 블록 1 :d7
블록 #2
입력 블록 2 :8d66a735a81a81c7
출력 블록 2 :3631fcbaf1b9dc29
암호문 블록 2 :5b
평문 블록 2 :6d
블록 #3
입력 블록 3 :66a735a81a81c75b
출력 블록 3 :75e7ba5ce56af327
암호문 블록 3 :78
평문 블록 3 :0d
블록 #4
입력 블록 4 :a735a81a81c75b78
출력 블록 4 :91c4862d22066e93
암호문 블록 4 :89
평문 블록 4 :18
블록 #5
입력 블록 5 :35a81a81c75b7889

출력 블록 5 :2e7acc08aa541fa5
암호문 블록 5 :1c
평문 블록 5 :32
블록 #6
입력 블록 6 :a81a81c75b78891c
출력 블록 6 :b917d9c0ed3c45ef
암호문 블록 6 :c7
평문 블록 6 :7e
블록 #7
입력 블록 7 :1a81c75b78891cc7
출력 블록 7 :fa77b0bbd5248abc
암호문 블록 7 :3f
평문 블록 7 :c5
블록 #8
입력 블록 8 :81c75b78891cc73f
출력 블록 8 :0a36065abbb6399c
암호문 블록 8 :68
평문 블록 8 :62
블록 #9
입력 블록 9 :c75b78891cc73f68
출력 블록 9 :f2851eb03884958e
암호문 블록 9 :43
평문 블록 9 :b1
블록 #10
입력 블록 10 :5b78891cc73f6843
출력 블록 10 :f0c22dcd817a9ad3
암호문 블록 10 :ae
평문 블록 10 :5e
블록 #11
입력 블록 11 :78891cc73f6843ae
출력 블록 11 :a6852ed06aff800a
암호문 블록 11 :cd
평문 블록 11 :6b
블록 #12
입력 블록 12 :891cc73f6843aecd
출력 블록 12 :0e5a844707c4057d
암호문 블록 12 :cd
평문 블록 12 :c3
블록 #13
입력 블록 13 :1cc73f6843aecdcd
출력 블록 13 :5bcec0e2256a7295
암호문 블록 13 :3e
평문 블록 13 :65

블록 #14
입력 블록 14 :c73f6843aecdcd3e
출력 블록 14 :7facf8da651ac408
암호문 블록 14 :d3
평문 블록 14 :ac
블록 #15
입력 블록 15 :3f6843aecdcd3ed3
출력 블록 15 :1a3523238c6dcad7
암호문 블록 15 :16
평문 블록 15 :0c
블록 #16
입력 블록 16 :6843aecdcd3ed316
출력 블록 16 :882dd8a5262e80fc
암호문 블록 16 :87
평문 블록 16 :0f
블록 #17
입력 블록 17 :43aecdcd3ed31687
출력 블록 17 :e8516bc3d6faead5
암호문 블록 17 :65
평문 블록 17 :8d
블록 #18
입력 블록 18 :aecdcd3ed3168765
출력 블록 18 :d6edd5ed737c563a
암호문 블록 18 :97
평문 블록 18 :41
블록 #19
입력 블록 19 :cdcd3ed316876597
출력 블록 19 :efa9898c07e988fb
암호문 블록 19 :0f
평문 블록 19 :e0
블록 #20
입력 블록 20 :cd3ed3168765970f
출력 블록 20 :5ab54977249b67bb
암호문 블록 20 :e1
평문 블록 20 :bb
블록 #21
입력 블록 21 :3ed3168765970fe1
출력 블록 21 :dedb6992472a8260
암호문 블록 21 :4d
평문 블록 21 :93
블록 #22
입력 블록 22 :d3168765970fe14d
출력 블록 22 :5b405bb9733dc092

```
        암호문 블록 22 :de
        평문 블록 22   :85
블록 #23
        입력 블록 23   :168765970fe14dde
        출력 블록 23   :1628daa1c7c74d37
        암호문 블록 23 :7e
        평문 블록 23   :68
블록 #24
        입력 블록 24   :8765970fe14dde7e
        출력 블록 24   :e2b0ee0ea9a6c1ba
        암호문 블록 24 :4c
        평문 블록 24   :ae
블록 #25
        입력 블록 25   :65970fe14dde7e4c
        출력 블록 25   :5f50f4f5b50a4585
        암호문 블록 25 :b4
        평문 블록 25   :eb
블록 #26
        입력 블록 26   :970fe14dde7e4cb4
        출력 블록 26   :6873fba41764e0d8
        암호문 블록 26 :95
        평문 블록 26   :fd
블록 #27
        입력 블록 27   :0fe14dde7e4cb495
        출력 블록 27   :b3a58d21794540d9
        암호문 블록 27 :21
        평문 블록 27   :92
블록 #28
        입력 블록 28   :e14dde7e4cb49521
        출력 블록 28   :6b714cac52833c1e
        암호문 블록 28 :86
        평문 블록 28   :ed
블록 #29
        입력 블록 29   :4dde7e4cb4952186
        출력 블록 29   :e809c0ef561ec09e
        암호문 블록 29 :f2
        평문 블록 29   :1a
블록 #30
        입력 블록 30   :de7e4cb4952186f2
        출력 블록 30   :be268810557603d5
        암호문 블록 30 :41
        평문 블록 30   :ff
블록 #31
```

입력 블록 31 :7e4cb4952186f241
출력 블록 31 :2a387e7d2d2964a3
암호문 블록 31 :8a
평문 블록 31 :a0
블록 #32
입력 블록 32 :4cb4952186f2418a
출력 블록 32 :087a8646d918186b
암호문 블록 32 :9e
평문 블록 32 :96

II.3.7. HIGHT CFB-1 평문2, 키2 - 암호화

블록 #1
입력 블록 1 :268d66a735a81a81
출력 블록 1 :96b71e0493e7e1fa
평문 블록 1 :6b
암호문 블록 1 :fd
블록 #2
입력 블록 2 :8d66a735a81a81fd
출력 블록 2 :59290ab0670e2bc6
평문 블록 2 :c1
암호문 블록 2 :98
블록 #3
입력 블록 3 :66a735a81a81fd98
출력 블록 3 :5d783fa976981fcd
평문 블록 3 :be
암호문 블록 3 :e3
블록 #4
입력 블록 4 :a735a81a81fd98e3
출력 블록 4 :ceaab94c98cf1d5a
평문 블록 4 :e2
암호문 블록 4 :2c
블록 #5
입력 블록 5 :35a81a81fd98e32c
출력 블록 5 :5f81a0697af2a6fe
평문 블록 5 :2e
암호문 블록 5 :71
블록 #6
입력 블록 6 :a81a81fd98e32c71
출력 블록 6 :c522ba313e61d845
평문 블록 6 :40
암호문 블록 6 :85

블록 #7
입력 블록 7 :1a81fd98e32c7185
출력 블록 7 :7f7c8b298da519d5
평문 블록 7 :9f
암호문 블록 7 :e0
블록 #8
입력 블록 8 :81fd98e32c7185e0
출력 블록 8 :86dd0145f9c95bfa
평문 블록 8 :96
암호문 블록 8 :10
블록 #9
입력 블록 9 :fd98e32c7185e010
출력 블록 9 :9d8df3f11d977a52
평문 블록 9 :e9
암호문 블록 9 :74
블록 #10
입력 블록 10 :98e32c7185e01074
출력 블록 10 :06e2b37e8cb80d6d
평문 블록 10 :3d
암호문 블록 10 :3b
블록 #11
입력 블록 11 :e32c7185e010743b
출력 블록 11 :9ca42b4ca2da3c7f
평문 블록 11 :7e
암호문 블록 11 :e2
블록 #12
입력 블록 12 :2c7185e010743be2
출력 블록 12 :e6a27ecf2233a734
평문 블록 12 :11
암호문 블록 12 :f7
블록 #13
입력 블록 13 :7185e010743be2f7
출력 블록 13 :895d114e0c22c063
평문 블록 13 :73
암호문 블록 13 :fa
블록 #14
입력 블록 14 :85e010743be2f7fa
출력 블록 14 :60f82f58bb520013
평문 블록 14 :93
암호문 블록 14 :f3
블록 #15
입력 블록 15 :e010743be2f7faf3
출력 블록 15 :aa92b8a7e955b60d

평문 블록 15 :17
암호문 블록 15 :bd
블록 #16
입력 블록 16 :10743be2f7faf3bd
출력 블록 16 :0b134a55050c693d
평문 블록 16 :2a
암호문 블록 16 :21
블록 #17
입력 블록 17 :743be2f7faf3bd21
출력 블록 17 :c9da20eac91823ea
평문 블록 17 :ae
암호문 블록 17 :67
블록 #18
입력 블록 18 :3be2f7faf3bd2167
출력 블록 18 :ae4c7e0c3fbeeb28
평문 블록 18 :2d
암호문 블록 18 :83
블록 #19
입력 블록 19 :e2f7faf3bd216783
출력 블록 19 :8531afa35f8392ff
평문 블록 19 :8a
암호문 블록 19 :0f
블록 #20
입력 블록 20 :f7faf3bd2167830f
출력 블록 20 :63ec332822bff7c3
평문 블록 20 :57
암호문 블록 20 :34
블록 #21
입력 블록 21 :faf3bd2167830f34
출력 블록 21 :24538cfd8acdb2b1
평문 블록 21 :1e
암호문 블록 21 :3a
블록 #22
입력 블록 22 :f3bd2167830f343a
출력 블록 22 :c7641dd3dd501c15
평문 블록 22 :03
암호문 블록 22 :c4
블록 #23
입력 블록 23 :bd2167830f343ac4
출력 블록 23 :e80da1aae7819bf7
평문 블록 23 :ac
암호문 블록 23 :44
블록 #24

입력 블록 24 :2167830f343ac444
출력 블록 24 :7c0f64967b4de65d
평문 블록 24 :9c
암호문 블록 24 :e0
블록 #25
입력 블록 25 :67830f343ac444e0
출력 블록 25 :33c47365ba630a18
평문 블록 25 :9e
암호문 블록 25 :ad
블록 #26
입력 블록 26 :830f343ac444e0ad
출력 블록 26 :a33074d2a0128f3b
평문 블록 26 :b7
암호문 블록 26 :14
블록 #27
입력 블록 27 :0f343ac444e0ad14
출력 블록 27 :5966407e3c631ced
평문 블록 27 :6f
암호문 블록 27 :36
블록 #28
입력 블록 28 :343ac444e0ad1436
출력 블록 28 :66691c46582b259b
평문 블록 28 :ac
암호문 블록 28 :ca
블록 #29
입력 블록 29 :3ac444e0ad1436ca
출력 블록 29 :0cebeca3258e38c8
평문 블록 29 :45
암호문 블록 29 :49
블록 #30
입력 블록 30 :c444e0ad1436ca49
출력 블록 30 :22af4d19ecaa677c
평문 블록 30 :af
암호문 블록 30 :8d
블록 #31
입력 블록 31 :44e0ad1436ca498d
출력 블록 31 :e9b171e487413ab4
평문 블록 31 :8e
암호문 블록 31 :67
블록 #32
입력 블록 32 :e0ad1436ca498d67
출력 블록 32 :04ad2c50e43bced3
평문 블록 32 :51

암호문 블록 32 :55

II.3.8. HIGHT CFB-8 평문2, 키2 - 복호화

블록 #1
입력 블록 1 :268d66a735a81a81
출력 블록 1 :96b71e0493e7e1fa
암호문 블록 1 :fd
평문 블록 1 :6b
블록 #2
입력 블록 2 :8d66a735a81a81fd
출력 블록 2 :59290ab0670e2bc6
암호문 블록 2 :98
평문 블록 2 :c1
블록 #3
입력 블록 3 :66a735a81a81fd98
출력 블록 3 :5d783fa976981fcd
암호문 블록 3 :e3
평문 블록 3 :be
블록 #4
입력 블록 4 :a735a81a81fd98e3
출력 블록 4 :ceaab94c98cf1d5a
암호문 블록 4 :2c
평문 블록 4 :e2
블록 #5
입력 블록 5 :35a81a81fd98e32c
출력 블록 5 :5f81a0697af2a6fe
암호문 블록 5 :71
평문 블록 5 :2e
블록 #6
입력 블록 6 :a81a81fd98e32c71
출력 블록 6 :c522ba313e61d845
암호문 블록 6 :85
평문 블록 6 :40
블록 #7
입력 블록 7 :1a81fd98e32c7185
출력 블록 7 :7f7c8b298da519d5
암호문 블록 7 :e0
평문 블록 7 :9f
블록 #8
입력 블록 8 :81fd98e32c7185e0
출력 블록 8 :86dd0145f9c95bfa

암호문 블록 8 :10
평문 블록 8 :96
블록 #9
입력 블록 9 :fd98e32c7185e010
출력 블록 9 :9d8df3f11d977a52
암호문 블록 9 :74
평문 블록 9 :e9
블록 #10
입력 블록 10 :98e32c7185e01074
출력 블록 10 :06e2b37e8cb80d6d
암호문 블록 10 :3b
평문 블록 10 :3d
블록 #11
입력 블록 11 :e32c7185e010743b
출력 블록 11 :9ca42b4ca2da3c7f
암호문 블록 11 :e2
평문 블록 11 :7e
블록 #12
입력 블록 12 :2c7185e010743be2
출력 블록 12 :e6a27ecf2233a734
암호문 블록 12 :f7
평문 블록 12 :11
블록 #13
입력 블록 13 :7185e010743be2f7
출력 블록 13 :895d114e0c22c063
암호문 블록 13 :fa
평문 블록 13 :73
블록 #14
입력 블록 14 :85e010743be2f7fa
출력 블록 14 :60f82f58bb520013
암호문 블록 14 :f3
평문 블록 14 :93
블록 #15
입력 블록 15 :e010743be2f7faf3
출력 블록 15 :aa92b8a7e955b60d
암호문 블록 15 :bd
평문 블록 15 :17
블록 #16
입력 블록 16 :10743be2f7faf3bd
출력 블록 16 :0b134a55050c693d
암호문 블록 16 :21
평문 블록 16 :2a
블록 #17

입력 블록 17 :743be2f7faf3bd21
출력 블록 17 :c9da20eac91823ea
암호문 블록 17 :67
평문 블록 17 :ae
블록 #18
입력 블록 18 :3be2f7faf3bd2167
출력 블록 18 :ae4c7e0c3fbeeb28
암호문 블록 18 :83
평문 블록 18 :2d
블록 #19
입력 블록 19 :e2f7faf3bd216783
출력 블록 19 :8531afa35f8392ff
암호문 블록 19 :0f
평문 블록 19 :8a
블록 #20
입력 블록 20 :f7faf3bd2167830f
출력 블록 20 :63ec332822bff7c3
암호문 블록 20 :34
평문 블록 20 :57
블록 #21
입력 블록 21 :faf3bd2167830f34
출력 블록 21 :24538cfd8acdb2b1
암호문 블록 21 :3a
평문 블록 21 :1e
블록 #22
입력 블록 22 :f3bd2167830f343a
출력 블록 22 :c7641dd3dd501c15
암호문 블록 22 :c4
평문 블록 22 :03
블록 #23
입력 블록 23 :bd2167830f343ac4
출력 블록 23 :e80da1aae7819bf7
암호문 블록 23 :44
평문 블록 23 :ac
블록 #24
입력 블록 24 :2167830f343ac444
출력 블록 24 :7c0f64967b4de65d
암호문 블록 24 :e0
평문 블록 24 :9c
블록 #25
입력 블록 25 :67830f343ac444e0
출력 블록 25 :33c47365ba630a18
암호문 블록 25 :ad

```
        평문 블록 25   :9e
    블록 #26
        입력 블록 26   :830f343ac444e0ad
        출력 블록 26   :a33074d2a0128f3b
        암호문 블록 26 :14
        평문 블록 26   :b7
    블록 #27
        입력 블록 27   :0f343ac444e0ad14
        출력 블록 27   :5966407e3c631ced
        암호문 블록 27 :36
        평문 블록 27   :6f
    블록 #28
        입력 블록 28   :343ac444e0ad1436
        출력 블록 28   :66691c46582b259b
        암호문 블록 28 :ca
        평문 블록 28   :ac
    블록 #29
        입력 블록 29   :3ac444e0ad1436ca
        출력 블록 29   :0cebeca3258e38c8
        암호문 블록 29 :49
        평문 블록 29   :45
    블록 #30
        입력 블록 30   :c444e0ad1436ca49
        출력 블록 30   :22af4d19ecaa677c
        암호문 블록 30 :8d
        평문 블록 30   :af
    블록 #31
        입력 블록 31   :44e0ad1436ca498d
        출력 블록 31   :e9b171e487413ab4
        암호문 블록 31 :67
        평문 블록 31   :8e
    블록 #32
        입력 블록 32   :e0ad1436ca498d67
        출력 블록 32   :04ad2c50e43bced3
        암호문 블록 32 :55
        평문 블록 32   :51
```

II.3.9. HIGHT CFB-64 평문1, 키1 - 암호화

```
    블록 #1
        입력 블록 1    :268d66a735a81a81
        출력 블록 1    :106240c41a85aa0b
        평문 블록 1    :d76d0d18327ec562
```

암호문 블록 1 :c70f4ddc28fb6f69
블록 #2
입력 블록 2 :c70f4ddc28fb6f69
출력 블록 2 :c129fd2d88e0b5b7
평문 블록 2 :b15e6bc365ac0c0f
암호문 블록 2 :707796eeed4cb9b8
블록 #3
입력 블록 3 :707796eeed4cb9b8
출력 블록 3 :5089db82d1c398a1
평문 블록 3 :8d41e0bb938568ae
암호문 블록 3 :ddc83b394246f00f
블록 #4
입력 블록 4 :ddc83b394246f00f
출력 블록 4 :a59bdf3ec505c839
평문 블록 4 :ebfd92ed1affa096
암호문 블록 4 :4e664dd3dffa68af
블록 #5
입력 블록 5 :4e664dd3dffa68af
출력 블록 5 :f58219f00d18e0fb
평문 블록 5 :394d20fc5277ddfc
암호문 블록 5 :cccf390c5f6f3d07
블록 #6
입력 블록 6 :cccf390c5f6f3d07
출력 블록 6 :9a591f98ec809a09
평문 블록 6 :4de8b0fce1eb2b93
암호문 블록 6 :d7b1af640d6bb19a
블록 #7
입력 블록 7 :d7b1af640d6bb19a
출력 블록 7 :67fd51ca1a1d6a42
평문 블록 7 :d4ae40ef4768c613
암호문 블록 7 :b35311255d75ac51
블록 #8
입력 블록 8 :b35311255d75ac51
출력 블록 8 :d608ff782e975cbf
평문 블록 8 :b50b8942f7d4b9b3
암호문 블록 8 :6303763ad943e50c

II.3.10. HIGHT CFB-64 평문1, 키1 - 복호화

블록 #1
입력 블록 1 :268d66a735a81a81
출력 블록 1 :106240c41a85aa0b
암호문 블록 1 :c70f4ddc28fb6f69

```
        평문 블록 1    :d76d0d18327ec562
블록 #2
        입력 블록 2    :c70f4ddc28fb6f69
        출력 블록 2    :c129fd2d88e0b5b7
        암호문 블록 2 :707796eeed4cb9b8
        평문 블록 2    :b15e6bc365ac0c0f
블록 #3
        입력 블록 3    :707796eeed4cb9b8
        출력 블록 3    :5089db82d1c398a1
        암호문 블록 3 :ddc83b394246f00f
        평문 블록 3    :8d41e0bb938568ae
블록 #4
        입력 블록 4    :ddc83b394246f00f
        출력 블록 4    :a59bdf3ec505c839
        암호문 블록 4 :4e664dd3dffa68af
        평문 블록 4    :ebfd92ed1affa096
블록 #5
        입력 블록 5    :4e664dd3dffa68af
        출력 블록 5    :f58219f00d18e0fb
        암호문 블록 5 :cccf390c5f6f3d07
        평문 블록 5    :394d20fc5277ddfc
블록 #6
        입력 블록 6    :cccf390c5f6f3d07
        출력 블록 6    :9a591f98ec809a09
        암호문 블록 6 :d7b1af640d6bb19a
        평문 블록 6    :4de8b0fce1eb2b93
블록 #7
        입력 블록 7    :d7b1af640d6bb19a
        출력 블록 7    :67fd51ca1a1d6a42
        암호문 블록 7 :b35311255d75ac51
        평문 블록 7    :d4ae40ef4768c613
블록 #8
        입력 블록 8    :b35311255d75ac51
        출력 블록 8    :d608ff782e975cbf
        암호문 블록 8 :6303763ad943e50c
        평문 블록 8    :b50b8942f7d4b9b3
```

II.3.11. HIGHT CFB-64 평문2, 키2 - 암호화

```
블록 #1
        입력 블록 1    :268d66a735a81a81
        출력 블록 1    :96b71e0493e7e1fa
        평문 블록 1    :6bc1bee22e409f96
```

```
        암호문 블록 1 :fd76a0e6bda77e6c
블록 #2
        입력 블록 2   :fd76a0e6bda77e6c
        출력 블록 2   :f58e2f64c477f37c
        평문 블록 2   :e93d7e117393172a
        암호문 블록 2 :1cb35175b7e4e456
블록 #3
        입력 블록 3   :1cb35175b7e4e456
        출력 블록 3   :bc390c6fe6f92f1e
        평문 블록 3   :ae2d8a571e03ac9c
        암호문 블록 3 :12148638f8fa8382
블록 #4
        입력 블록 4   :12148638f8fa8382
        출력 블록 4   :fed88067eb516b04
        평문 블록 4   :9eb76fac45af8e51
        암호문 블록 4 :606fefcbaefee555
블록 #5
        입력 블록 5   :606fefcbaefee555
        출력 블록 5   :9f50aa44b7c80088
        평문 블록 5   :30c81c46a35ce411
        암호문 블록 5 :af98b6021494e499
블록 #6
        입력 블록 6   :af98b6021494e499
        출력 블록 6   :ceb6d24f0de9158e
        평문 블록 6   :e5fbc1191a0a52ef
        암호문 블록 6 :2b4d135617e34761
블록 #7
        입력 블록 7   :2b4d135617e34761
        출력 블록 7   :f100cf09d9a19973
        평문 블록 7   :f69f2445df4f9b17
        암호문 블록 7 :079feb4c06ee0264
블록 #8
        입력 블록 8   :079feb4c06ee0264
        출력 블록 8   :aa691fa90bcd224b
        평문 블록 8   :ad2b417be66c3710
        암호문 블록 8 :07425ed2eda1155b
```

II.3.12. HIGHT CFB-64 평문2, 키2 - 복호화

```
블록 #1
        입력 블록 1   :268d66a735a81a81
        출력 블록 1   :96b71e0493e7e1fa
        암호문 블록 1 :fd76a0e6bda77e6c
```

```
        평문 블록 1    :6bc1bee22e409f96
블록 #2
        입력 블록 2    :fd76a0e6bda77e6c
        출력 블록 2    :f58e2f64c477f37c
        암호문 블록 2 :1cb35175b7e4e456
        평문 블록 2    :e93d7e117393172a
블록 #3
        입력 블록 3    :1cb35175b7e4e456
        출력 블록 3    :bc390c6fe6f92f1e
        암호문 블록 3 :12148638f8fa8382
        평문 블록 3    :ae2d8a571e03ac9c
블록 #4
        입력 블록 4    :12148638f8fa8382
        출력 블록 4    :fed88067eb516b04
        암호문 블록 4 :606fefcbaefee555
        평문 블록 4    :9eb76fac45af8e51
블록 #5
        입력 블록 5    :606fefcbaefee555
        출력 블록 5    :9f50aa44b7c80088
        암호문 블록 5 :af98b6021494e499
        평문 블록 5    :30c81c46a35ce411
블록 #6
        입력 블록 6    :af98b6021494e499
        출력 블록 6    :ceb6d24f0de9158e
        암호문 블록 6 :2b4d135617e34761
        평문 블록 6    :e5fbc1191a0a52ef
블록 #7
        입력 블록 7    :2b4d135617e34761
        출력 블록 7    :f100cf09d9a19973
        암호문 블록 7 :079feb4c06ee0264
        평문 블록 7    :f69f2445df4f9b17
블록 #8
        입력 블록 8    :079feb4c06ee0264
        출력 블록 8    :aa691fa90bcd224b
        암호문 블록 8 :07425ed2eda1155b
        평문 블록 8    :ad2b417be66c3710
```

II.4. HIGHT OFB 운영 모드

II.4.1. HIGHT OFB 평문1, 키1 - 암호화

```
블록 #1
        입력 블록 1   :268d66a735a81a81
        출력 블록 1   :106240c41a85aa0b
        평문 블록 1   :d76d0d18327ec562
        암호문 블록 1 :c70f4ddc28fb6f69
블록 #2
        입력 블록 2   :106240c41a85aa0b
        출력 블록 2   :95258664a3fd18fb
        평문 블록 2   :b15e6bc365ac0c0f
        암호문 블록 2 :247beda7c65114f4
블록 #3
        입력 블록 3   :95258664a3fd18fb
        출력 블록 3   :654a261a0897df25
        평문 블록 3   :8d41e0bb938568ae
        암호문 블록 3 :e80bc6a19b12b78b
블록 #4
        입력 블록 4   :654a261a0897df25
        출력 블록 4   :ae92b022caf5cb5b
        평문 블록 4   :ebfd92ed1affa096
        암호문 블록 4 :456f22cfd00a6bcd


블록 #5
        입력 블록 5   :ae92b022caf5cb5b
        출력 블록 5   :ba84cb3daddd77db
        평문 블록 5   :394d20fc5277ddfc
        암호문 블록 5 :83c9ebc1ffaaaa27
블록 #6
        입력 블록 6   :ba84cb3daddd77db
        출력 블록 6   :f0c27558f1fa5f81
        평문 블록 6   :4de8b0fce1eb2b93
        암호문 블록 6 :bd2ac5a410117412
블록 #7
        입력 블록 7   :f0c27558f1fa5f81
        출력 블록 7   :e61f61bbceb64ad0
        평문 블록 7   :d4ae40ef4768c613
        암호문 블록 7 :32b1215489de8cc3
블록 #8
```

입력 블록 8 :e61f61bbceb64ad0
출력 블록 8 :5b12b7e03e4114f2
평문 블록 8 :b50b8942f7d4b9b3
암호문 블록 8 :ee193ea2c995ad41

II.4.2. HIGHT OFB 평문1, 키1 - 복호화

블록 #1
입력 블록 1 :268d66a735a81a81
출력 블록 1 :106240c41a85aa0b
암호문 블록 1 :c70f4ddc28fb6f69
평문 블록 1 :d76d0d18327ec562
블록 #2
입력 블록 2 :106240c41a85aa0b
출력 블록 2 :95258664a3fd18fb
암호문 블록 2 :247beda7c65114f4
평문 블록 2 :b15e6bc365ac0c0f
블록 #3
입력 블록 3 :95258664a3fd18fb
출력 블록 3 :654a261a0897df25
암호문 블록 3 :e80bc6a19b12b78b
평문 블록 3 :8d41e0bb938568ae
블록 #4
입력 블록 4 :654a261a0897df25
출력 블록 4 :ae92b022caf5cb5b
암호문 블록 4 :456f22cfd00a6bcd
평문 블록 4 :ebfd92ed1affa096
블록 #5
입력 블록 5 :ae92b022caf5cb5b
출력 블록 5 :ba84cb3daddd77db
암호문 블록 5 :83c9ebc1ffaaaa27
평문 블록 5 :394d20fc5277ddfc
블록 #6
입력 블록 6 :ba84cb3daddd77db
출력 블록 6 :f0c27558f1fa5f81
암호문 블록 6 :bd2ac5a410117412
평문 블록 6 :4de8b0fce1eb2b93
블록 #7
입력 블록 7 :f0c27558f1fa5f81
출력 블록 7 :e61f61bbceb64ad0
암호문 블록 7 :32b1215489de8cc3
평문 블록 7 :d4ae40ef4768c613
블록 #8

입력 블록 8 :e61f61bbceb64ad0
출력 블록 8 :5b12b7e03e4114f2
암호문 블록 8 :ee193ea2c995ad41
평문 블록 8 :b50b8942f7d4b9b3

II.4.3. HIGHT OFB 평문2, 키2 - 암호화

블록 #1
입력 블록 1 :268d66a735a81a81
출력 블록 1 :96b71e0493e7e1fa
평문 블록 1 :6bc1bee22e409f96
암호문 블록 1 :fd76a0e6bda77e6c
블록 #2
입력 블록 2 :96b71e0493e7e1fa
출력 블록 2 :b8f001cf9d2cd485
평문 블록 2 :e93d7e117393172a
암호문 블록 2 :51cd7fdeeebfc3af
블록 #3
입력 블록 3 :b8f001cf9d2cd485
출력 블록 3 :81508bf029610e7b
평문 블록 3 :ae2d8a571e03ac9c
암호문 블록 3 :2f7d01a73762a2e7
블록 #4
입력 블록 4 :81508bf029610e7b
출력 블록 4 :f2775ee91a49138b
평문 블록 4 :9eb76fac45af8e51
암호문 블록 4 :6cc031455fe69dda
블록 #5
입력 블록 5 :f2775ee91a49138b
출력 블록 5 :19634e377b10410a
평문 블록 5 :30c81c46a35ce411
암호문 블록 5 :29ab5271d84ca51b
블록 #6
입력 블록 6 :19634e377b10410a
출력 블록 6 :f2881f2e8bb5f382
평문 블록 6 :e5fbc1191a0a52ef
암호문 블록 6 :1773de3791bfa16d
블록 #7
입력 블록 7 :f2881f2e8bb5f382
출력 블록 7 :1b49c0bfda305570
평문 블록 7 :f69f2445df4f9b17
암호문 블록 7 :edd6e4fa057fce67
블록 #8

입력 블록 8 :1b49c0bfda305570
출력 블록 8 :0d3ab6730e1a2168
평문 블록 8 :ad2b417be66c3710
암호문 블록 8 :a011f708e8761678

II.4.4. HIGHT OFB 평문2, 키2 - 복호화

블록 #1
입력 블록 1 :268d66a735a81a81
출력 블록 1 :96b71e0493e7e1fa
암호문 블록 1 :fd76a0e6bda77e6c
평문 블록 1 :6bc1bee22e409f96
블록 #2
입력 블록 2 :96b71e0493e7e1fa
출력 블록 2 :b8f001cf9d2cd485
암호문 블록 2 :51cd7fdeeebfc3af
평문 블록 2 :e93d7e117393172a
블록 #3
입력 블록 3 :b8f001cf9d2cd485
출력 블록 3 :81508bf029610e7b
암호문 블록 3 :2f7d01a73762a2e7
평문 블록 3 :ae2d8a571e03ac9c
블록 #4
입력 블록 4 :81508bf029610e7b
출력 블록 4 :f2775ee91a49138b
암호문 블록 4 :6cc031455fe69dda
평문 블록 4 :9eb76fac45af8e51
블록 #5
입력 블록 5 :f2775ee91a49138b
출력 블록 5 :19634e377b10410a
암호문 블록 5 :29ab5271d84ca51b
평문 블록 5 :30c81c46a35ce411
블록 #6
입력 블록 6 :19634e377b10410a
출력 블록 6 :f2881f2e8bb5f382
암호문 블록 6 :1773de3791bfa16d
평문 블록 6 :e5fbc1191a0a52ef
블록 #7
입력 블록 7 :f2881f2e8bb5f382
출력 블록 7 :1b49c0bfda305570
암호문 블록 7 :edd6e4fa057fce67
평문 블록 7 :f69f2445df4f9b17
블록 #8

입력 블록 8 :1b49c0bfda305570
출력 블록 8 :0d3ab6730e1a2168
암호문 블록 8 :a011f708e8761678
평문 블록 8 :ad2b417be66c3710

II.5. HIGHT CTR 운영 모드

II.5.1. HIGHT CTR 평문1, 키1 - 암호화

블록 #1
카운터 블록 1 :00000000000000fe
입력 블록 1 :00000000000000fe
출력 블록 1 :b3d0fdffc6a49dc7
평문 블록 1 :d76d0d18327ec562
암호문 블록 1 :64bdf0e7f4da58a5
블록 #2
카운터 블록 2 :00000000000000ff
입력 블록 2 :00000000000000ff
출력 블록 2 :1b04cb6910553797
평문 블록 2 :b15e6bc365ac0c0f
암호문 블록 2 :aa5aa0aa75f93b98
블록 #3
카운터 블록 3 :0000000000000100
입력 블록 3 :0000000000000100
출력 블록 3 :8ad6c79844a7d3be
평문 블록 3 :8d41e0bb938568ae
암호문 블록 3 :07972723d722bb10
블록 #4
카운터 블록 4 :0000000000000101
입력 블록 4 :0000000000000101
출력 블록 4 :5f73d502baac92ac
평문 블록 4 :ebfd92ed1affa096
암호문 블록 4 :b48e47efa053323a
블록 #5
카운터 블록 5 :0000000000000102
입력 블록 5 :0000000000000102
출력 블록 5 :d76b4738f30e0d6b
평문 블록 5 :394d20fc5277ddfc
암호문 블록 5 :ee2667c4a179d097
블록 #6
카운터 블록 6 :0000000000000103
입력 블록 6 :0000000000000103

출력 블록 6 :70475bbc64de12e0
평문 블록 6 :4de8b0fce1eb2b93
암호문 블록 6 :3dafeb4085353973
블록 #7
카운터 블록 7 :0000000000000104
입력 블록 7 :0000000000000104
출력 블록 7 :b35ff5f95b025d0e
평문 블록 7 :d4ae40ef4768c613
암호문 블록 7 :67f1b5161c6a9b1d
블록 #8
카운터 블록 8 :0000000000000105
입력 블록 8 :0000000000000105
출력 블록 8 :976943156c92cc1c
평문 블록 8 :b50b8942f7d4b9b3
암호문 블록 8 :2262ca579b4675af

II.5.2. HIGHT CTR 평문1, 키1 - 복호화

블록 #1
카운터 블록 1 :00000000000000fe
입력 블록 1 :00000000000000fe
출력 블록 1 :b3d0fdffc6a49dc7
암호문 블록 1 :64bdf0e7f4da58a5
평문 블록 1 :d76d0d18327ec562
블록 #2
카운터 블록 2 :00000000000000ff
입력 블록 2 :00000000000000ff
출력 블록 2 :1b04cb6910553797
암호문 블록 2 :aa5aa0aa75f93b98
평문 블록 2 :b15e6bc365ac0c0f
블록 #3
카운터 블록 3 :0000000000000100
입력 블록 3 :0000000000000100
출력 블록 3 :8ad6c79844a7d3be
암호문 블록 3 :07972723d722bb10
평문 블록 3 :8d41e0bb938568ae
블록 #4
카운터 블록 4 :0000000000000101
입력 블록 4 :0000000000000101
출력 블록 4 :5f73d502baac92ac
암호문 블록 4 :b48e47efa053323a
평문 블록 4 :ebfd92ed1affa096

블록 #5
카운터 블록 5 :0000000000000102
입력 블록 5 :0000000000000102
출력 블록 5 :d76b4738f30e0d6b
암호문 블록 5 :ee2667c4a179d097
평문 블록 5 :394d20fc5277ddfc
블록 #6
카운터 블록 6 :0000000000000103
입력 블록 6 :0000000000000103
출력 블록 6 :70475bbc64de12e0
암호문 블록 6 :3dafeb4085353973
평문 블록 6 :4de8b0fce1eb2b93
블록 #7
카운터 블록 7 :0000000000000104
입력 블록 7 :0000000000000104
출력 블록 7 :b35ff5f95b025d0e
암호문 블록 7 :67f1b5161c6a9b1d
평문 블록 7 :d4ae40ef4768c613
블록 #8
카운터 블록 8 :0000000000000105
입력 블록 8 :0000000000000105
출력 블록 8 :976943156c92cc1c
암호문 블록 8 :2262ca579b4675af
평문 블록 8 :b50b8942f7d4b9b3

II.5.3. HIGHT CTR 평문2, 키2 - 암호화

블록 #1
카운터 블록 1 :00000000000000fe
입력 블록 1 :00000000000000fe
출력 블록 1 :d87517609a044818
평문 블록 1 :6bc1bee22e409f96
암호문 블록 1 :b3b4a982b444d78e
블록 #2
카운터 블록 2 :00000000000000ff
입력 블록 2 :00000000000000ff
출력 블록 2 :6d55ea20d96d9aa9
평문 블록 2 :e93d7e117393172a
암호문 블록 2 :84689431aafe8d83
블록 #3
카운터 블록 3 :0000000000000100
입력 블록 3 :0000000000000100

출력 블록 3 :3002f715f9ebdf1f
평문 블록 3 :ae2d8a571e03ac9c
암호문 블록 3 :9e2f7d42e7e87383
블록 #4
카운터 블록 4 :0000000000000101
입력 블록 4 :0000000000000101
출력 블록 4 :e1826386977d7c3f
평문 블록 4 :9eb76fac45af8e51
암호문 블록 4 :7f350c2ad2d2f26e
블록 #5
카운터 블록 5 :0000000000000102
입력 블록 5 :0000000000000102
출력 블록 5 :83ea798e469d83f0
평문 블록 5 :30c81c46a35ce411
암호문 블록 5 :b32265c8e5c167e1

블록 #6
카운터 블록 6 :0000000000000103
입력 블록 6 :0000000000000103
출력 블록 6 :80eb004e3508e6f6
평문 블록 6 :e5fbc1191a0a52ef
암호문 블록 6 :6510c1572f02b419
블록 #7
카운터 블록 7 :0000000000000104
입력 블록 7 :0000000000000104
출력 블록 7 :f288891750b97d97
평문 블록 7 :f69f2445df4f9b17
암호문 블록 7 :0417ad528ff6e680
블록 #8
카운터 블록 8 :0000000000000105
입력 블록 8 :0000000000000105
출력 블록 8 :8b1086eaad0c41bb
평문 블록 8 :ad2b417be66c3710
암호문 블록 8 :263bc7914b6076ab

II.5.4. HIGHT CTR 평문2, 키2 - 복호화

블록 #1
카운터 블록 1 :00000000000000fe
입력 블록 1 :00000000000000fe
출력 블록 1 :d87517609a044818

암호문 블록 1 :b3b4a982b444d78e
평문 블록 1 :6bc1bee22e409f96
블록 #2
카운터 블록 2 :00000000000000ff
입력 블록 2 :00000000000000ff
출력 블록 2 :6d55ea20d96d9aa9
암호문 블록 2 :84689431aafe8d83
평문 블록 2 :e93d7e117393172a
블록 #3
카운터 블록 3 :0000000000000100
입력 블록 3 :0000000000000100
출력 블록 3 :3002f715f9ebdf1f
암호문 블록 3 :9e2f7d42e7e87383
평문 블록 3 :ae2d8a571e03ac9c

블록 #4
카운터 블록 4 :0000000000000101
입력 블록 4 :0000000000000101
출력 블록 4 :e1826386977d7c3f
암호문 블록 4 :7f350c2ad2d2f26e
평문 블록 4 :9eb76fac45af8e51
블록 #5
카운터 블록 5 :0000000000000102
입력 블록 5 :0000000000000102
출력 블록 5 :83ea798e469d83f0
암호문 블록 5 :b32265c8e5c167e1
평문 블록 5 :30c81c46a35ce411
블록 #6
카운터 블록 6 :0000000000000103
입력 블록 6 :0000000000000103
출력 블록 6 :80eb004e3508e6f6
암호문 블록 6 :6510c1572f02b419
평문 블록 6 :e5fbc1191a0a52ef
블록 #7
카운터 블록 7 :0000000000000104
입력 블록 7 :0000000000000104
출력 블록 7 :f288891750b97d97
암호문 블록 7 :0417ad528ff6e680
평문 블록 7 :f69f2445df4f9b17
블록 #8
카운터 블록 8 :0000000000000105

입력 블록 8 :0000000000000105
출력 블록 8 :8b1086eaad0c41bb
암호문 블록 8 :263bc7914b6076ab
평문 블록 8 :ad2b417be66c3710

부 록 III
관련 문헌

다음 문서들은 본 표준의 이해를 돕기 위한 문서로서 특정 문서(발행일 및 판 번호 또는 개정 번호를 명시한 것)와 일반 문서로 구별된다.

- 특정 문서인 경우 해당 판본 이후의 개정판은 적용되지 않는다.
- 일반 문서인 경우 최신 판본이 적용된다.

[1] NIST SP 800-38A, 'Recommendation for Block Cipher Modes of Operation - Methods and Techniques', 2001.

[2] ISO/IEC 10116, 'Information technology — Security techniques — Modes of operation for an n-bit block cipher', 2006.

방송통신표준

64 비트 블록 암호 HIGHT 운영 모드
(Modes of Operation for the 64-bit Block Cipher HIGHT)

발행인 : 미래창조과학부 장관
발행처 : 미래창조과학부 국립전파연구원
140-848, 서울 용산구 원효로41길 29
발행일 : 2013.12.
국립전파연구원 고시 제 2013-20호