**REPORT**

**[ Assignment 2 : 페이스텔 구조 분석]**



|  |  |
| --- | --- |
| 과 목 명 | 정보보호론 |
| 교 수 명 | 김 효 승 |
| 학 번 | 20237107 |
| 작 성 자 | 하 태 영 |
| 제 출 일 | 2025.03.28 |

**한림대학교**

1. 페이스텔 2라운드 구조를 그리시오.  // 라운드키 k = (k\_1, k\_2)

텍스트, 도표, 스크린샷, 라인이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

2. (L\_0, R\_0)를 입력한 암호화 과정의 1라운드 결과인 (L\_1, R\_1)과 2라운드의 결과인 (L\_2, R\_2)를 식으로 표현하시오.

**1라운드 결과**

* L\_1 = R\_0; R\_1 = L\_0﻿ ⊕ F(k\_1, R\_0);

**2라운드 결과**

* L\_2 = L\_1 ⊕ F(k\_2, R\_1); R\_2 = R\_1;

3. (L\_2, R\_2)를 입력한 복호화 과정의 결과가 (L\_0, R\_0)로 올바르게 되는 것을 단계별로 작성하시오.

텍스트, 스크린샷, 도표, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

**복호화 과정**

* L\_2 = L\_1 ⊕ F(k\_2, R\_1); R\_2 = R\_1;
* L\_1 = R\_2; R\_1 = L\_2﻿ ⊕ F(k\_2, R\_2);
* L\_1 =R\_1; R\_1 = L\_1 ⊕ F(k\_2, R\_1) ⊕ F(k\_1, R\_0);
* L\_1 = L\_2﻿ ⊕ F(k\_2, R\_2); R\_1 = L\_1;
* L\_1 = L\_1 ⊕ F(k\_2, R\_1);
* L\_1 ⊕ L\_1 = F(k\_2, R\_1);
* 0 = F(k\_2, R\_1);
* L\_0 = L\_1 ⊕ F(k\_1, R\_1); R\_0 = R\_1
* L\_0 = L\_1 ⊕ F(k\_1, R\_1);
* L\_0 = L\_1 ⊕ F(k\_2, R\_1) ⊕ F(k\_1, R\_1);
* L\_0 = L\_1;

**복호화 결과**

* L\_0 = L\_1;
* R\_0 = R\_1;