2021 국민대학교 정보보안암호수학과 동아리 연합 암호분석경진대회

3번 문제 - 암호 분석 (출제: 동아리 CaS)

암호에 대한 공격은 사용자가 사용한 키를 찾는 것을 목표로 한다. 이러한 공격에는 모든 값을 대입하여 원하는 결과를 얻는 무차별 대입 공격(Brute Force Attack)이 있다. 무차별 대입 공격보다 더 빠르고 효율적으로 공격을 수행하기 위해 여러 가지 분석법이 제안됐다. 제안된 여러 가지 분석법 중 대표적인 분석법으로는 차분 분석(Differential Cryptanalysis)이 있다. 차분 분석은 1991년 Eli Biham과 Adi Shamir에 의해 제안되었으며 현재까지도 많은 블록암호를 분석하는데 사용된다. 차분 분석이 무차별 대입 공격보다 더 빠르고 효율적인 이유는 키를 찾는데 사용되는 복잡도가 더 적기 때문이다. 예를들어, 키 사이즈가 32-bit인 암호에 대해 무차별 대입 공격을 적용한다면 전체 키를 2^{32}의 복잡도로 찾을 수 있을것으로 예상된다. 그러나 차분 분석을 이용하여 2^{20}의 복잡도로 부분 키 4-bit를 복구한다면, 전체 키를 $2^{20}+2^{28}\approx 2^{28}$($2^{20}$: 차분 분석을 통한 4-bit 복구 복잡도, 2^{28}: 나머지 28-bit 키에 대한 전수조사 복잡도)의 복잡도로 찾을 수 있게된다. 이는 무차별 대입 공격의 복잡도인 2^{32}보다 적은 복잡도이다.

문제의 블록암호는 철수가 만든 차분 분석에 취약한 암호이다. 또한 별도의 키 스케쥴을 거치지않고 각 라운드에 같은 키가 Xor된다. 철수's 블록암호에 대한 정보는 아래와 같다.

● 철수's 블록암호

☞ **Rounds: 7**

☞ **Key sizes: 32**

☞ **Block sizes: 32**

☞ **Rounds function: Substitution-Permutation-Addroundkey로 이루어져있다. Substitution에 쓰인 sbox와 permutation table은 [표 1,2]와 같다. 마지막 라운드에서는 Permutation이 생략된다.**

(철수's 블록암호에 평문은 오른쪽에서 왼쪽으로 0번째 비트부터 63번째 비트까지 차례로 입력된다.)

입력	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
출력	6	5	12	10	1	14	7	9	11	0	3	13	8	15	4	2

[표 1] 철수's 블록암호에서 사용된 sbox

입력	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
출력	18	23	25	20	16	3	21	6	24	19	22	13	12	26	27	9
입력	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
출력	4	1	31	10	2	29	15	8	30	17	7	0	28	11	5	14

[표 2] 철수's 블록암호에서 사용된 permutation table

- 철수's 블록암호의 pseudo code

Encryption(plaintext, key):
tmp_state ← plaintext ⊕ key
For i = 1 to 6 do
    tmp_state ← Substitution(tmp_state)
    tmp_state ← Permutation(tmp_state)
    tmp_state ← Addroundkey(tmp_state)
tmp_state ← Substitution(tmp_state)
tmp_state ← Addroundkey(tmp_state)
ciphertext ← tmp_state

철수's 블록암호의 도식은 "철수의 블록암호" 그림파일 참조.

철수's 블록암호에 대해 다음 문제를 푸시오.

[3 - 1 문제] - 배점 10점

해당 블록암호의 Differential Distribution Table에서 원소 4의 개수를 제시하시오. (Differential Distribution Table을 출력하는 소스코드도 함께 제출.)

[3 - 2 문제] - 배점 20점

3 - 1 문제의 Differential Distribution Table을 이용하여 해당 알고리즘의 Differential Trail을 제시하시오. (그림으로 제출.)

[3 - 3 문제] - 배점 70점

3 - 2 문제에서 구성한 Differential Trail와 "철수의 블록암호.exe" 실행파일을 이용하여 주어진 알고리즘의 키를 구하시오. (전체 키가 아니어도 상관없음. 어느 부분의 키인지만 명시. 공격 과정을 간단하게라도 설명. 공격 복잡도가 적을수록 높은 점수를 부여.)

● 참고 사항

1) [Textbooks in Mathematics] Douglas R. Stinson, Maura B. Paterson - Cryptography. Theory and Practice (2019, CRC Press) 파일, 117p-124p (4.4절 Differential Cryptanalysis).
2) 철수의 블록암호.pdf 그림
3) 철수의 블록암호.exe 파일

문의: ghfaos7708@kookmin.ac.kr