|  |
| --- |
| **2021 국민대학교 정보보안암호수학과 동아리 연합 암호경진대회** |
| 3번 문제 답안 |
| 정보보안암호수학과 20192243 이용진 |
| 3-1.    원소 4의 개수는 24개이다.  3-2.  그림(pdf 파일)으로 제출  3-3.  <차분 공격 요약>   1. 차분분포표를 활용하여 가장 높은 확률을 가지는 6라운드 차분 특성을 찾는다. 2. 공격자가 가지고 있는 암호문 2개를 Key를 예측하여 7라운드 복호화를 진행한다. 3. 복호화 값의 차분을 계산하고 6라운드 차분 특성과 일치하는지 확인한다. 4. 만약 일치한다면, 키 후보로 등록한다. 5. 2~4번의 과정을 반복하여 가장 많이 추천된 키 후보를 올바른 키로 등록한다.   평문 2개의 차분이 [0x0, 0x0, 0x0, 0x0, 0xB, 0x0, 0x0, 0x0] 일 경우,  6라운드 차분 특성은 [0x1, 0x2, 0x1, 0x4, 0x0, 0x0, 0x0, 0x0]이고 확률은 대략적으로1.5e-05이다.  (더 좋은 차분 특성이 있을 것으로 생각된다)  즉, 입력차분: [0x0, 0x0, 0x0, 0x0, 0xB, 0x0, 0x0, 0x0]를 만족하는 평문 쌍, 100000개를 생성해야 한다.  그 후, “철수의 블록암호.exe”를 이용하여 암호문 또한 생성해준다.  생성한 암호문을 2개씩 읽는다. => 6라운드 차분 특성을 확인해야하기 때문이다.  공격하고자 하는 부분을 정하고, 읽은 암호문 2개를 공격하는 부분의 Key를 예측하여  7라운드 복호화를 진행하고 공격 부분의 둘의 차분 값을 계산한다.  차분 값이 6라운드 차분 특성의 공격 부분의 값과 일치하면, Key의 빈도수를 추가한다.  <차분 공격 과정>  <1. 6-Round 차분 특성 찾기>    <2. 평문, 암호문 쌍, 200000개 생성 => 암호문 차분 값이 100000개 필요하기 때문>  평문의 차분 값이 [0, 0, 0, 0, 11, 0, 0, 0]이 되도록 평문, 암호문 쌍을 생성한다.    암호문 생성은 문제에서 주어진 exe 파일을 사용했다.  <3. 6-Round 차분 특성을 활용하여 앞의 4-bit Key 4개를 추측한다.>    위의 소스코드를 통해 target 위치의 Key 후보를 찾는다.  target은 공격하고자 하는 부분이다.  위의 소스코드는 target이 0임으로, 맨 앞의 첫번째 Key후보를 찾는다.  target을 0~3으로 변경하여 앞의 4개의 Key 후보를 찾는다.  # Key = [k0, k1, k2, k3, k4, k5, k6, k7]  소스코드를 실행하면 target 부분의 6-Round 차분 특성을 만족하는  Key의 빈도수를 확인할 수 있다. 빈도수가 가장 높은 Key가 Key후보가 된다.  위의 경우 첫번째 4-bit Key를 빈도수가 가장 높은 4로 예측한다.  traget의 값을 1 or 2 or 3으로 바꿔 앞의 4-bit Key 후보 4개를 찾는다.    Key 후보 결과:   * Key = [0x4, 0x3, 0x1, 0x0, ? ,? ,? ,?] or [0x4, 0x3, 0x1, 0x2, ?, ? ,? ,?]   # target이 3인 경우, 0x0과 0x2의 빈도수가 같음으로 Key후보가 2개 생긴다.  <4. 나머지 4-bit Key 4개를 조사한다.>  아직 구하지 못한 나머지 4-bit Key 4개를 전수 조사한다.  2^16의 복잡도로 Key 전체를 복구할 수 있다.    위의 소스코드를 활용하여 나머지 4-bit Key 4개를 전수 조사하면    Key = [0x4, 0x3, 0x1, 0x2, 0x4, 0x3, 0x8, 0x6]이 나온다.  즉, 철수의 블록암호에서 사용한 Key는 [0x4, 0x3, 0x1, 0x2, 0x4, 0x3, 0x8, 0x6]이다.  # 평문과 암호문은 “철수의 블록암호.exe”의 결과를 이용하였다.  그럼으로 이 차분 공격의 복잡도는   * 2^16 + 100000(평/암호문 생성) +   4(차분 공격 키 4개 찾기) x 16(예측 키 개수) x  100000(암호문 2개, 7라운드 복호화 차분 계산 횟수)  = 2^16 + 2^23 ≈ 2^23으로 예상된다.    만약, 미리 평문/암호문을 생성하고, 암호문 2개의 7라운드 복호화 차분을 계산하는데 시간이 많이 걸리지 않는 다면, 차분 공격 복잡도는   * 2^16 + 4 \* 16 ≈ 2^16으로 예상된다. |