문제 1-PT01: 주어진 암호문 집합들을 암호 알고리즘 E에 의해 생성된 것과 랜덤 함수에 의해 생성된 것으로 분류하고 그러한 결론을 내리게 된 과정을 상세히 기술하시오.

이 문제는 기존 AES와 다른 구조(ARK-SR-SB'-MK- ARK-SR-SB'-MK- ARK-SR-SB'-MK-ARK)로 축소 된 알고리즘이다.
해당 문제를 풀기 위해 차분 분석을 생각하였는데, 그 이유는 평문과 비밀키가 주어졌기 때문이다. 평문과 비밀키를 갖고 있을 경우 선택 평문 공격을 할 수 있기 때문이다.
먼저 주어진 평문 데이터 PT01.dat를 분석해보자. PT01.dat에 있는 평문들을 2개씩 짝을 지어 XOR 할 경우 모든 값이 '00 00 00 b3 09 00 00 00 00 45 00 00 00 00 0b 00'을 나타낸다. 이를 보기 쉽게 나타내면 아래 그림과 같다.

PlainText01 XOR PlainText02 =

00	00	00	b3
09	00	00	00
00	45	00	00
00	00	0b	00

위 표를 차분 분석하기 위해 문제에서 제공하는 AES 구조로 따라가 보았다.

ARK:

00	00	00	b3
09	00	00	00
00	45	00	00
00	00	0b	00

-> SR:

00	00	00	b3
00	00	00	09
00	00	00	45
00	00	00	0b

->

SB':

00	00	00	X
00	00	00	09
00	00	00	Y
00	00	00	0b

-> MK:

00	00	00	A
00	00	00	B
00	00	00	C
00	00	00	D

->

ARK:

00	00	00	A
00	00	00	B
00	00	00	C
00	00	00	D

-> SR:

00	00	00	A
00	00	B	00
00	C	00	00
D	00	00	00

->

SB':

00	00	00	S(A)
00	00	B	00
00	S(C)	00	00
D	00	00	00

-> MK:

D	S(C)	3B	2S(A)
D	3S(C)	2B	S(A)
3D	2S(C)	B	S(A)
2D	S(C)	B	3S(A)

->

ARK:

D	S(C)	3B	2S(A)
D	3S(C)	2B	S(A)
3D	2S(C)	B	S(A)
2D	S(C)	B	3S(A)

-> SR:

D	S(C)	3B	2S(A)
3S(C)	2B	S(A)	D
B	S(A)	3D	2S(C)
3S(A)	2D	S(C)	B

->

SB':

?	?	?	?
3S(C)	2B	S(A)	D
?	?	?	?
3S(A)	2D	S(C)	B

차분 분석을 하기 위해서는 입력 단계의 마지막 차분 값과 출력 차분 값을 비교해야 한다. 그

렇다면 출력 차분을 구해보자.
출력 차분을 구하기 위해서는 비밀키 쌍을 XOR 해준 뒤, XOR 한 값을 역연산을 해주면 된다.
CT0X의 비밀키 쌍을 XOR한 값을 SC라고 칭할 경우,

SC:

SC00	SC01	SC02	SC03
SC04	SC05	SC06	SC07
SC08	SC09	SC10	SC11
SC12	SC13	SC14	SC15

-> ARK:

SC00	SC01	SC02	SC03
SC04	SC05	SC06	SC07
SC08	SC09	SC10	SC11
SC12	SC13	SC14	SC15

->

Inverse MK:

?	?	?	?
?	?	?	?
?	?	?	?
?	?	?	?

이렇게 출력 차분을 구할 수 있다. 이때 3라운드에서 나온 마지막 SB' 값과 출력 결과물인 비밀키의 차분 값이 같은 경우를 찾아주면 해당 비밀키가 PT01으로부터 나온 암호문임을 확인할 수 있다.
이 방식으로 전체 데이터를 비교한 결과 높은 확률로 PT01으로부터 나온 암호문은 CT04임을 확인할 수 있었다.

문제 1-PT02:
PT02 같은 경우는 PT01과 같이 접근을 하려고 했으나 PT02는 PT01처럼 일관성 있는 차분 특성을 가진 평문들의 집합이 아니었다. 다른 특징을 찾아보니 아래와 같은 특징을 발견할 수 있었다.

A9	AA	??	95
F3	8F	98	E9
80	88	C8	9C
1A	41	44	A4

위 표를 이용하여 차분 분석을 시작해보겠다.

00	00	X	00
00	00	00	00
00	00	00	00
00	00	00	00

-> ARK:

00	00	X	00
00	00	00	00
00	00	00	00
00	00	00	00

-> SR:

00	00	X	00
00	00	00	00
00	00	00	00
00	00	00	00

-> SB':

00	00	Y	00
00	00	00	00
00	00	00	00
00	00	00	00

-> MC:

00	00	Y	00
00	00	3Y	00
00	00	2Y	00
00	00	Y	00

->

ARK:

00	00	2Y	00
00	00	Y	00
00	00	Y	00
00	00	3Y	00

-> SR:

00	00	2Y	00
00	Y	00	00
Y	00	00	00
00	00	00	3Y

->

SB': | 00 | 00 | Z | 00 |
|---|---|---|---|
| 00 | Y | 00 | 00 |
| Z | 00 | 00 | 00 |
| 00 | 00 | 00 | 3Y |

-> MC: | Z | 3Y | 2Z | 3Y |
|---|---|---|---|
| 3Z | 2Y | Z | 3Y |
| 2Z | Y | Z | F |
| Z | Y | 3Z | F |

->

ARK: | Z | 3Y | 2Z | 3Y |
|---|---|---|---|
| 3Z | 2Y | Z | 3Y |
| 2Z | Y | Z | F |
| Z | Y | 3Z | F |

-> SR: | Z | 3Y | 2Z | 3Y |
|---|---|---|---|
| 2Y | Z | 3Y | 3Z |
| Z | F | 2Z | Y |
| Y | 3Z | F | Z |

->

SB' : | ? | ? | ? | ? |
|---|---|---|---|
| 2Y | Z | 3Y | 3Z |
| ? | ? | ? | ? |
| Y | 3Z | F | Z |

차분 분석을 하기 위해서는 입력 단계의 마지막 차분 값과 출력 차분 값을 비교해야 한다. 그렇다면 출력 차분을 구해보자.

출력 차분을 구하기 위해서는 비밀키 쌍을 XOR 해준 뒤, XOR 한 값을 역연산을 해주면 된다.

CT0X의 비밀키 쌍을 XOR한 값을 SC라고 칭할 경우,

SC: | SC00 | SC01 | SC02 | SC03 |
|---|---|---|---|
| SC04 | SC05 | SC06 | SC07 |
| SC08 | SC09 | SC10 | SC11 |
| SC12 | SC13 | SC14 | SC15 |

-> ARK: | SC00 | SC01 | SC02 | SC03 |
|---|---|---|---|
| SC04 | SC05 | SC06 | SC07 |
| SC08 | SC09 | SC10 | SC11 |
| SC12 | SC13 | SC14 | SC15 |

->

Inverse MK: | ? | ? | ? | ? |
|---|---|---|---|
| ? | ? | ? | ? |
| ? | ? | ? | ? |
| ? | ? | ? | ? |

이렇게 출력 차분을 구할 수 있다. 이때 3라운드에서 나온 마지막 SB' 값과 출력 결과물인 비밀키의 차분 값이 같은 경우를 찾아주면 해당 비밀키가 PT02으로부터 나온 암호문임을 확인할 수 있다.

이 방식으로 전체 데이터를 비교한 결과 높은 확률로 PT02으로부터 나온 암호문은 CT01임을 확인할 수 있었다.

문제 2: 다음 평문-암호문을 만족시키는 키의 * 부분을 복구 하고, 풀이를 위한 구현코드를 제출하시오.

키 : b2 5b 75 67 f4 4f 64 d6 07 f0 ef de b1 db 6d 26

위 문제는 5군대의 키 값을 복구하는 문제로 전수조사를 하면 되겠다고 생각하여 그렇게 접근하였다.

마지막 '2*'을 제외한 부분을 00으로 채우고 5중 for 문을 돌려 1씩 증가하는 형태로 키 값을 복구 하였으며 마지막 '2*'은 앞자리가 2임을 밝혔으므로 20~30까지의 값들로만 조사하였다. 뒤에서부터 '++' 하는 방식으로 다소 시간이 오래 걸렸지만 앞에서부터 '++'했을 경우에는 전자보다 시간이 감소되었음을 확인할 수 있었다.