1번 문제 답안

정답)

1. 평문

cryptanalysisisthestudyofanalyxinginformationsystemsinthestudyofanalyzinginformationsystemsinorder tostudythehiddenaspectsofthesystemscryptanalysisisusedtobreachcryptographicsecuritysystemsandgain accesstothecontentsofencryptedmessageseveniftheryptographickeyisunknowninadditiontomathematica lanalysisofcryptographicalgorithmscryptanalysisincludesthestudyofsidechannelattacksthatdonottargetw eaknessesinthecryptographicalgorithmsthemselvesbutinsteadexploitweaknessesintheirweakimplementati oneventhoughthegoalhasbeenthesamethemethodsandtechniquesofcryptanalysishavechangeddrasticallyt hroughthehistoryofcryptographyadaptingtoincreasingcryptographiccomplexityrangingfromthepenandpa permethodsofthepastthroughmachineslikethebritishbombesandbolossuscomputersatbletchleyparkinworl dwartwotothemathematicallyadvancedcomputerizedschemesofthepresentmethodsforbreakingmoderncry ptosystemsoftenineinvolvesolvingcarefullyconstructedproblemsinpurematheticsthebestknownbeinginteg erfactorizationgivensomeencrypteddatathegoalofthecryptanalystistogainasmuchinformationaspossiblea bouttheoriginalunencrypteddatatisusefultoconsidertwoaspectsofachievingthisthefirstisbreakingthesyste mthatisdiscoveringhowtheenciphermentprocessworksthesecondissolvingthekeythatisuniqueforaparticul arencryptedmessageorgroupofmessage

2. 복호화 키 행렬

$$\begin{bmatrix} 3 & 17 & 12 & 9 & 18 \\ 19 & 24 & 18 & 7 & 12 \\ 11 & 13 & 4 & 12 & 6 \\ 2 & 11 & 9 & 20 & 16 \\ 3 & 21 & 0 & 13 & 23 \end{bmatrix}$$

풀이)

1. 개요 및 세팅

문제에서 주어진 암호문은 힐 암호의 암호문이다. 암호문의 길이는 1285 = 5*257이므로 d와 블록의 개수는 각각 5, 257일 것이다.

암호문 C를 257블록으로 나눈 것을 $C_1, \cdots, C_{257}$라 하자. 그리고 $C_i = [c_{i1} c_{i2} \cdots c_{i5}]$ $(1 \le i \le 257)$이다.
평문 P를 257블록으로 나눈 것을 $P_1, \cdots, P_{257}$라 하자. 그리고 $P_i = [p_{i1} p_{i2} \cdots p_{i5}]$ $(1 \le i \le 257)$이다.

복호화 키 행렬을 $K^{-1} = \begin{bmatrix} t_{11} t_{12} \cdots t_{15} \\ t_{21} t_{22} \cdots t_{25} \\ \vdots \ \vdots \ \ddots \ \vdots \\ t_{51} t_{52} \cdots t_{55} \end{bmatrix}$라 하자. 그러면 $p_{ij} = c_{i1}t_{1j} + c_{i2}t_{2j} + \cdots + p_{i5}t_{5j} \pmod{26}$이다.

1번 문제 답안

2. 방법

힐 암호는 단순 치환 암호와는 달리 둘 이상의 알파벳을 함께 다른 문자로 바꾸기 때문에 일반적인 빈도 분석에 쉽게 깨지지 않는다. $p_{ij} = c_{i1}t_{1j} + c_{i2}t_{2j} + \cdots + p_{i5}t_{5j} \pmod{26}$ $(1 \le i \le 257, 1 \le j \le 5)$이므로 각 평문 블록들의 j번째 자리는 복호화 키 행렬에서 j번째 행만의 영향만 받는다. 따라서 1×5 행렬을 전수조사하여 빈도 분석을 진행하였다.

$IC(P) = \sum_i \hat{f}_i f_i$을 이용하여 빈도 분석을 진행하였다. 이때, P는 문자열, $\hat{f}_i$는 관측된 빈도 확률 (즉, $\sum_{i=0}^{26} \hat{f}_i = 1$), f_i는 일반 영어 문장에서의 빈도 확률이다. 만약 문장이 의미 있을수록 IC의 값은 커질 것이다. 그리고 역행렬이 존재해야 하므로 $\mod 2$ 또는 $\mod 13$에서 모두 0인 행은 제외한다. 이를 통해 IC가 큰 행들을 조합하여 평문을 알아낼 수 있다.

3. 복호화

계산한 IC의 값이 큰 순서대로 5개를 뽑아 조합한 결과 의미 있는 평문을 구할 수 있었다.

따라서 복호화 키 행렬은 $\begin{bmatrix} 3 & 17 & 12 & 9 & 18 \\ 19 & 24 & 18 & 7 & 12 \\ 11 & 13 & 4 & 12 & 6 \\ 2 & 11 & 9 & 20 & 16 \\ 3 & 21 & 0 & 13 & 23 \end{bmatrix}$ 이고,

평문은

cryptanalysisisthestudyofanalyxinginformationsystemsinthestudyofanalyzinginformationsystemsinordertostudythehiddenaspectsofthesystemscryptanalysisisusedtobreachcryptographicsecuritysystemsandgainaccesstothecontentsofencryptedmessageseveniftheCryptographickeyisunknowninadditiontomathematicalanalysisofcryptographicalgorithmscryptanalysisincludesthestudyofsidechannelattacksthatdonottargetweaknessesinthecryptographicalgorithmsthemselvesbutinsteadexploitweaknessesintheirweakimplementationeventhoughthegoalhasbeenthesamethemethodsandtechniquesofcryptanalysishavechangeddrasticallythroughthehistoryofcryptographyadaptingtoincreasingcryptographiccomplexityrangingfromthepenandpapermethodsofthepastthroughmachineslikethebritishbombesandbolossuscomputersatbletchleyparkinworldwartwotothemathematicallyadvancedcomputerizedschemesofthepresentmethodsforbreakingmoderncryptosystemsoftenInvolvesolvingcarefullyconstructedproblemsinpuremathematicsthebestknownbeingintegerfactorizationgivensomeencrypteddatathegoalofthecryptanalystistogainasmuchinformationaspossibleabouttheoriginalunencrypteddatatisusefultoconsidertwoaspectsofachievingthisthefirstisbreakingthesystemthatisdiscoveringhowtheenciphermentprocessworksthesecondissolvingthekeythatisuniqueforaparticularencryptedmessageorgroupofmessage 이다.