2023-1학기 암호분석(Cryptanalysis) 과제 1

과제 부여	2022년 3월 30일
제출 마감	2022년 4월 8일 자정까지

1. 파일 "TEXT-1.txt"에 대하여 다음을 수행하고 결과를 정리하라.
   (a) 8자 이하의 패스워드(암호키)를 설정하여 파일을 Vigenere 암호로 암호화하고 "CIPHER-1.txt"에 저정한다.
   (b) "CIPHER-1.txt"에 대한 암호문 단독공격을 수행하여 암호키를 찾고, 과정을 설명하라.

2. 영문자를 다른 영문자로 변환하는 단순치환 암호(substitution cipher)를 다음과 같이 구현하라.
   (a) 암호화 복호화를 위한 라이브러리 SubstLib.py를 작성하라.
   (b) 임호키를 랜덤하게 생성하는 함수와 암호키가 유효한지 확인하는 함수를 작성하라. (암호키에는 대문자 'A'부터 'Z'가 중복되지 않게 나온다)
   (c) 이를 이용하여 랜덤하게 생성한 암호키로 파일 "TEXT-1.txt"를 암호화하라.
   (d) 평문과 암호문 각각에 대하여 영문자의 빈도를 조사하고 가장 많이 나오는 문자부터 순서대로 출력하라.

3. 단순치환 암호로 암호화된 파일 "CIHPER-2.txt"에 대한 암호문 단독공격을 수행하라.
   (a) 평문을 복구하고, 사용된 암호키를 찾는 과정을 단계별로 제시하라.
   (b) 공격과정에서 독창적인 기법을 사용한 경우 부가점을 부여하며, 공격 사이트를 단순 이용하여 해독한 결과는 인정하지 않는다.

☞ 제출 내용:
- 과제 보고서: 각 문항에 대한 풀이 과정과 실행결과 캡처를 포함해야 함
- Python 소스코드: 문항 2의 SubstLib.py, RunSubstCipher.py,
  문항 3의 공격에서 직접 작성한 소스 코드
- 복호화된 파일: 문항 3의 해독에 성공한 경우 평문 파일