

201603867 조성환

xor 연산

대칭키의 특징은 같은 값을 가지는 대신, 알고리즘을 통해 암호문 비교하는 형식.

이 때 xor의 특성은 같은 값을 두번 xor 연산을 하면 원래 값이 나오는 형식을 테스트 하기 위해 해당 과제를 수행함.

먼저 ord()연산을 ascii 코드로 바꾼 후 두 값을 xor 연산을 통해 암호화 시켰다. 나머지 한 값은 key로 사용자가 key라는 값을 입력하면 평문의 각 자리수에 key가 순서대로 반복하며 들어간다. 각 자리에서 평문과 key 문을 xor 연산을 통해 나온 값을 저장함.

복호화는 마찬가지로 xor 연산의 특징상 같은 값을 그대로 연산하면 되기 때문에 별도의 key 값 조작을 하지 않았다.

예외처리 부분을 추가했다. xor 연산에서 결과가 13 이나오면 ascii 13 에서 cr 문자로 연산이 된다. txt 파일에서 개행을 하기 위해서는 cr 후 lf 를 하는데, cr 은 행의 첫번째로 커서를 옮긴 후 lf 는 줄바꿈을 하는 문자이다. 그런데 텍스트 파일에서는 cr 과 lf 가 같은 ascii code 10 으로 처리돼서 만약 108 ^ 97 연산시 13 이 나오는데, 파일에는 10(개행)이 저장돼 다시 연산을 하면 107 이 나오는 문제가 발생했다. 이를 해결하기 위해 rb, wb 옵션을 이용해 파일을 binary 모드로 읽고 쓰는데, 그 이유는 단순히 텍스트로 저장시 13 과 10 이 같은 문자로 처리가 되는데, binary 로 작성시 같은 문자로 처리되지 않기 때문에 binary 모드로 처리했다.