**1. 출품자 수강 과정명 :**

(디지털컨버전스) 통합 응용 SW 개발자 (C#, JAVA)

**2. 출품자 성명 :**

지상준

**3. 작품명 :**

사각행렬을 이용한 전치기법을 개선한 새로운 암호체계

**4. 지도교수 성명 :**

이동준 선생님

**5. 작품 제작의도 :**

전치기법에서 더 개선하여, 좀 더 복잡하고, 평문 사이사이에 랜덤한 문자를 더 많이 넣을 수 있게 하였다.

새로운 아이디어를 추가해서 사각행렬(2차원 배열)의 크기가 증가하고, 그 사이에 끼인 랜덤한 문자로 인해 암호문이 더 난해해진다. (기존 전치기법에서는 랜덤한 문자가 사이에 끼는게 아닌 단순히 뒤쪽 남는 공간에 채워넣는다)

**6. 작품 상세설명 :**

아이디어의 핵심은 기존의 전치기법에서 사각행렬을 단순히 만드는 것이 아니라, 사이즈가 더 크고 평문 사이사이에 더 많은 랜덤한 문자를 끼어 넣을 수 있는 행렬을 만드는 것이다. 사각행렬은 프로그래밍언어에서 2차원 배열로 생각할 수 있다. 또한 1차원 배열이라도 배열 포인터를 이용하여 포인터계산을 통해 2차원 배열처럼 쓸 수 있다. 하지만 고급언어 C#이나 Java에서는 포인터계산이 안되지만, 배열의 인덱스 값을 계산해서 2차원 배열처럼 이용할 수 있다.

키길이와 키깊이의 개념을 도입했다. 키길이가 만약에 3이라 설정하면 2차원 배열의 열이 3개라는 뜻이다. 키깊이는 각각의 열의 유의미한 행의 계수다. 예시로 “ABCDEF”를 암호화해보자. 키깊이를 {3, 1, 2}로 설정했다고 가정하자. 그리고 랜덤한 문자는 ‘X’로 표현하겠다. 그렇다면 행렬은 {{A, B C}, {D, X, E}, {F, X, X}} 다음과 같다. 또한 여기서 키깊이 각각의 크기를 비교해 오름차순으로 정렬한다. 1 < 2 < 3으로 정렬된다. 2차원 배열에서 1차원 암호문으로 뽑아낼 때는 같은 열끼리 뽑아낸다. 키깊이가 1인 2열의 {B, X, X}가 먼저 뽑히고, 키깊이가 2인 3열의 {C, E, X} 그 다음으로 키깊이가 3인 1열의 {A, D, F}가 뽑힌다. 따라서 B, X, X, C, E, X, A, D, F가 된다. 이를 순차적으로 읽으면 암호문이 된다. “BXXCEXADF”

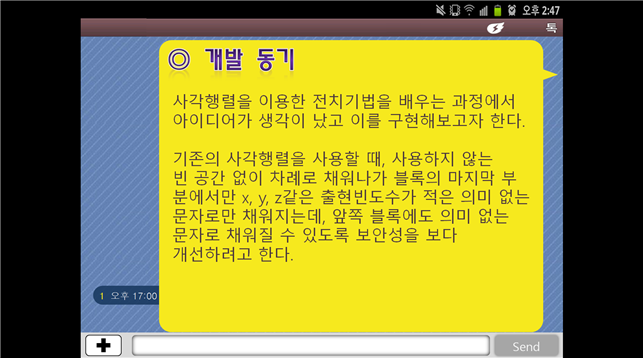
사각행렬의 모든 값을 채우기 위해 부족한 부분은 padding 된다.

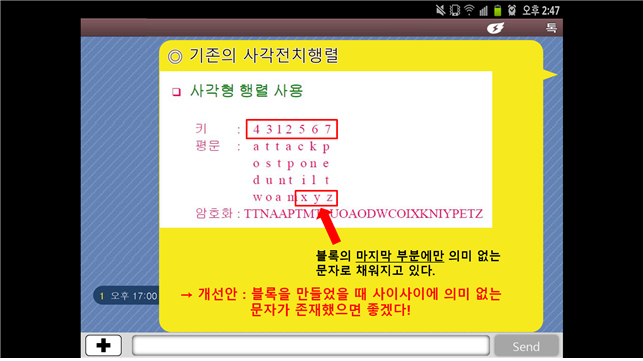
복호화는 역순으로한다. padding 값이 없어도 평문이 노출된다. 하지만 노출된 평문 뒷부분에 의미없는 랜덤한 문자가 지저분하게 붙게된다.

중요!) 키깊이는 오름차순으로 정리하므로 중복된 깊이를 가질 수 없다.

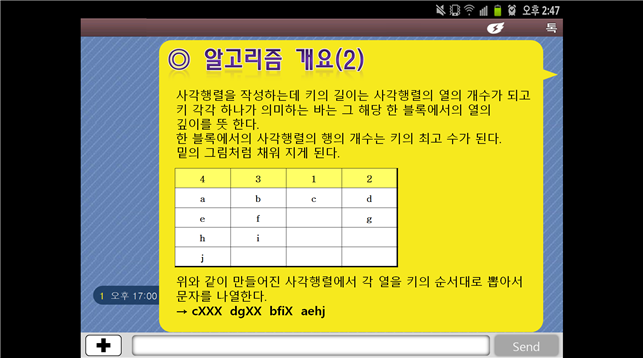
얻는 이점!) 키길이가 길어지고 키깊이가 어느정도 차이나면 사각행렬 사이사이에 랜던한 문자가 많이 들어가 암호문이 난해해진다. 새로운 나만의 암호를 만들어 보았다.

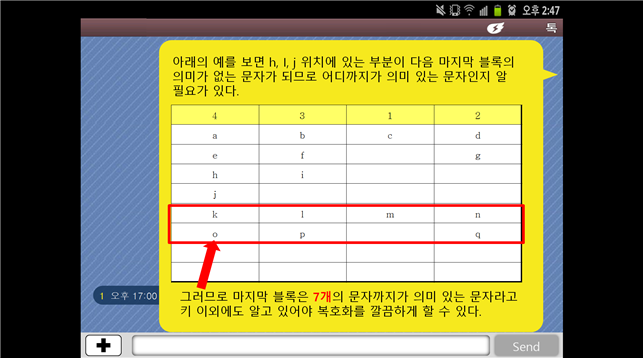
**(PPT 자료)**

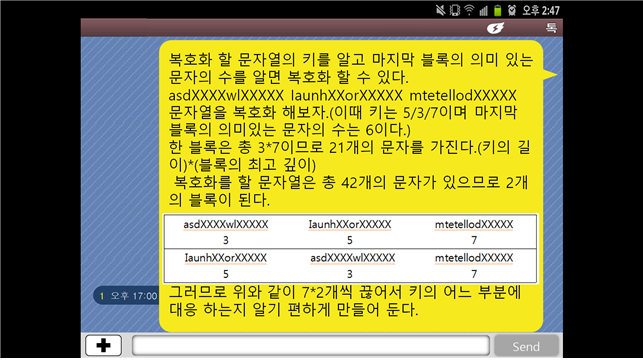


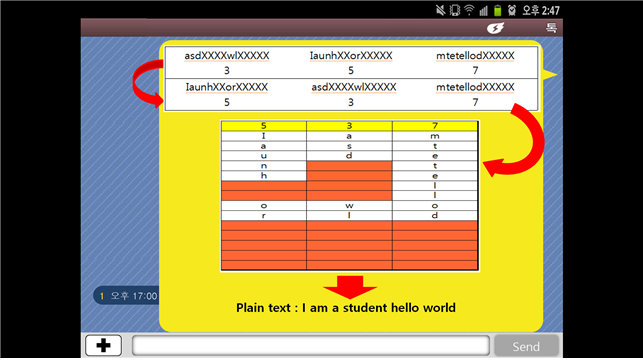


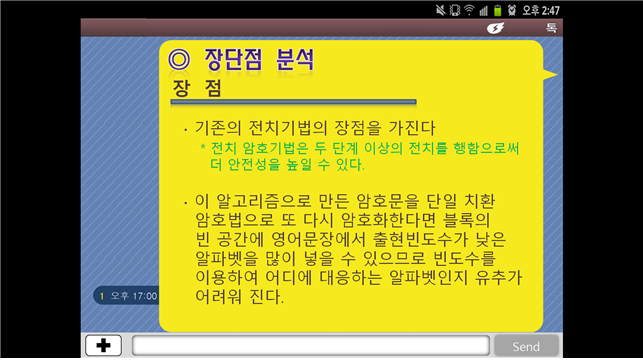












**(실행 예시)**



=> 초기화면 안내글



=> 암호화, 복호화 기능을 사용하기 위해선 키설정을 해주셔야 합니다. (설정된 키가 없다면 강제로 키설정으로 넘어갑니다.)



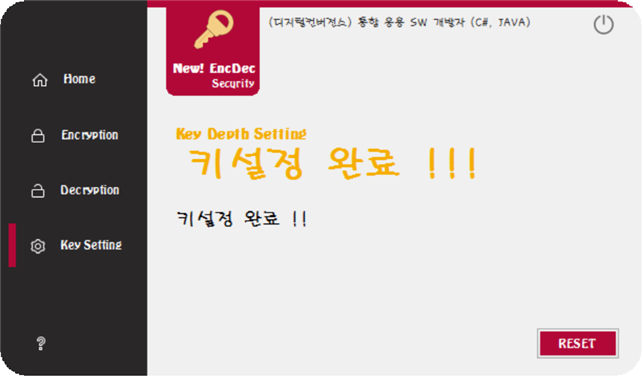
=> 위에서 키길이를 3으로 설정했으므로 총 3개의 키깊이를 입력해주셔야 합니다. 그 중에 첫번째



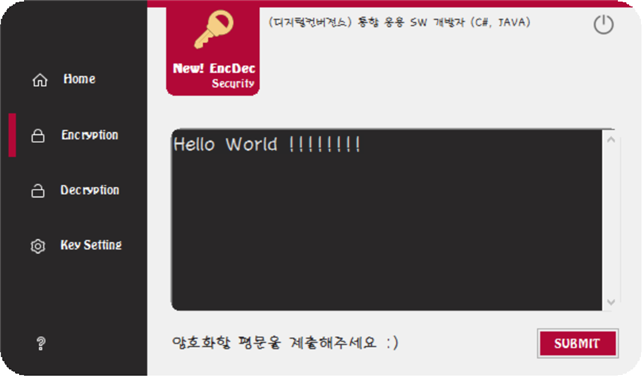
=> 두번째 키깊이 설정



=> 세번째 키깊이 설정



=> 키설정 완료. 이제 암호화, 복호화 기능을 사용할 수 있습니다.



=> 바로 테스트 할 수 있도록, 초기값으로 기본 "Hello World !!!!!!!!"가 주워집니다. 해당 평문 말고도 암호화 하고 싶은 문장이 있다면 텍스트박스에 해당 문장을 지우고 써넣으시면 됩니다. 텍스트박스 안에서 Enter키 나 우측 하단 붉은색 SUBMIT 버튼을 누르시면 입력하신 문장이 암호화 됩니다.



=> 암호화 완료. Padding 된 문자수도 알려줍니다.



=> 바로 테스트 할 수 있도록, 초기값으로 암호화한 문장과 Padding 된 문자수가 주워집니다. 다른 암호문을 복호화 하고 싶다면 텍스트 박스에 해당 내용을 지우고 입력 후 Entery키 또는 우측 하단 붉은버튼 SUBMIT을 누릅니다.



=> 암호문을 복호화한 후 평문이 노출됩니다. (키길이와 키깊이가 맞다면 !!!, Padding은 틀리더라도 앞부분에 평문이 노출됩니다.)