

2019.12.15

반유진

201811853

IT융합응용공학과

신상욱 교수님

정보보호공학

제출일

이름

학번

학 과

교수님

과목명

REPORT

**<대칭키 암호를 이용한 데이터 암/복호화>**

**□ 구현 환경 :** Java eclipse

**□ 특징**

- Padding 방식 : PKCS5Padding

- AES는 16byte, DES 8byte, DESede는 24byte이다.

- CBC, CFB, OFB, CTR는 초기화벡터 값이 필요하다.

- 아래의 실행 화면은

평문 : jinjinzara

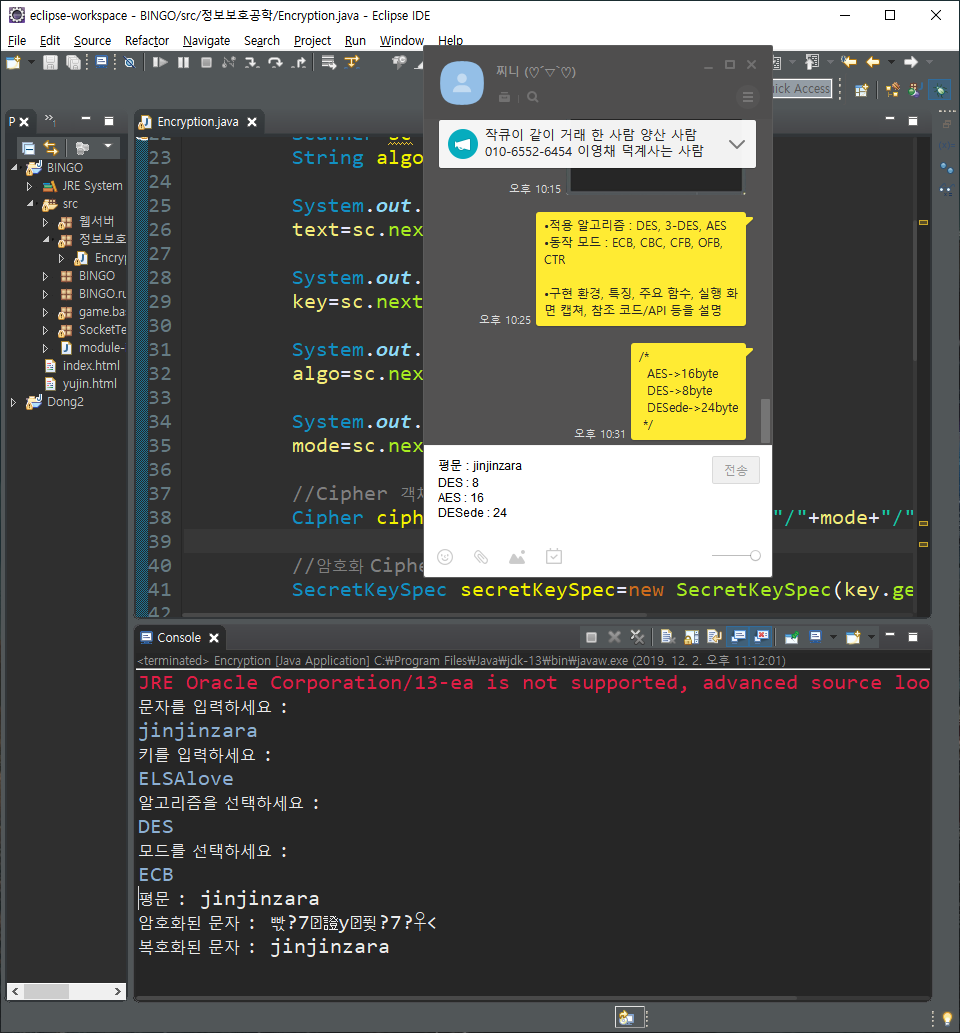
DES 키 : ELSAlove

3-DES 키 : FrozenElsaAnnaOlafLuvLuv

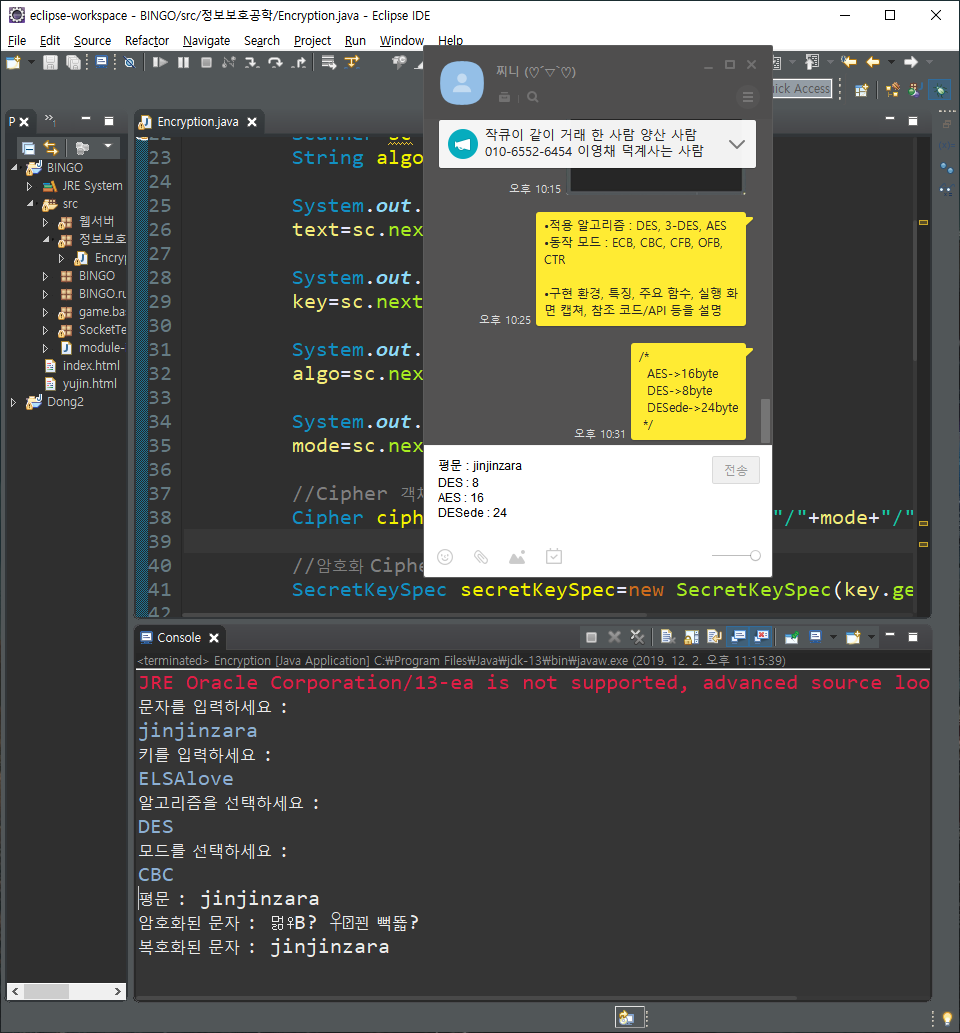
AES 키 : ElsaAnnaOlafLove 로 입력한 것이다.

**□ 실행 화면 캡쳐**

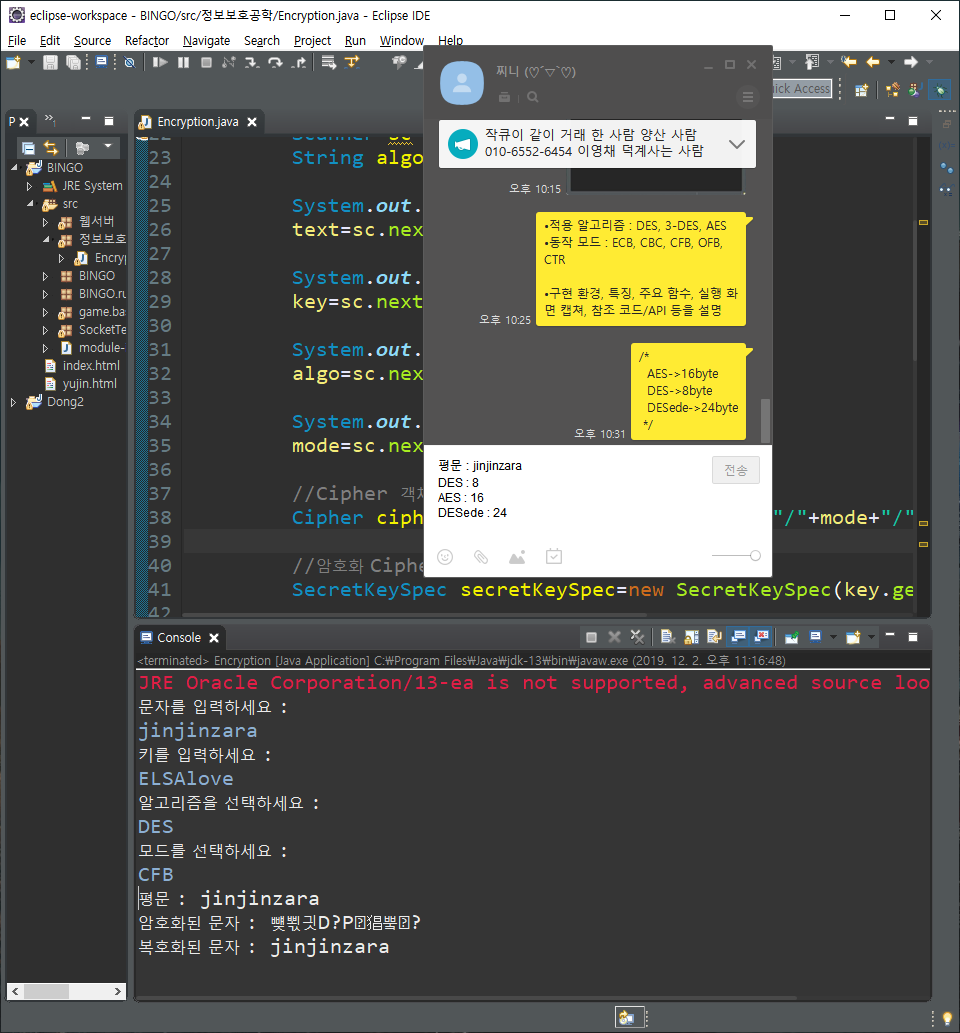
• **DES**



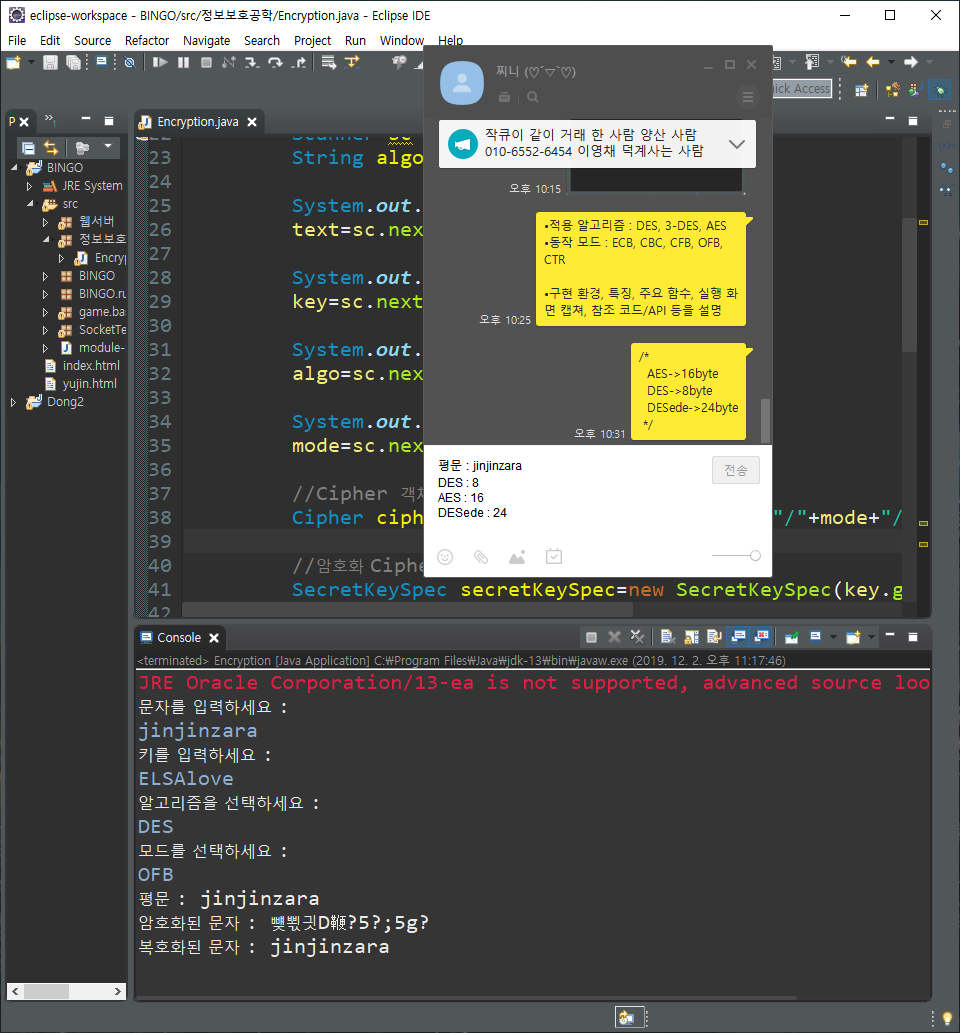
- DES / ECB



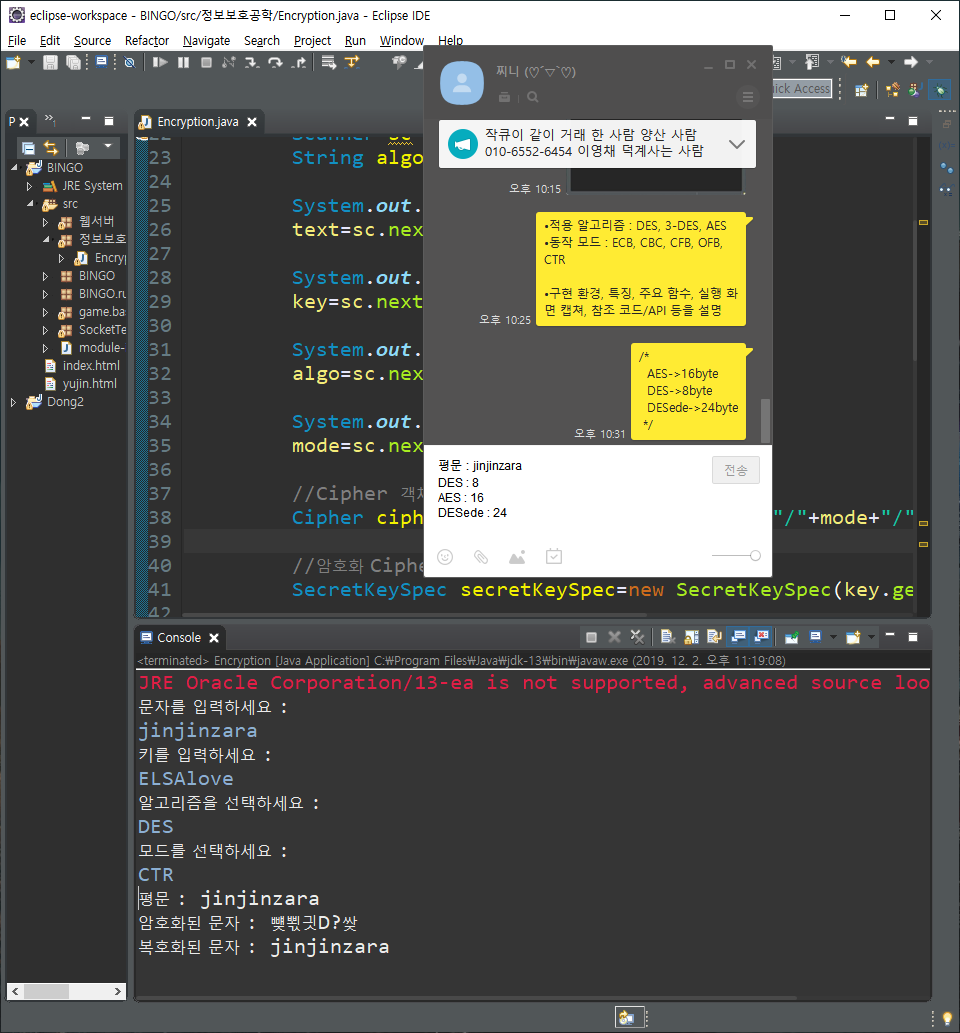
- DES / CBC



- DES / CFB

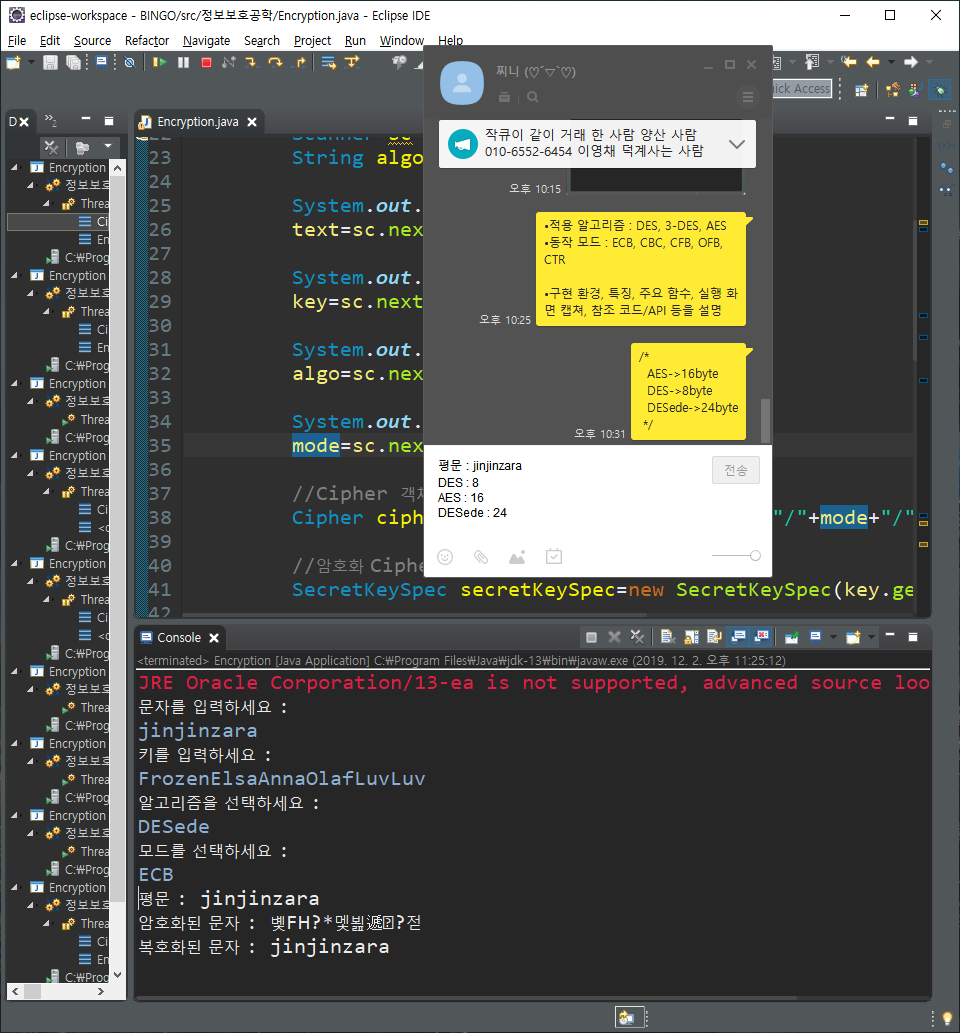


- DES / OFB

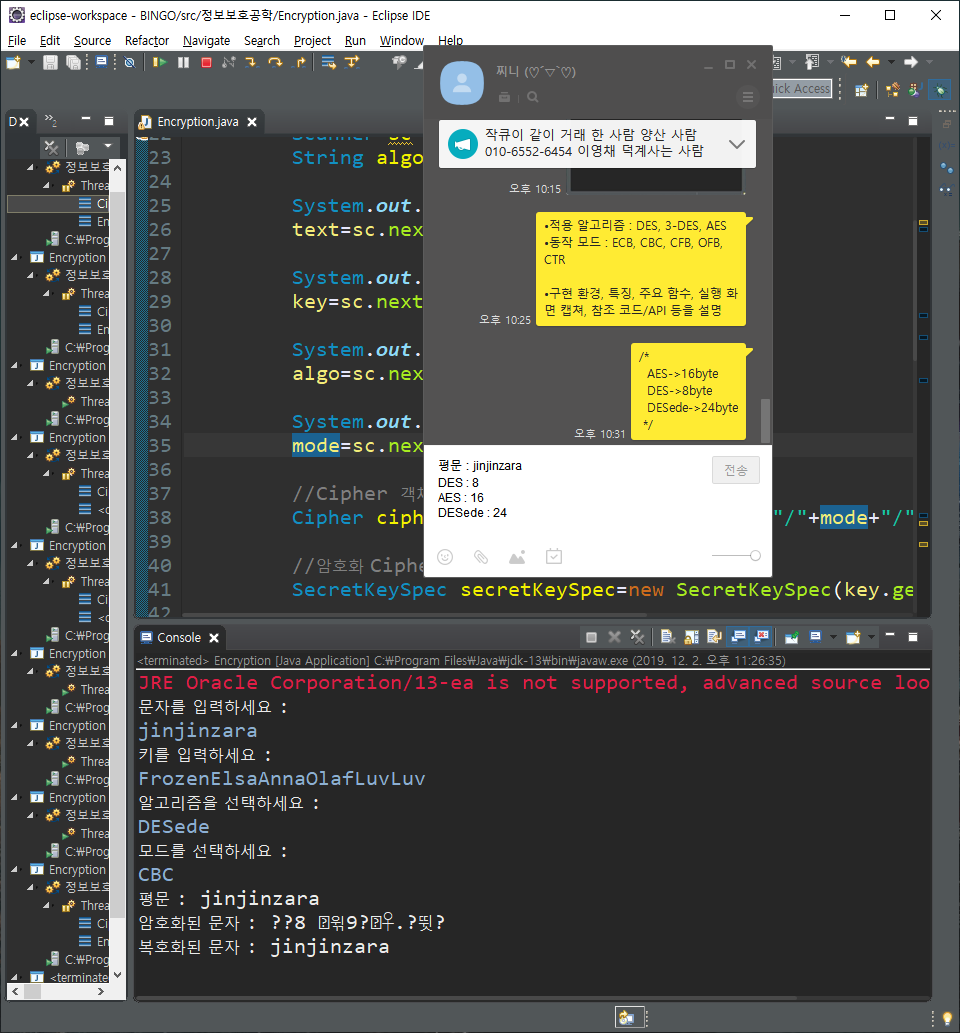


- DES / CTR

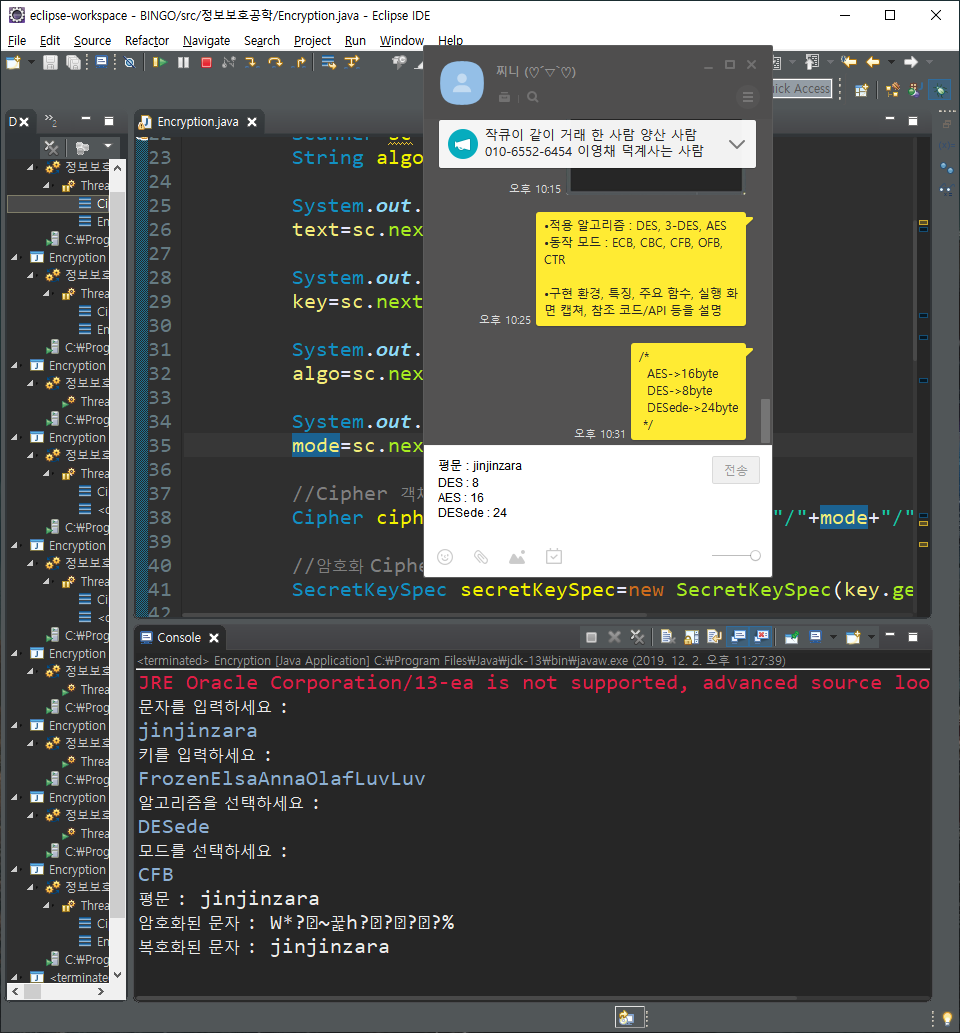
• **3-DES**



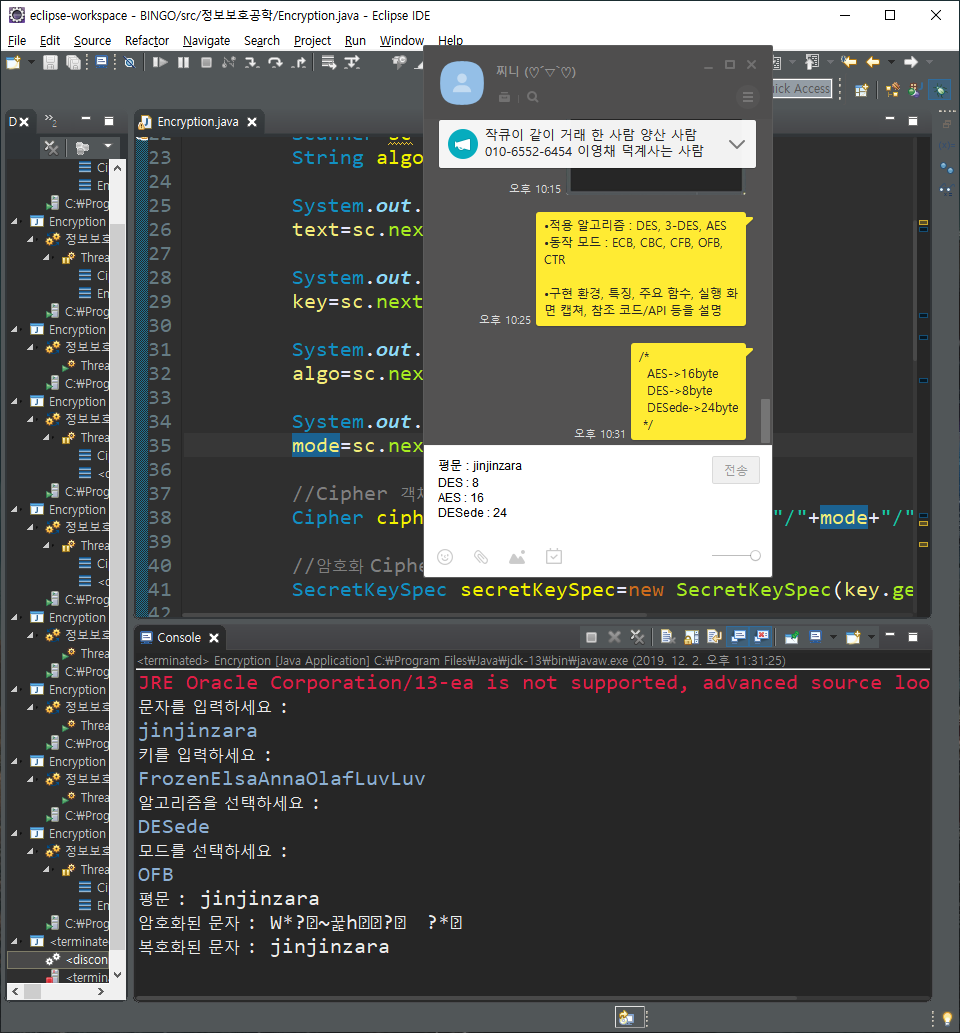
- 3-DES / ECB



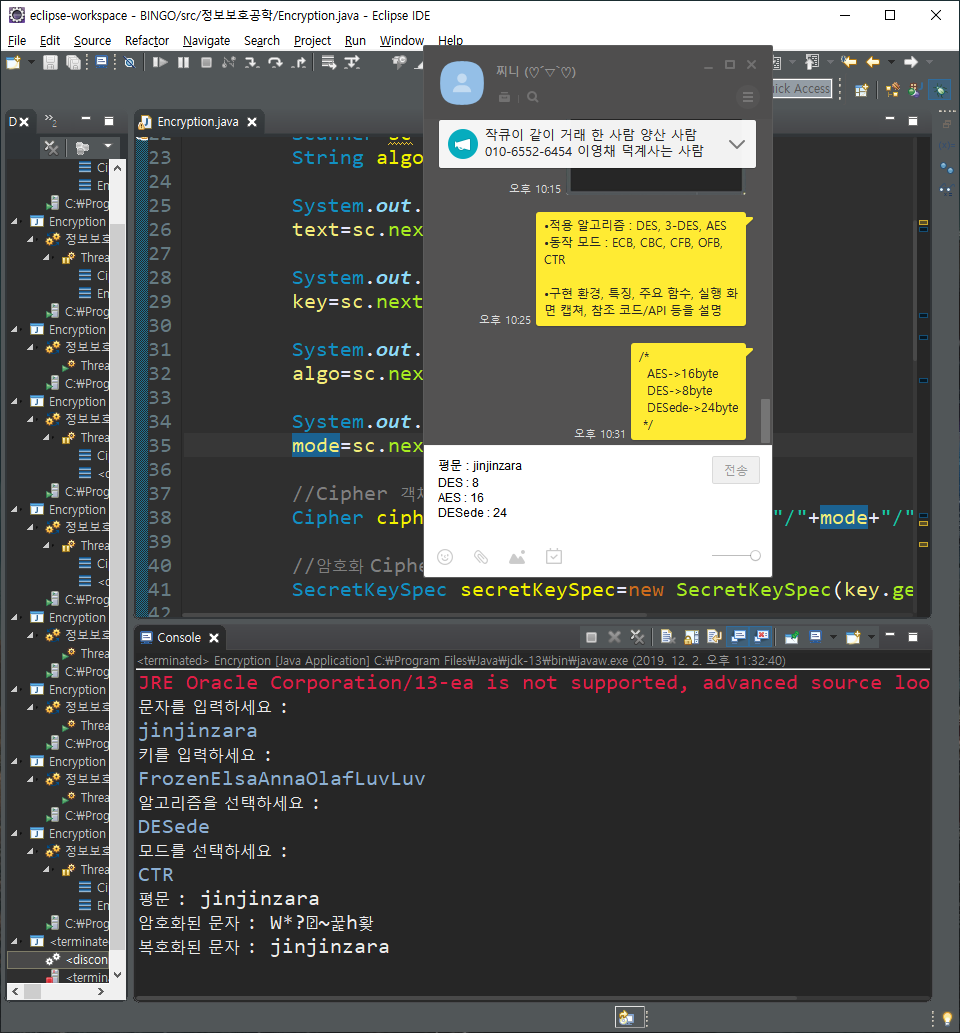
- 3-DES / CBC



- 3-DES / CFB

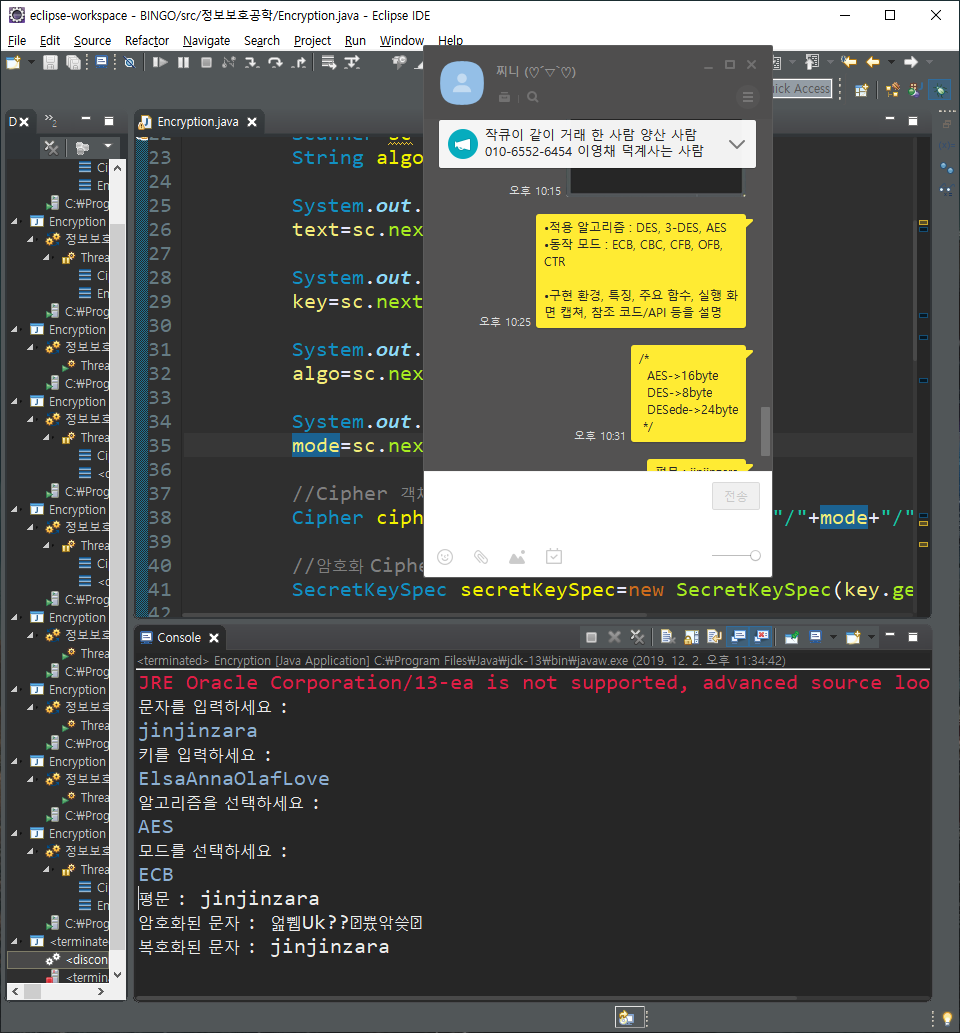


- 3-DES / OFB

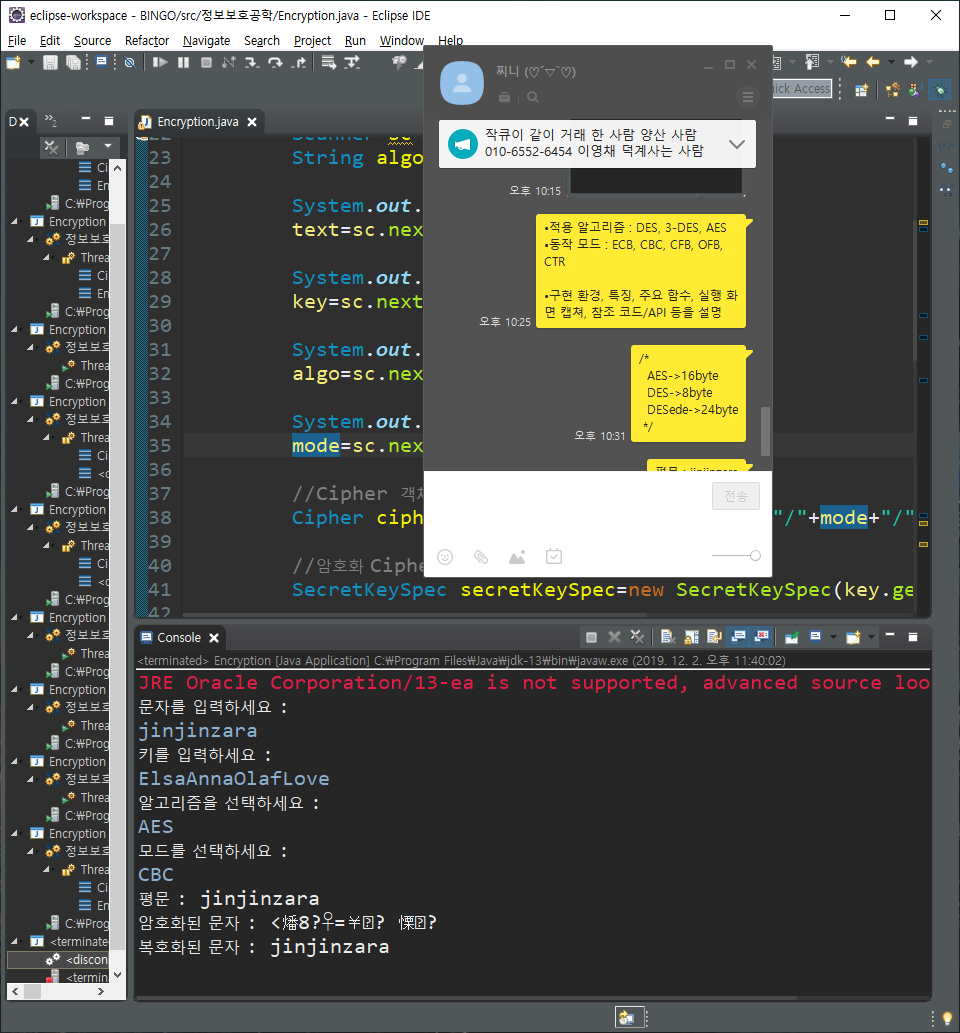


- 3-DES / CTR

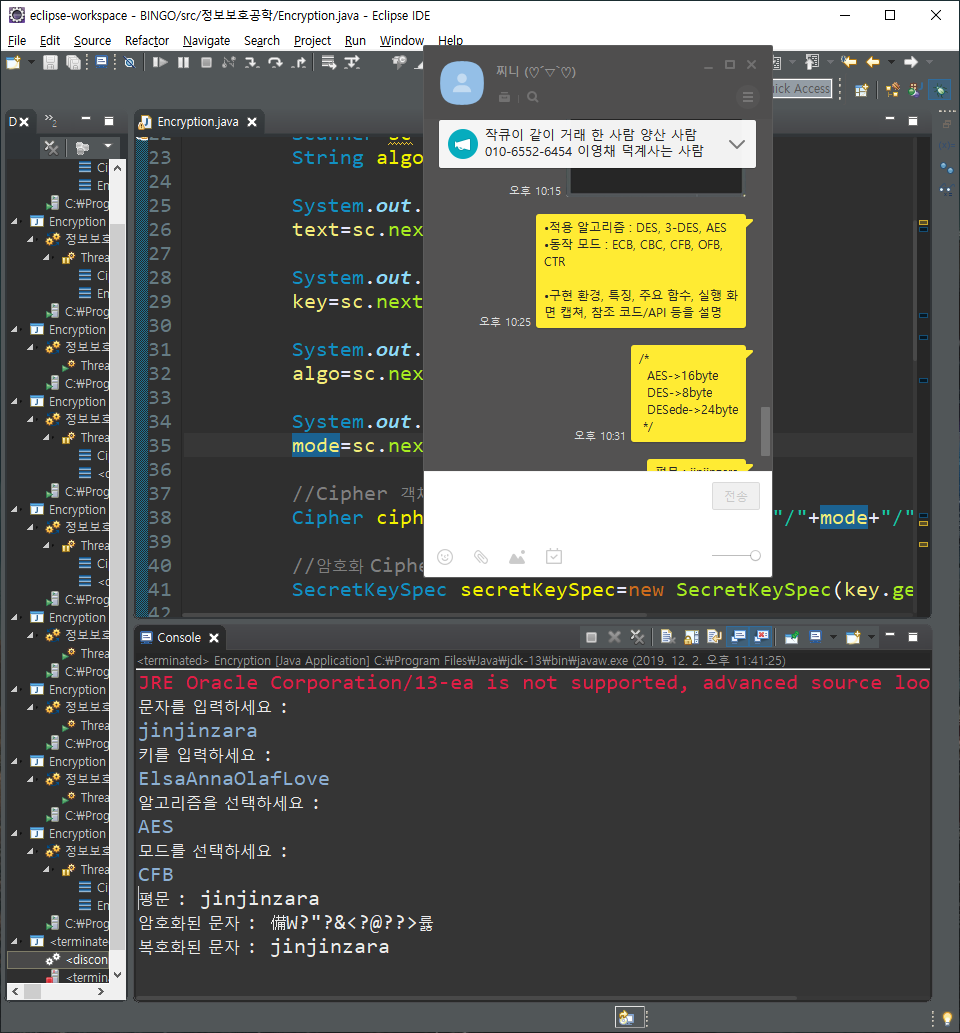
• **AES**



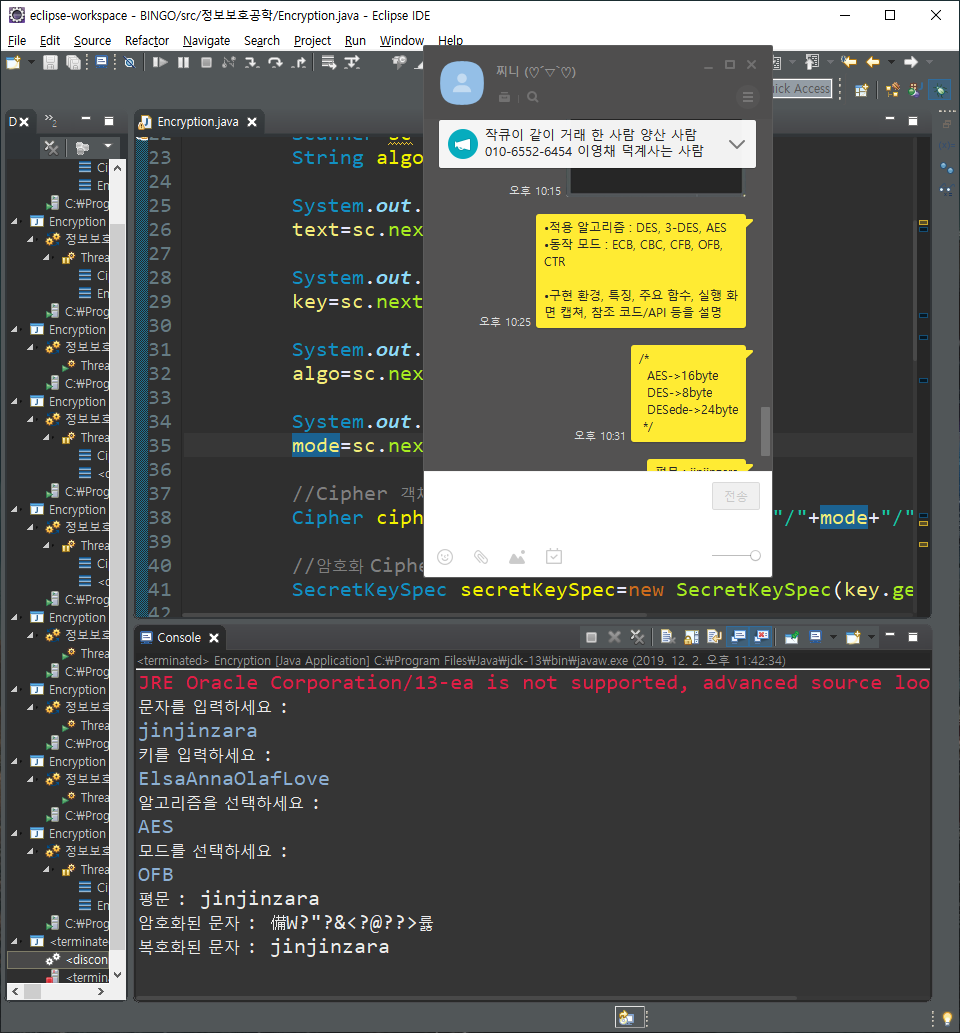
- AES / ECB



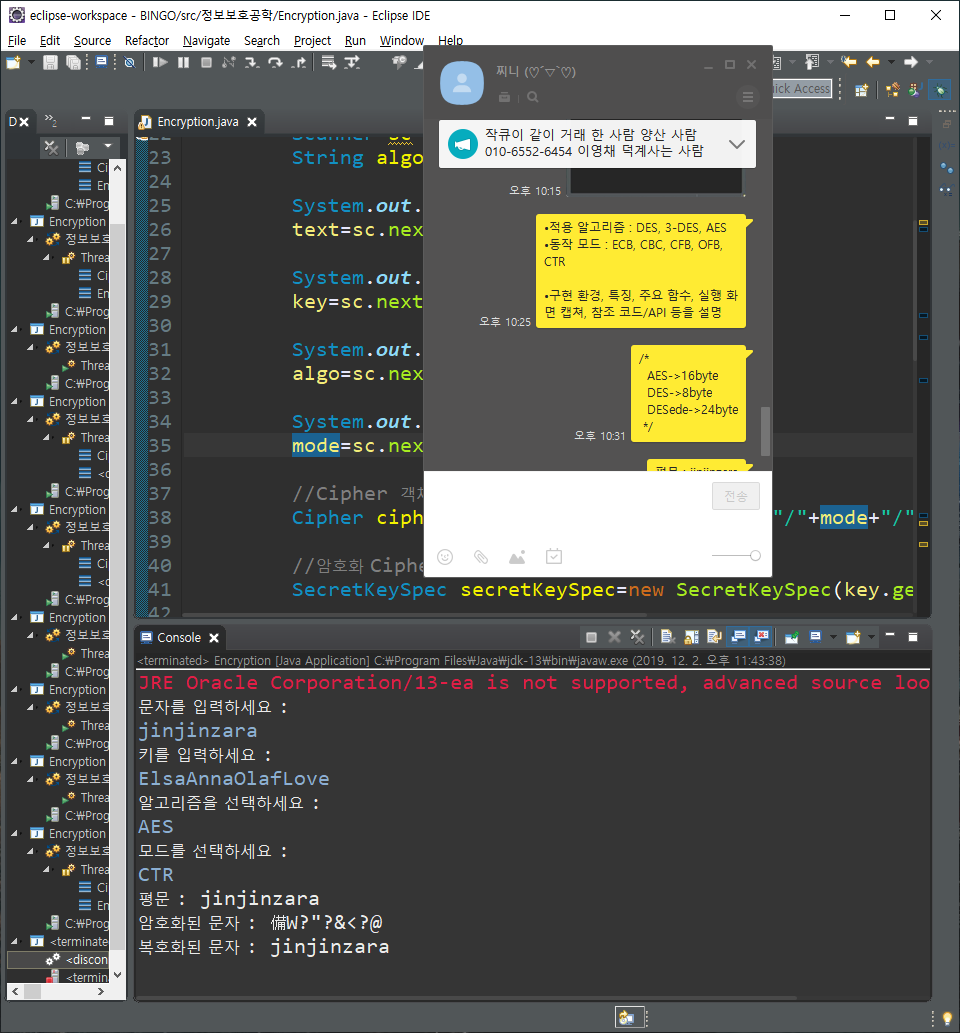
- AES / CBC



- AES / CFB



- AES / OFB



- AES / CTR

**□ 참조 코드**

<http://happinessoncode.com/2019/04/06/java-cipher-algorithm-mode-padding/>를 참고하여 코드를 짰으며, [블로그] Javaking :: 자바킹 - IT 정복의 아래 코드를 참고하였다.   
        Cipher cipher = Cipher.getInstance("AES");

        SecretKeySpec secretKeySpec = new SecretKeySpec(encryptionKey.getBytes(),"AES");  
        cipher.init(Cipher.ENCRYPT\_MODE, secretKeySpec);  
           byte[] encryptBytes = cipher.doFinal(target.getBytes("UTF-8"));  
        System.out.println(new String(encryptBytes));   
        cipher.init(cipher.DECRYPT\_MODE, secretKeySpec);  
        byte[] decryptBytes = cipher.doFinal(encryptBytes);  
        System.out.println(new String(decryptBytes, "UTF-8"));  
    }