코드 리뷰 보고서

<table>
<tr><td>리뷰번호</td><td>001</td><td>작성자</td><td>곽채원</td><td>작성날짜</td><td>2023.05.31</td></tr>
<tr><td>관련규칙</td><td colspan="5">12. Do not use insecure or weak cryptographic algorithms</td></tr>
<tr><td>중요도</td><td colspan="5">상</td></tr>
<tr><td rowspan="3">대상코드</td><td colspan="5">Before</td></tr>
<tr><td colspan="5">

```
private static String signAlgorithm = "SHA256withRSA";
private static String cipherAlgorithm = "DES";
private static String keyAlgorithm = "RSA";
```

</td></tr>
<tr><td colspan="5">After</td></tr>
<tr><td colspan="5">

```
private static String signAlgorithm = "SHA256withRSA";
private static String cipherAlgorithm = "AES";
private static String keyAlgorithm = "RSA";
```

</td></tr>
<tr><td>보안약점/
보안취약점
이유 및
해결법</td><td colspan="5">Before 코드에서 서명과 평문을 암호화하기 위한 대칭 암호로 DES 알고리즘을 활용하였다. 그러나 DES는 암호 강도가 낮다고 밝혀져 사용할 시 보안에 취약할 수 있다.

이를 해결하기 위해 대칭 암호 알고리즘으로 AES를 활용하도록 코드를 수정해주었다.</td></tr>
</table>