The purpose of writing this report is to explain the implementation of Feistel cipher algorithm, which is one of the most well known symmetric cryptography. DES algorithm has been implemented using Java programming language for this project. The project services get some plain text or cipher and a key and outputs cipher or plain text respectively.

For downloading the code you can go to
https://code.google.com/p/uis-security-asignments/
Or checkout the source with subversion using this URL

```
svn checkout http://uis-security-asignments.googlecode.com/svn/trunk/ uis-security-asignments-read-only
```

You need to go to Oracle website to download Java JDK for compiling the source code.
After downloading and installing JDK you may set JAVA_HOME environment variable to the path that JDK has been installed.
Use

```
	java –version
```

To check your Java installed correctly.
For building the project you need to download and install in your hard drive apache Maven project.
Again you can use

```
	mvn  -version .
```

To install the project you just need to go to the root of source code which pom.xml located and type

```
	mvn install
```

Whole source codes will be compiled and 28 unit tests will run after compiling the jar files will be copied into target folder.
By running run.sh in UNIX environment or run.bat in windows the command user interface will come and you can input your data.
In this project tried to used Object Oriented concepts, Dependency injection using Spring framework, JUnit and Spring test framework were used for unit and integration testing of the project which was tried to developed base on TDD, Finally SLF4J over LOG4j was used for logging.
All dependency libraries were added using maven to the project.
The objection of the project is to use DES algorithm to encrypt and decrypt data by given key.

As Martin Fowler says the code should be itself it`s document, it was tried to using clean code and refactoring in this project.

Three service interfaces named EncryptionService, RoundFunction and SubKeyGeneratorare main services and FeistelCipher, DESRoundFunction and DesSubKeyGenerator classes are implementations respectively.

DesSubKeyGenerator

Init()

It gets array of byte in order to convert it to array of bits , permute bits and returns Block object which holds half left and right bits.

generateNextKey()

In each level of encryption it is needed to shift some bits to left, that what this function does.

DESRoundFunction

Init()

Gets text message permute bits using IP table.

inverseInit()

At the last level this method permutes bits again with revere table of IP using FP table.

generateNextLevel()

For each level of operation this method permutes and substitutes bits regarding to DES structure.

FeistelCipher

encrypt()

This is what a client wants to work with just getting text and key as inputs and uses other previous services to generate 16 level of sub key generator and DES function

decrypt()

Does same operation like encrypt() in revers order sub key generator.

For each service class there is a test class which tests unit and integration of frame work DESRoundFunctionTest, DesSubKeyGeneratorTest, FeistelCipherTest are test classes.

As mentioned earlier this is an encryption and decryption service which can be used as a service like web services, web or SOA clients to encrypt data using a key and decrypt it just with the same key.
Obviously the all security issues relating to Data Encryption Standard (DES) does include this implementation also.