INSTITUT TEKNOLOGI DEL

MATERI PRAKTIKUM

Keamanan Perangkat Lunak
SEMESTER GASAL TAHUN AJAR 2024/2025

Session Date	**:**	23 Oktober 2024
Semester	**:**	V
Courses	**:**	Keamanan Perangkat Lunak
Week/Session	**:**	03/03
Key Topics	**:**	**Data Encryption Standard (DES)**
Activity	**:**	Mahasiswa mengerjakan review question, problem dan computer programming.
Duration	**:**	170 menit
Delivery	**:**	Laporan Tugas *Softcopy*
Deadline of delivery	**:**	-
Place of delivery	**:**	e-Course
Goal	**:**	Mahasiswa mampu memahami konsep Simple Data Encryption Standard dan Data Encryption Standard

PENUGASAN:

Sebelum bekerja, setiap mahasiswa harus membaca instruksi di bawah ini.

Sangat disarankan bagi anda untuk:

1. ***Membaca soal-soal yang diberikan secara.***
2. ***Mencari sumber-sumber lain seperti buku, artikel, bahkan video untuk memperkaya wawasan dan meningkatkan pemahaman anda.***
3. ***Jika anda merasa ada hal yang belum dipahami, silakan untuk berkonsultasi pada TA.***
4. ***Dengan demikian diharapkan anda mampu mengikuti materi kuliah dan praktikum sebaik mungkin.***

Selamat Belajar & Good Luck!

Review questions

1. Briefly define stream cipher and block cipher and explain the differences.
2. Briefly explain reversible and irreversible cryptographic mapping.
3. What is the difference between diffusion and confusion?

Problems

S-DES

1. Using S-DES, encrypt and decrypt the string (1011 0110) using key (01110 11010).

DES

2. Key: 3 4 1 A 3 9 B F 0 5 7 E 6 2 0 D (**64-bit**)
   Show the output of **PC-1** .
3. In the 5th round, the results of PC-1 are:
   C_5: 1100100 0010110 1001011 1001110
   D_5: 0110111 0110110 1100110 0011001
   Show the results of the **left shift** stage.
4. Given the output from expansion table:
   A1: 101100 001110 110001 101010 101110 111111 100011 101100 (**48-bit**)
   Show the results of the S-BOX stage.

S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Computer programming (Java Language)

Copy the source code below into you IDE (e.g. Netbeans), run the program, and analyze the program

```
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.spec.AlgorithmParameterSpec;

import javax.crypto.Cipher;
import javax.crypto.CipherInputStream;
import javax.crypto.CipherOutputStream;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;
import javax.crypto.spec.IvParameterSpec;

public class DES {
	private static Cipher encryptCipher;
	private static Cipher decryptCipher;
	private static final byte[] iv = { 11, 22, 33, 44, 99, 88, 77, 66 };
//initialization vector

	public static void main(String[] args) {
		String clearTextFile = "source.txt";
		String cipherTextFile = "cipher.txt";
		String clearTextNewFile = "source-new.txt";

		try {
			// create SecretKey using KeyGenerator
			SecretKey key =
KeyGenerator.getInstance("DES").generateKey();
			AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);

			// get Cipher instance and initiate in encrypt mode
			encryptCipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
			encryptCipher.init(Cipher.ENCRYPT_MODE, key, paramSpec);

			// get Cipher instance and initiate in decrypt mode
			decryptCipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
			decryptCipher.init(Cipher.DECRYPT_MODE, key, paramSpec);

			// method to encrypt clear text file to encrypted file
			encrypt(new FileInputStream(clearTextFile), new
FileOutputStream(cipherTextFile));

			// method to decrypt encrypted file to clear text file
			decrypt(new FileInputStream(cipherTextFile), new
FileOutputStream(clearTextNewFile));
			System.out.println("DONE");
		} catch (NoSuchAlgorithmException | NoSuchPaddingException |
InvalidKeyException
				| InvalidAlgorithmParameterException | IOException e)
{
			e.printStackTrace();
		}

	}
```

```
        private static void encrypt(InputStream is, OutputStream os) throws
IOException {

                // create CipherOutputStream to encrypt the data using
encryptCipher
                os = new CipherOutputStream(os, encryptCipher);
                writeData(is, os);
        }

        private static void decrypt(InputStream is, OutputStream os) throws
IOException {

                // create CipherOutputStream to decrypt the data using
decryptCipher
                is = new CipherInputStream(is, decryptCipher);
                writeData(is, os);
        }

        // utility method to read data from input stream and write to output
stream
        private static void writeData(InputStream is, OutputStream os) throws
IOException {
                byte[] buf = new byte[1024];
                int numRead = 0;
                // read and write operation
                while ((numRead = is.read(buf)) >= 0) {
                        os.write(buf, 0, numRead);
                }
                os.close();
                is.close();
        }

}
```

Deliverables

Answer to review question, problems on handwritten paper, scan, and then upload it to e-Course.