
Symmetric Key Encryption and Message Digest

50.005 Computer System Engineering

Due date: 08 Apr 08:30 AM (Week 11)

Overview

[Learning objectives](#)

[Starter Code](#)

[Submission](#)

[Part 1: Symmetric key encryption for a text file](#)

[Generate key for DES](#)

[Create and configure Cipher object](#)

[Perform the cryptographic operation](#)

[Tasks for Part 1](#)

[Part 2: Symmetric key encryption for an image file](#)

[Task for part 2](#)

[Part 3: Signed message digests](#)

[Create a MessageDigest object](#)

[Update MessageDigest object](#)

[Compute digest](#)

[Sign message digest](#)

[Generate RSA key pair](#)

[Configure cipher for use with RSA](#)

[Task for Part 3](#)

Overview

In NS Module 3, we examined how the security properties of confidentiality and data integrity could be protected by using symmetric key cryptography and signed message digests. In this lab exercise, you will learn how to write a program that makes use of DES for data encryption, MD5 for creating message digests and RSA for digital signing.

Learning objectives

At the end of this lab exercise, you should be able to:

- Understand how symmetric key cryptography (e.g., DES or AES encryption algorithms) can be used to encrypt data and protect its confidentiality.
- Understand how multiple blocks of data are handled using different block cipher modes and padding.
- Compare the different block cipher modes in terms of how they operate.
- Understand how hash functions can be used to create fixed-length message digests.
- Understand how public key cryptography (e.g., RSA algorithm) can be used to create digital signatures.
- Understand how to create message digest using hash functions (e.g., MD5, SHA-1, SHA-256, SHA-512, etc) and sign it using RSA to guarantee data integrity.

Starter Code

We will use the Java Cryptography Extension (JCE) to write our program instead of implementing DES, RSA and MD5 directly. The JCE is part of the Java platform and provides an implementation for commonly used encryption algorithms.

Download the starter code:

```
git clone https://github.com/natalieagus/50005Lab5.git
```

There's no makefile for you. By now, you should be able to write your own makefile to make compilation more convenient.

UPDATE 05/04/2020: the file name and the class name have been modified to match.

Submission

The total marks for this Lab is 50 pts.

Make sure your Java code compiles properly for all 3 parts [10pts] and answer the questions in this sheet [40pts].

Zip all the following:

1. Pdf export of this sheet and your answers (as usual, fill in the spaces denoted in blue).
2. Your Java source codes for the three tasks (3 scripts in total). Don't change the script names.
3. The encrypted images (ecb.bmp and cbc.bmp) for the second task, and (triangle_new.bmp) for the third task. Name it properly!

Upload to @cse-submitbot telegram bot using the command /submitlab5

CHECK your submission by using the command /checksubmission

Part 1: Symmetric key encryption for a text file

Data Encryption Standard (DES) is a US encryption standard for encrypting electronic data. It makes use of a 56-bit key to encrypt 64-bit blocks of plaintext input through repeated rounds of processing using a specialized function. DES is an example of symmetric key cryptography, wherein the parties encrypting and decrypting the data both share the same key. This key is then used for both encryption and decryption operations.

In this task, we will make use of the Cipher and KeyGenerator classes from the Java Cryptography Extension (JCE) to encrypt and decrypt data from a text file. The steps involved in encryption and decryption are:

1. **Generate a key for DES** using a KeyGenerator instance
2. Create and configure a **Cipher** object for use with DES
3. **Use the doFinal()** method to perform the actual operation

While the steps for both operations are similar, take note that the working mode of the Cipher object must be configured correctly for encryption or decryption, and the key used for decryption should be the same as that used for encryption.

Generate key for DES

A 56-bit key for DES can be generated using a KeyGenerator instance. This can be obtained by calling the getInstance() method of the KeyGenerator class:

```
KeyGenerator keyGen = KeyGenerator.getInstance("DES");
```

The getInstance() method takes in one parameter specifying the algorithm with which the key will be used. Since we are generating a key for use with DES, this should be specified as "DES". Once the KeyGenerator instance has been obtained, the key can be generated by calling the generateKey() method of the KeyGenerator instance. This will return a key of the type SecretKey.

```
SecretKey desKey = keyGen.generateKey();
```

Create and configure Cipher object

Now that we have generated our key, the next step is to create a Cipher object that will be used to perform the encryption or decryption. Cipher objects are created using the `getInstance()` method of the Cipher class:

```
Cipher desCipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
```

The `getInstance()` method takes in a parameter specifying the algorithm to be used for encryption, as well as the cipher mode and padding method.

The input "DES/ECB/PKCS5Padding" configures the Cipher object to be used with the DES algorithm in ECB mode. This means that when the input data is larger than the block size of 64 bits, it will be divided into smaller blocks that are padded using the "PKCS5Padding" method if necessary.

The ECB mode of operation is used to specify how multiple blocks of data are handled by the encryption algorithm. ECB stands for 'electronic codebook' – when using ECB mode, identical input blocks always encrypt to the same output block.

After the Cipher object has been created, it must be configured to work in either encryption or decryption mode by using the following method:

```
desCipher.init(mode, desKey);
```

The mode should be specified as `Cipher.ENCRYPT_MODE` for encryption and `Cipher.DECRYPT_MODE` for decryption.

Perform the cryptographic operation

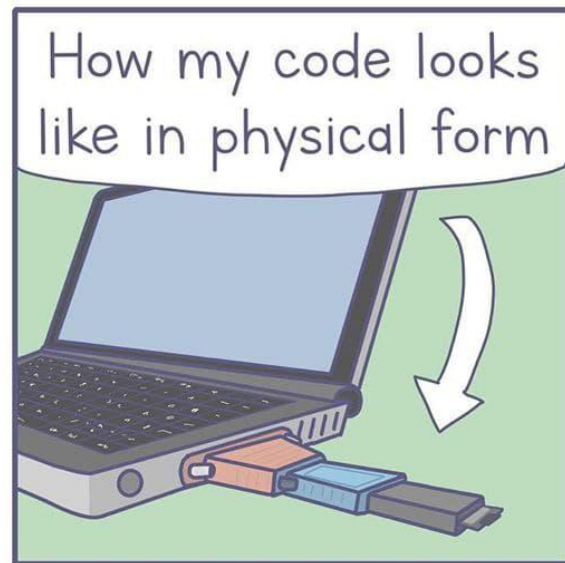
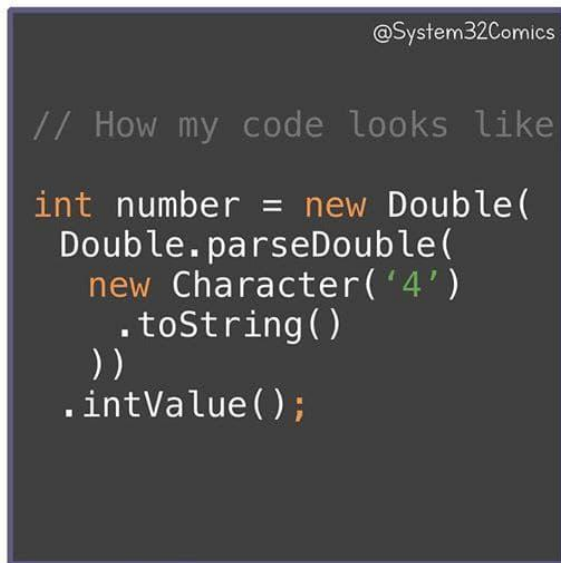
Once the Cipher object has been configured, the actual encryption or decryption operation (depending on how the object was configured) can be performed by calling the `doFinal()` method:

```
desCipher.doFinal();
```

Note that the method takes in a byte array containing the plaintext as input, and returns a byte array containing the ciphertext as output. If your plaintext input is stored in a string, you can convert it to a byte array using the `getBytes()` method before passing it to the `doFinal()` method. To inspect the ciphertext output, you can convert it to a printable string using:

```
String base64format =  
Base64.getEncoder().encodeToString(encryptedByteArray)
```

Kinda long winded, but we gotta do what we gotta do to print bytecode out.



@System32Comics

Tasks for Part 1[15pt]

Complete the file `DesSolution.java` so that it can encrypt an input text file using DES. Use your program to encrypt the provided files (`shorttext.txt` and `longtext.txt`) and answer the following questions:

Question 1 (1pt): Try to print to your screen the content of the input files, i.e., the plaintexts, using `System.out.println()`. What do you see? Are the files printable and human readable?

Your answer: yes files are printable and human readable. Entire plaintext file is printed.

Question 2 (1pt): Store the output ciphertext (in `byte[]` format) to a variable, say `cipherBytes`.

Try to print the ciphertext of the smaller file using `System.out.println(new String(cipherBytes))`.

Describe what you see, is it printable? Is it human readable?

Your answer: it is printable but not human readable. What was printed:

[illegible]

Question 3 (3pt): Now convert the ciphertext in Question 2 into Base64 format and print it to the screen. Describe this output with comparison to question (2). What changed?

Your answer: While it can still be printed and it still not human readable. The output is now a proper string.

[illegible]

Question 4 (3pt): Is Base64 encoding a cryptographic operation? Why or why not?

Your answer: no it is not. There is no using of keys to encrypt and decrypt the message.

Question 5 (3pt): Print out the decrypted ciphertext for the small file. Is the output the same as the output for question 1?

Your answer: yes it is.

Question 6 (4pt): Compare the lengths of the encryption result (in `byte[]` format) for `shorttext.txt` and `longtext.txt`. Does a larger file give a larger encrypted byte array? Why?

Your answer:

byte array length for `shorttext.txt`: 1480

byte array length for `longtext.txt`: 17360

Yes a larger file gives a larger encrypted byte array. The longer the text, the more 64-bit blocks are encrypted, hence there will be a larger byte array..

Part 2: Symmetric key encryption for an image file

In the previous task, we used DES in ECB mode to encrypt a text file. In this task, we will use DES to encrypt an image file and vary the cipher mode used to observe any effects on the encryption.

Task for part 2 [20pt]

Complete the file `DesImageSolution.java` to encrypt the input file, a `.bmp` image file using DES in ECB mode. You will need to specify the parameter `"DES/ECB/PKCS5Padding"` for creating your instance of the Cipher object.

Note: Your encrypted file should also be in `.bmp` format. **Please ensure that your encrypted `.bmp` file can be opened using any image viewer you have in your computer.**

Question 1 (4pt): Compare the original image with the encrypted image. List at least 2 similarities and 1 difference. Also, can you identify the original image from the encrypted one?

Your answer:

Yes, I can identify the original image from the encrypted one.

Difference: The words 'Singapore University of Technology and Design' and 'Established in collaboration with MIT' can no longer be read.

Similarity:

- 1. The SUTD logo can still be read in both original and encrypted images**
- 2. Placement of the words 'Singapore University of Technology and Design' and 'Established in collaboration with MIT' can still be identified.**

Question 2 (3pt): Why do those similarities that you describe in the above question exist? Explain the reason based on what you find out about how the ECB mode works. Your answer here should be as concise as possible. Remember, this is a 5pt question.

Your answer: ECB works by dividing a message into blocks, and each block is encrypted separately. However, it encrypts identical plaintext blocks into identical ciphertext blocks. While the color of each individual pixel is encrypted, the overall image may still be discerned, as the pattern of identically colored pixels in the original remains in the encrypted version. Hence it does not hide data patterns well.

Question 3 (6pt): Now try to encrypt the image using the CBC mode instead (i.e., by specifying "DES/CBC/PKCS5Padding"). Compare the result with that obtained using ECB mode). State 2 differences that you observe. For each of the differences, explain its cause based on what you find out about how CBC mode works. **Your answer should refer to ecb.bmp output that you produce.**

Your answer:

1. The SUTD logo can no longer be read in the CBC encrypted image
2. Placement of the words 'Singapore University of Technology and Design' and 'Established in collaboration with MIT' cannot be identified from the CBC encrypted image.

This is because in CBC encryption, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. Thus, referring to cbcSUTD.bmp, we can see that as the image is encrypted from left to right, top to bottom, the beginning of the 'S' letter in SUTD logo is where the algorithm can be seen to suddenly change the encrypted pixel.

Question 4 (3pt): Do you observe any security issue with image obtained from CBC mode encryption of "SUTD.bmp"? What is the reason for such an issue to surface?

Your answer:

CBC with a static or predictable initialisation vector is vulnerable for the first blocks that could be identical, which is the case for the image. The first block of ciphertext is decrypted and then XORed with the initialization vector, the result is the first plaintext block. However, decrypting with the incorrect initialisation vector causes the first block of plaintext to be corrupt but subsequent plaintext blocks will be correct. This means that a plaintext block can be recovered from two adjacent blocks of ciphertext. As a consequence, a one-bit change to the ciphertext causes complete corruption of the corresponding block of plaintext, and inverts the corresponding bit in the following block of plaintext, but the rest of the blocks remain intact.

Question 5 (4pt): Can you explain and try on what would be the result if the data were to be taken from bottom to top along the columns of the image? (As opposed to top to bottom). Can you try your new approach on "triangle.bmp" and comment on observation? Name the resulting image as triangle_new.bmp.

Your answer:

For triangle_new.bmp, the XORed plaintext block starts when it encounters the edge of the triangle, where image data changes from black to white. Thus the heavily encrypted (dotted) part.



Part 3: Signed message digests

In NS Module 3, we learned how a signed message digest could be used to guarantee the integrity of a message. Signing the digest instead of the message itself gives much better efficiency. In the final task, we will use JCE to create and sign a message digest:

1. Create message digest:
 - a. Create a MessageDigest object
 - b. Update the MessageDigest object with an input byte stream
 - c. Compute the digest of the byte stream
2. Sign message digest
 - a. Generate an RSA key pair using a KeyPairGenerator object instance
 - b. Create and configure a Cipher object for use with RSA
 - c. Use the doFinal() method to sign the digest

Create a MessageDigest object

A MessageDigest object can be obtained by using the getInstance() method of the MessageDigest class:

```
MessageDigest md = MessageDigest.getInstance("MD5");
```

The getInstance() method takes in a parameter specifying the hash function to be used for creating the message digest. In this lab, we will use the MD5 function; other valid algorithms include SHA-1 and SHA-256.

Update MessageDigest object

After creating the MessageDigest object, you'll need to supply it with input data, by using the object's update() method. Note that the input data should be specified as a byte array.

```
md.update(input);
```

Compute digest

Once you have updated the `MessageDigest` object, you can use the `digest()` method to compute the stream's digest as output:

```
byte[] digest = md.digest();
```

Sign message digest

Generate RSA key pair

To generate an RSA key pair, we will use the `KeyPairGenerator` class. The `generateKeyPair()` method returns a `KeyPair` object, from which the public and private keys can be extracted:

```
KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");  
keyGen.initialize(1024);  
KeyPair keyPair = keyGen.generateKeyPair(); Key publicKey =  
keyPair.getPublic(); Key privateKey = keyPair.getPrivate();
```

Configure cipher for use with RSA

To sign a message, we will make use of RSA encryption using the private key. The steps for initializing the cipher object for RSA are similar to the steps for initializing it for DES:

```
Cipher rsaCipher =  
Cipher.getInstance("RSA/ECB/PKCS1Padding");  
rsaCipher.init(Cipher.ENCRYPT_MODE, privateKey);
```

Task for Part 3 [5pt]

Complete the file `DigitalSignatureSolution.java` so that it can generate a signed message digest of an input file.

Apply your program to the provided text files (`shorttext.txt`, `longtext.txt`) and answer the following questions:

Question 1 (2pt): What are the sizes in bytes of the message digests that you created for the two different files?

Your answer:

Shorttext.txt:

byte to hex string: 5044643FCA56CF59FD8143DFFA5E13C9

digest array length: 16

Longtext.txt:

byte to hex string: A07D79C37A85635C67C8D13467CFA44D

digest array length: 16

Question 2 (3pt): Compare the sizes of the signed message digests (in `byte[] encryptedBytes = eCipher.doFinal(data.getBytes());`

format) for `shorttext.txt` and `longtext.txt`. Does a larger file size give a longer signed message digest? Why or why not? Explain your answer concisely.

Your answer:

No, a larger file size does not give a longer signed message digest. This is because MD5 is a hash function that always produces a 128-bit hash value.