**Symmetric Key Encryption and Message Digest**

*50.005 Computer System Engineering*

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

[Overview](#_qa5my8prznk0)

[Learning objectives](#_y2a7l1wm02e0)

[Starter Code](#_nk8ecz82y2e8)

[Submission](#_1n0hfo1tpsz2)

[Part 1: Symmetric key encryption for a text file](#_56q3p9spdrpz)

[Generate key for DES](#_95pkon1n7lms)

[Create and configure Cipher object](#_9twb7qde2drl)

[Perform the cryptographic operation](#_hvp48la463ze)

[Tasks for Part 1](#_590bcljbk01e)

[Part 2: Symmetric key encryption for an image file](#_9hr6k1gtcbbm)

[Task for part 2](#_r6dolay2ruwe)

[Part 3: Signed message digests](#_w9c0b1ygbqz)

[Create a MessageDigest object](#_g3iwj6yoh8bf)

[Update MessageDigest object](#_bq36jqrztce5)

[Compute digest](#_km2npafyx2ge)

[Sign message digest](#_t10lleyfywdw)

[Generate RSA key pair](#_aqagcgug9iqn)

[Configure cipher for use with RSA](#_rcmneggq4tga)

[Task for Part 3](#_fhzsztoibkx5)

# 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 @csesubmitbot 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.

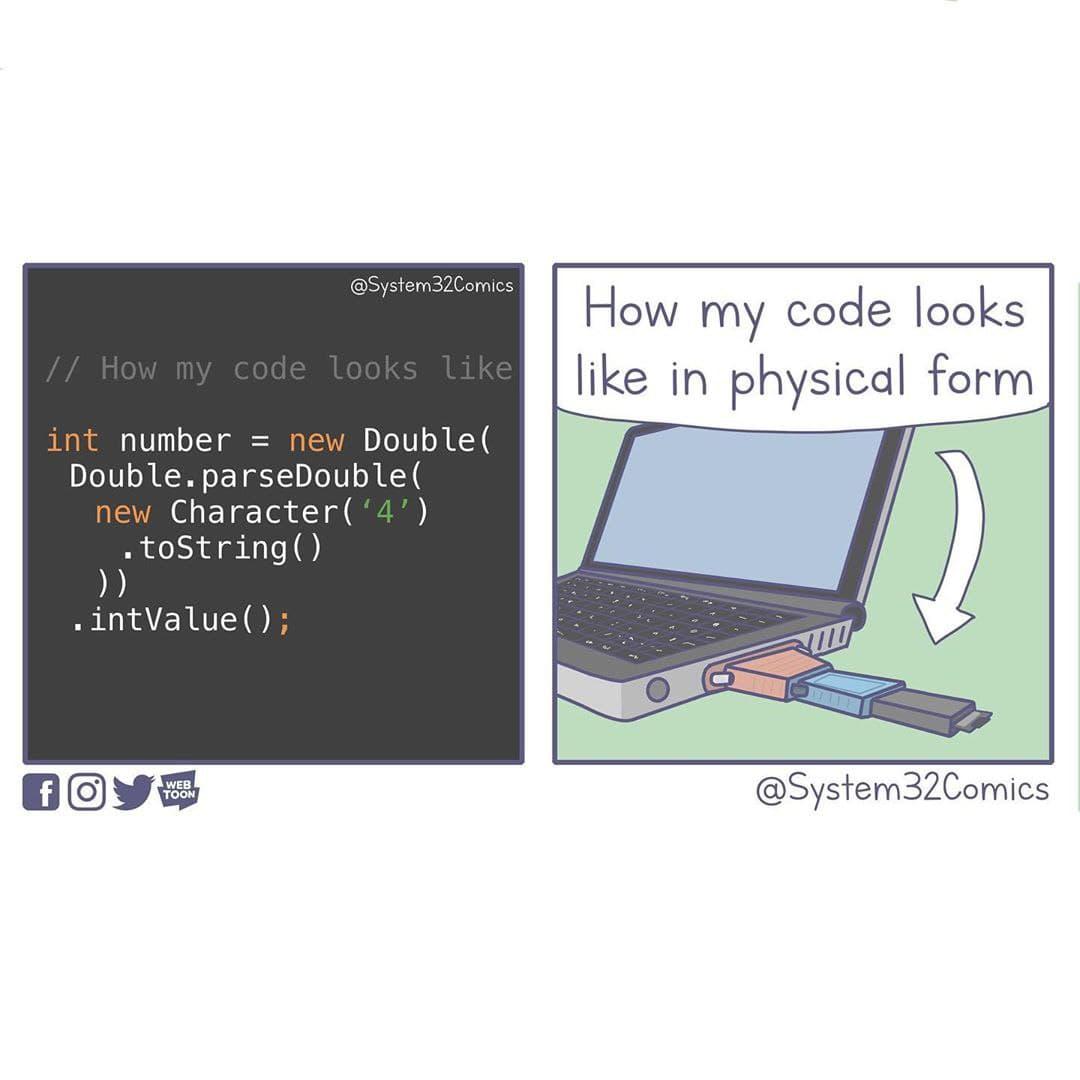
## Perform the cryptographic operation

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(encryptedBytesArray)

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

## 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: The texts in the shorttext.txt and longtext.txt. The files are printable and human readable.**

**Original content:**

**I've seen the world**

**Done it all**

**Had my cake now**

**Diamonds, brilliant**

**And Bel Air now**

**Hot summer nights, mid July**

**When you and I were forever wild**

**The crazy days, city lights**

**The way you'd play with me like a child**

**Will you still love me**

**When I'm no longer young and beautiful?**

**Will you still love me**

**When I got nothing but my aching soul?**

**I know you will, I know you will**

**I know that you will**

**Will you still love me when I'm no longer beautiful?**

**I've seen the world, lit it up**

**As my stage now**

**Channeling angels in the new age now**

**Hot summer days, rock 'n' roll**

**The way you play for me at your show**

**And all the ways I got to know**

**Your pretty face and electric soul**

**Will you still love me**

**When I'm no longer young and beautiful?**

**Will you still love me**

**When I got nothing but my aching soul?**

**I know you will, I know you will**

**I know that you will**

**Will you still love me when I'm no longer beautiful?**

**Dear Lord, when I get to heaven**

**Please let me bring my man**

**When he comes tell me that you'll let him in**

**Father tell me if you can**

**Oh that grace, oh that body**

**Oh that face makes me wanna party**

**He's my sun, he makes me shine like diamonds**

**Will you still love me**

**When I'm no longer young and beautiful?**

**Will you still love me**

**When I got nothing but my aching soul?**

**I know you will, I know you will**

**I know that you will**

**Will you still love me when I'm no longer beautiful?**

**Will you still love me when I'm no longer beautiful?**

**Will you still love me when I'm not young and beautiful?**

**Original content:**

**The Project Gutenberg EBook of The Sign of the Four, by Arthur Conan Doyle**

**This eBook is for the use of anyone anywhere at no cost and with**

**almost no restrictions whatsoever. You may copy it, give it away or**

**re-use it under the terms of the Project Gutenberg License included**

**with this eBook or online at www.gutenberg.net**

**Title: The Sign of the Four**

**Author: Arthur Conan Doyle**

**Posting Date: November 19, 2008 [EBook #2097]**

**Release Date: March, 2000**

**[This file last updated March 2, 2011]**

**Language: English**

**\*\*\* START OF THIS PROJECT GUTENBERG EBOOK THE SIGN OF THE FOUR \*\*\***

**The Sign of the Four**

**By**

**Sir Arthur Conan Doyle**

**Contents**

**Chapter I**

**The Science of Deduction**

**Sherlock Holmes took his bottle from the corner of the mantel-piece and**

**his hypodermic syringe from its neat morocco case. With his long,**

**white, nervous fingers he adjusted the delicate needle, and rolled back**

**his left shirt-cuff. For some little time his eyes rested thoughtfully**

**upon the sinewy forearm and wrist all dotted and scarred with**

**innumerable puncture-marks. Finally he thrust the sharp point home,**

**pressed down the tiny piston, and sank back into the velvet-lined**

**arm-chair with a long sigh of satisfaction.**

**Three times a day for many months I had witnessed this performance, but**

**custom had not reconciled my mind to it. On the contrary, from day to**

**day I had become more irritable at the sight, and my conscience swelled**

**nightly within me at the thought that I had lacked the courage to**

**protest. Again and again I had registered a vow that I should deliver**

**my soul upon the subject, but there was that in the cool, nonchalant**

**air of my companion which made him the last man with whom one would**

**care to take anything approaching to a liberty. His great powers, his**

**masterly manner, and the experience which I had had of his many**

**extraordinary qualities, all made me diffident and backward in crossing**

**him.**

**Yet upon that afternoon, whether it was the Beaune which I had taken**

**with my lunch, or the additional exasperation produced by the extreme**

**deliberation of his manner, I suddenly felt that I could hold out no**

**longer.**

**"Which is it to-day?" I asked,--"morphine or cocaine?"**

**He raised his eyes languidly from the old black-letter volume which he**

**had opened. "It is cocaine," he said,--"a seven-per-cent. solution.**

**Would you care to try it?"**

**"No, indeed," I answered, brusquely. "My constitution has not got over**

**the Afghan campaign yet. I cannot afford to throw any extra strain**

**upon it."**

**He smiled at my vehemence. "Perhaps you are right, Watson," he said.**

**"I suppose that its influence is physically a bad one. I find it,**

**however, so transcendently stimulating and clarifying to the mind that**

**its secondary action is a matter of small moment."**

**"But consider!" I said, earnestly. "Count the cost! Your brain may,**

**as you say, be roused and excited, but it is a pathological and morbid**

**process, which involves increased tissue-change and may at last leave a**

**permanent weakness. You know, too, what a black reaction comes upon**

**you. Surely the game is hardly worth the candle. Why should you, for**

**a mere passing pleasure, risk the loss of those great powers with which**

**you have been endowed? Remember that I speak not only as one comrade to**

**another, but as a medical man to one for whose constitution he is to**

**some extent answerable."**

**He did not seem offended. On the contrary, he put his finger-tips**

**together and leaned his elbows on the arms of his chair, like one who**

**has a relish for conversation.**

**"My mind," he said, "rebels at stagnation. Give me problems, give me**

**work, give me the most abstruse cryptogram or the most intricate**

**analysis, and I am in my own proper atmosphere. I can dispense then**

**with artificial stimulants. But I abhor the dull routine of existence.**

**I crave for mental exaltation. That is why I have chosen my own**

**particular profession,--or rather created it, for I am the only one in**

**the world."**

**"The only unofficial detective?" I said, raising my eyebrows.**

**"The only unofficial consulting detective," he answered. "I am the**

**last and highest court of appeal in detection. When Gregson or**

**Lestrade or Athelney Jones are out of their depths--which, by the way,**

**is their normal state--the matter is laid before me. I examine the**

**data, as an expert, and pronounce a specialist's opinion. I claim no**

**credit in such cases. My name figures in no newspaper. The work**

**itself, the pleasure of finding a field for my peculiar powers, is my**

**highest reward. But you have yourself had some experience of my**

**methods of work in the Jefferson Hope case."**

**"Yes, indeed," said I, cordially. "I was never so struck by anything**

**in my life. I even embodied it in a small brochure with the somewhat**

**fantastic title of 'A Study in Scarlet.'"**

**He shook his head sadly. "I glanced over it," said he. "Honestly, I**

**cannot congratulate you upon it. Detection is, or ought to be, an**

**exact science, and should be treated in the same cold and unemotional**

**manner. You have attempted to tinge it with romanticism, which**

**produces much the same effect as if you worked a love-story or an**

**elopement into the fifth proposition of Euclid."**

**"But the romance was there," I remonstrated. "I could not tamper with**

**the facts."**

**"Some facts should be suppressed, or at least a just sense of**

**proportion should be observed in treating them. The only point in the**

**case which deserved mention was the curious analytical reasoning from**

**effects to causes by which I succeeded in unraveling it."**

**I was annoyed at this criticism of a work which had been specially**

**designed to please him. I confess, too, that I was irritated by the**

**egotism which seemed to demand that every line of my pamphlet should be**

**devoted to his own special doings. More than once during the years**

**that I had lived with him in Baker Street I had observed that a small**

**vanity underlay my companion's quiet and didactic manner. I made no**

**remark, however, but sat nursing my wounded leg. I had a Jezail bullet**

**through it some time before, and, though it did not prevent me from**

**walking, it ached wearily at every change of the weather.**

**"My practice has extended recently to the Continent," said Holmes,**

**after a while, filling up his old brier-root pipe. "I was consulted**

**last week by Francois Le Villard, who, as you probably know, has come**

**rather to the front lately in the French detective service. He has all**

**the Celtic power of quick intuition, but he is deficient in the wide**

**range of exact knowledge which is essential to the higher developments**

**of his art. The case was concerned with a will, and possessed some**

**features of interest. I was able to refer him to two parallel cases,**

**the one at Riga in 1857, and the other at St. Louis in 1871, which have**

**suggested to him the true solution. Here is the letter which I had**

**this morning acknowledging my assistance." He tossed over, as he**

**spoke, a crumpled sheet of foreign notepaper. I glanced my eyes down**

**it, catching a profusion of notes of admiration, with stray**

**"magnifiques," "coup-de-maitres," and "tours-de-force," all testifying**

**to the ardent admiration of the Frenchman.**

**"He speaks as a pupil to his master," said I.**

**"Oh, he rates my assistance too highly," said Sherlock Holmes, lightly.**

**"He has considerable gifts himself. He possesses two out of the three**

**qualities necessary for the ideal detective. He has the power of**

**observation and that of deduction. He is only wanting in knowledge;**

**and that may come in time. He is now translating my small works into**

**French."**

**"Your works?"**

**"Oh, didn't you know?" he cried, laughing. "Yes, I have been guilty of**

**several monographs. They are all upon technical subjects. Here, for**

**example, is one 'Upon the Distinction between the Ashes of the Various**

**Tobaccoes.' In it I enumerate a hundred and forty forms of cigar-,**

**cigarette-, and pipe-tobacco, with colored plates illustrating the**

**difference in the ash. It is a point which is continually turning up**

**in criminal trials, and which is sometimes of supreme importance as a**

**clue. If you can say definitely, for example, that some murder has**

**been done by a man who was smoking an Indian lunkah, it obviously**

**narrows your field of search. To the trained eye there is as much**

**difference between the black ash of a Trichinopoly and the white fluff**

**of bird's-eye as there is between a cabbage and a potato."**

**"You have an extraordinary genius for minutiae," I remarked.**

**"I appreciate their importance. Here is my monograph upon the tracing**

**of footsteps, with some remarks upon the uses of plaster of Paris as a**

**preserver of impresses. Here, too, is a curious little work upon the**

**influence of a trade upon the form of the hand, with lithotypes of the**

**hands of slaters, sailors, corkcutters, compositors, weavers, and**

**diamond-polishers. That is a matter of great practical interest to the**

**scientific detective,--especially in cases of unclaimed bodies, or in**

**discovering the antecedents of criminals. But I weary you with my**

**hobby."**

**"Not at all," I answered, earnestly. "It is of the greatest interest**

**to me, especially since I have had the opportunity of observing your**

**practical application of it. But you spoke just now of observation and**

**deduction. Surely the one to some extent implies the other."**

**"Why, hardly," he answered, leaning back luxuriously in his arm-chair,**

**and sending up thick blue wreaths from his pipe. "For example,**

**observation shows me that you have been to the Wigmore Street**

**Post-Office this morning, but deduction lets me know that when there**

**you dispatched a telegram."**

**"Right!" said I. "Right on both points! But I confess that I don't**

**see how you arrived at it. It was a sudden impulse upon my part, and I**

**have mentioned it to no one."**

**"It is simplicity itself," he remarked, chuckling at my surprise,--"so**

**absurdly simple that an explanation is superfluous; and yet it may**

**serve to define the limits of observation and of deduction.**

**Observation tells me that you have a little reddish mould adhering to**

**your instep. Just opposite the Seymour Street Office they have taken**

**up the pavement and thrown up some earth which lies in such a way that**

**it is difficult to avoid treading in it in entering. The earth is of**

**this peculiar reddish tint which is found, as far as I know, nowhere**

**else in the neighborhood. So much is observation. The rest is**

**deduction."**

**"How, then, did you deduce the telegram?"**

**"Why, of course I knew that you had not written a letter, since I sat**

**opposite to you all morning. I see also in your open desk there that**

**you have a sheet of stamps and a thick bundle of post-cards. What**

**could you go into the post-office for, then, but to send a wire?**

**Eliminate all other factors, and the one which remains must be the**

**truth."**

**"In this case it certainly is so," I replied, after a little thought.**

**"The thing, however, is, as you say, of the simplest. Would you think**

**me impertinent if I were to put your theories to a more severe test?"**

**"On the contrary," he answered, "it would prevent me from taking a**

**second dose of cocaine. I should be delighted to look into any problem**

**which you might submit to me."**

**"I have heard you say that it is difficult for a man to have any object**

**in daily use without leaving the impress of his individuality upon it**

**in such a way that a trained observer might read it. Now, I have here**

**a watch which has recently come into my possession. Would you have the**

**kindness to let me have an opinion upon the character or habits of the**

**late owner?"**

**I handed him over the watch with some slight feeling of amusement in my**

**heart, for the test was, as I thought, an impossible one, and I**

**intended it as a lesson against the somewhat dogmatic tone which he**

**occasionally assumed. He balanced the watch in his hand, gazed hard at**

**the dial, opened the back, and examined the works, first with his naked**

**eyes and then with a powerful convex lens. I could hardly keep from**

**smiling at his crestfallen face when he finally snapped the case to and**

**handed it back.**

**"There are hardly any data," he remarked. "The watch has been recently**

**cleaned, which robs me of my most suggestive facts."**

**"You are right," I answered. "It was cleaned before being sent to me."**

**In my heart I accused my companion of putting forward a most lame and**

**impotent excuse to cover his failure. What data could he expect from**

**an uncleaned watch?**

**"Though unsatisfactory, my research has not been entirely barren," he**

**observed, staring up at the ceiling with dreamy, lack-lustre eyes.**

**"Subject to your correction, I should judge that the watch belonged to**

**your elder brother, who inherited it from your father."**

**"That you gather, no doubt, from the H. W. upon the back?"**

**"Quite so. The W. suggests your own name. The date of the watch is**

**nearly fifty years back, and the initials are as old as the watch: so**

**it was made for the last generation. Jewelry usually descends to the**

**eldest son, and he is most likely to have the same name as the father.**

**Your father has, if I remember right, been dead many years. It has,**

**therefore, been in the hands of your eldest brother."**

**"Right, so far," said I. "Anything else?"**

**"He was a man of untidy habits,--very untidy and careless. He was left**

**with good prospects, but he threw away his chances, lived for some time**

**in poverty with occasional short intervals of prosperity, and finally,**

**taking to drink, he died. That is all I can gather."**

**I sprang from my chair and limped impatiently about the room with**

**considerable bitterness in my heart.**

**"This is unworthy of you, Holmes," I said. "I could not have believed**

**that you would have descended to this. You have made inquires into the**

**history of my unhappy brother, and you now pretend to deduce this**

**knowledge in some fanciful way. You cannot expect me to believe that**

**you have read all this from his old watch! It is unkind, and, to speak**

**plainly, has a touch of charlatanism in it."**

**"My dear doctor," said he, kindly, "pray accept my apologies. Viewing**

**the matter as an abstract problem, I had forgotten how personal and**

**painful a thing it might be to you. I assure you, however, that I**

**never even knew that you had a brother until you handed me the watch."**

**"Then how in the name of all that is wonderful did you get these facts?**

**They are absolutely correct in every particular."**

**"Ah, that is good luck. I could only say what was the balance of**

**probability. I did not at all expect to be so accurate."**

**"But it was not mere guess-work?"**

**"No, no: I never guess. It is a shocking habit,--destructive to the**

**logical faculty. What seems strange to you is only so because you do**

**not follow my train of thought or observe the small facts upon which**

**large inferences may depend. For example, I began by stating that your**

**brother was careless. When you observe the lower part of that**

**watch-case you notice that it is not only dinted in two places, but it**

**is cut and marked all over from the habit of keeping other hard**

**objects, such as coins or keys, in the same pocket. Surely it is no**

**great feat to assume that a man who treats a fifty-guinea watch so**

**cavalierly must be a careless man. Neither is it a very far-fetched**

**inference that a man who inherits one article of such value is pretty**

**well provided for in other respects."**

**I nodded, to show that I followed his reasoning.**

**"It is very customary for pawnbrokers in England, when they take a**

**watch, to scratch the number of the ticket with a pin-point upon the**

**inside of the case. It is more handy than a label, as there is no risk**

**of the number being lost or transposed. There are no less than four**

**such numbers visible to my lens on the inside of this case.**

**Inference,--that your brother was often at low water. Secondary**

**inference,--that he had occasional bursts of prosperity, or he could**

**not have redeemed the pledge. Finally, I ask you to look at the inner**

**plate, which contains the key-hole. Look at the thousands of scratches**

**all round the hole,--marks where the key has slipped. What sober man's**

**key could have scored those grooves? But you will never see a**

**drunkard's watch without them. He winds it at night, and he leaves**

**these traces of his unsteady hand. Where is the mystery in all this?"**

**"It is as clear as daylight," I answered. "I regret the injustice**

**which I did you. I should have had more faith in your marvellous**

**faculty. May I ask whether you have any professional inquiry on foot**

**at present?"**

**"None. Hence the cocaine. I cannot live without brain-work. What else**

**is there to live for? Stand at the window here. Was ever such a**

**dreary, dismal, unprofitable world? See how the yellow fog swirls down**

**the street and drifts across the dun-colored houses. What could be**

**more hopelessly prosaic and material? What is the use of having**

**powers, doctor, when one has no field upon which to exert them? Crime**

**is commonplace, existence is commonplace, and no qualities save those**

**which are commonplace have any function upon earth."**

**I had opened my mouth to reply to this tirade, when with a crisp knock**

**our landlady entered, bearing a card upon the brass salver.**

**"A young lady for you, sir," she said, addressing my companion.**

**"Miss Mary Morstan," he read. "Hum! I have no recollection of the**

**name. Ask the young lady to step up, Mrs. Hudson. Don't go, doctor.**

**I should prefer that you remain."**

**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.**

**ҶPn�v��&�L�ʌ�tU�N��\_�S� �%��:h�g�2qp[�7c�f�!K��kݏs|C�<'�6a���\_�^\�֕ ?�V�+\_�o�Ek!9a�z��X**

**\{�d�����ޏ���Y,��!=��f�m� �Q&�ۏ��=�\*�I\�e��w\*�X�m���&�"�!��p���@�YI"醼��,��Sþw.^aE�٩ ����2��<o�,���>0���**

**��Um�;����8����S^Kx��֍������4���0�I,d�#��Y���fV|�t`Kj!WO�,6�fXT�D��V���**

**�&�g�Jܪb�,H������4LY�r���J���-���꒑������`T�|���X���=��\��vCϯ皒W�4\*���P$Ʉ�ΐ㢾�3�0**

**\_L\_.��@i��وQ��$1��U���]w**

**�j��**

**lp�e5���4\*)\��U"�r2���R=�l�- Qࢁ�r���\_�**

**'W����Z&����sH>HÅ�.]E�i�%�Y�� P�4ҫl=��~]A�X�U��&���**

**E�䠝V�|'3���x��2>:��M/\�ݻ�ޣQ˿�{���W��|�yC��`,ݩ�q�:�1F(IFGvᕩLa^�?����hM�{O�2T�dݶ��5��<s��&VzDR�he&�5�?��B�l�)�FR����5g;���Zt�^��)Ђ��|�>ض͕��~��`��W��j���і**

**#��P��8����x0����$P@�K���aҷC�X�یg��,��G\*�O��2����.D�P���1�<������|�F9�f�\��z�'��l�˚�Py�Y�z�I�ݞ����vł�q��+��쨭P��-�Wͻ`/�P��nr�̉k��k�NZ�/�S**

**Q�����.���o ��,^߳�e**

**QrQ�dH������3���t(E�$JI�6�-�ƮO�y�N�/U��Srm�K�'�V����u��l3�>�8�i��g.��׳���x�#��N"�,+�{�`�����eI9�-��Ne3����`��(��\_��ị l#���6 ��o�q�߸�&;**

**s���:ѡ�����L�����0V�=/���"��a:7zg����͸��Xy���D�I���X�/~5�ی^%@�3'�v�^�0�����\*܏ƣ������`o�C-**

**kv� �6����C������w���U�|��!nt���=�-镩La^�?;N�@���ge��}!��gÝ�]��L�����N���#f�� ���w��z�(�ݬ��� n�f�+���k31�����֢��\_{��vI��o�U�d�f��ÿ���r�I]���a\��!���Ԕ**

**��˱dT�}ǉb�ܺRo5oo��cs�z]��0K�cH��U�ܔ��(̠�|��F�&��w��� ��W.0����>r��@Ue�h��o�~"e�^Ǫ��. �9���Q��Ww0p�**

**\*�tk&y�"�(�z��m cY0�o/p���yJ��7��)���%�M�U�D�+����-�q�5�΁O�o��%�Ύ}u�z�u�`3xA犧�+M�]nF��C��^>�����W�dL~�<��LLo� Z���3��s�c�;}�d;���^W<��0���o���;9c����8�i�[�Negd2**

**��P+E���V���**

**#**

**y0S���]]W-��7޷�%n�S��V��=M�� �q����7�{$�@62\_|�\_$S�ZT�|��q**

**�#���ۣ�� n�{�N�\_D]�&����"��V��$LZ���D�.��Ǆ�DZW8���qe��M��I["q� 2���/��**

**μ2���R��3�\��N�=��1�ω�Y`پ=��~q�\_��D��r�2��ْؤ"2�%�E������n�l�3���HT �bO�F�M6d�]���P�i�\*x�yܥ�3**

**��ל��>�Y#[mI������**

**��bP�zTſ�>Ѯ�ڏ**

**38Ļ��Rg�ʸ,��E������m��8��@D�xDVe�;UR�0���f�V�`�Y8n�/d[���:���l�O�� �B���?��(�L��(Q��kBpO2�1�7Hk���$#9q1Lb���.@�8�s�rPzH�O�!�==y|F!>�XHߞ,��l�fX�!�)"��5�ԇ����h|ǯC��?�}؁�1��?�i�W�O�p��b�;2�|�ߔ(��iBëa$�pwCL�)"Q��u�[�8���ܼ����$�U�mT�**

**��K���ﴮ.��s�6��C��7�l|~�����D���τ\*�@���}���JJ9�jUA$**

**�Ա���D�&[GC�B%���F�&����S��\_�m ��$��-�Z"N�p��2�0�&j���n# (�n�Y:�1v�2u m\_Rp��=��\z�@�܊B����ٮ�**

**�/\*Q�p���b�U�?n}� �-�/Ɇ&��Q�s**

**���y��Z���݇���v?��J9�jUA$**

**�@��4�6|�u\_�á�**

**��AG#��w�G����92��@G�IM��\_�}�� ��-���+��쨭�!^1�)�6���D��0p��%=�{���|�4F2��\/԰��**

**�����{�~���Ϊ**

**ų��<��n����ֵ;��9F����\��I�� <f�Ҩ��kr���LK�l���<$�2d���,1��Ж�n�T�(@��7����JML\*m�h��C�wKPW��°**

**�[>HrU� >���[vo�d.�e{�W�^2�@��v�]��0+|(��a����K�#\_�j�WHV��do�m�Y�W\_Z=��\0��އ�\*�:z��?�2�#\_�#t�����=���ܪ\*U�y~+��ώ\_����o����[["ҳ|��M��l��u��M�iQ��S.^�**

**R�**

**�������YЀb�?�$,gi�&��{��F^Xl�Zn�G+**

**H�P�kP��/O��!�V�/�`𪱒�)18��7��K��ie\*s����v��^�c�9�����ꯁ�+�v=՝'��.��yג�٘�voЗ�)�0���G����7���;��|K�3�6�"���Q���.zl�C�**

**=h���se8c=y+5�)����[�����7�V�> �r�\_�0�@��q�c֦���ٖ.�A�8��+�\�v���jlp�e5���gܾإtN����31��}���v�������v�E/�}%��N����0Q����tFp��2\_GWU\*����I8�"����eW]ĵ�<�p�܈�pI5F����}sŢ�D�HJƸ̖A�aze�HVq dٰE�^{�Y-�?6G�+N�����X�**

**k�F���sh&�Pa��=\*�����x�v܊�3�'���`pE����gl8��[�MO�3�����R!��Ŏ�,Y5?.�t�tW��)y�J3��(G�[�C�e�a��$��3o\I{�&�:-ж�m�7�I.��`\¹�WC,��~�����(��7e'$(�-UH�9�6p)Vġdh�mw�ˋ��3�q����s�a�Wo�F��k�~I����[�T�!��\_���=�S��{#cCc=�p�U,�ps���w���gf&�����,ʬ ��`�\_�T�l��0�I�&ص]�X�&**

**�.�N.rS�G}!:�6�"���Q��u,v�G�0{�����'���**

**��gt��k����(/�$ʫ��k0���K����s�Yp|��ZH:4o7��u=zW[�~4��B�{Q6+#,�E���� :��/��0�G8]��cd@�l%�#t���Q���Wj�T˯}�x���U[`:E�����%�?�o@;��#5����"�M�;�mG�f;CE~�j**

**�2�s�Yp|��(��z^�f��t�A��8�XE�?���bjW'|�**

**��������\*��8pe%4,����R .)�^)�2+؀!y�����X&�<�j+��z��{�yR��8�6�ƣ��9,(�9��j:,�<�(��i��NL�O��9���\*�)�:kk�R;�L\_Su��7��5X�9�H�g�ߞB�$\*������?��{�**

**2�0��K1�Rq�X9�o�f�{=�]/����L)qE?v�5�4��^zĽSV��zpZgk�f��/� �V}��� e,**

**x&���p�<�\N�\FԴz\�\_�d�g=d}�H:����M��Z����Z���d���r**

**(>�Z�p6�v}����,�\�%��`�'9=�56g��7�5t�%hZ��Ҁ9C�v�?bK�P�]n���׳ޝ�]��**

**��ρ�@J;��Y�**

**��6�B�Y)]���f�au��1z2�=��S�#!��~~��\*�(r߆mwێ\_(��Q��悾ż{@|Yn+�$�Q���%��?�ϞWf��r��hzE�����W5��Ҁ�7�������9e�**

**g�-Zk'�, �>gD�`��3�к���Yt��~k������T�Yт��/y灨�Q���W�y�֪��6��p�b��$�y'Ϫ�8M���~�+�E����[�" �6);:}��e���F��eR~-��C��@�Ʒ��h [��3^,��f���GRb>�嚏M�`b����Gv��=|�y��Řl��k��**

**��`����8��>Rrж���������|,W����i5�9Dw���**

**��;�uӔCn���\*��6����� m0��GavK�ZB**

**m�!����隿��a��`��s���K��n��H/<\*�D�:ZQ�r��֧�S?���(R/�çP7�i;q��g�� �?�$�\*����v4� �P��e��-��imx�Lakl�n��**

**�ӲA]a�n��ZDd��]F�nW�'���º�����=�>��**

**�Wt�ߥ�U���FoF�eq7����%ۻ�F����7lJk�1�7X��D��ԩ��B��>T���IaaUi��Qz(���=��z�î����5������}�i��,�ػEo�-�(}�^**

**�**

**��/��Qa��.�����B��c���ƀ���{�ւm�w�Ng9^\*����Y�u�y��+̲g�,$���(D�qJ���N��'��h�j`y��°[��7**

**��F>�V�@z�ќo�>�x��h]�|�,`�0��o�-�l�x�<�**

**�O��A�+�����O�^�2�~�?�D/m����FLm^��S��8S�$�S�R�+��.�`�`�ՅC$��v��3x���x'��oP���O$�M**

**\_���\և�ҝC�����̵4F�F|��X��V�C�}znt�r�ͱ+�%t��A;��A���**

**9�n�svN�Cd������U=B�go�m�3.��֜�:F#dT.�$ϣ|���w7S�-��&���SX�j5TNh�/�,�%�˟��Nϔc�[�<7ސ]��-��F��WY�1L���2�/��v[��o΂twN�)���1+f�**

**߈���x����\_���ҵ6�O��"����. �t�3D�aS?T|B��-&Ŏ�**

**��**

**�F+'���!,�e�����ʦV|Ӹ�����Z���D]XpaJ��;�Fh-�o�꒺i�x=�R#��}{NЖ������p)e�7�T�KR�!�"��;NG~�$��n9OFC�\_"YV�C����:rbU$V~**

**����K�-7#�(**

**> �ڳq���y��W��i�U��)�2�NX�m�r�=u�j0g'�<f�q�M ��`!��gI�贕B�� WԲ����6���eC޽�[�-�J%������9HU�����I�(!��sӅ��uc�]1��m**

**��K�y�g��O؆�?A6���p��6?��M��^]���쁚��C�4����=����piح9�;5)?~A��{7InT�}��:�C������9�UH��U�N��'�i�W9#�ө��^���{�Yf����f7+���ʖS�7��˫�-B�Hꃑ�'�5�D+�)�vc��u�z���4���6���C�58��GZ��\}��p̢�,l��EoC�B����)a**

**�~�X�Tp��1�7�U-gQL=Z#TKC�H6AZ�d[wŁ�7�;���B�l�+q�����\_��f�����g����:3�����p��ԁL����дk{T�|~Rk�>48L�c�S �уJ1�Rbl������p���D���pF����,lN�N�{��qᕝ���^��%���K��2����d�**

**��C��t�8pq�]��!=��wV**

**��^�]�T�[2�E�밀B)ׂ��n�LT9M����=�����\FԴz\�y��)~���^�ə����F����ʸ�ƕqh�^Z��Rr���c�~8(ͽ��W!��E5���8��I��;l��!�L)ר�ߑ.��+��쨭�)����~\_P;��QI�**

**����|h�kZ���F��v�zb�)o���^�P.���t�**

**e�Nȱ���^�+g���`4$�cܔ4y���w؝$|�e�Xk¡ŉ���!+wE�l��v�/A�krO����o�^��xC��1���պ�A���2/��e\%R�d���:=�**

**^b⧘�9�l���#��,��?�Te,nu��֔!�|�@����lkty�D�9�&\_�����L��`�}���ך-�v�K@r0�ݿ�"��YH�k�6Ԣ������إ�`�7\�M��8��@��X~�Z��}���d�%��-��鋾����>**

**��|�R@��3�!�Y�3 ���� [q����Уr�r}�**

**����U�[�A0����@q3�O���u�΂�iт�ؑ��}.��Z3'G'%c��Q�8�ԣ**

**� ����~ �I'**

**?V�I'��[�ʤ,��W�ǌ0����**

**XT��N�=,?/�+2�μp�j�|���鵺**

**�߃�Yɕ�.CD�`��ި�be��ce.|z��w�����C�**

**�.�|A{���1zd�e�[<0Id�����(��,Bқڙzx�R�$rB�3.�a**

**�N�&I8�"����h?��C��gLN5L���**

**�����!��[���0�H��a��,�w\*��41�5���J�o����o��rR,�,����**

**J��A������.�D��}N�a��p�"0�\*�5T�Iё�C**

**Nd��hS�C��u�[�8���73�~��>�\���,��x梃�A����q**

**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: It is printable and human readable. However, it does not make sense when read.**

****

****

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

**Your answer: It is not a cryptographic operation. It does not encrypt the message but solely encode the message. One can easily encode and decode the message. It lacks mutability and has no secret key.**

**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: Same as the output for question 1.**

**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:**

**shorttext.txt: 1480**

**longtext.txt: 17360**

**Yes, a larger file gives a larger encrypted byte array. For DES, a 64-bit input will result in a 64-bit encrypted output. The size of the encrypted byte array depends on the input file size.**

# 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:**

**Similarities: The outlines are similar. The size of the image remains even after being encrypted.**

**Difference: The encrypted images are in a different colour than the original ones.**

**The encrypted images are still identifiable from the original ones.**

**For example, the SUTD logo before and after encryption:**

****

****

**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 encrypts each input block of 64 bits independently so identical input blocks always encrypt to the same output block. ECB encrypts a bitmap image which uses large areas of uniform colour. Hence, the pattern of the image remains but the colour changed.**

**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:**

**Differences:**

1. **The outline of the CBC encrypted SUTD logo is no longer identifiable but the outline of the CBC encrypted triangle is still visible.**
2. **The background of the CBC encrypted images are horizontal stripes of colourful lines but the background of the ECB encrypted images are horizontal lines of consistent colour throughout the image.**

**Explanation:**

**CBC encrypts each current input block with XOR with the previous encrypted block. As seen in the CBC encrypted SUTD logo, the top of the image still has the slight outline of the logo but the bottom of the image is totally different.**

**The image of CBC encrypted SUTD logo:**

****

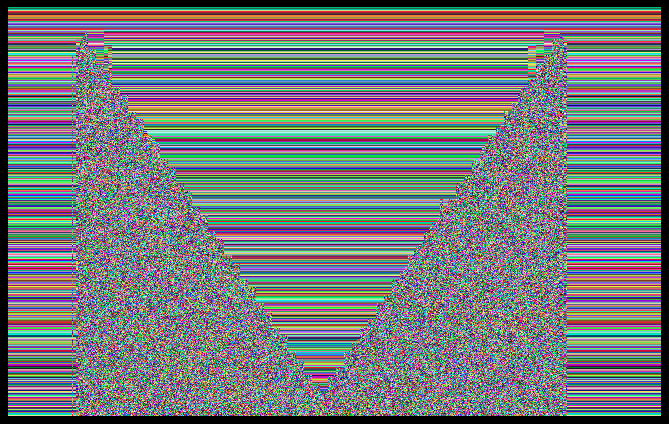
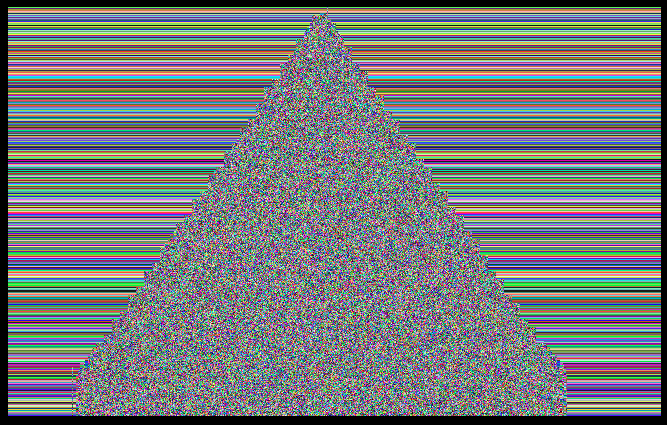
**Question 4** (3pt): Do you observe any security issue with image obtained from CBC mode encryption of “SUTD.bmp”? What is the reason for such an issue to surface?

**Your answer: Yes, as mentioned in the Q3, the top of the encrypted SUTD logo still has the outline of the original logo. A malicious user with relevant knowledge will be able to recognise the encrypted image.**

**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: The triangle image is the inverted version. As mentioned in Q3, CBC encrypts with the previous encrypted blocks. In the previous triangle image, there is a transition from lines to dots as the encrypting enters the triangle. However, in the new image, there is a transition from lines to dots and back to lines. This is due to the change of the initial encrypting block which will be used in encrypting the next block.**

**The images of CBC encrypted images of the triangle before and after inverting from bottom to top:**

****

# 

# 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:
   1. Create a MessageDigest object
   2. Update the MessageDigest object with an input byte stream
   3. Compute the digest of the byte stream

1. Sign message digest
   1. Generate an RSA key pair using a KeyPairGenerator object instance
   2. Create and configure a Cipher object for use with RSA
   3. Use the doFinal() method to sign the digest

## Create a MessageDigest object

A MessageDigest object can 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: Both sizes are in 16 bytes.**

**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: Both sizes are in 128 bytes. Unlike Part 1, the size depends on the key and not the size of the input text. Both files are signed with keys of 1024 bits so they will have the same sizes of the signed message digests.**