

SWE314 Project

Fall 2019



|  |  |
| --- | --- |
| *Section*: *56739* | |
| Name | ID |
| Majd Bandar Bin Musibeh | 438200829 |
| Ghada Abdurrahman AlGhurairi | 438201865 |
| Shahad Omar AlHarbi | 438201706 |
| Lujain Abdullah Almuhaitheef | 438201099 |
| Rahaf Mohammed Al-Omar | 438202048 |

Cipher program

# Introduction:

Information nowadays become more valuable than ever, and as everything that is valuable it can be targeted. Information – sensitive information to be more specific- need to be secured in order to transmit it without it being exposed to unauthorized parties.

In our system (Whisper), we are encrypting texts to a ciphertext using our own modern block cipher and decrypt it to the original plaintext.

Whisper consist of two rounds, each have a s-box, p-box and rail fence techniques, after these two rounds it will use the result text from round 2 and convert it again then it will swap the converted text.

How can Whisper Encrypt a plaintext?

The plaintext should be either letters a-z (capital, small or both) , digits 0-9 and spaces . If the user entered some characters like (!@#$%^\*(){} etc.) the system will not work (instead it will ask the user to enter a valid input consists of letters and digits). After that, the plaintext will go through the first round of encryption.

1. First, every letter and number in the plaintext should be converted to another letter or digit based on a special substitution boxes.

For letters:

|  |  |  |  |
| --- | --- | --- | --- |
| A → N | B → W | C → E | D → C |
| E → D | F → V | G → B | H → O |
| I → A | J → X | K → M | L → T |
| M → S | N → Z | O → J | P → K |
| Q → U | R → R | S → F | T → L |
| U → I | V → H | W → Q | X → P |
| Y → G | Z → Y |  |  |

For digits:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 → 4 | 1 → 3 | 2 → 0 | 3 → 6 | 4 → 9 |
| 5 → 5 | 6 → 8 | 7 → 1 | 8 → 7 | 9 → 2 |

In case the user entered a space, the system will convert it to (~) and works with it as if its work with any letter.

1. Second, we will use a special straight p-box. We will divide the result of the substitution to four parts, if the input was just a one letter, we will add ~|} to make it four, if it two letters we will add ~| and if it three we will use ~. After the division, we will use the following p-box.

4

3

2

1

Straight P-Box

2

1

3

4

1. Finally in the round, we will do a simple rail fence and the width is 2.

Then, the second round is started by the same steps.

After the 2 rounds we have a more two steps.

1. Convert the result of the second round to ASCII code (every character will take 3 digits after the converting).
2. The resulting ASCII codes, we will do a simple swap between each 2 digits.

Now we got the ciphertext!

Now, how can Whisper Decrypt a ciphertext?

First, we will check if the ciphertext is digits only, the number of digits is multiple of 12 (since we use 3 digits ASCII codes).

1. we will do a simple swap between each 2 digits.
2. Take every three digits and convert it to characters based on the ASCII code.
3. The round id started:
4. Simple rail fence with width 2.
5. The result is used in the next straight p-box after dividing the ciphertext to 4 parts as we mentioned.

4

3

2

1

Straight P-Box

1

2

4

3

1. The last par in the round will be a substitution based on:

For letters:

|  |  |  |  |
| --- | --- | --- | --- |
| A → I | B → G | C → D | D → E |
| E → C | F → S | G → Y | H → V |
| I → U | J → O | K → P | L → T |
| M → K | N → A | O → H | P → X |
| Q → W | R → R | S → M | T → L |
| U → Q | V → F | W → B | X → J |
| Y → Z | Z → N |  |  |

For digits:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 → 2 | 1 → 7 | 2 → 9 | 3 → 1 | 4 → 0 |
| 5 → 5 | 6 → 3 | 7 → 8 | 8 → 6 | 9 → 4 |

If the character is (~) the system will convert it to a space.

The we will do another round by steps a-c, after finish this round we will get the plaintext!

# Whisper Model:صورة تحتوي على لقطة شاشة تم إنشاء الوصف تلقائياً

صورة تحتوي على لقطة شاشة

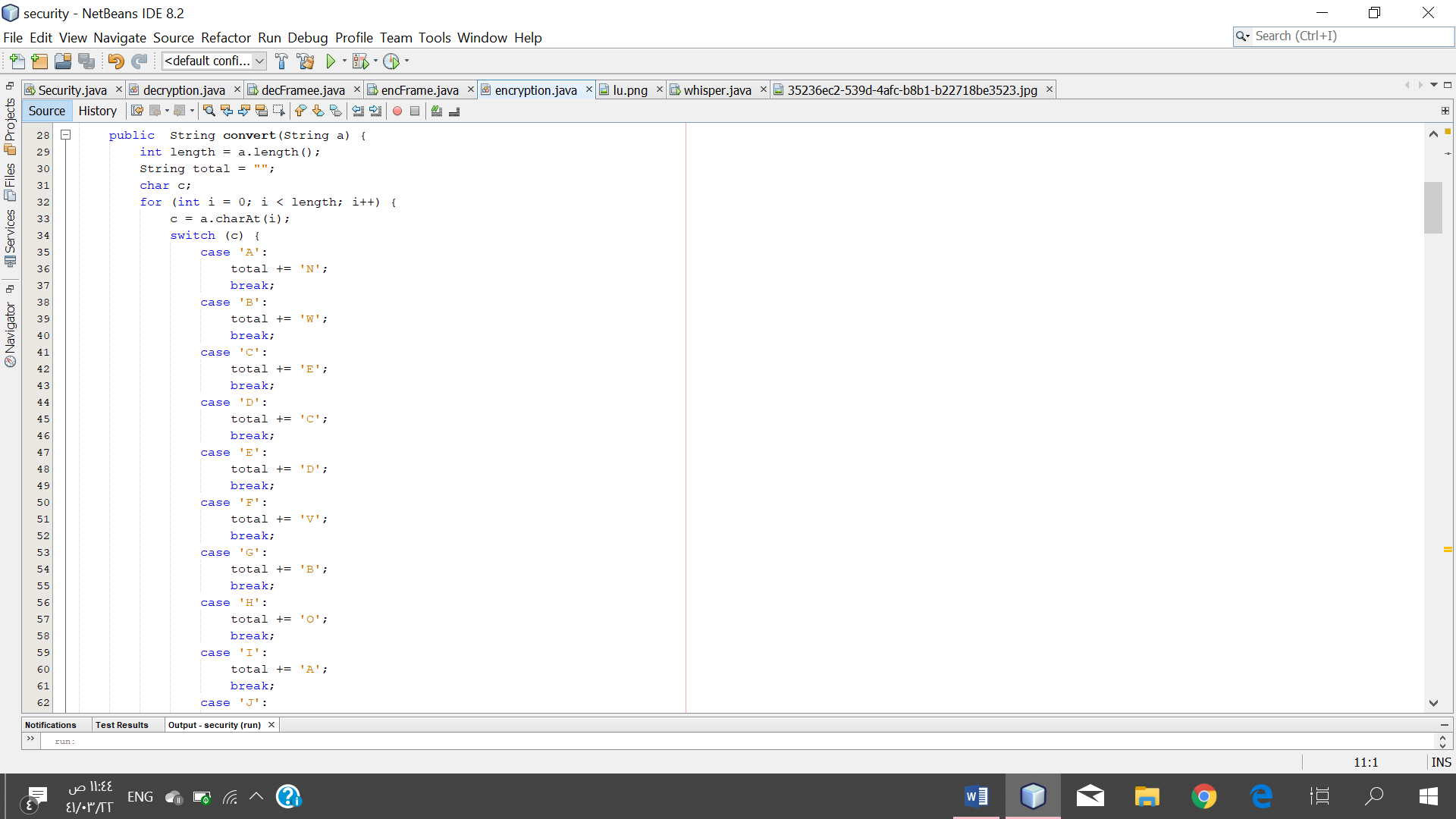
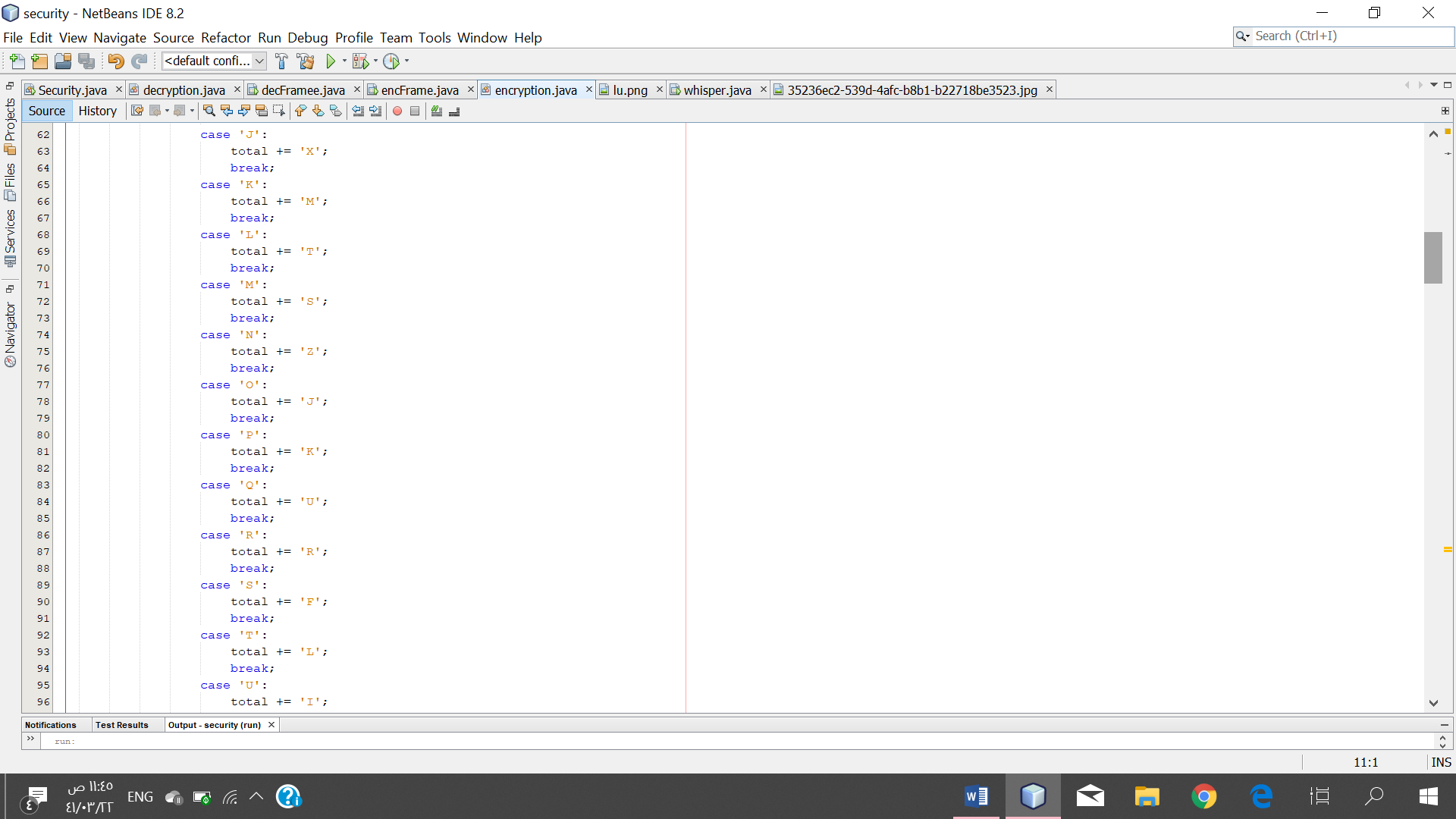
تم إنشاء الوصف تلقائياًصورة تحتوي على لقطة شاشة

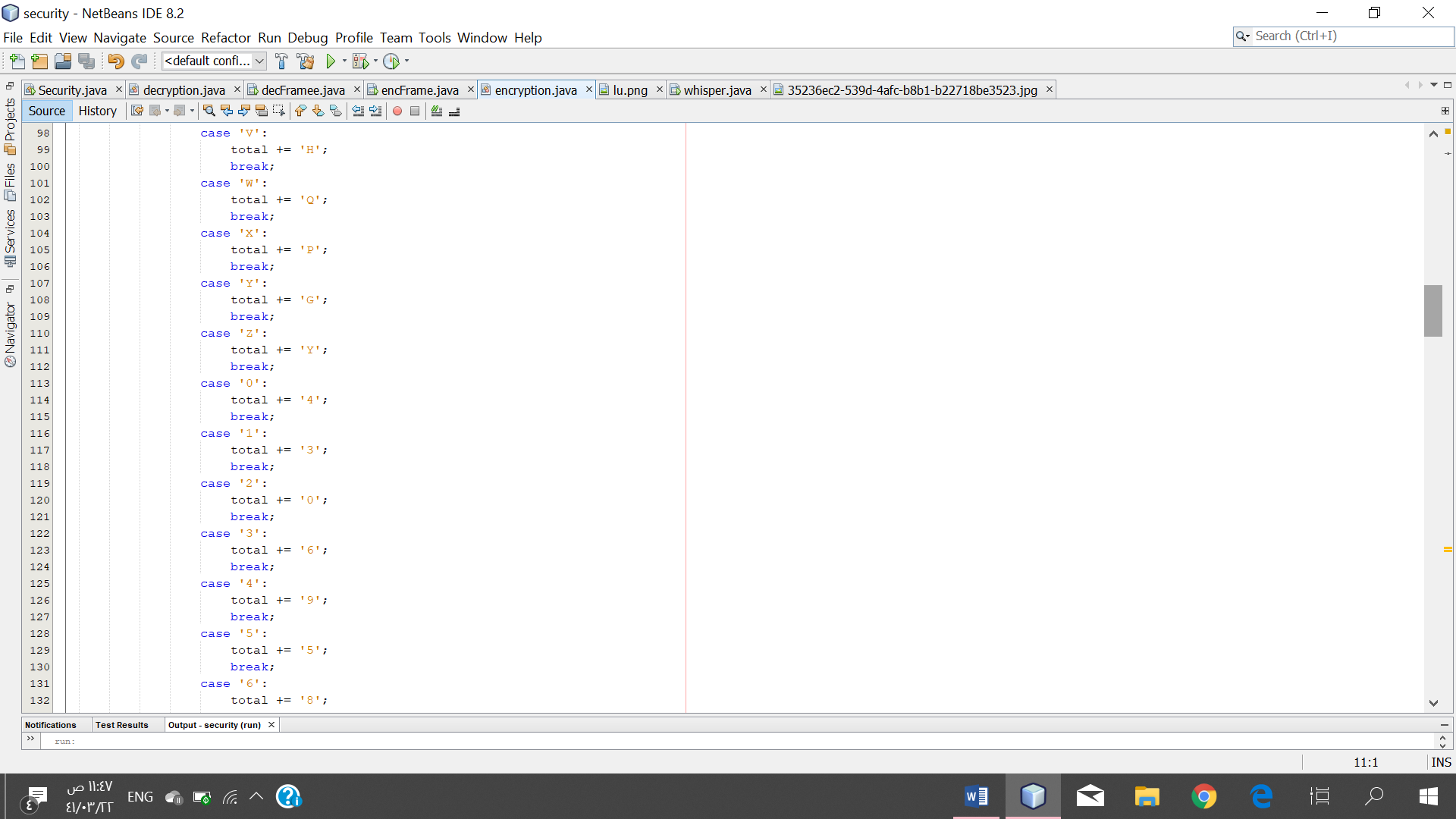
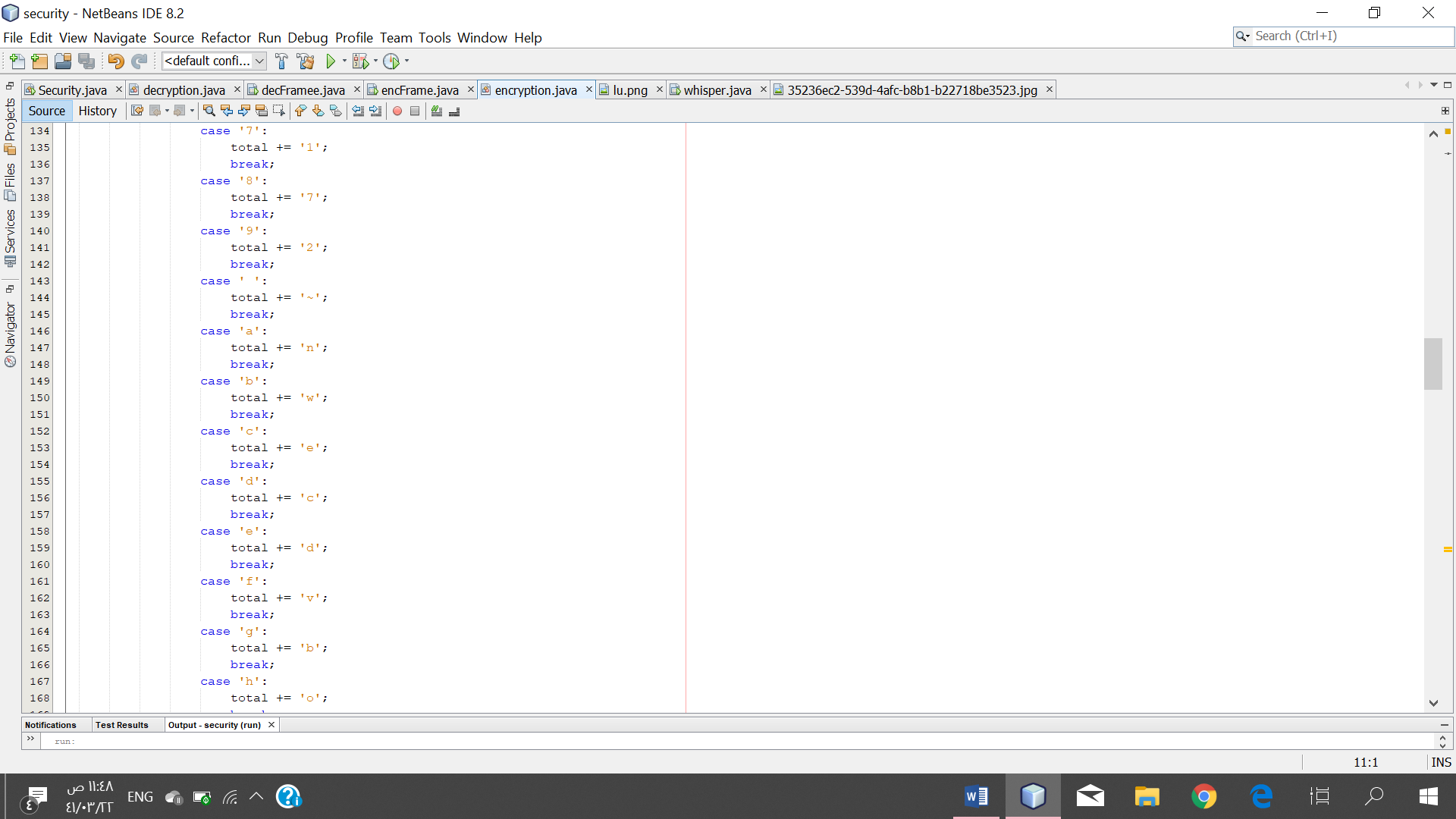
تم إنشاء الوصف تلقائياً

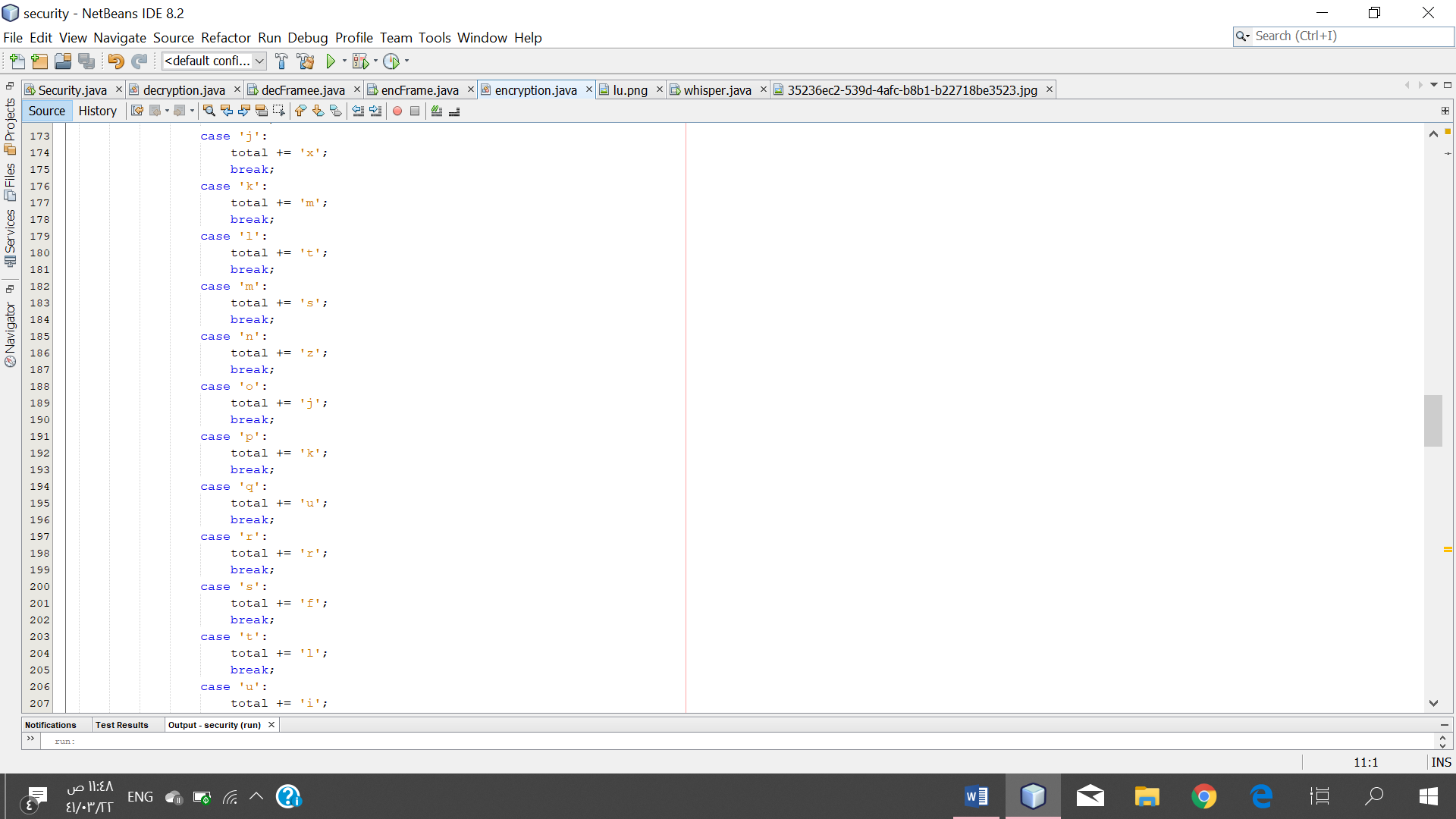
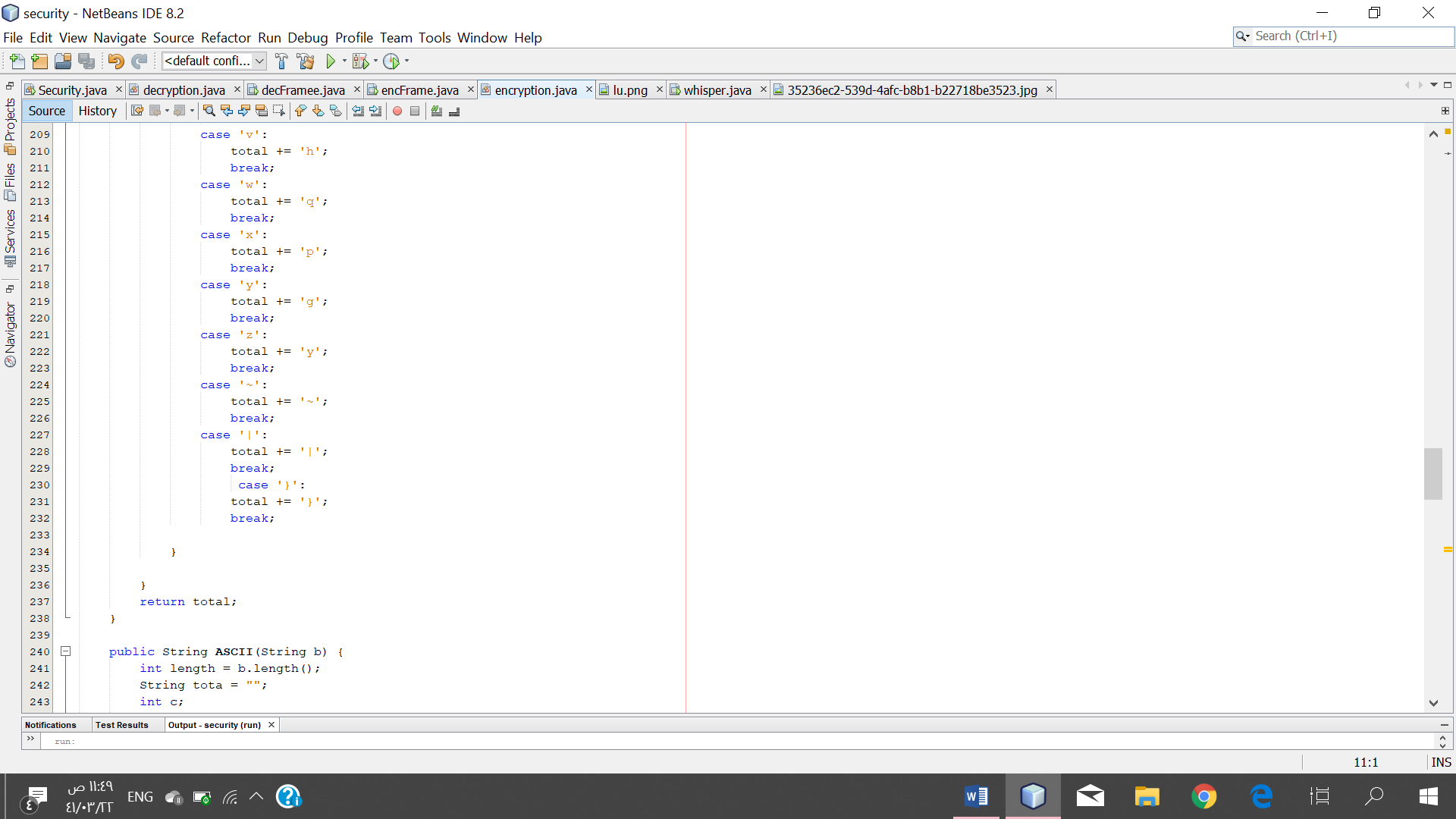
# snaps of the source code:

Class encryption:

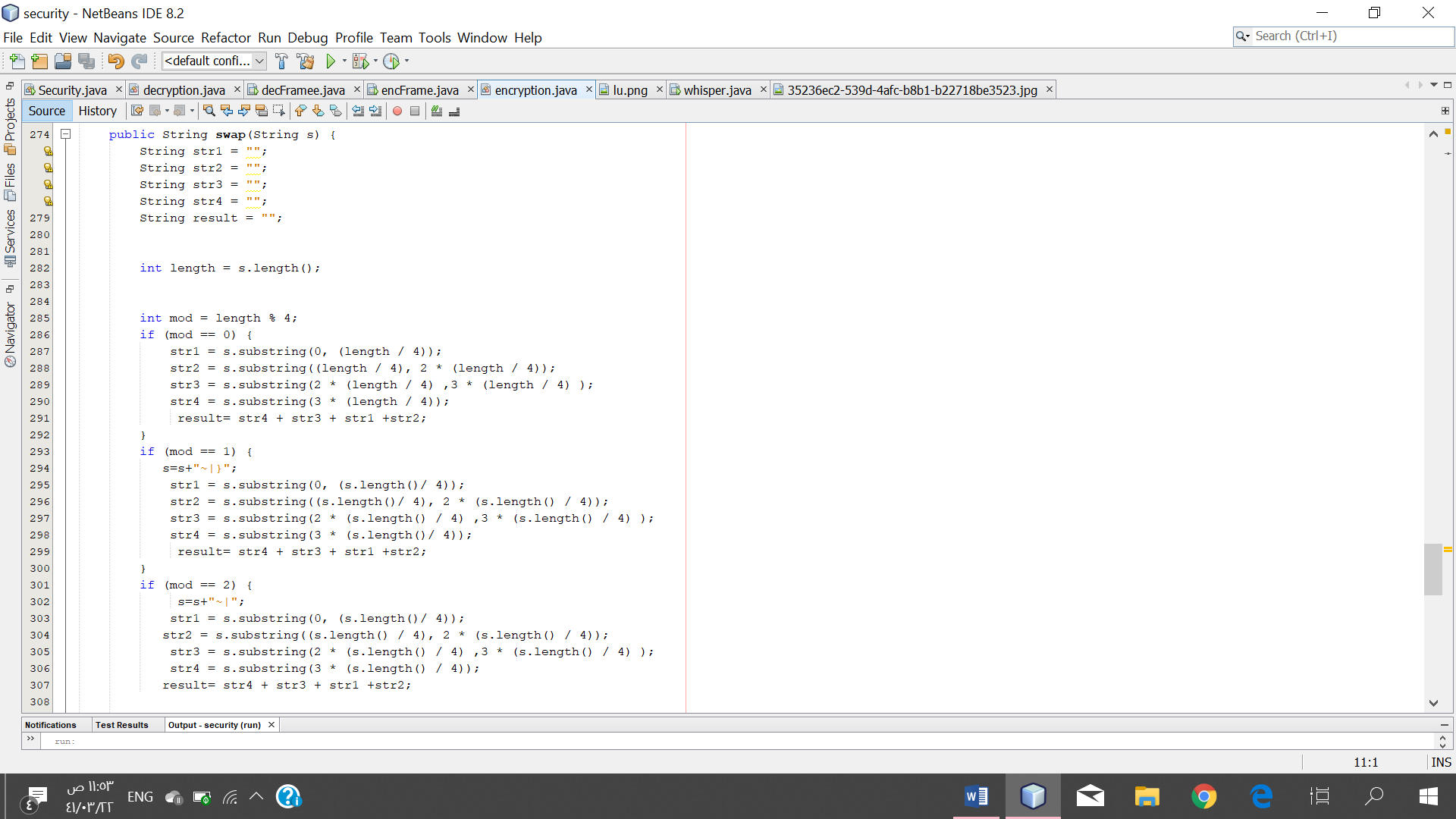
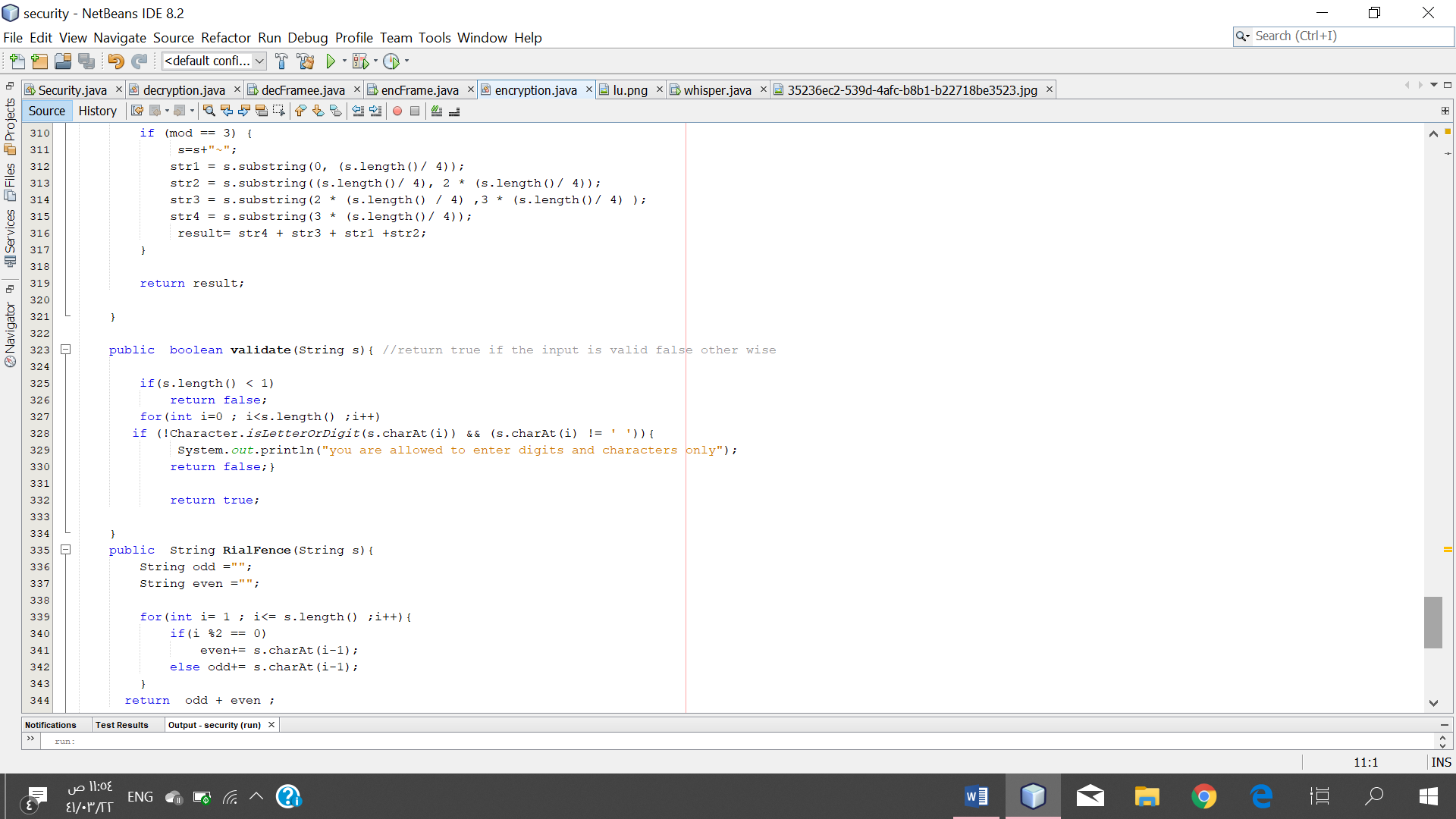
* The substitution method (convert):

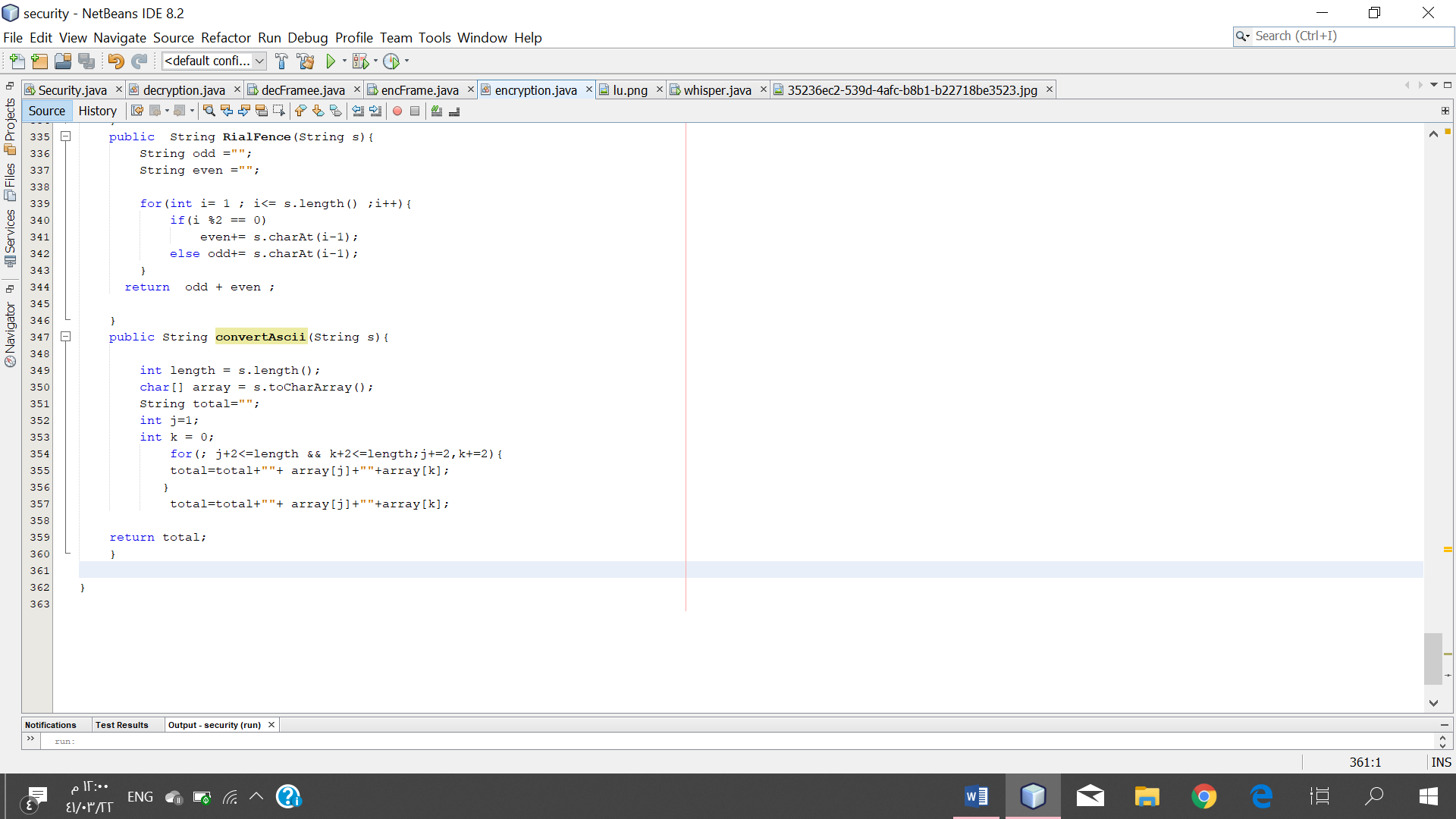
 

* The permutation method (swap):



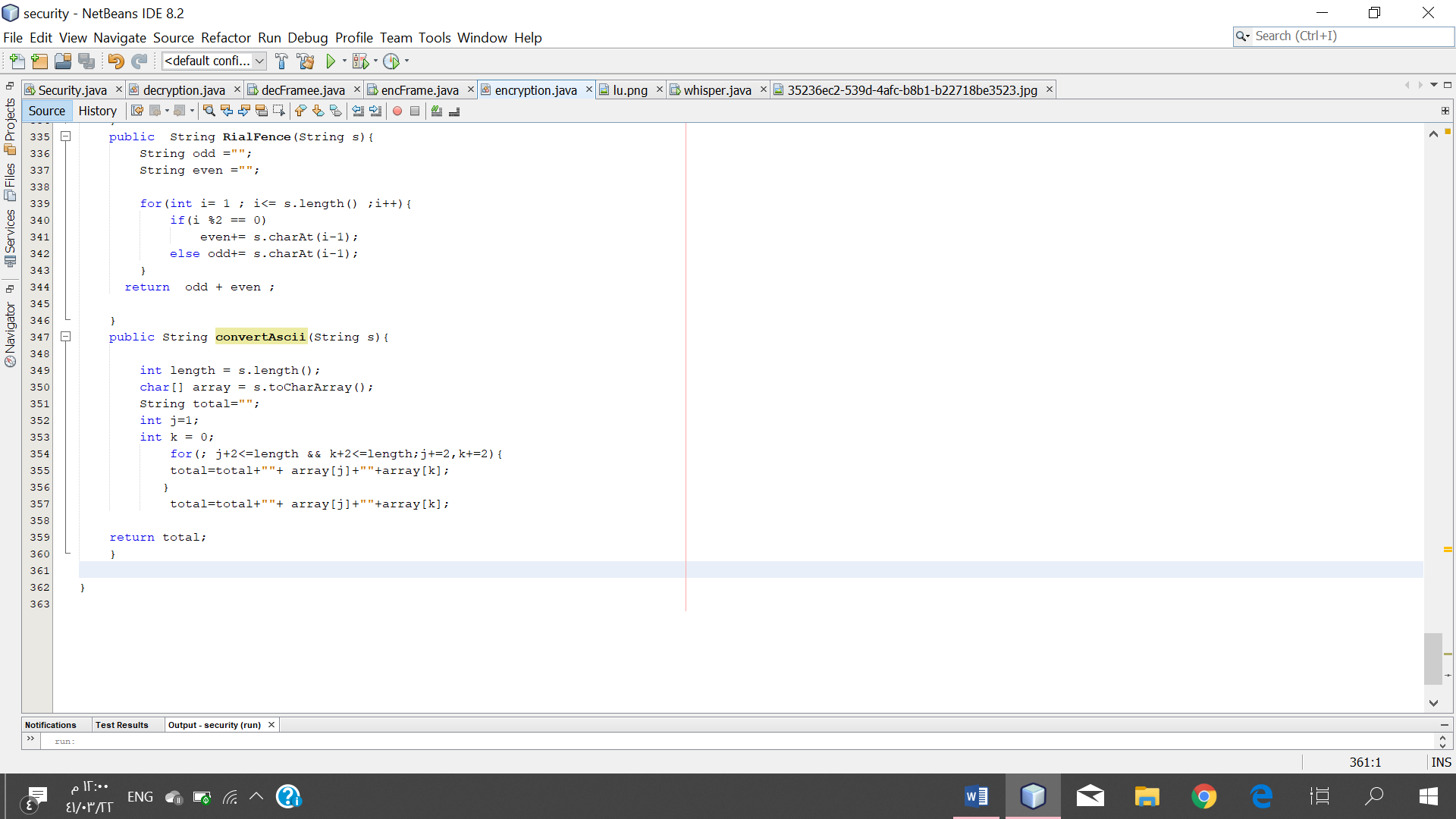
* Rail Fence method (Railfence):



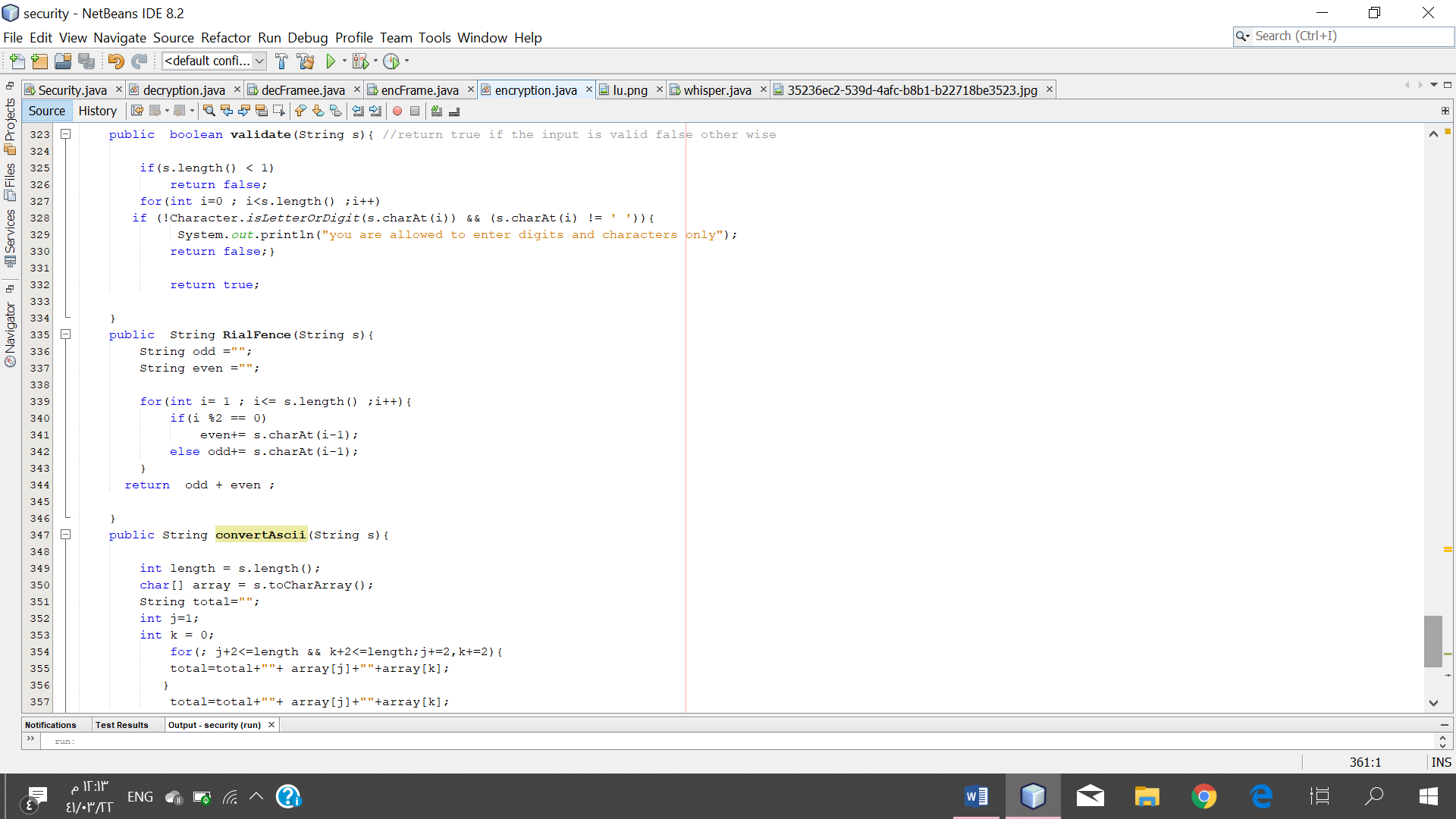
* Converting to ASCII method (ASCII):

# 

* Swap ASCII method (convert Ascii):

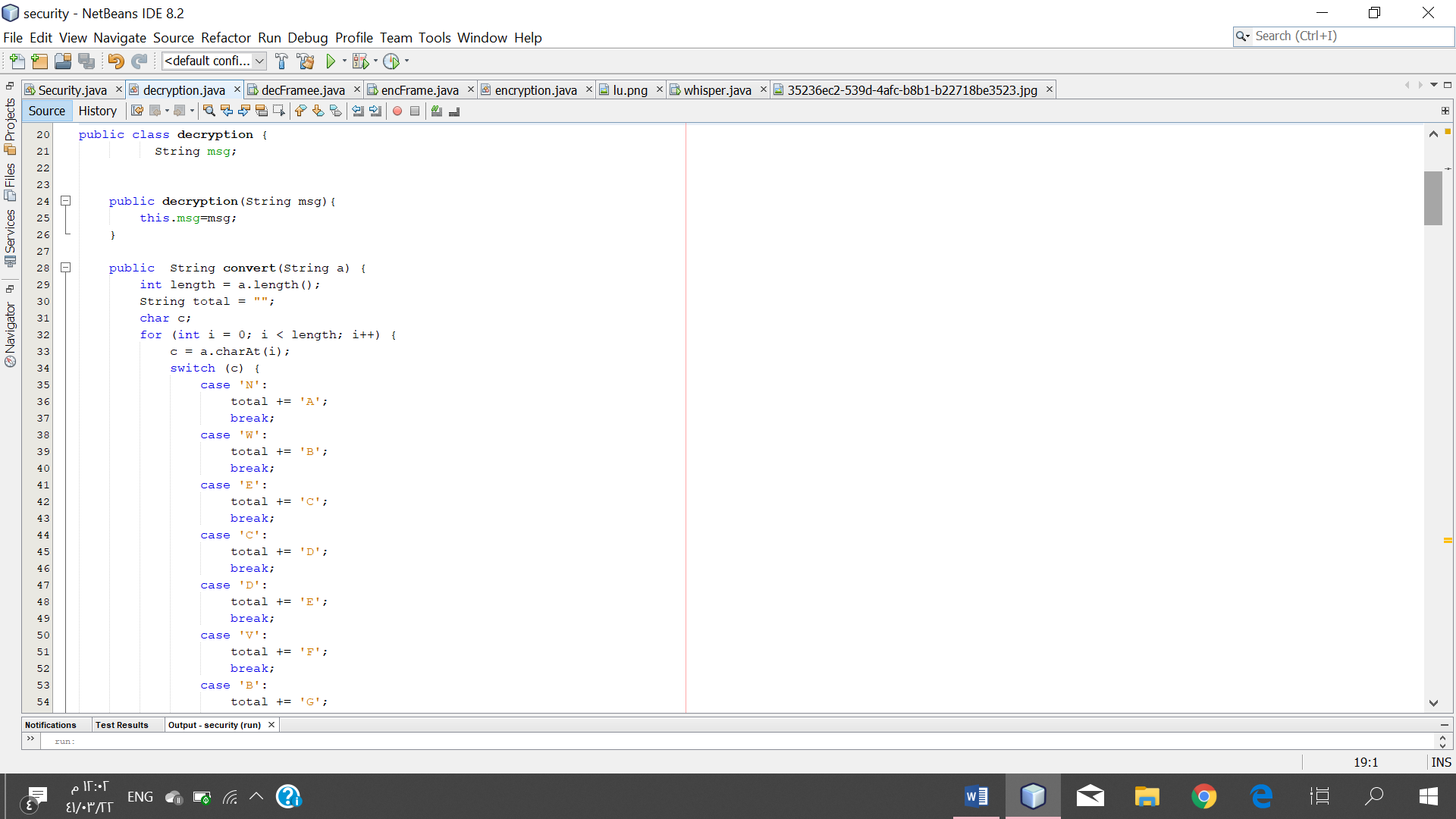
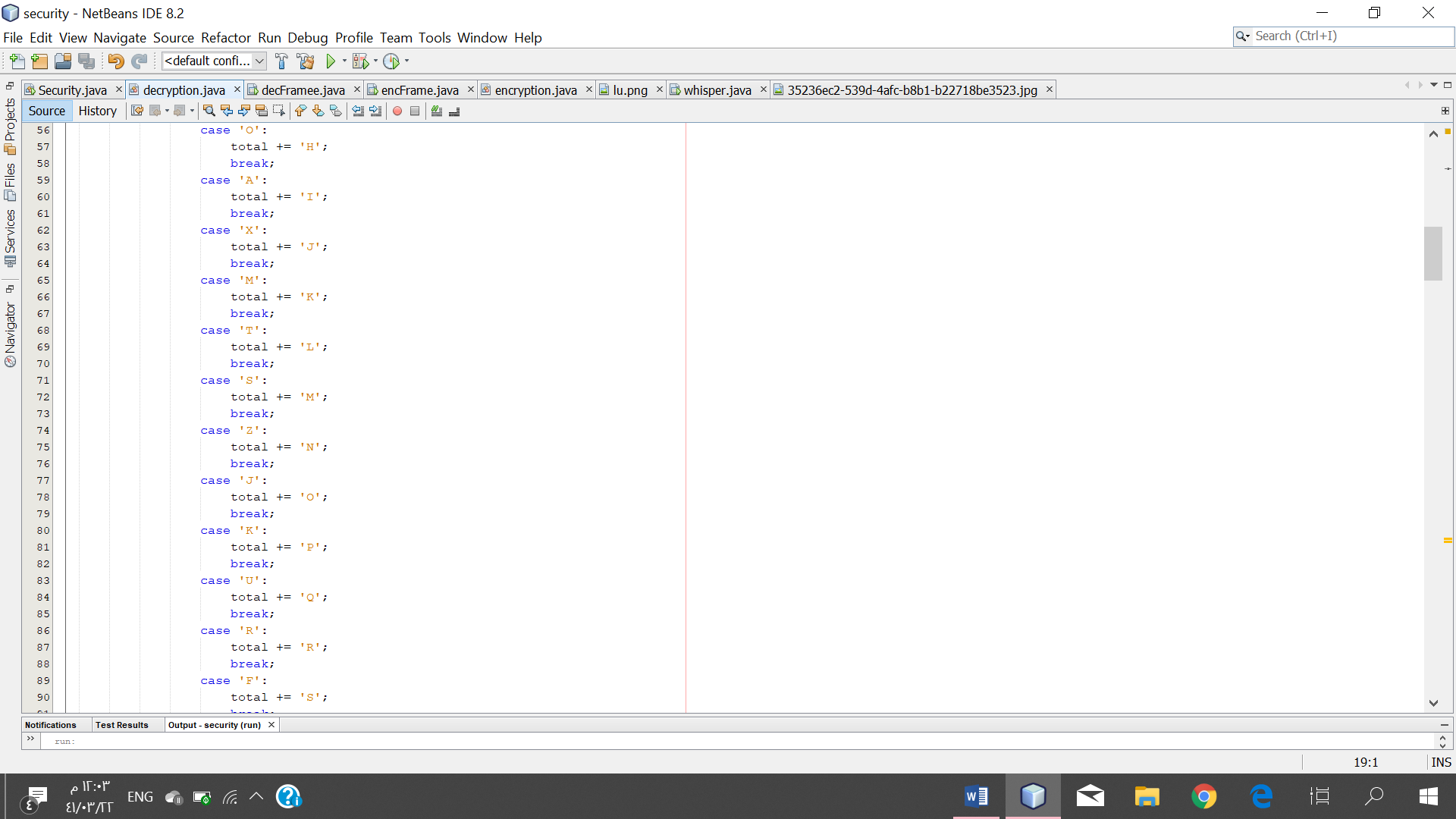


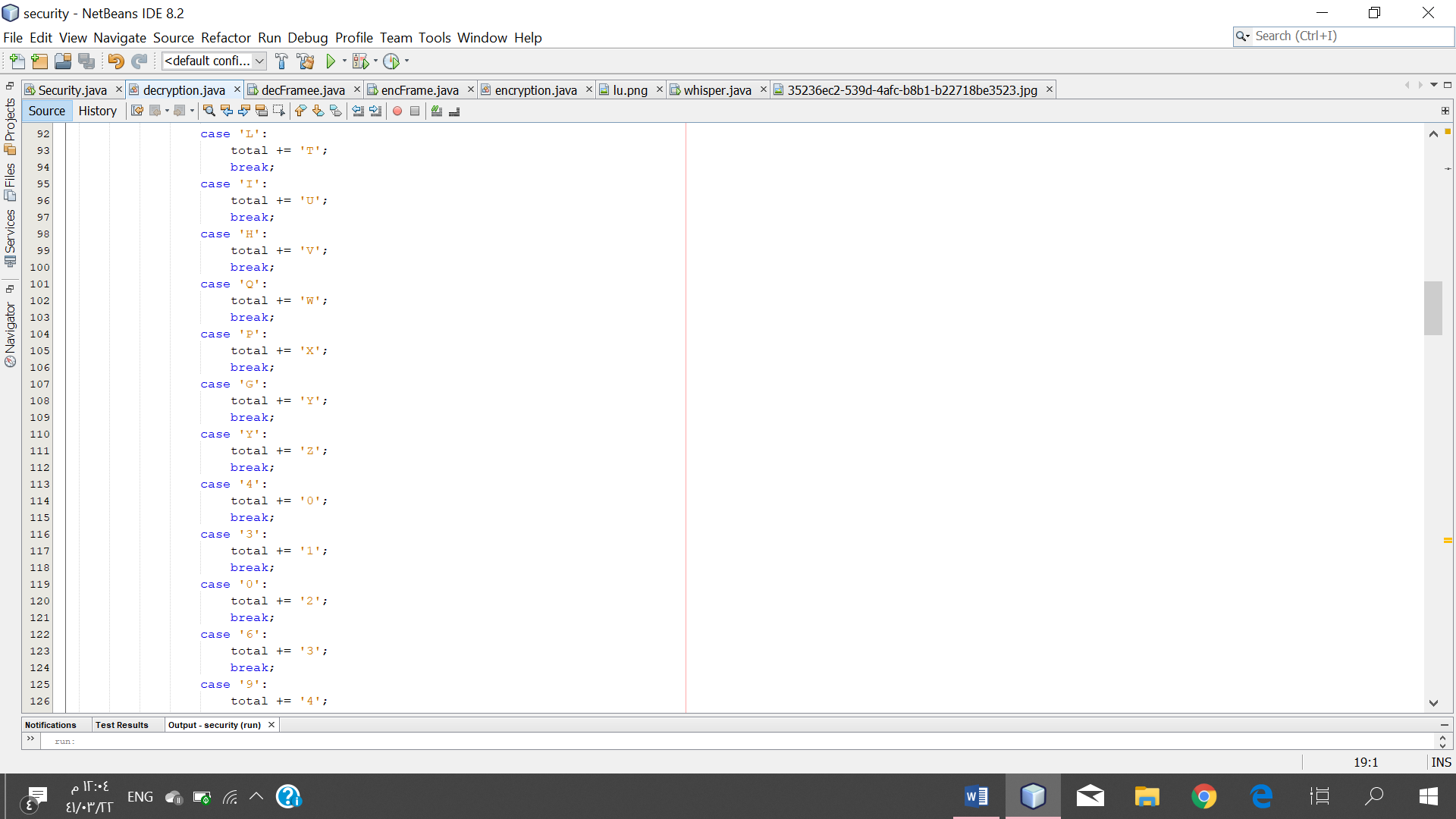
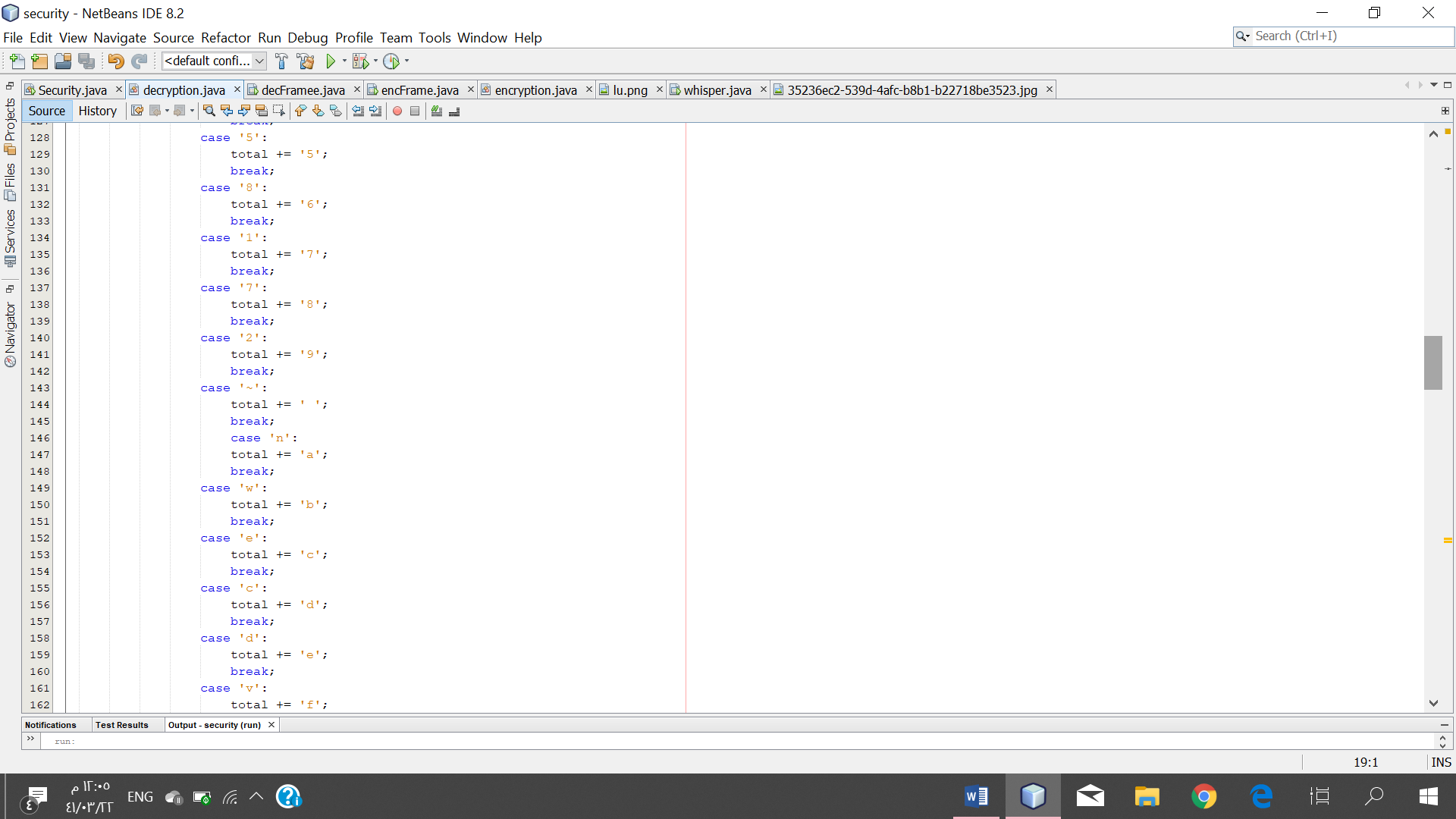
* Method (validate):

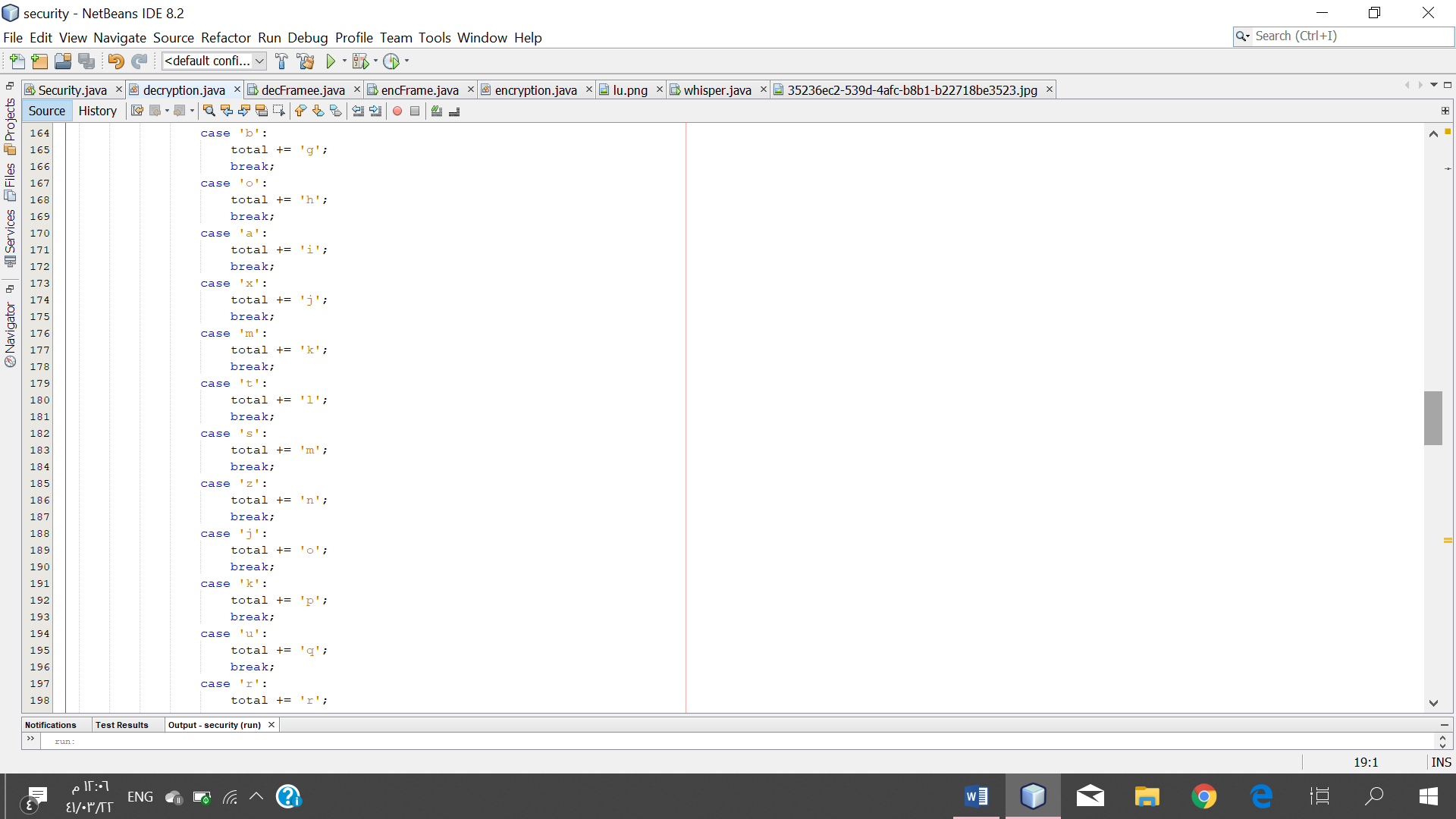
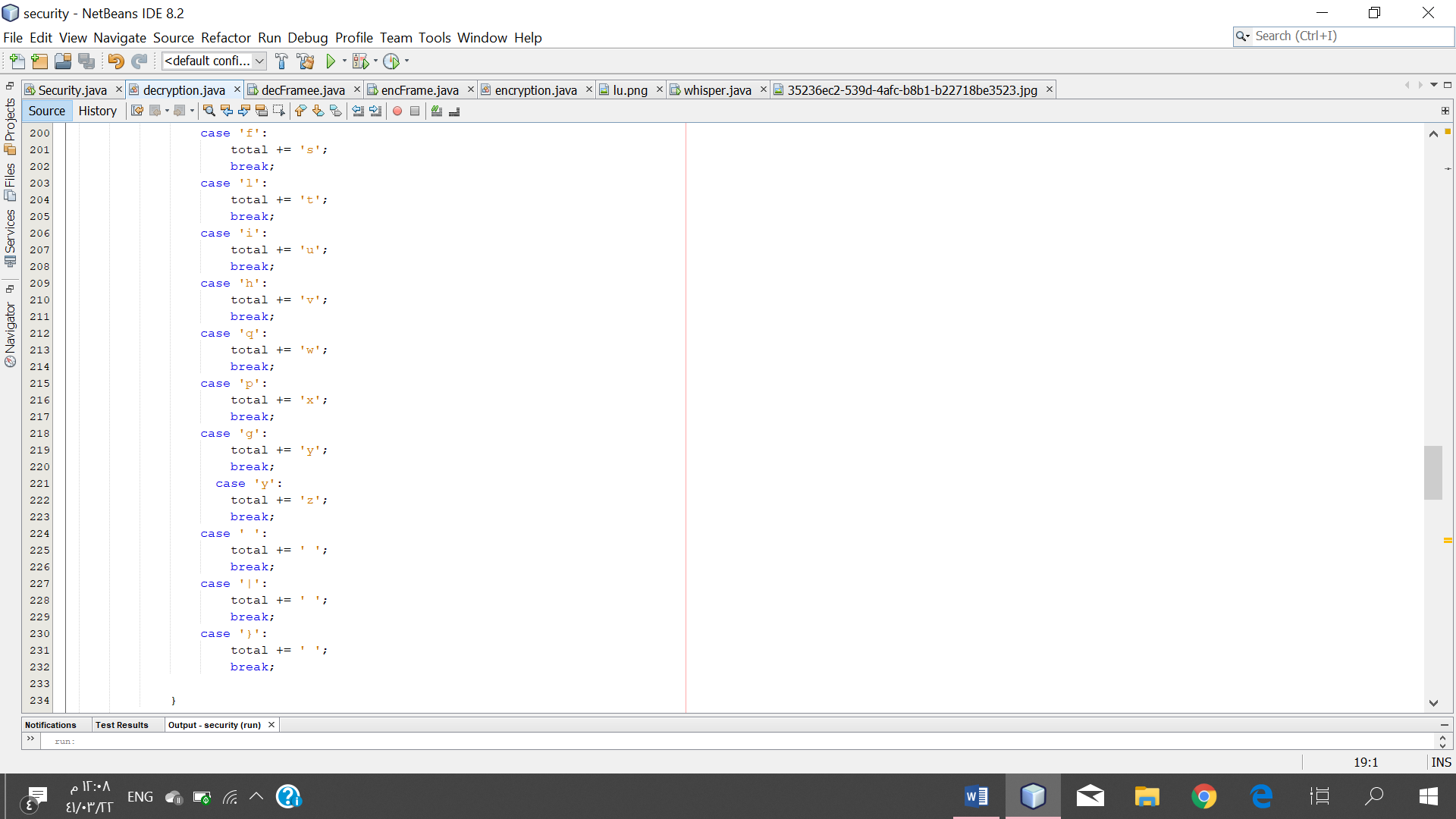


Class decryption:

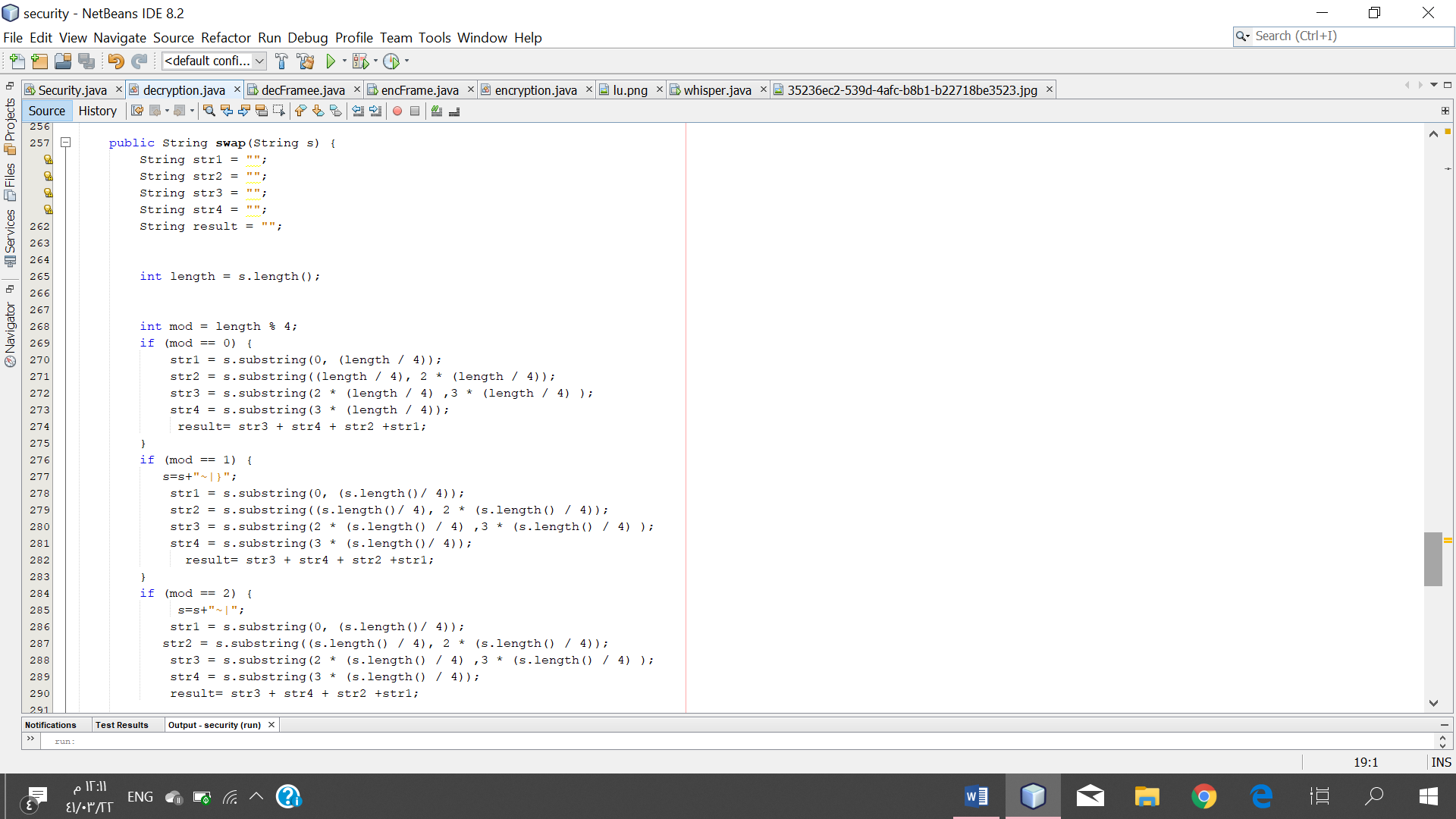
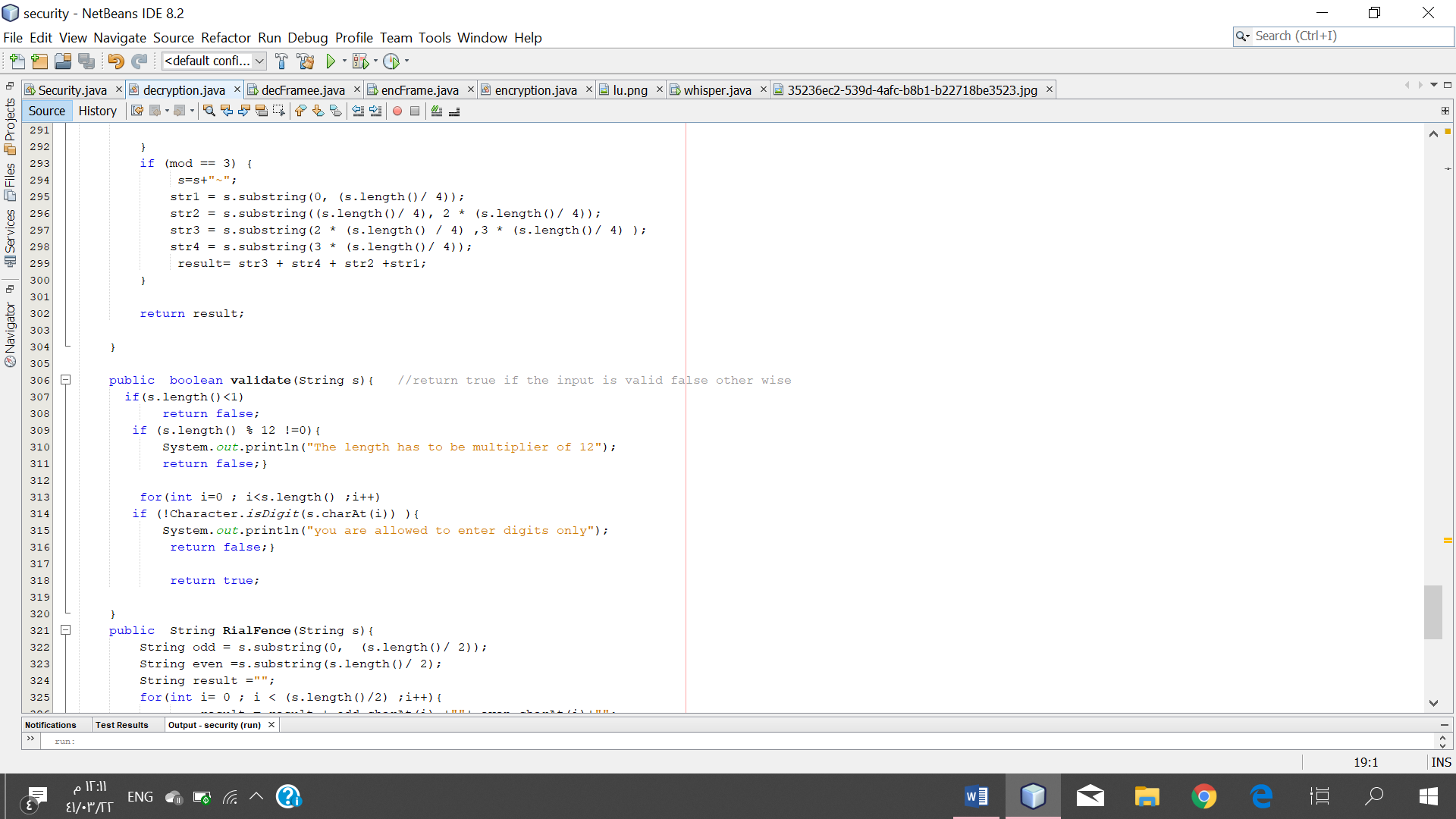
* The substitution method (convert):

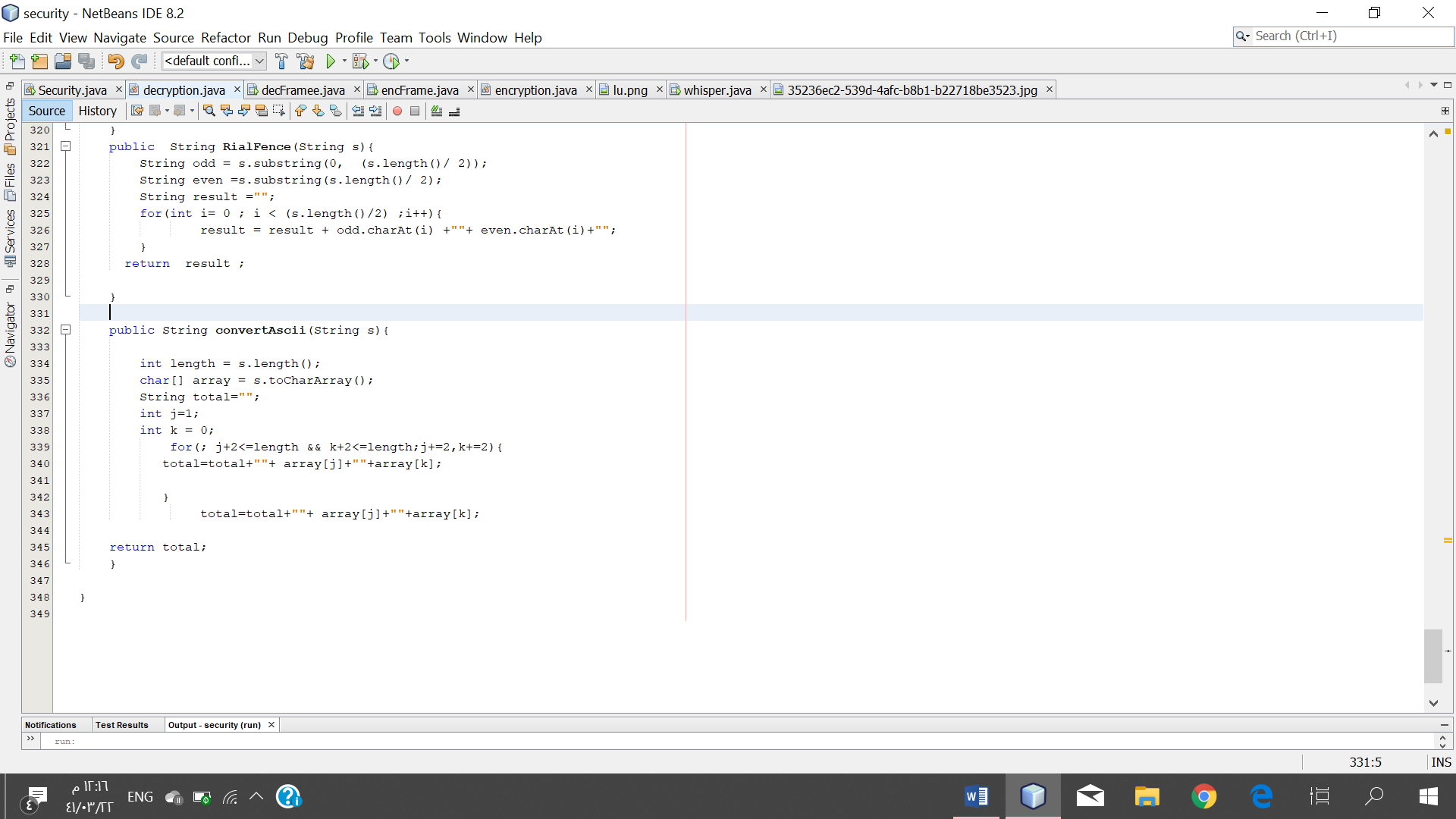
 

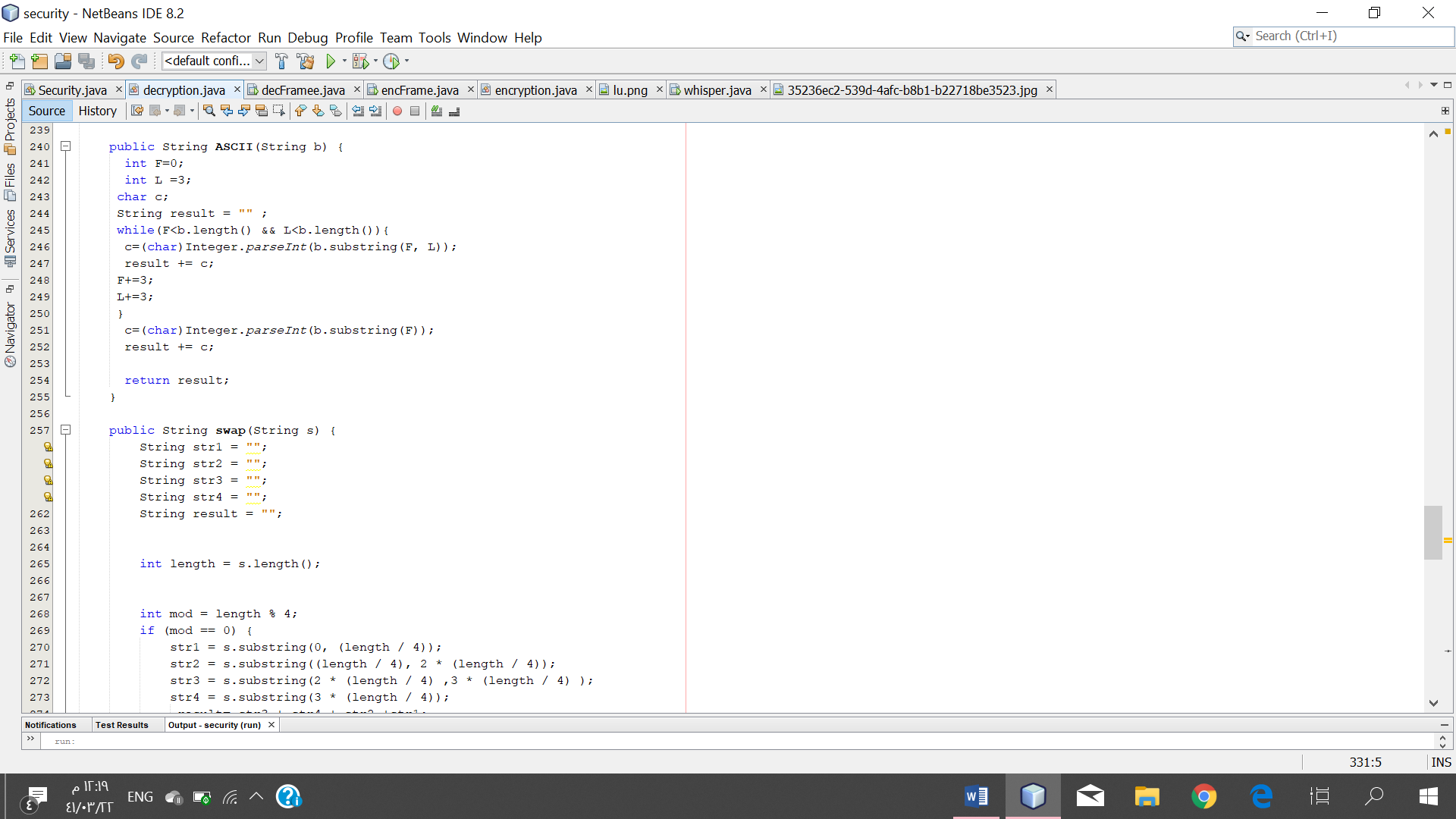
* The permutation method (swap):



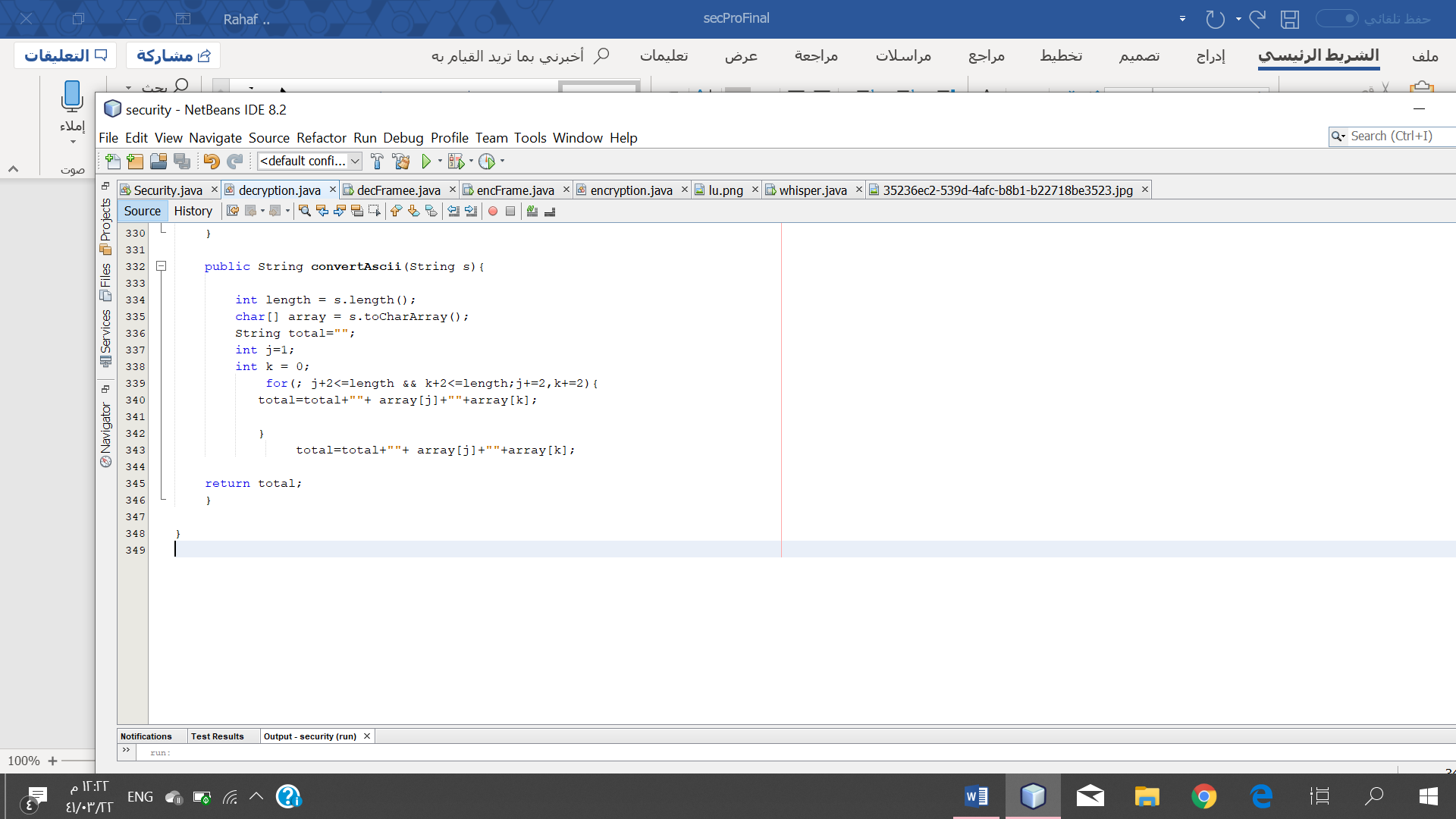
* Rail Fence method (Railfence):



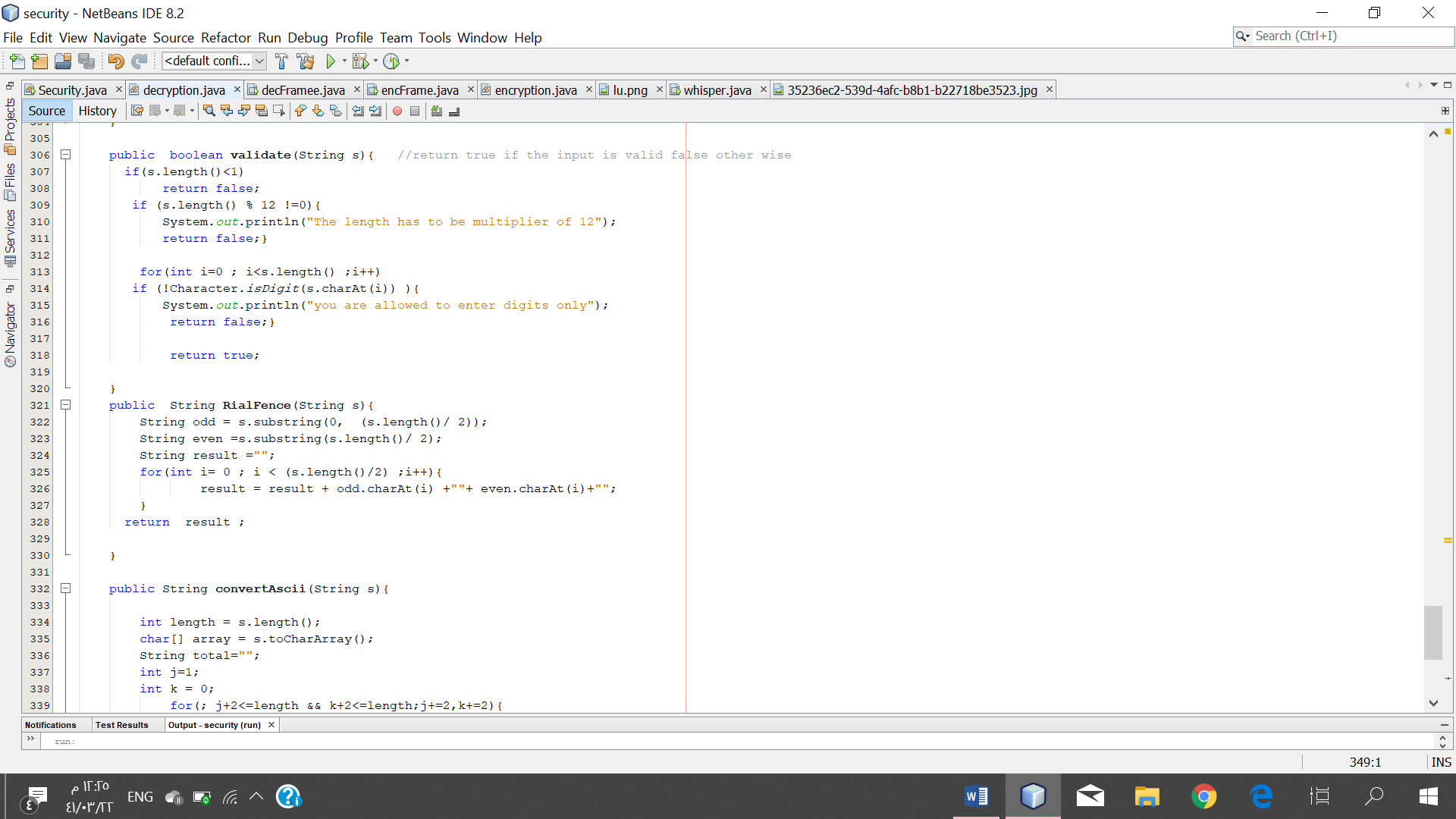
* Converting to ASCII method (ASCII):



* Swap ASCII method (convert Ascii):

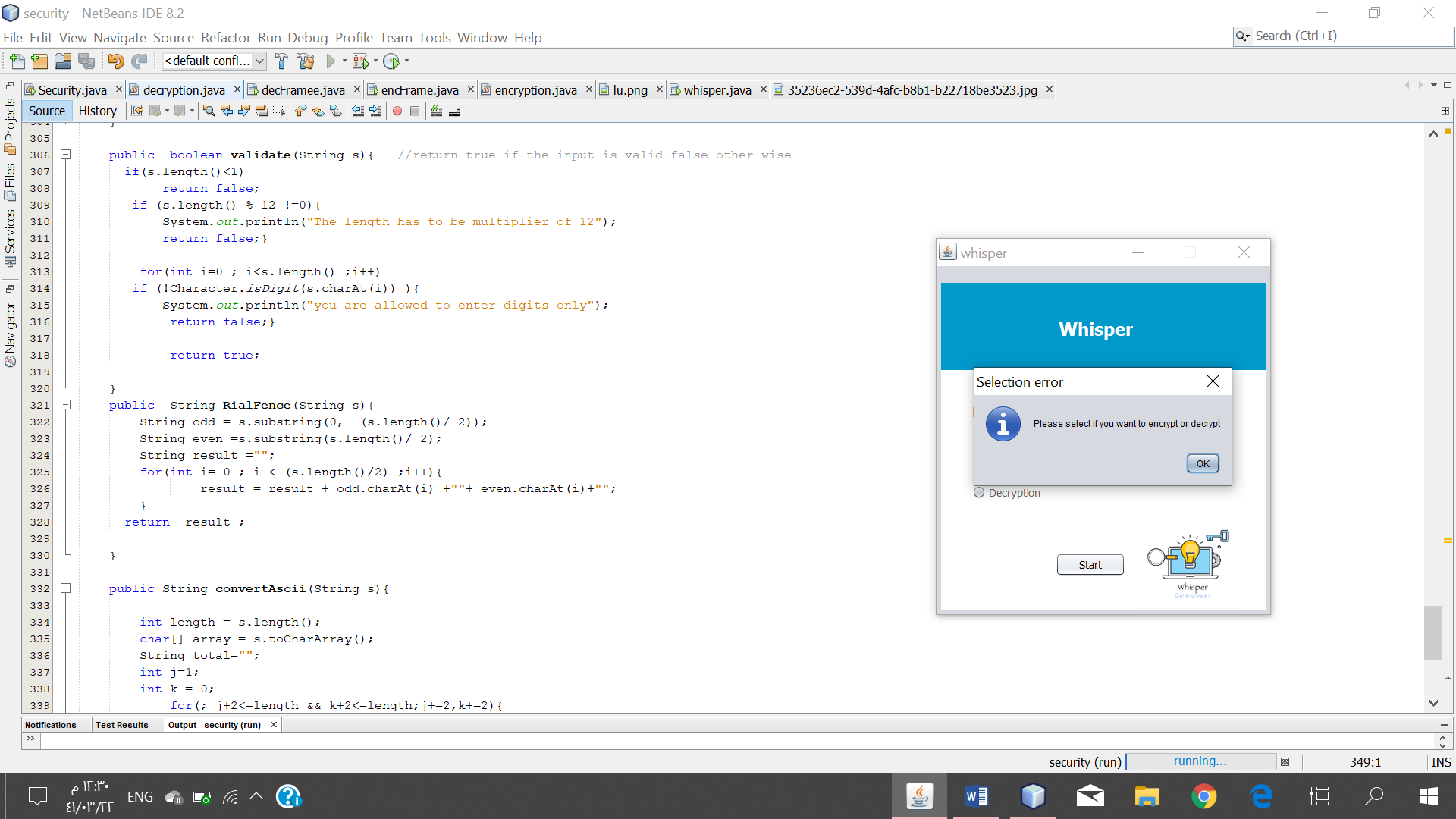


* Method (validate):



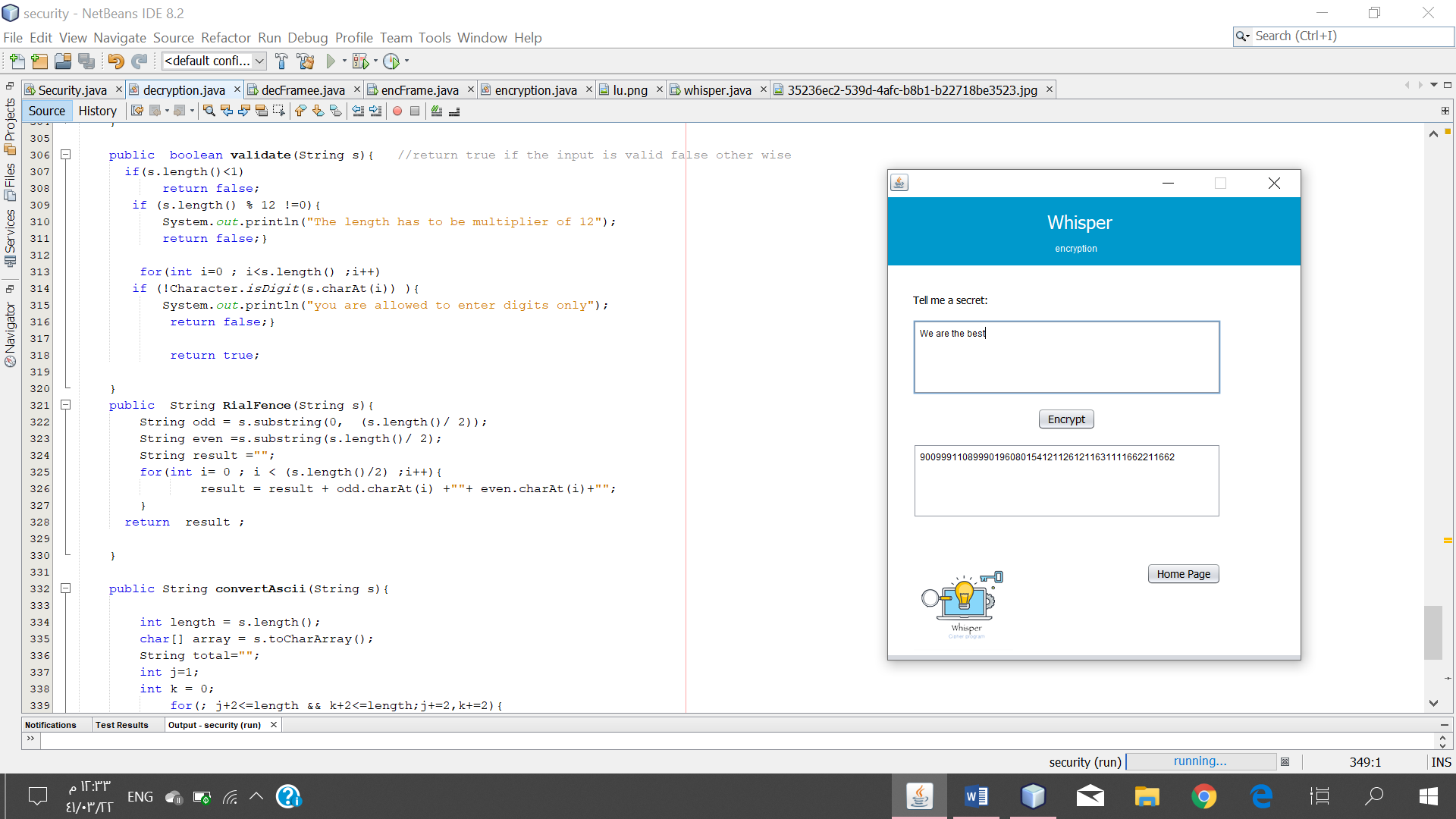
# sample of the tests:

**1- The user selects Start without selecting an option.**

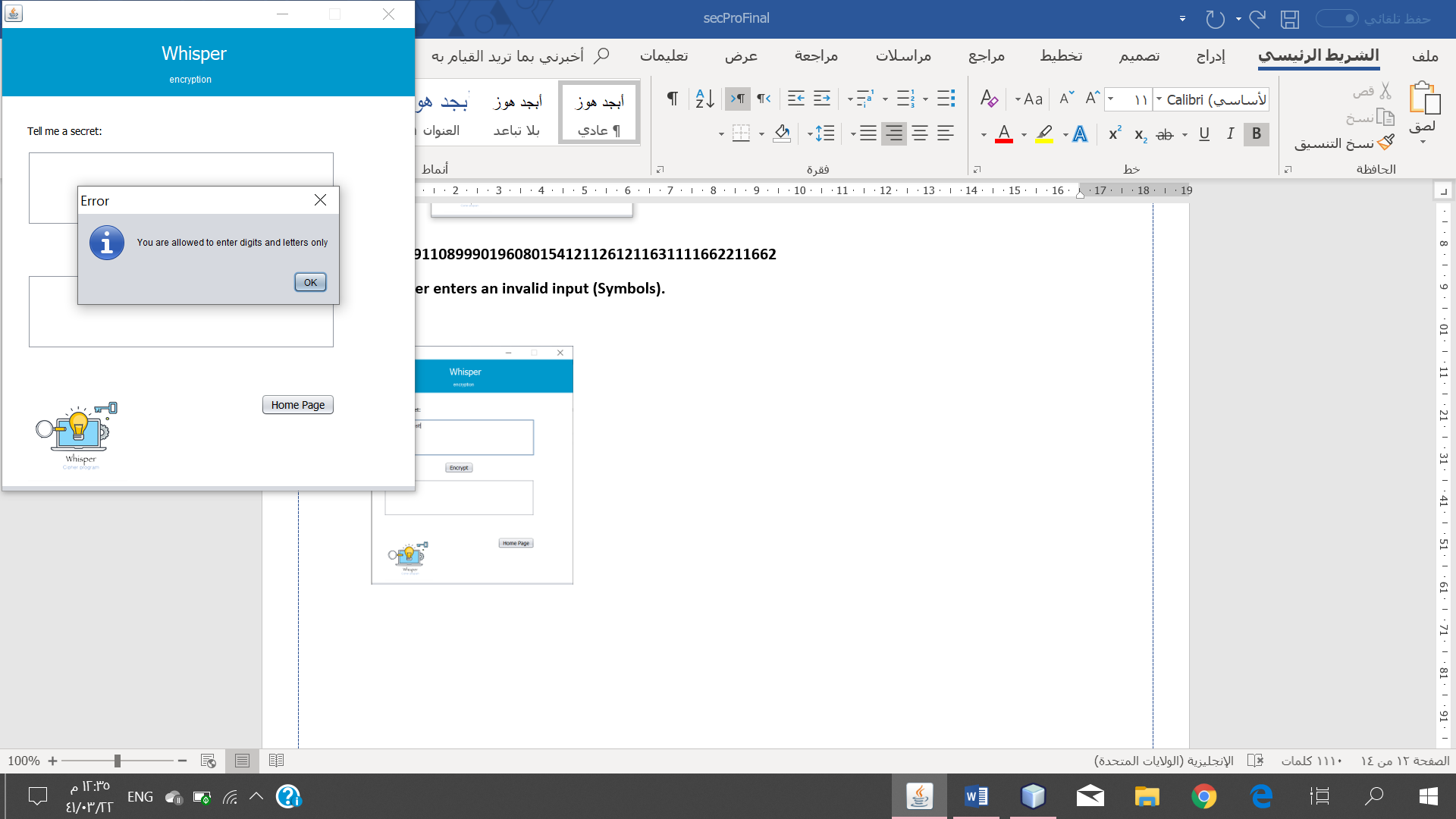
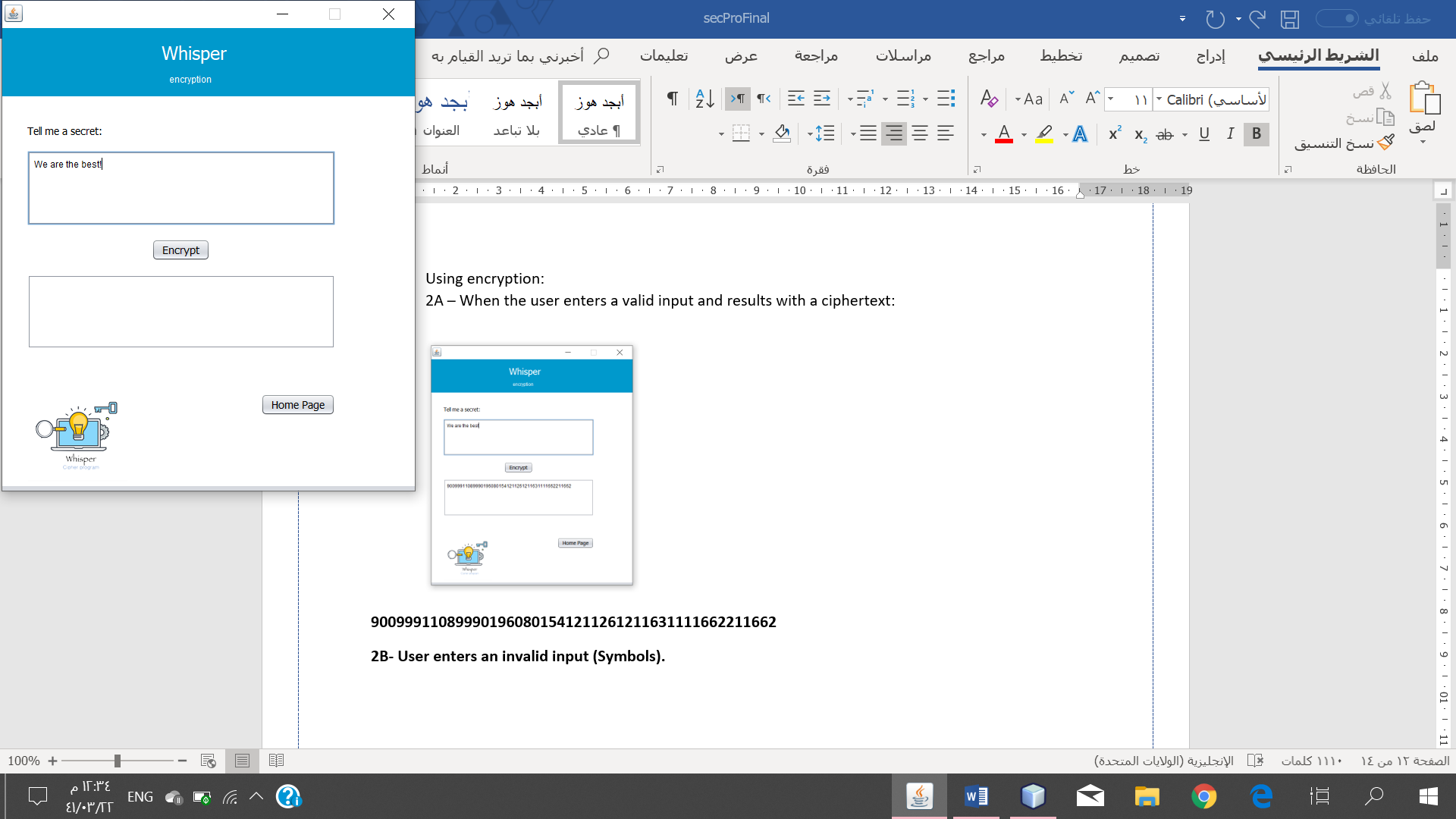


**2-Using encryption:**

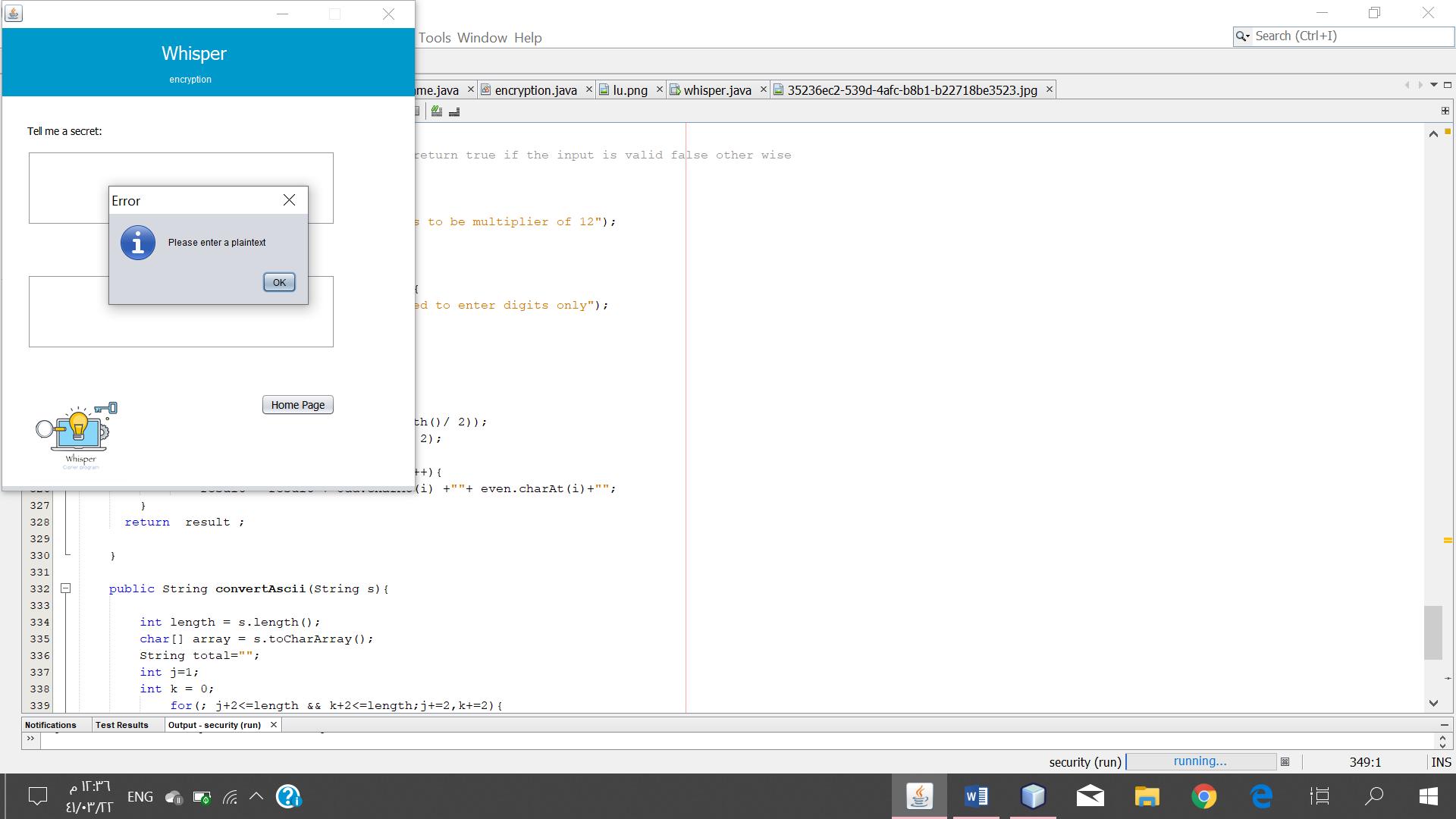
**2A – When the user enters a valid input(letters and spaces) and results with a ciphertext.**



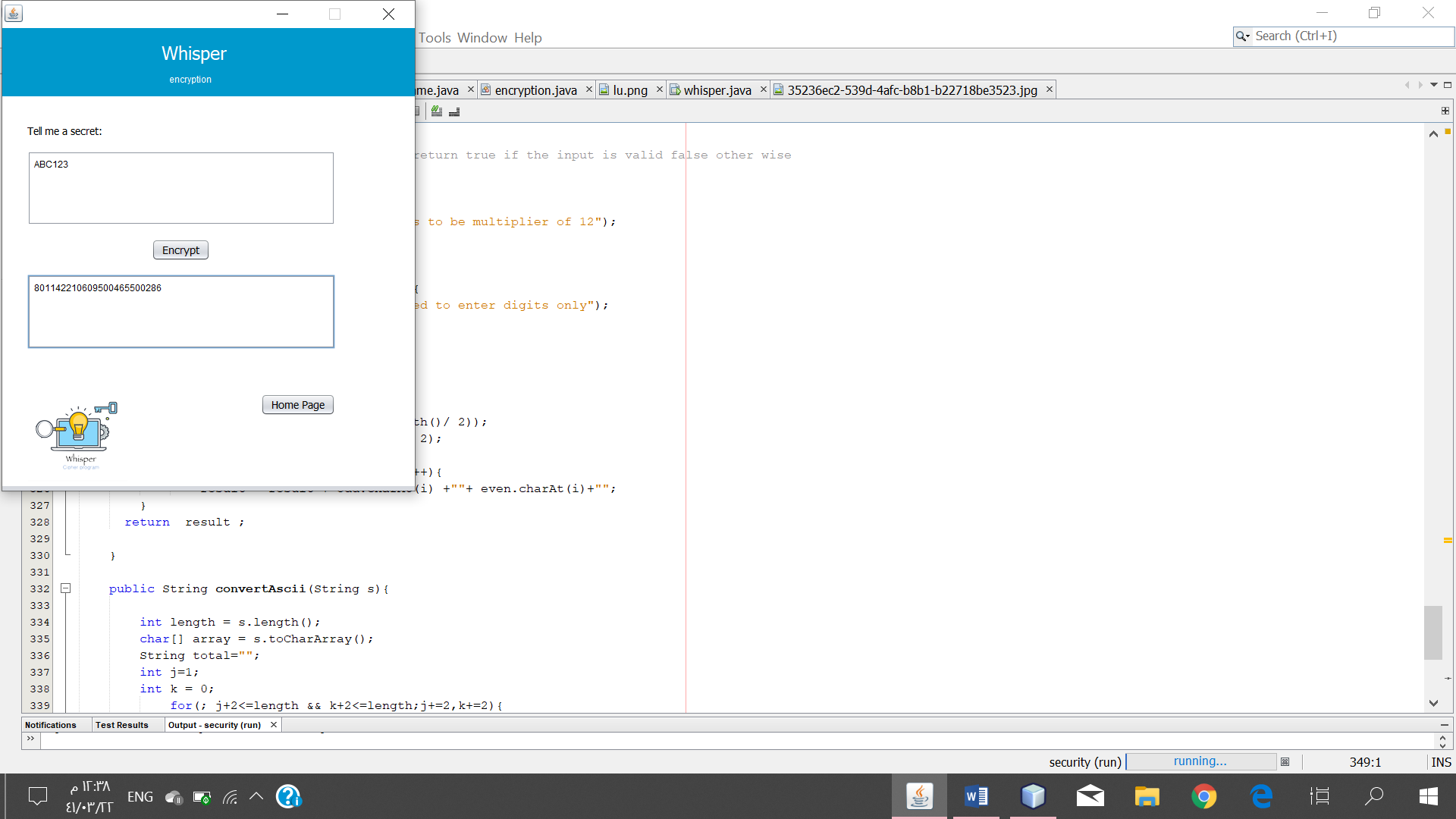
**2B- User enters an invalid input (letters with symbols).**



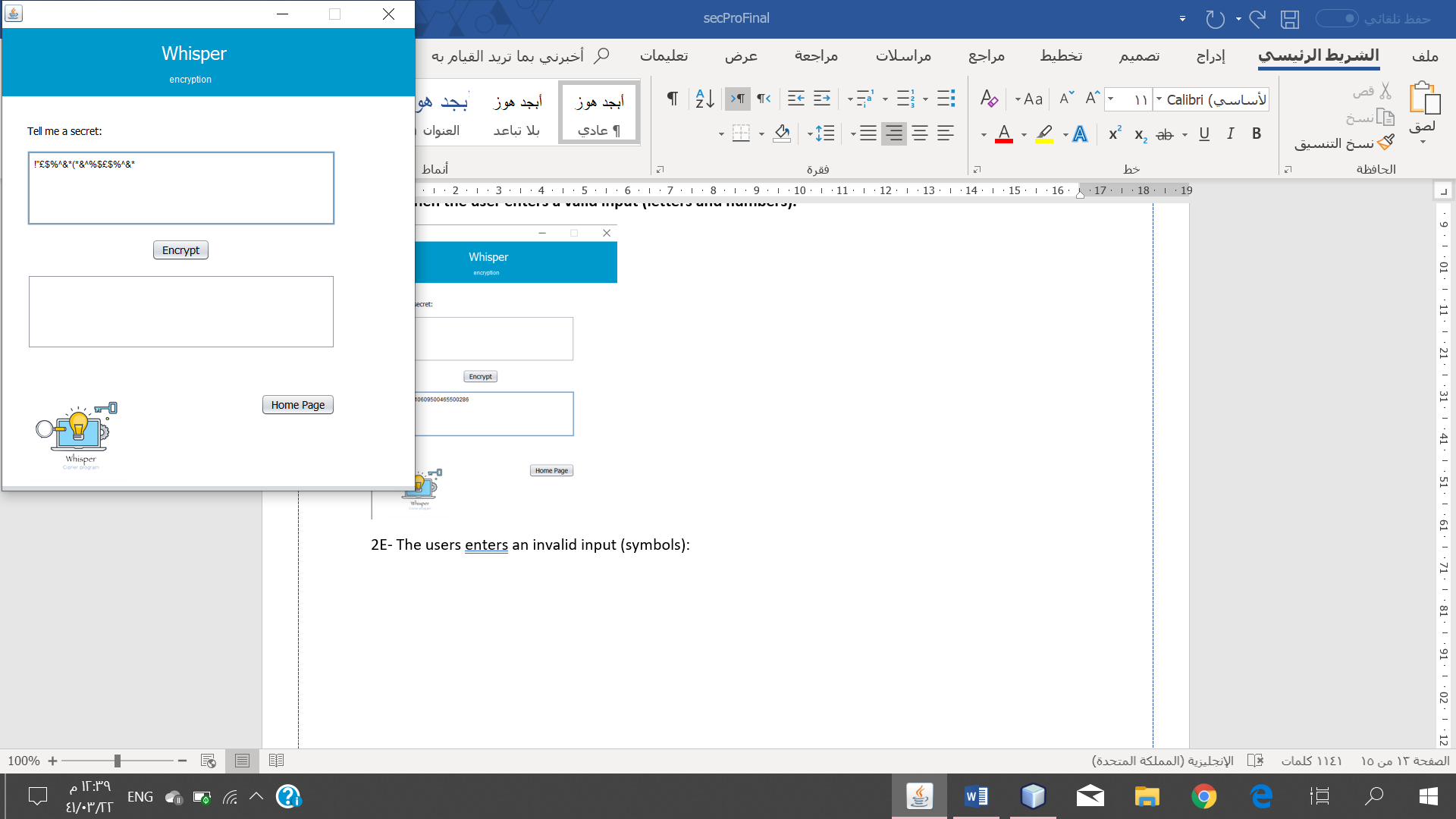
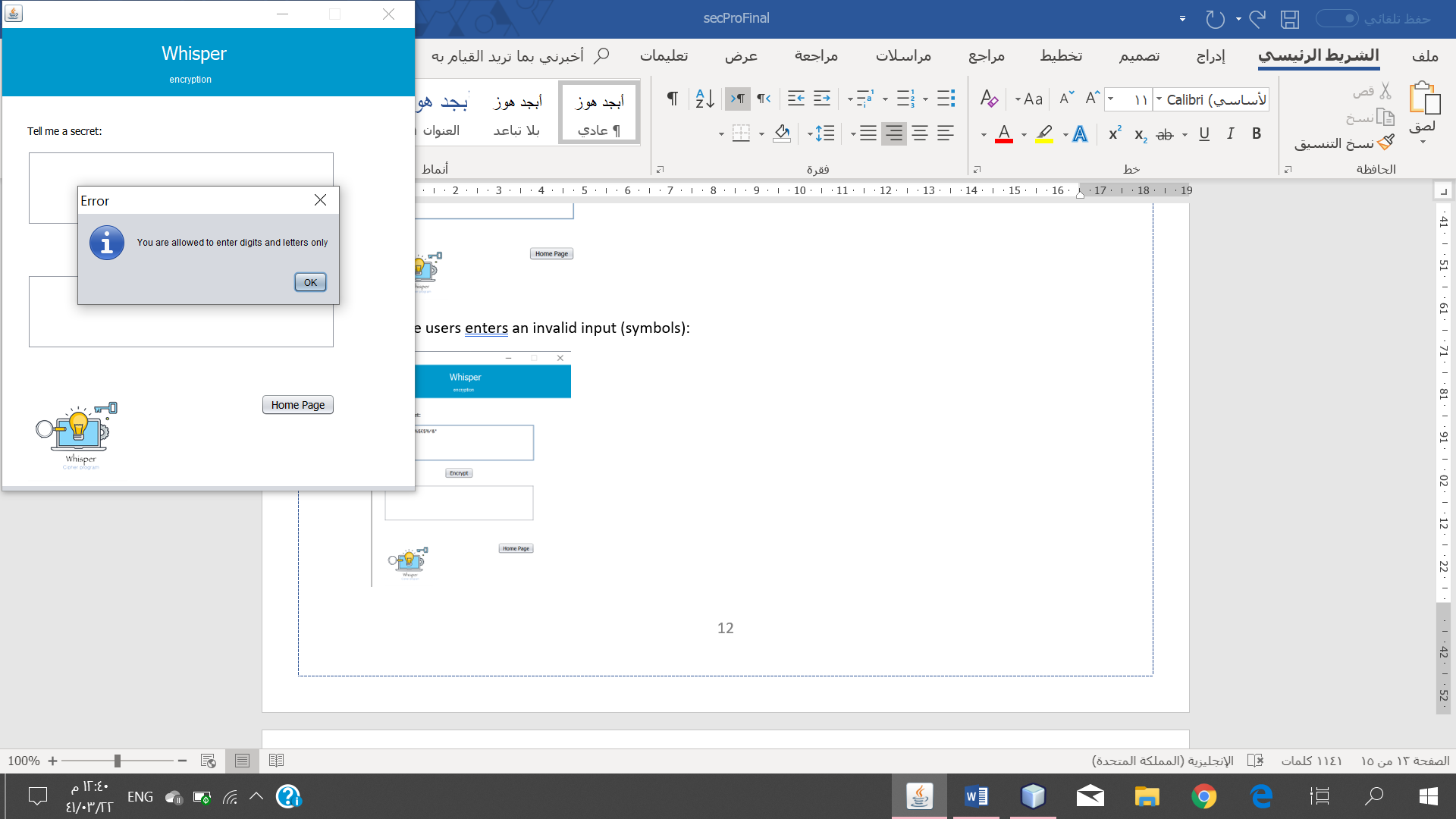
**2C- When the user selects on Encrypt without typing a plaintext.**



**2D- When the user enters a valid input (letters and numbers) and results with a ciphertext.**

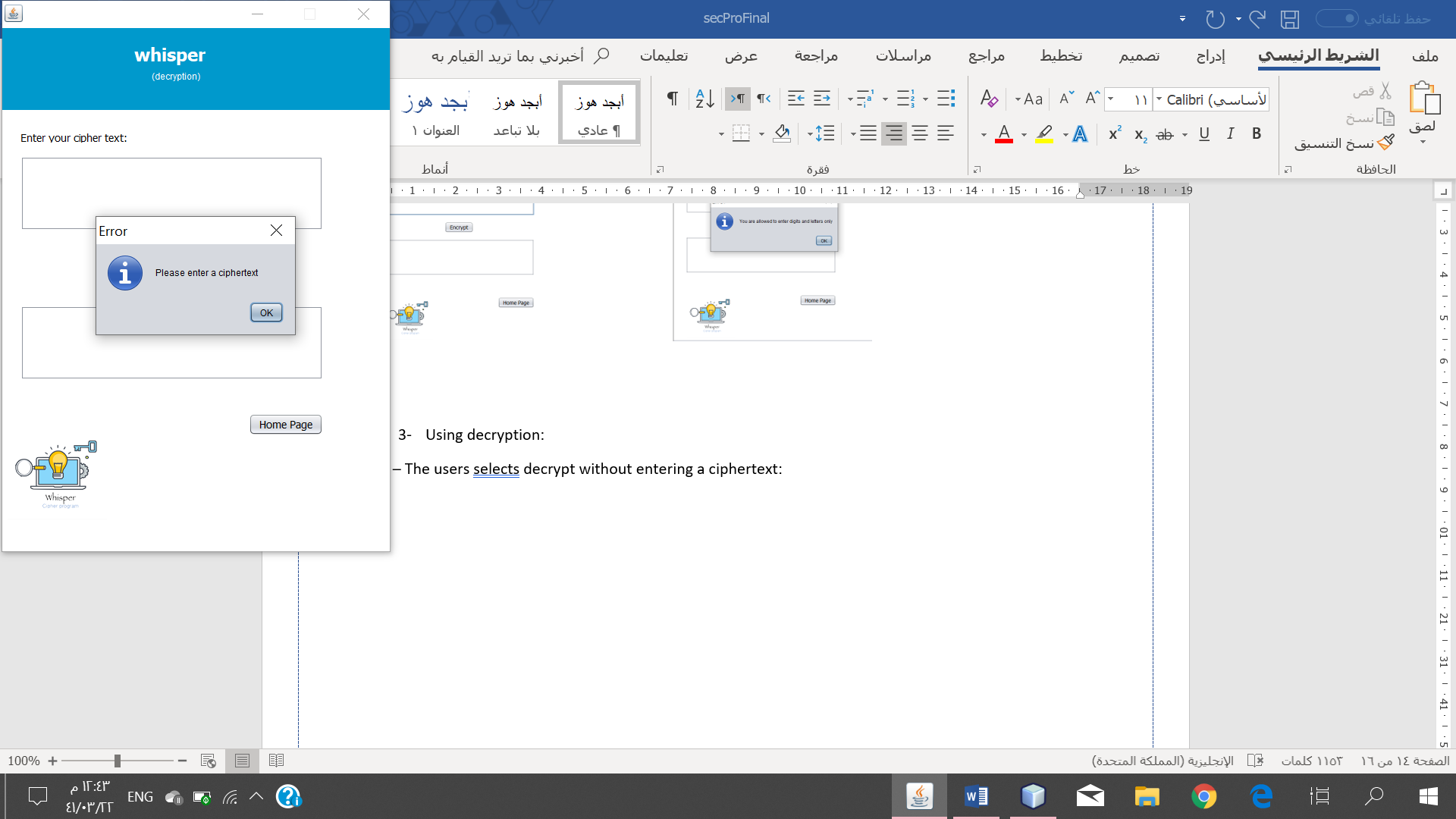


**2E- The user enters an invalid input (symbols).**

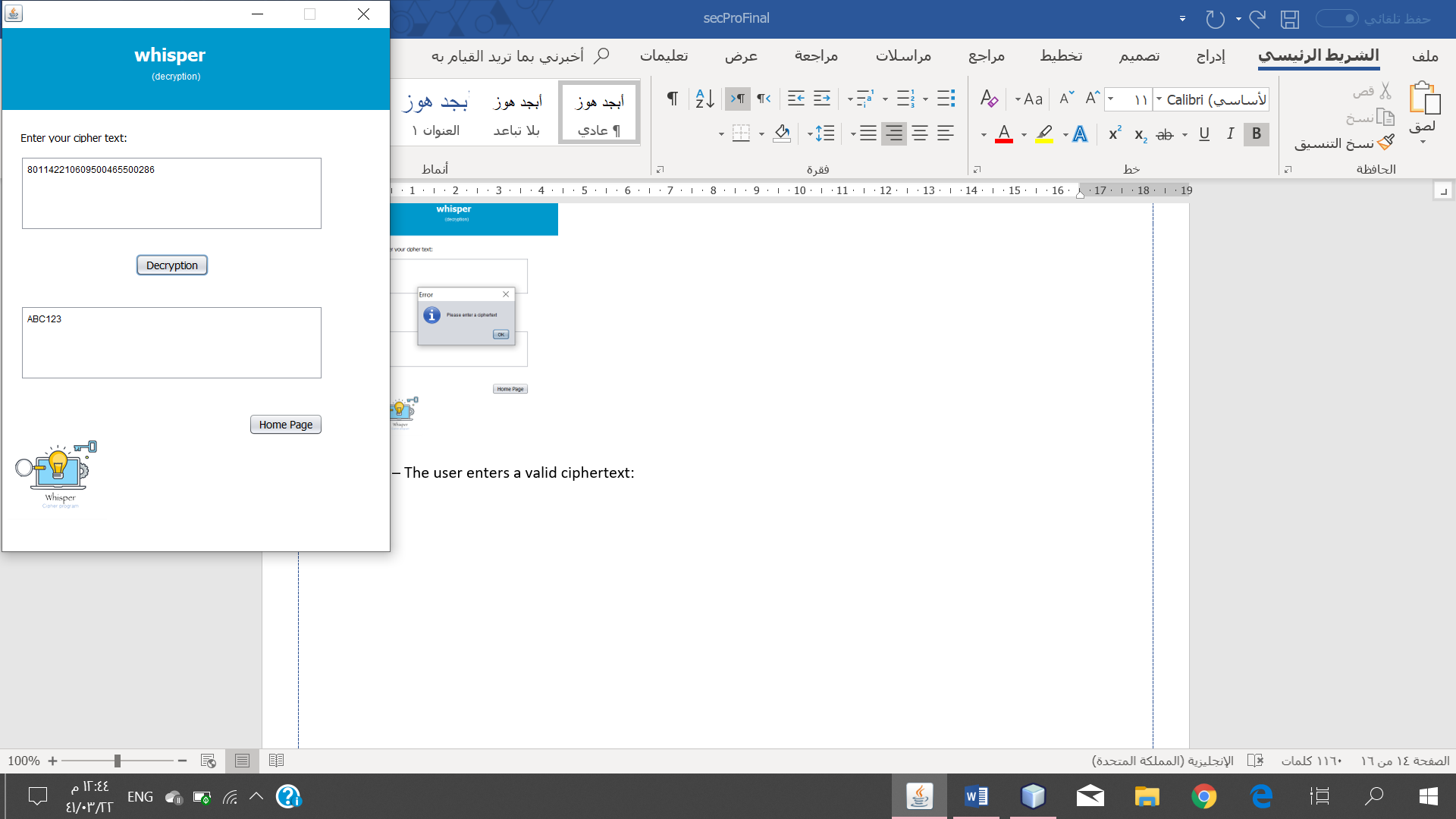
 

**3-Using decryption:**

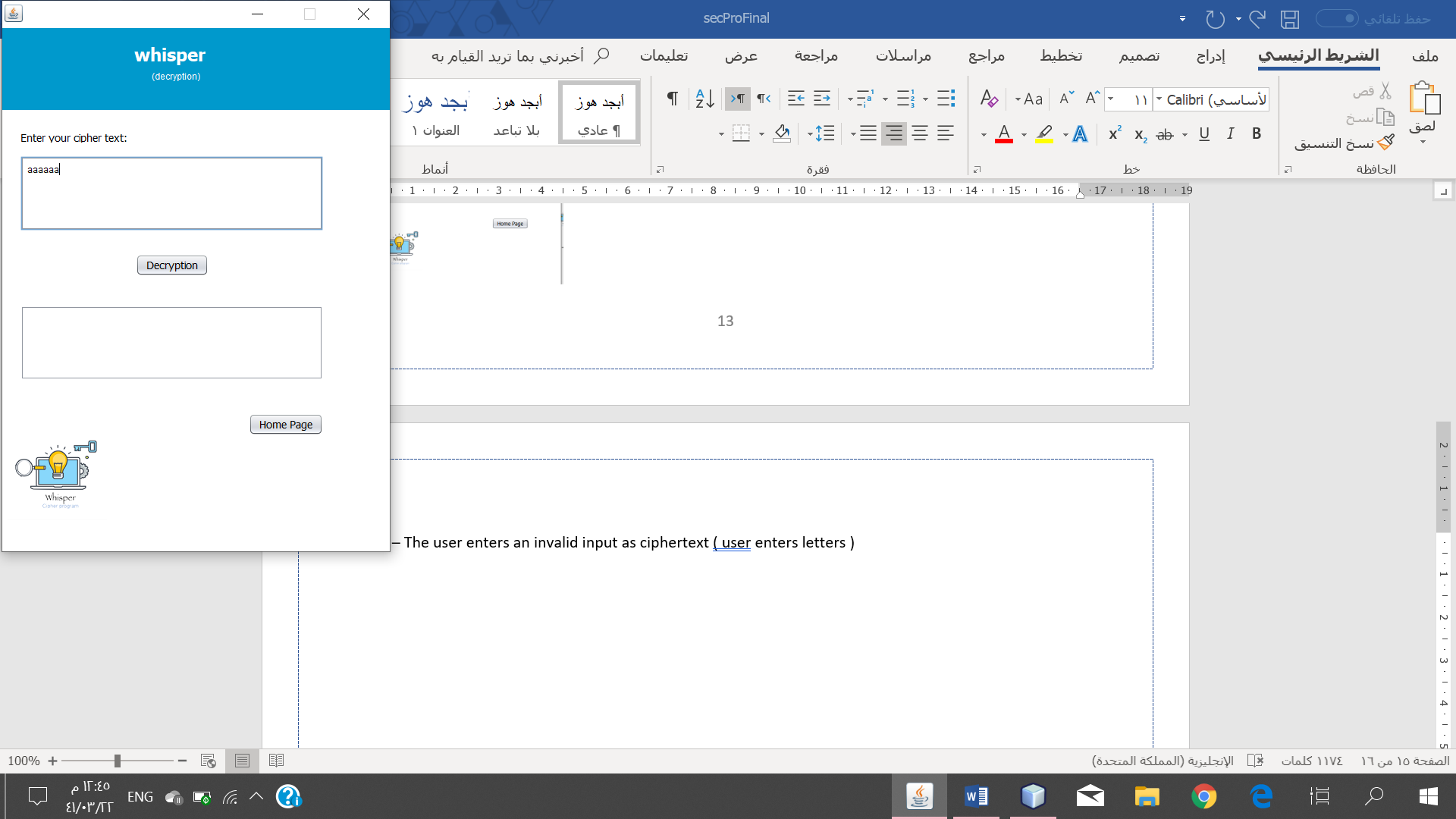
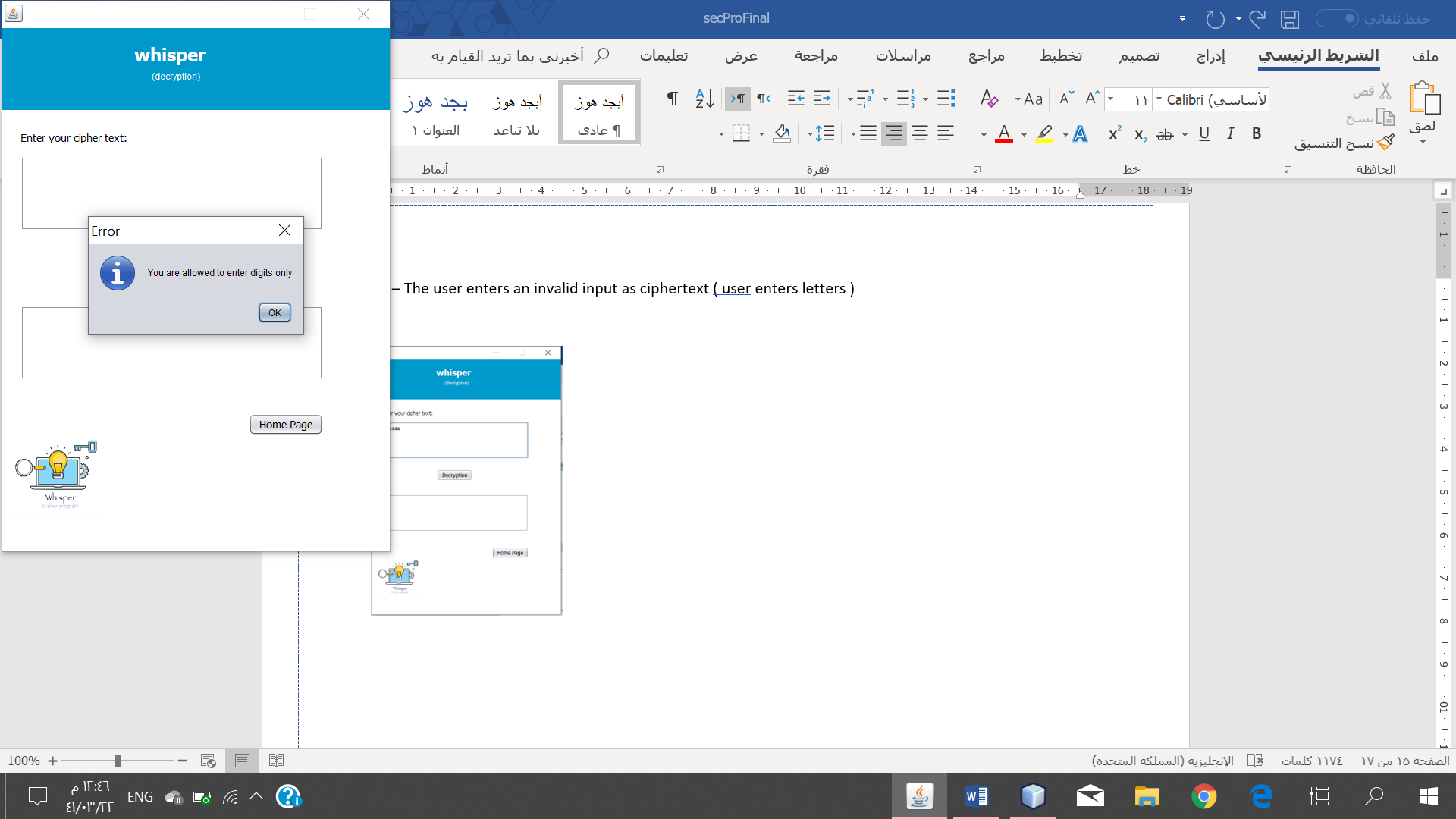
**3A – The user selects decrypt without entering a ciphertext.**



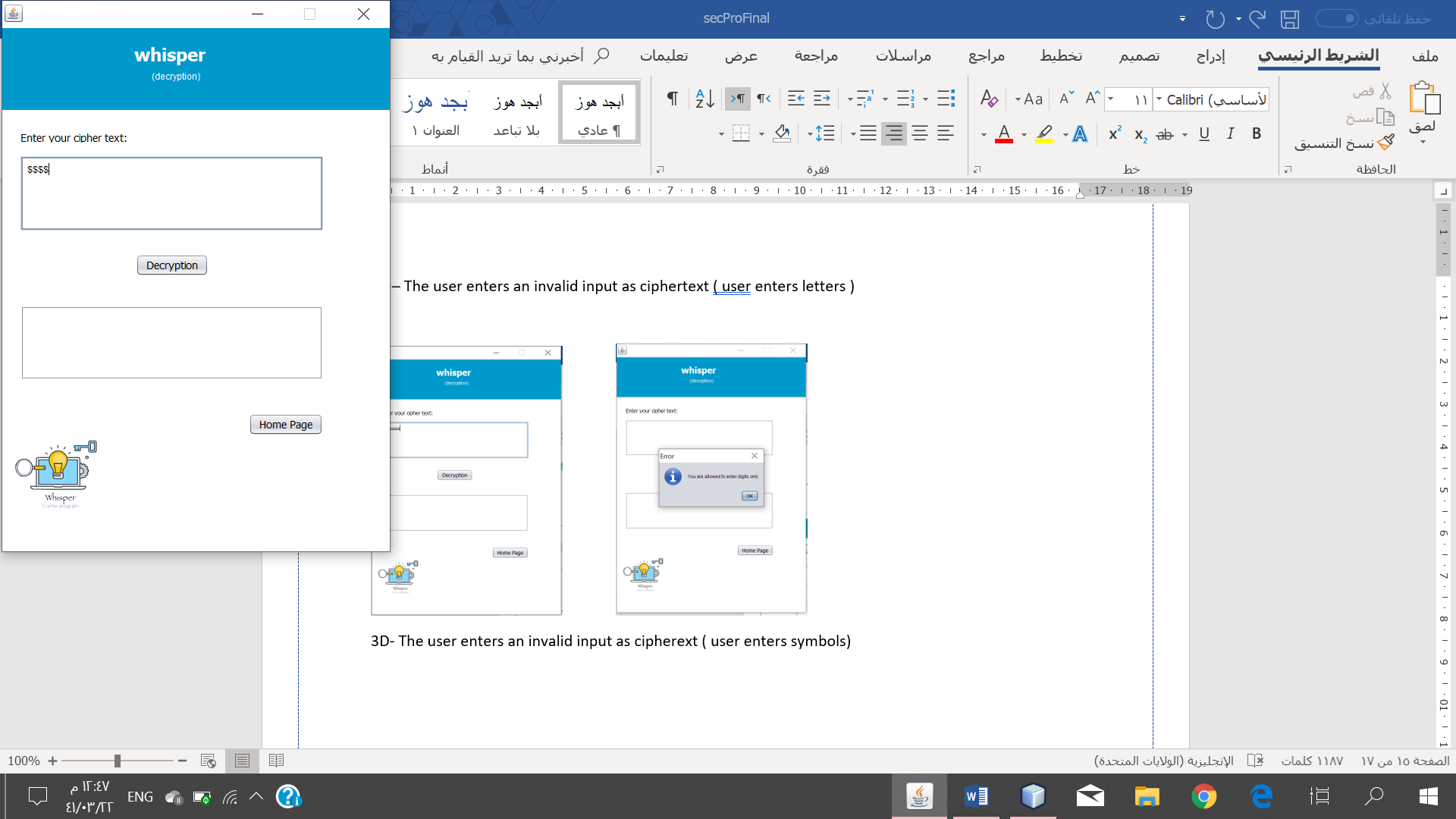
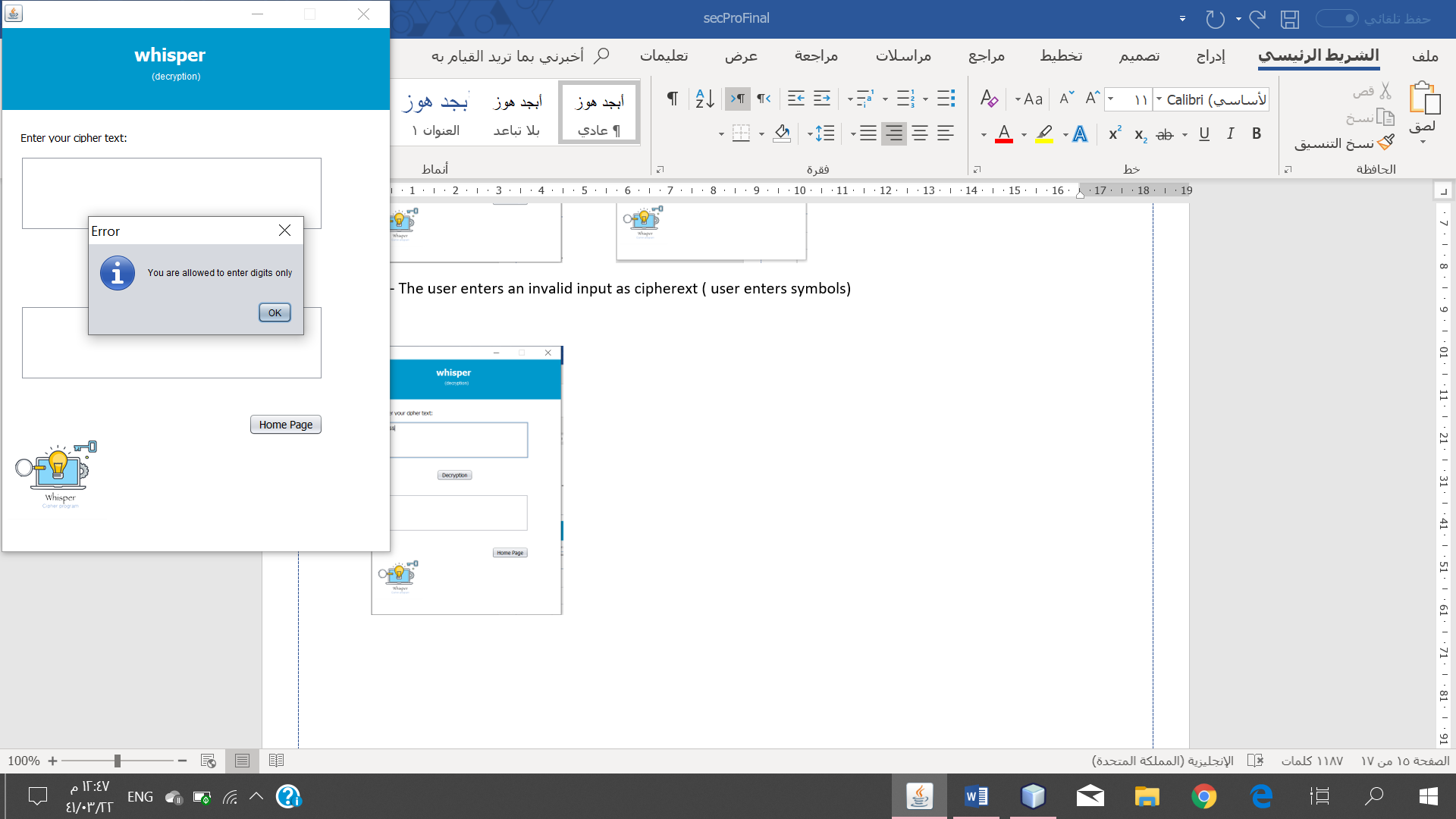
**3B – The user enters a valid ciphertext and results with a plaintext.**



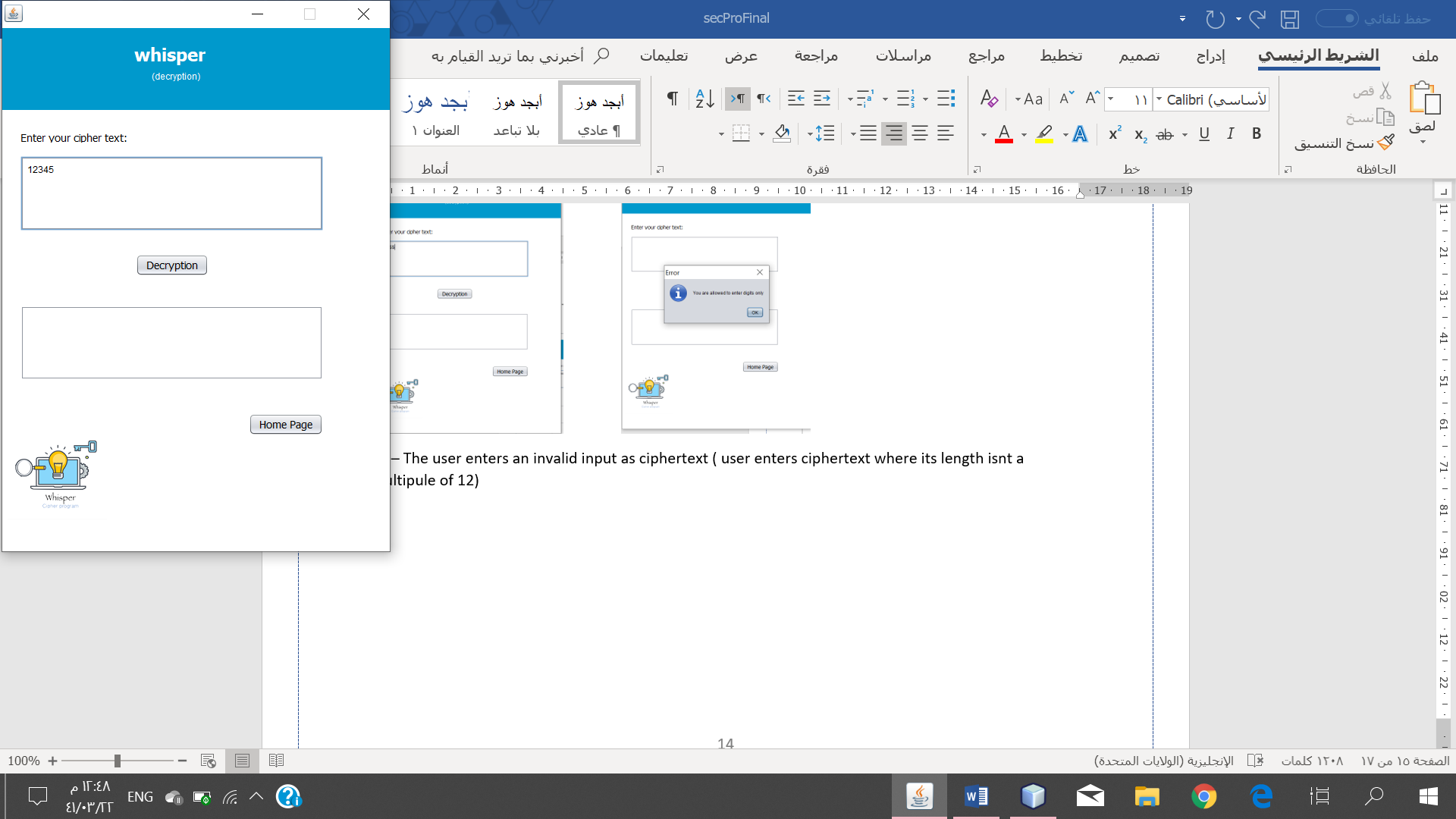
**3C – The user enters an invalid input as ciphertext (user enters letters).**

**3D- The user enters an invalid input as cipherext ( user enters symbols).**

**3E – The user enters an invalid input as ciphertext ( user enters ciphertext where its length isnt a multipule of 12).**

**3F- The user enters an invalid input as ciphertext ( user enters a ciphertext that the system does not recognize).**



At the end, as a team, we have a great experience to work together on this project. And we saw that Whisper has more than three components and it can encrypt and decrypt both letters (dealing with capital and small letters) and numbers which make it a strong model, the two rounds influence the strength of the model. Because of these reasons, Whisper system achieved the goal of security and protected the valuable information.

# References :

[1] Richardson, T. and Thies, C. (2013). *Secure software design*. Burlington, Mass.: Jones & Bartlett Learning.

[2] Wu, C. (2010). *An introduction to object-oriented programming with Java*. 5th ed. New York: McGraw-Hill Higher Education.

[3] C. Baziotis, “How to go back to a JFrames in Java,” Stack Overflow, 01-Mar-1962. [Online]. Available: https://stackoverflow.com/questions/8771558/how-to-go-back-to-a-jframes-in-java/8771756. [Accessed: 18-Nov-2019].

[4] P. K. P. Kharbuja, “How to add radio buttons in button group?,” Stack Overflow, 01-Feb-1963. [Online]. Available: https://stackoverflow.com/questions/13832209/how-to-add-radio-buttons-in-button-group. [Accessed: 18-Nov-2019].

[5] Java #N3 - Making a GUI in NetBeans. [Online]. Available: https://www.youtube.com/watch?v=LFr06ZKIpSM. [Accessed: 18-Nov-2019].

[6] "GUI Programming - Java Programming Tutorial", *Ntu.edu.sg*, 2019. [Online]. Available: https://www.ntu.edu.sg/home/ehchua/programming/java/J4a\_GUI.html. [Accessed: 19- Nov- 2019].

[7] J. resizing?, Z. Junejo, I. Gaur, B. Vijay, C. Latte and D. Gavkar, "JFrame: How to disable window resizing?", *Stack Overflow*, 2019. [Online]. Available: https://stackoverflow.com/questions/18031704/jframe-how-to-disable-window-resizing. [Accessed: 19- Nov- 2019].

[8] J. NetBeans, A. Thompson and Y. K., "JFrame Resizing in Desktop Application - NetBeans", *Stack Overflow*, 2019. [Online]. Available: https://stackoverflow.com/questions/8265548/jframe-resizing-in-desktop-application-netbeans. [Accessed: 19- Nov- 2019].