**Network Security**

**Student Name: Emmanuel Opara**

**Eagle ID: 900-**

**Module 02 – Ciphers – DES – AES (50 points)**

1. **Find a research article using university’s online digital library.** (10 points)
   1. Go to Georgia Southern University Library homepage at <http://library.georgiasouthern.edu/> (make sure you have already logged into mygeorgiasouthern portal)
   2. Through the **A-Z Databases (under “Research Services and Collections”)** find the **ACM Digital Library** (under letter “A”) where you can search for articles
   3. Use the keyword search function to search for papers related to **AES** cipher
   4. On the results page, use the “**Publication Date**” filter on the left to narrow down your search to papers published in the **past 2 years**; then sort the results using “Cited” instead of “Relevance” by default.
   5. Click on a(n) paper/article (not a proceeding) in the list, then in the newly opened paper page browse the **abstract** and **author information**
   6. Find and use the “Export Citation” feature above the Abstract to export the citation in ACM Ref format. Copy the citation reference and paste it below (this is the reference, in ACM Reference format, listed at the end of another paper manuscript citing this paper)

**Eakachai Charoenchaimonkon, Paul Janecek, and Vatcharin Hamratanaphon. 2009. Using advanced encryption standard to secure the content dissemination of electronic Braille books. In Proceedings of the 3rd International Convention on Rehabilitation Engineering &amp; Assistive Technology (i-CREATe '09). Association for Computing Machinery, New York, NY, USA, Article 32, 1–5. https://doi.org/10.1145/1592700.1592737**

* 1. Specify **what keywords** you have used for the search and the **total citations** (as a number found on the paper page) of the paper.

**Keywords: Advanced Encryption standard**

**Citations:5**

1. **Data Encryption Standard (DES).** Go to <http://des.online-domain-tools.com/> where you can encrypt plaintext or file using a list of different **symmetric key** ciphers. Try DES encryption using **different keys** and **input values/lengths**, then answer the questions below. (5 points for each question, 20 points in total)
   1. What (choose from: length of plaintext, content of plaintext, and/or content/value of key) affect(s) the length of ciphertext?

**After inputting the plain text, I observed that the length of the input plaintext affects the ciphertext although the content of the plaintext affects the ciphertext itself it doesn’t affect the length of the ciphertext.**

* 1. What (choose from: length of plaintext, content of plaintext, and/or content/value of key) affect(s) the content of ciphertext?

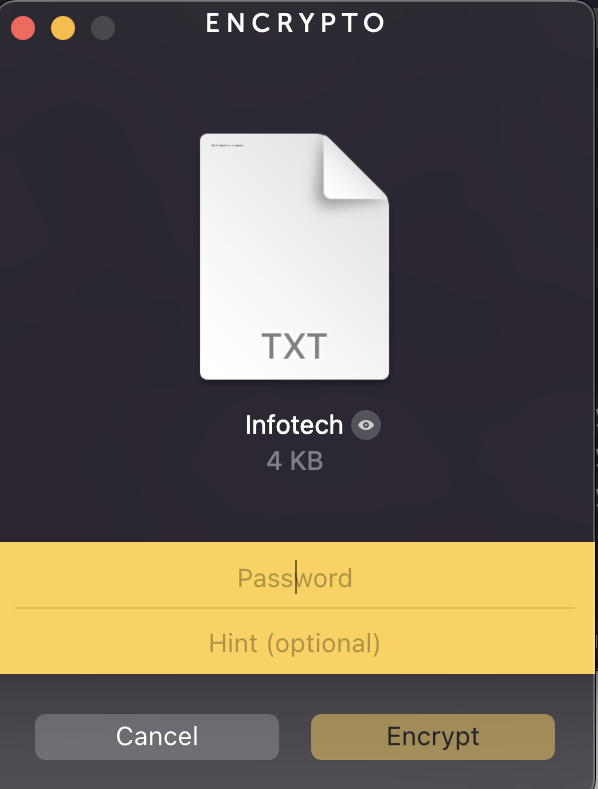
The ciphertext is affected by the **content of plaintext and value of key** .

* 1. What happens to the ciphertext when plaintext changes from 7 characters to 8 characters, and then to 9 characters in length? What do you think is the reason for this (hint: DES is a block cipher, refer to lecture slides)?

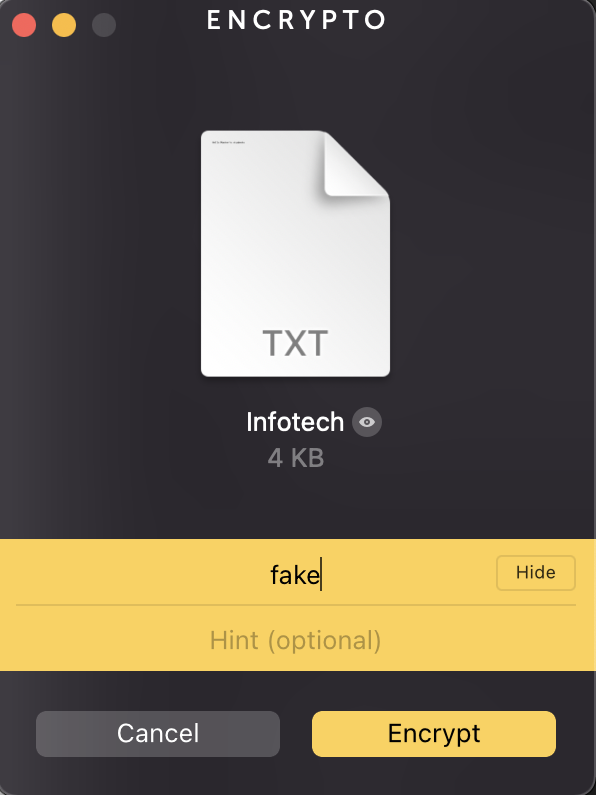
When the plaintext is 7 characters the ciphertext is also 8 hexadecimal characters, when the plaintext is 8 characters the cipher text is also 8 characters however when the plaintext is 9 characters in length the cipher text becomes 16 hexadecimal characters, this is because DES is a block by block cipher which takes a 6-bit block as input and yields a 4-bit block as output so because the 9 characters is greater than the initial 4 bit block it iterates by 1 and adds another using the key space of 2^n == 2^4 == 16 this make it have 16 characters in the ciphertext

* 1. Search on Google then download and install **MEO Encryption Software version 2.17**. Attach screenshots to show that you can encrypt a file (e.g., a .txt file with some random content in it) using DES with a chosen key and decrypt it back to plaintext with the same key.

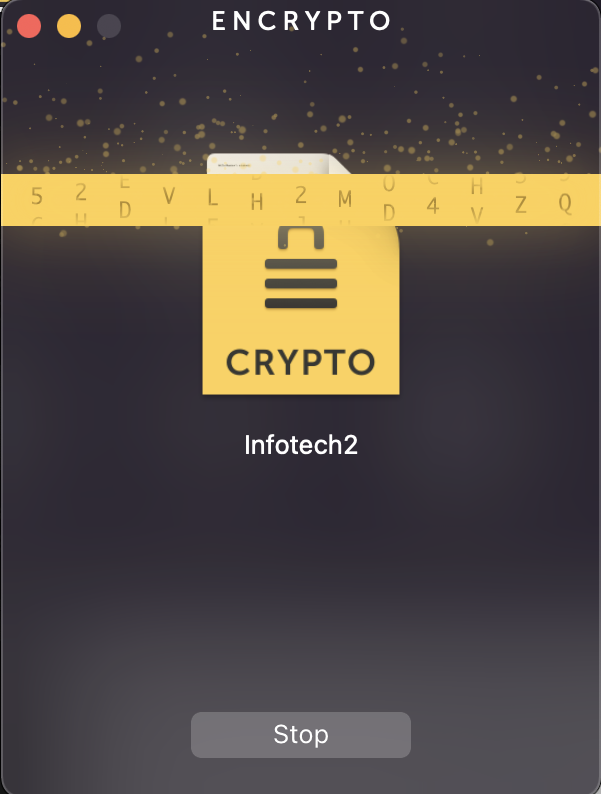
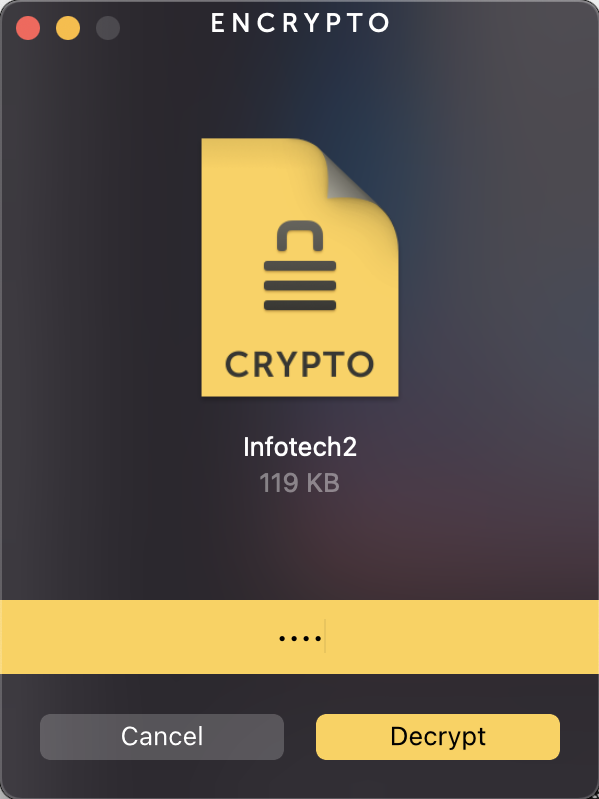
**I tried downloading the MEO Encryption software version 2.17 on my laptop, but it rejected because it is an outdated version for my Macbook, so i utilized the Encrypto tool, which utilizes the AES-256 encryption which is a highly secured encryption algorithm for encrypting files, it uses a key/password to encrypt the file inputed in it.**



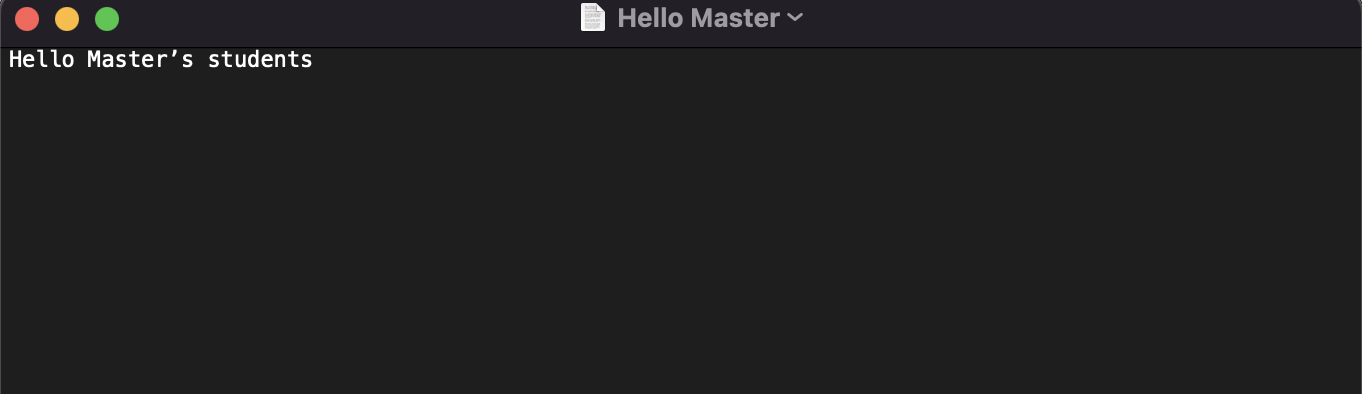
**The text file I wanted to encrypt is called Infotech, and the key I used was fake. The second screenshot shows the encryption process.**

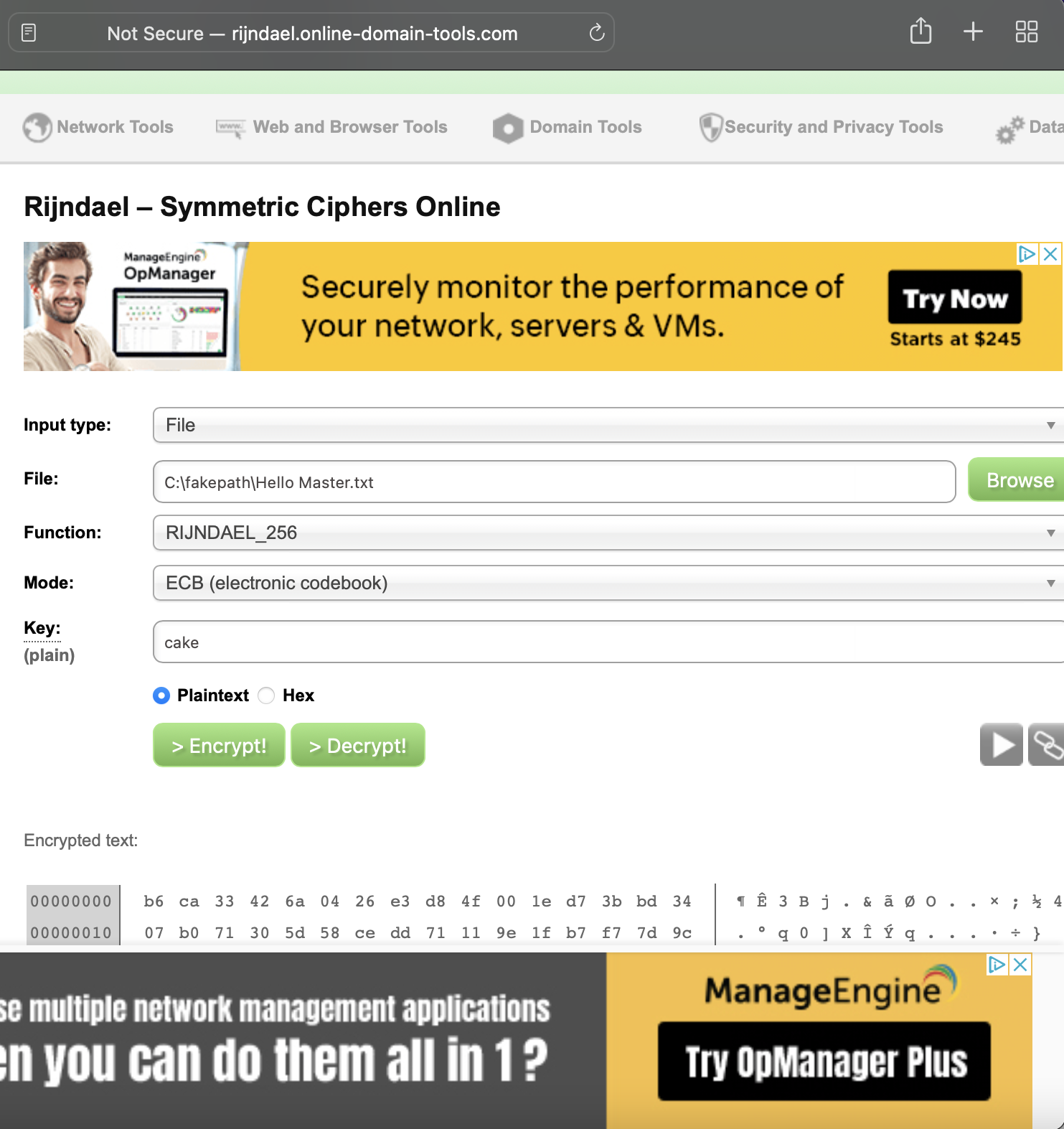


**The screenshot below shows the decryption process the tool utilizes.**



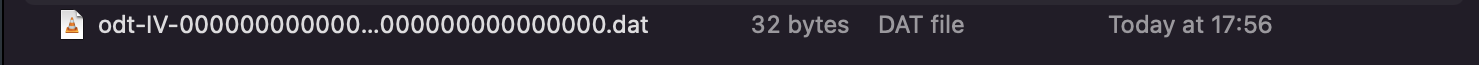
1. **Advanced Encryption Standard (AES).** Go to <http://aes.online-domain-tools.com/> where you can encrypt a file using AES (use **RIJNDAEL\_256**). Prepare a text file (.txt) with some random content to be encrypted. Then complete the following tasks. (4 points each, 20 points in total)
   1. Encrypt the text file using RIJNDAEL\_256 with a key/password you created. Download the ciphertext as binary file (**DAT file**) and save it to your computer.

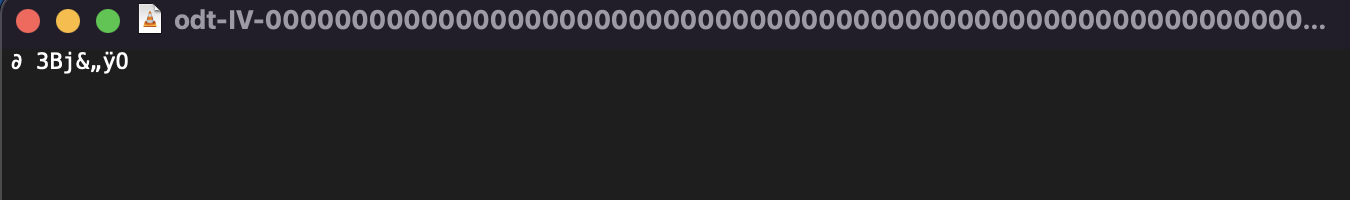




* 1. Use Windows Notepad (or a text viewer/editor) to open the DAT file. What do you see?

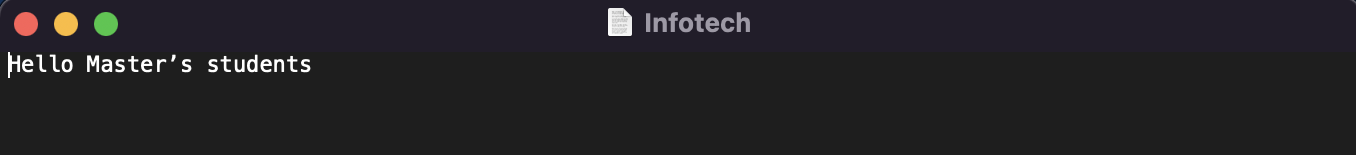
**It produced a ciphertext**



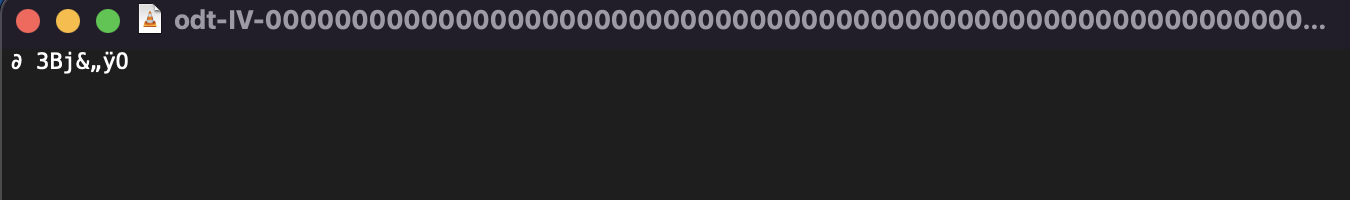


* 1. Create another .txt file with the exact same content but with a **different file name**. Encrypt this text file using the same cipher and same key/password. Do you obtain the same ciphertext?

**I named the new file Infotech with the same content “Hello Master’s Student”**

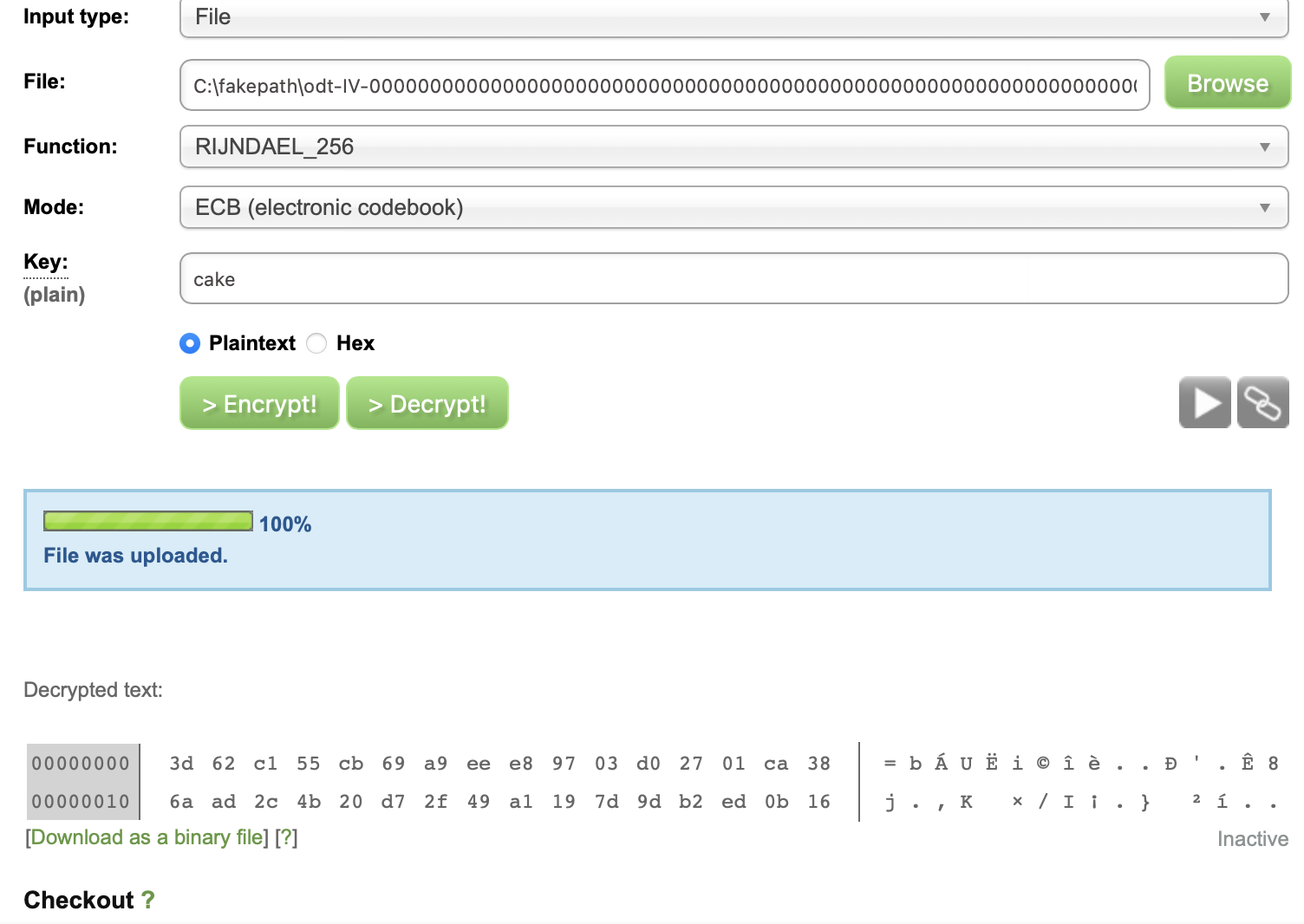


**After downloading the file, I observed the ciphertext turned out to be the same as the ciphertext above.**

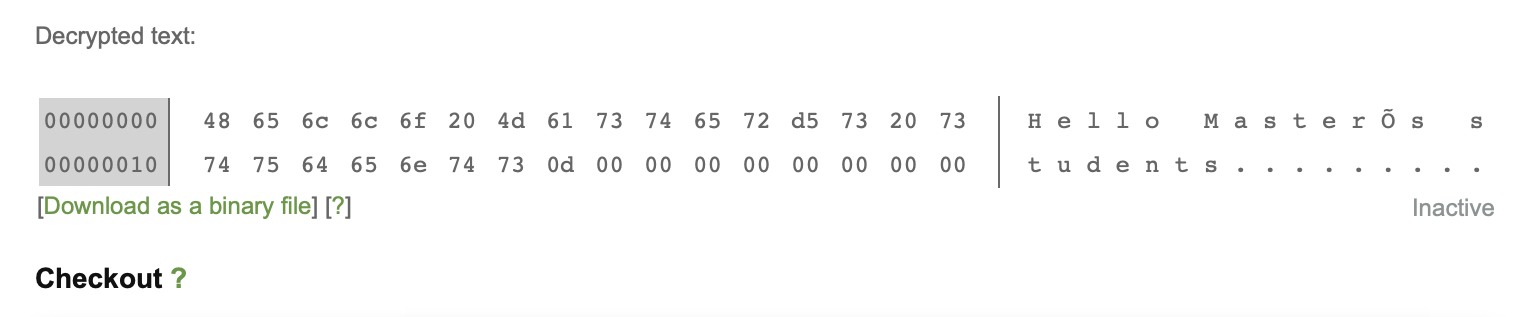


* 1. Go back to the website and decrypt the DAT file in step (a) using the same key/password. Attach screenshot to show it decrypts back to the plaintext.

**Decrypting the DAT file produced the initial plaintext “Hello Master’s students”.**

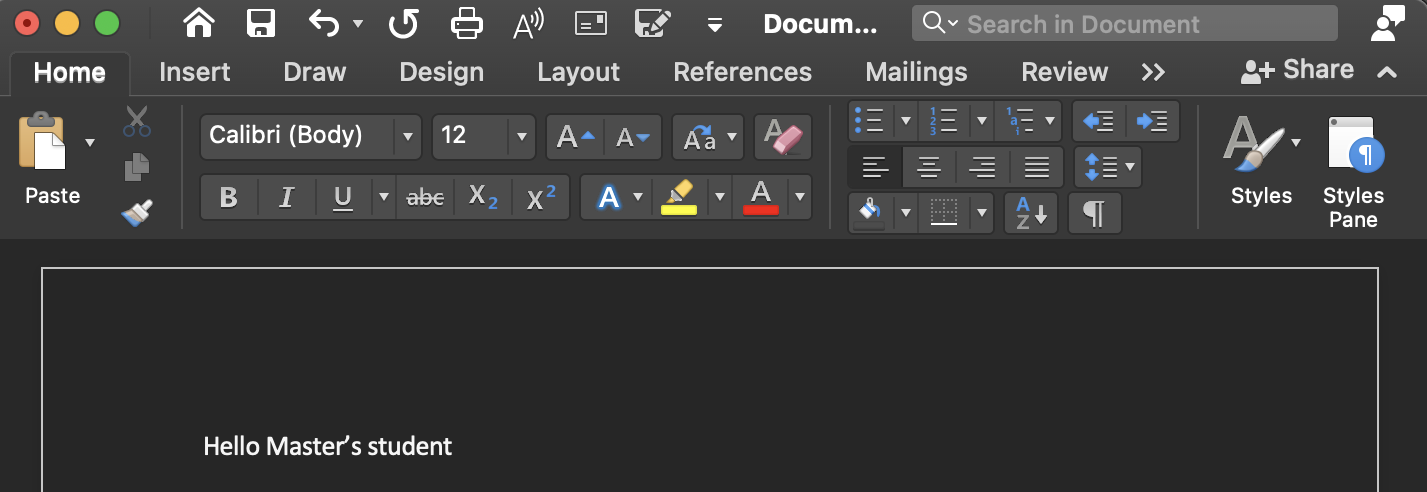


**After Decrypting the text, it produced the same content of the file.**

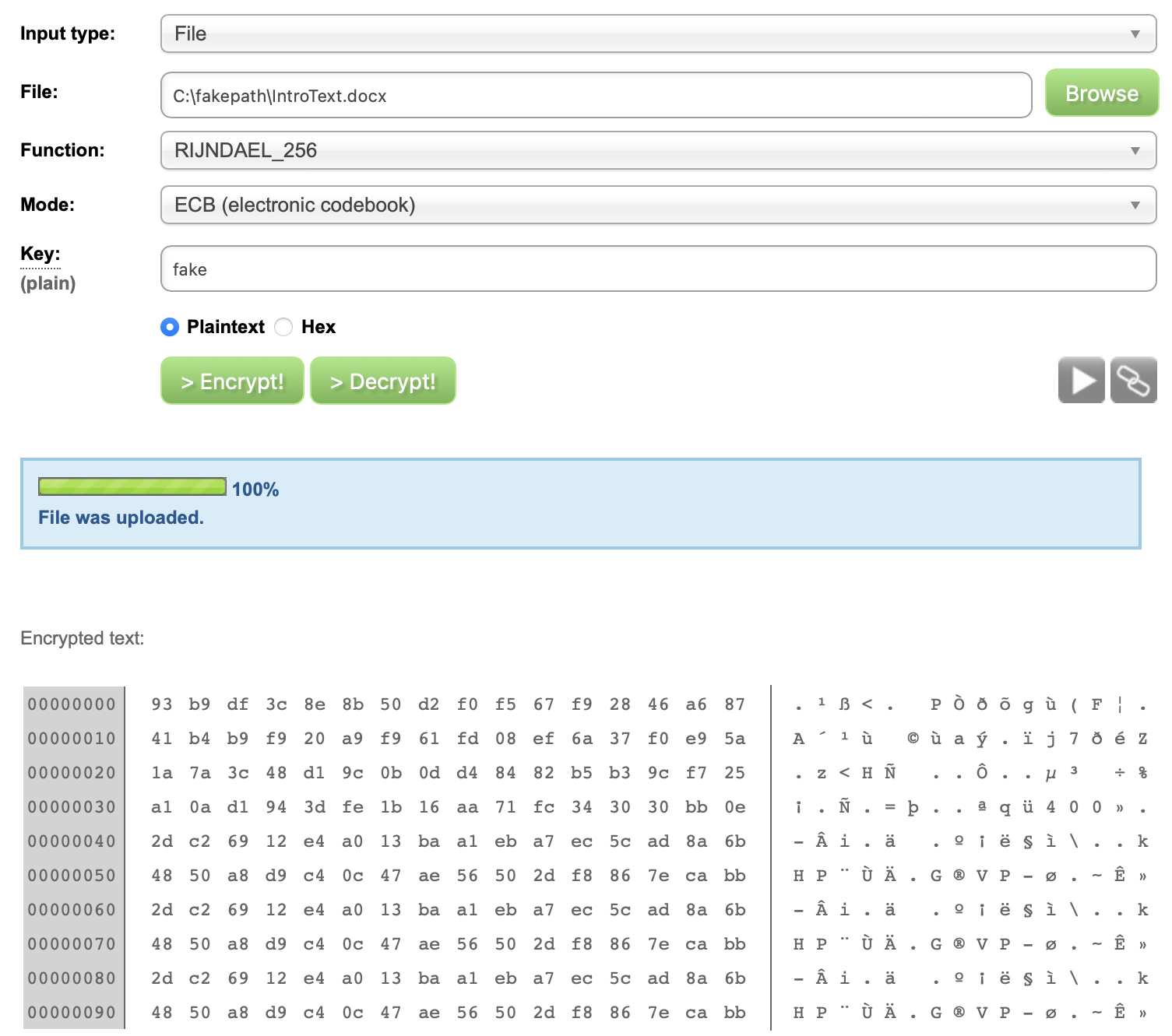


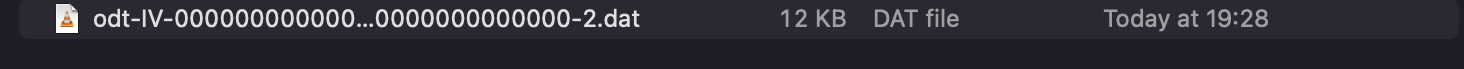
* 1. Repeat steps **a, b, and d** while using a **Word document instead** (but with exact same content as you had in the .txt file). What have you discovered?

**I created a word file with name “IntroText” with content “Hello Master’s student”.**

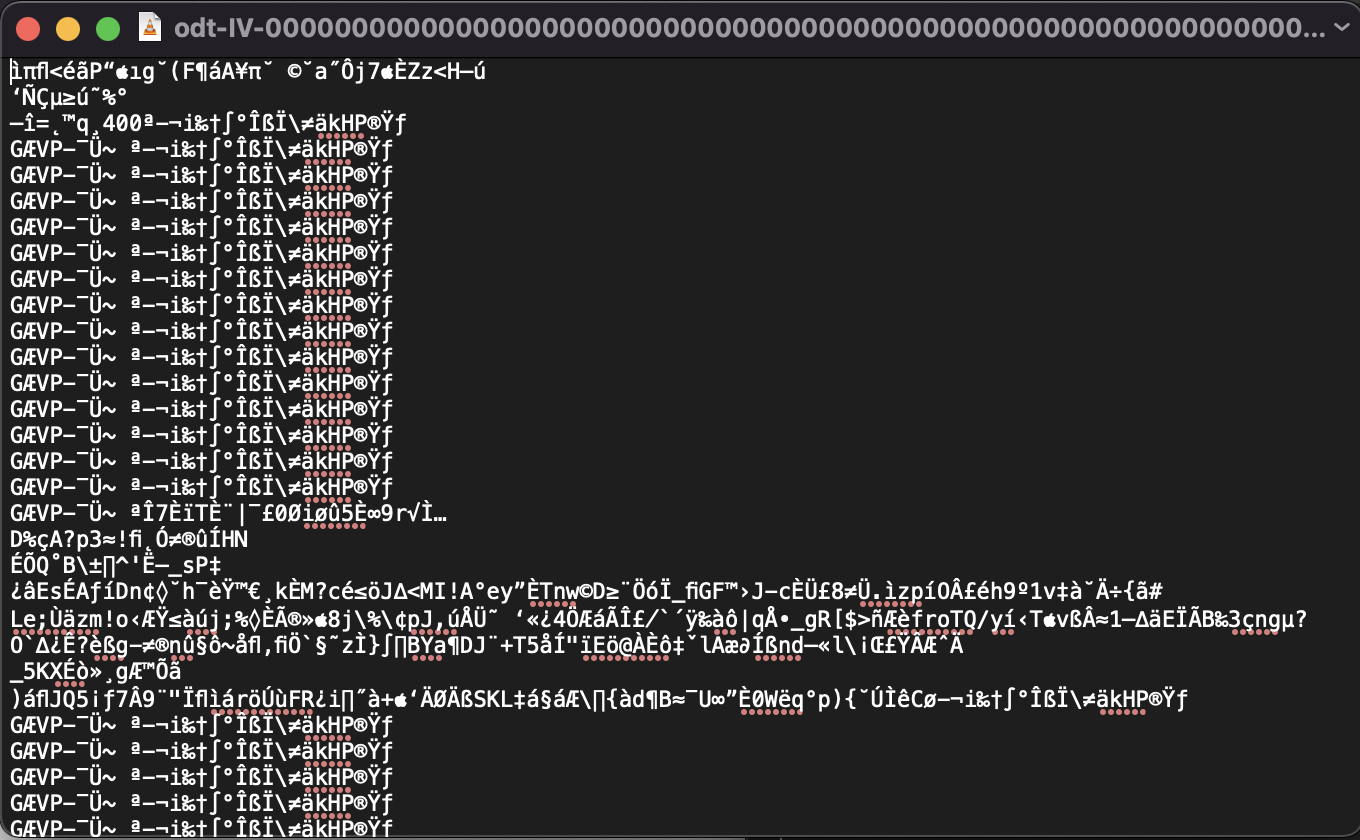


**Then I encrypted the word file and downloaded the encrypted DAT(Binary) file.**

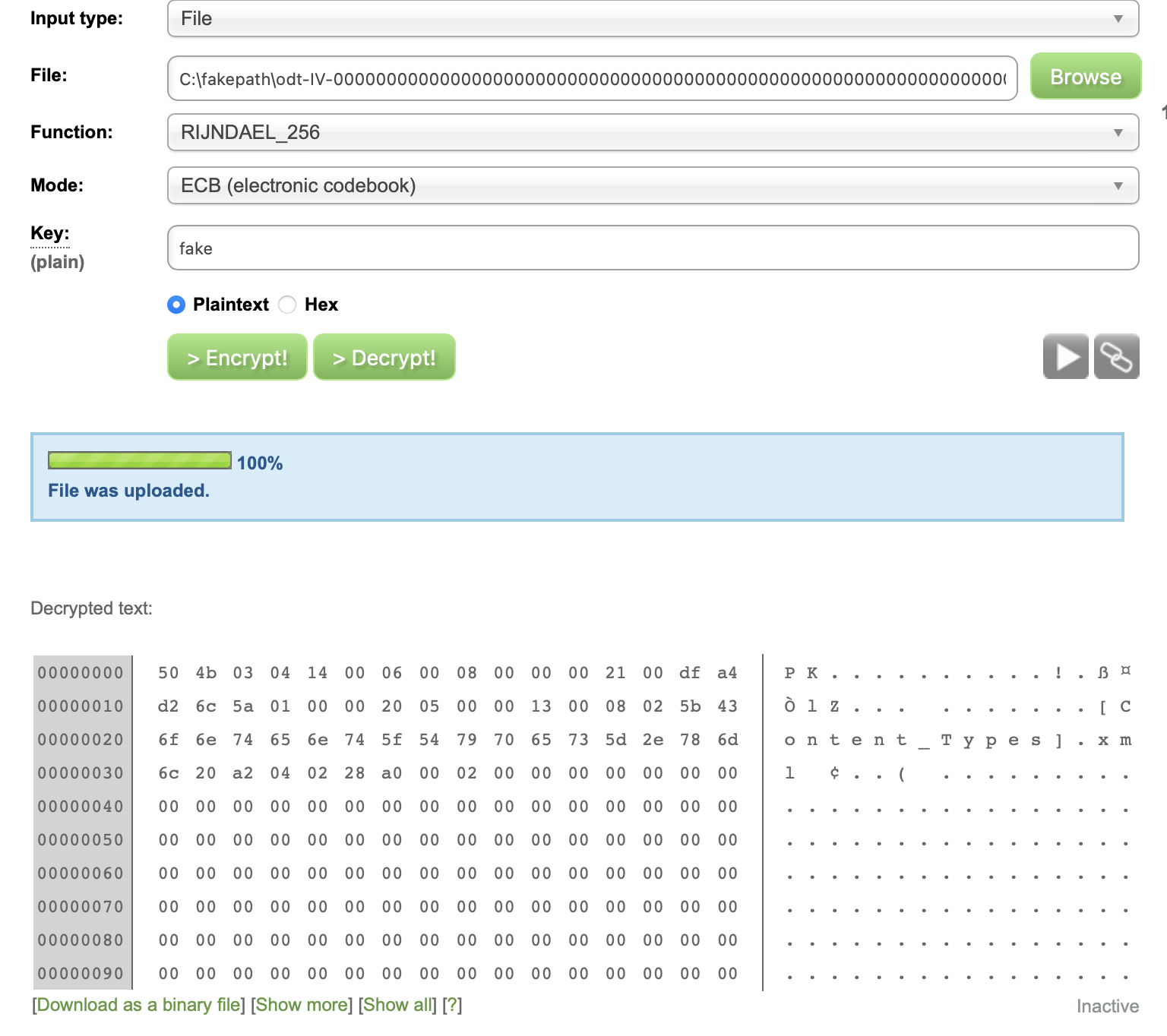


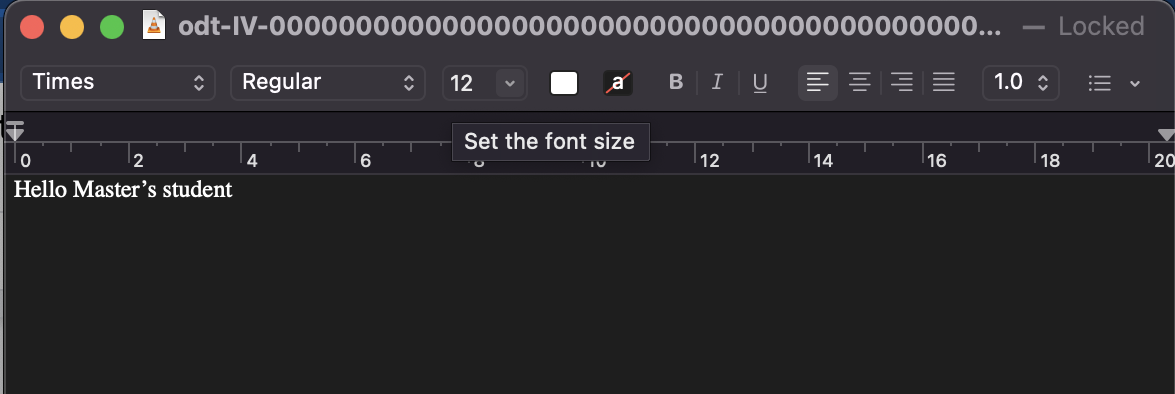


**After downloading the DAT file, I opened it with TextEdit on Macbook and observed that the ciphertext appeared to be longer than the cipher text in the text file. Also the size of the text file is smaller than the size of the word document file. That is Text file = 32 bytes, while Word document = 12KB**

****

**After decrypting the DAT file, I opened it with TextEdit and observed that the same content “Hello Master’s student'' was in the file.**

****

****