**Department of Information Systems and Cyber Security University of Texas in San Antonio**

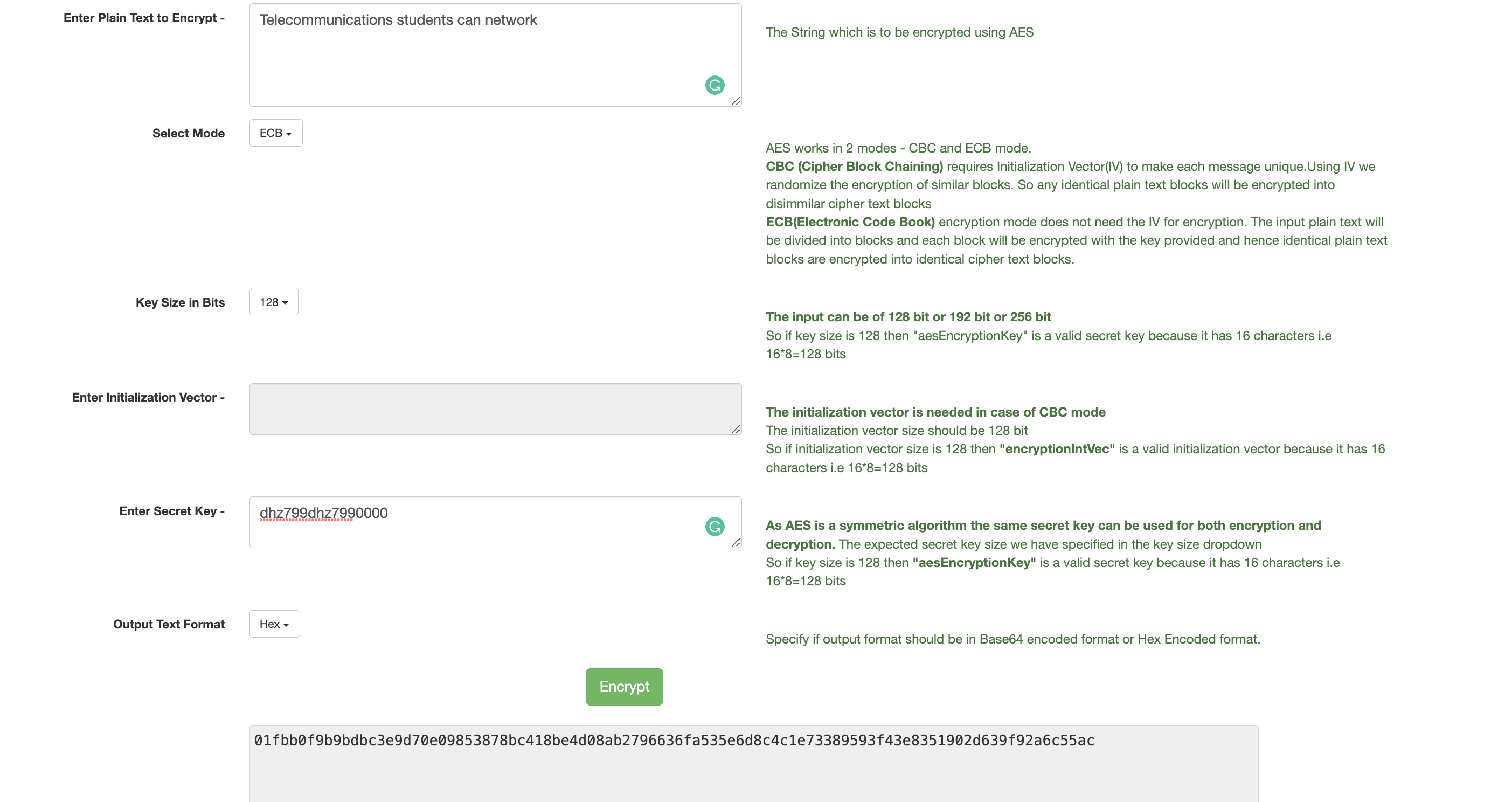


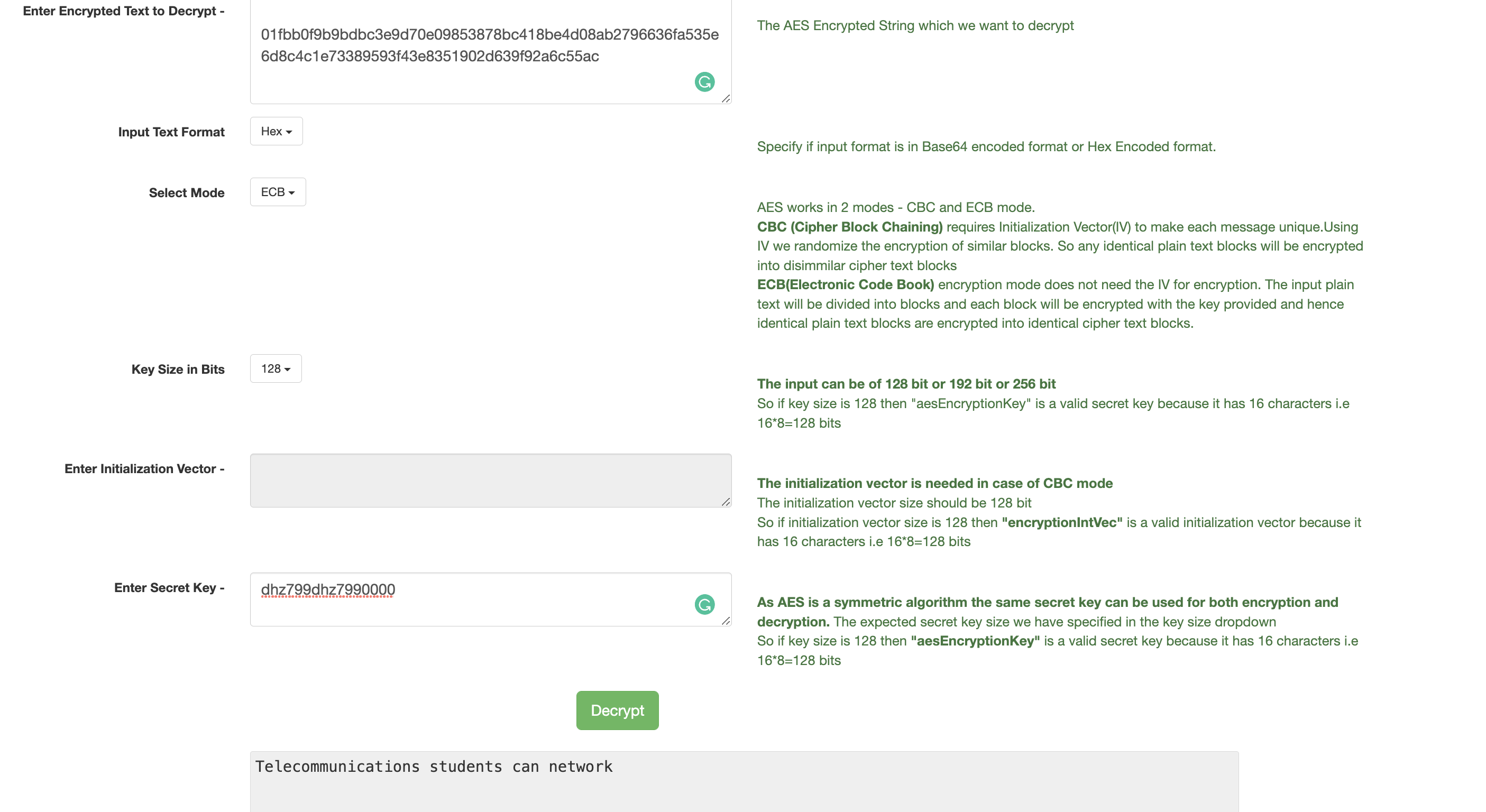
IS 3413: Telecom and Networking-001, Fall, 2022

Name: Daniel Cook  
UTSA ID: dhz799  
Email address: *danielwcook5@gmail.com*

Lab Assignment: Lab: M11 – Encryption  
Date Due: 11/12/2022  
Date Submitted: 11/12/2022

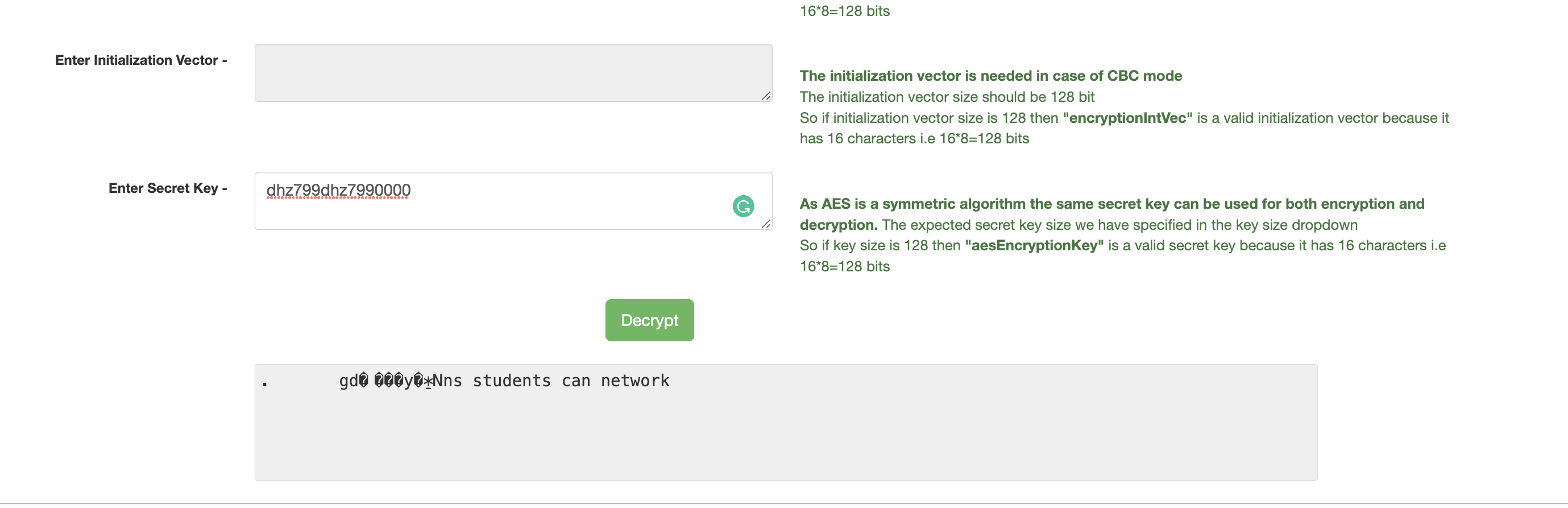
PART I:





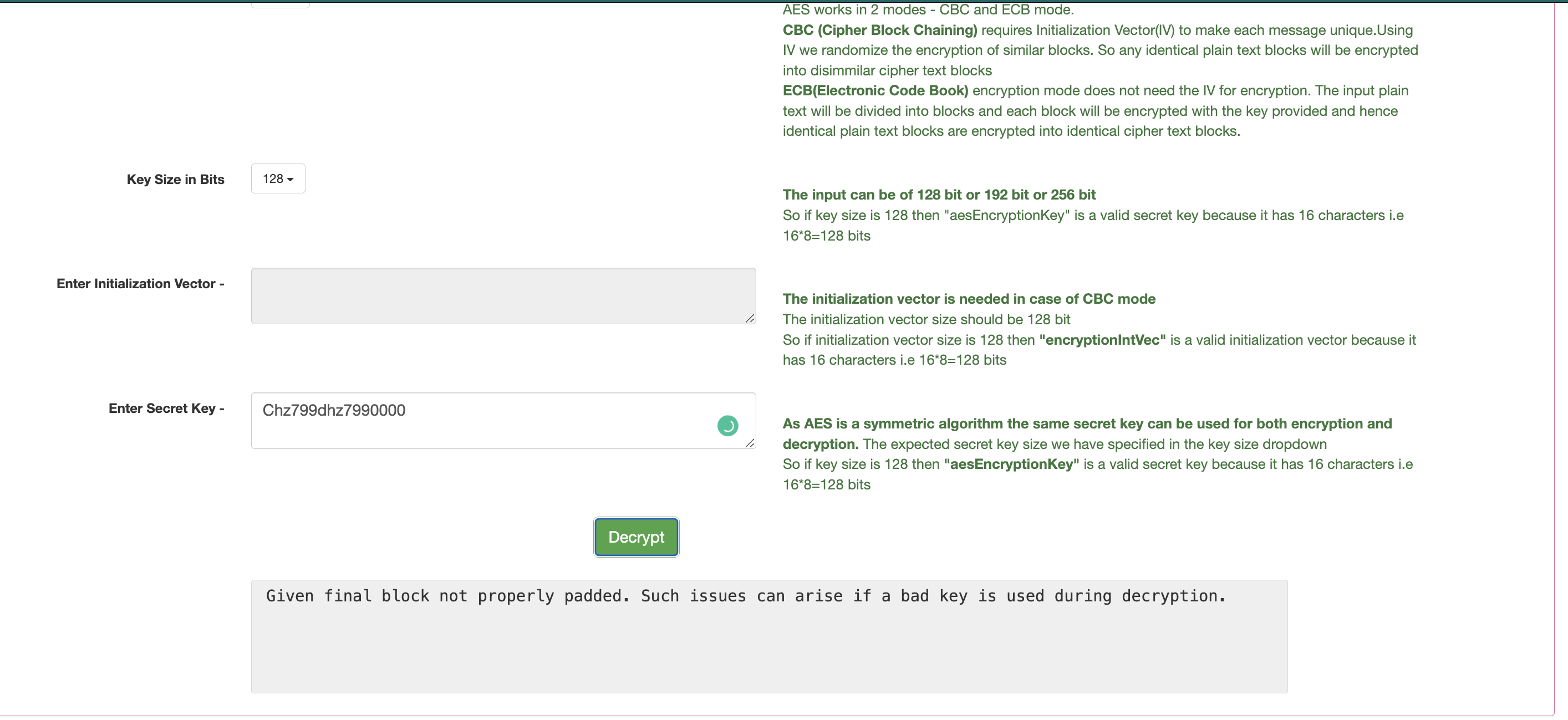
Question 1: What did your encrypted message look like? Document (copy/paste) the AES Encrypted text from Part 1?

It looked the same as it did as when to encrypt it, “Telecommunications students can network”.



Question 2: In Part 2, after changing the text and decrypting it, how does this text compare to the original plain text? In particular, since only a single hexadecimal character was changed, shouldn’t the decrypted text be identical except for the first character? Why or why not?

The first word was encrypted but the rest of the sentence was decrypted. The change of the character changed the word completely unable to decrypt that text, but with the correct key present it was able to decode the rest of the text.



Question 3: Briefly describe the results of the attempt to decode with an incorrect key in Part 3. Did this match what you expected to happen?

Without a key present It was unable to decode the actual text, it was expect that this would be true, without authorization or secret key it was unable to unlock it.