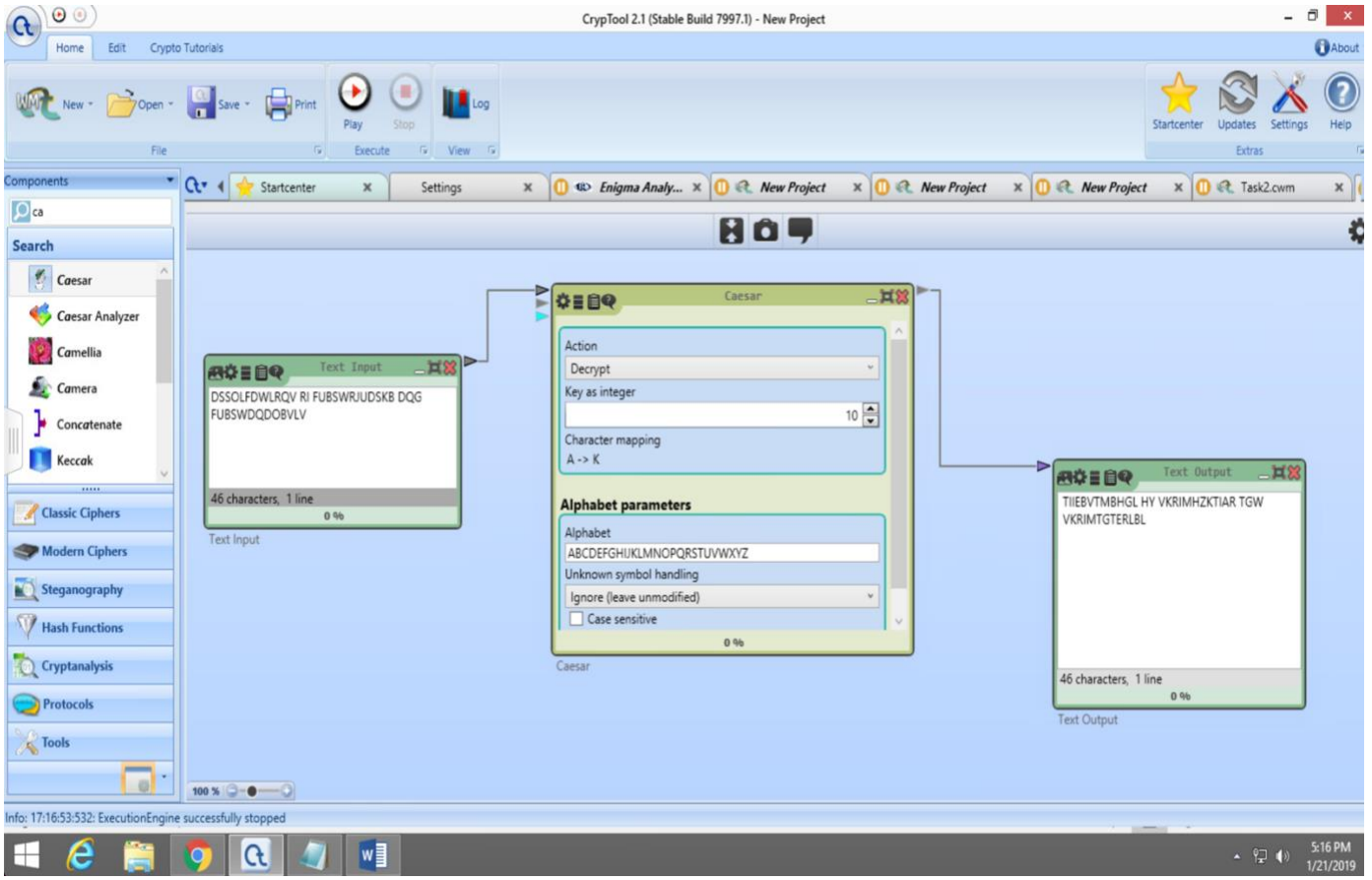
Homework 1

Applied Cryptography

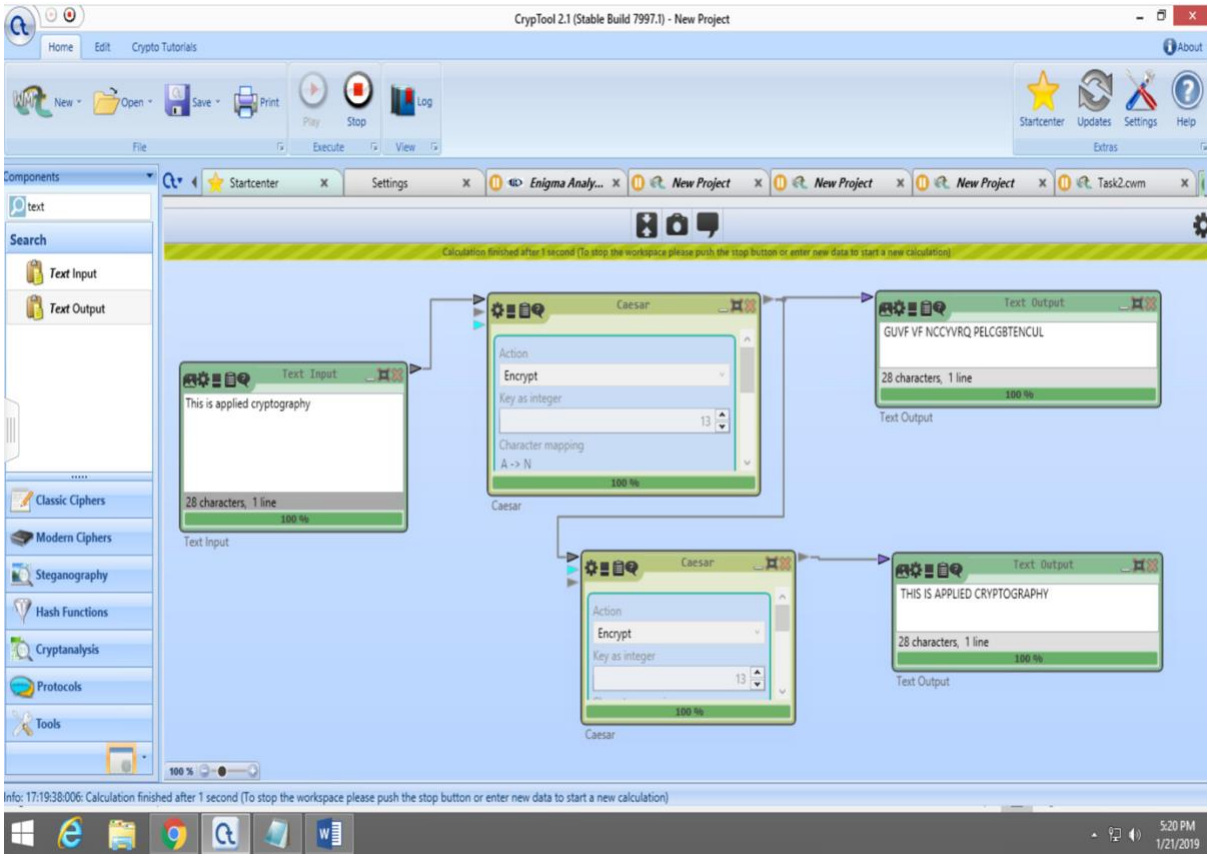
Mukesh Dangi

Task 1.1: Decrypt following text with **K=10**
Plain Text: TIIEBVTMBHGL HY VKRIMHZKTIAR TGW VKRIMTGTERLBL
Screenshot:



Task 1.2: K=13, double encryption with Caesar Cipher
Input Text: This is applied cryptography
Once we do the double encryption we get cipher text as input text. Because we shifted every char by 13 letters twice which is full circle.

Screenshot:



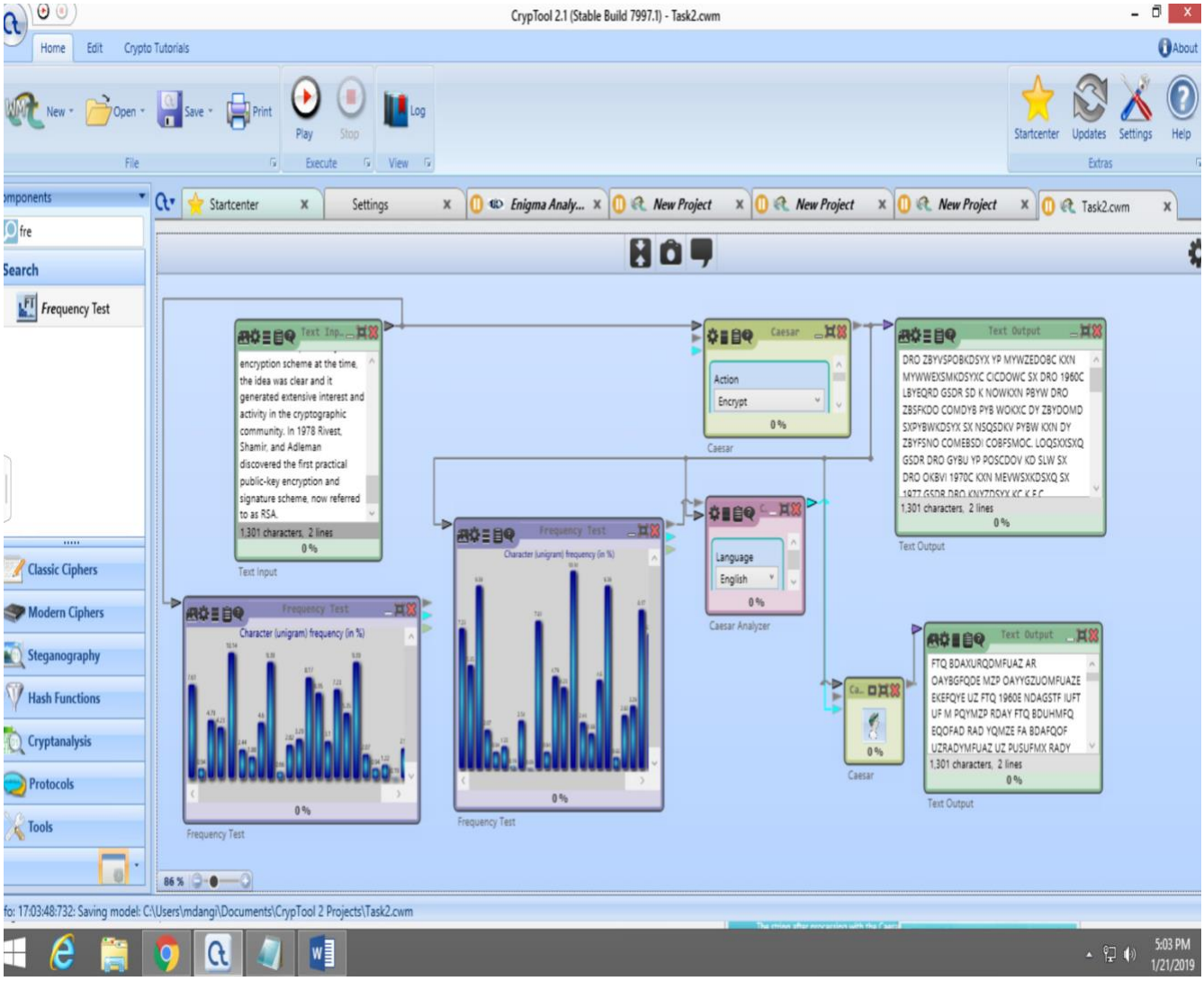
Task 1.3: If we take key=2 then to get a full circled or same cipher text as input, we need to encrypt the input text 13 times. In this encryption, we shift every letter by 2 next of it and there are 26 letters, we need 13 tries to get the same output as Task 1.2

Task 2: Frequency of Unigrams

In this Cipher, we see that input text consists of 7.6%-> A, 10.4%-> E, 9%->I, 8%-> N and 9%->T which is more than 50% of all letters in the text. And when we observe cipher text, it contains 7%->B, 9%->D, 7%->K, 10%->O, 9%->S and 8%->X which is again more than 50% of all unigram frequency. So Here by observing the cipher texts of multiple i/p text, Eve or man in middle can figure out the more than 50% of the plain text.

However, another observation is than most popular unigrams in the input text are no longer popular that means it would realty difficult to make a direct relationship between input text and cipher text. More popular letters in English are ‘A’, ‘E’, are not so frequent in the cipher text so it wouldn’t be easy task to decipher the text.

Screenshot:

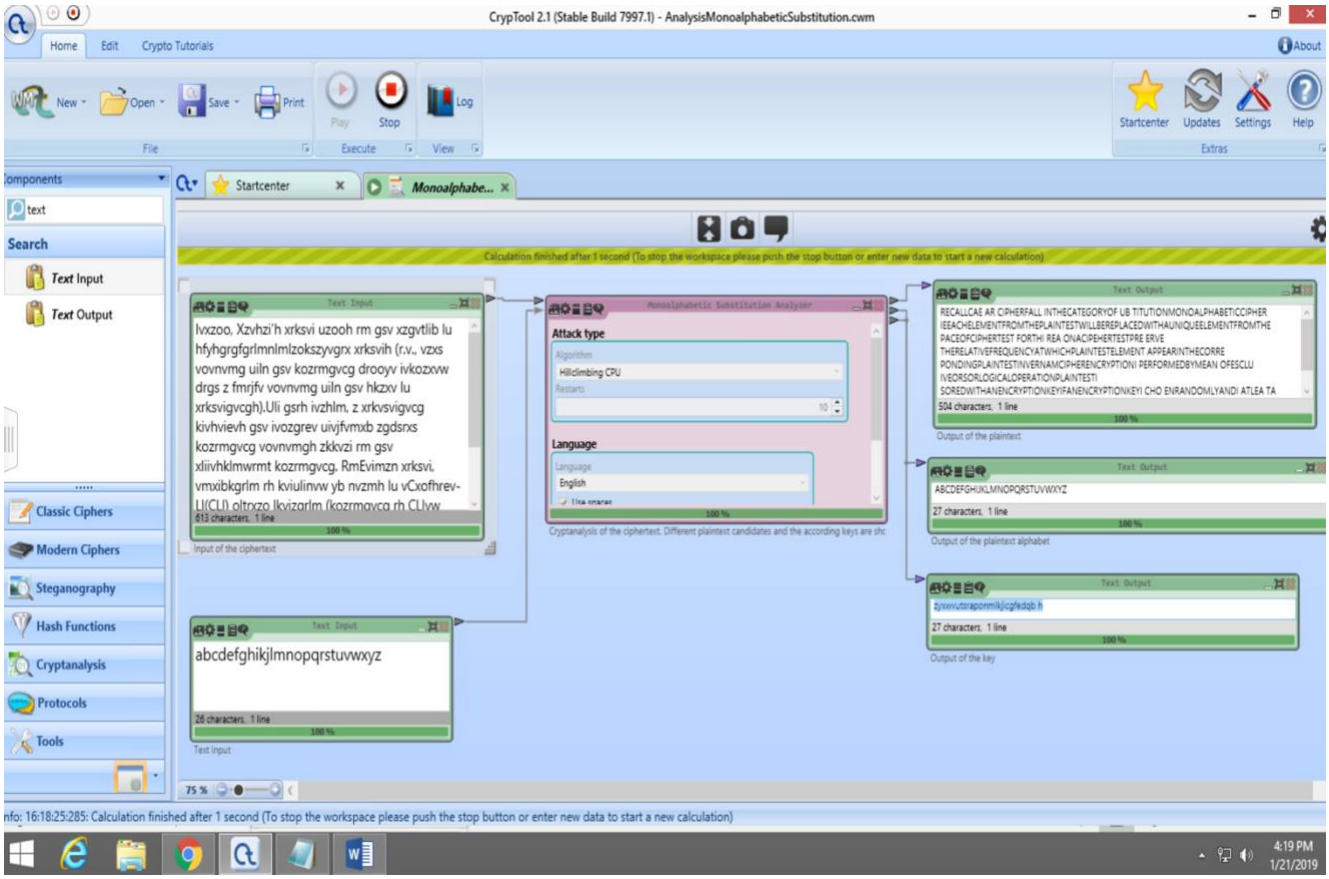


Task 3:

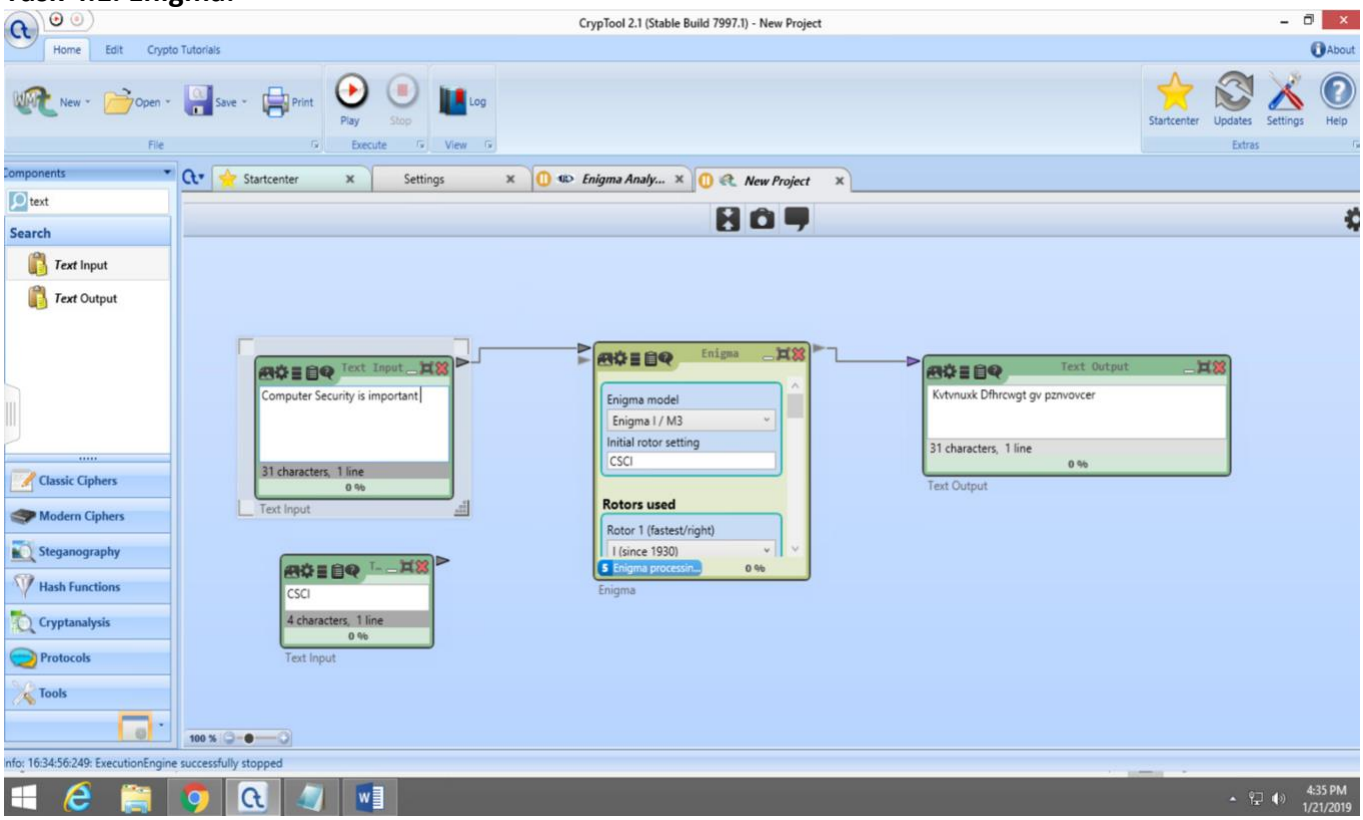
Key: zyxwvutsraponmlkjicgfedqb h

Plain Text: RECALLCAE AR CIPHERFALL INTHECATEGORYOF UB TITUTIONMONOALPHABETICCIPHER IEEACHELEMENTFROMTHEPLAINTESTWILLBEREPLACEDWITHAUNIQUEELEMENTFROMTHE PACEOFCIPHERTEST FORTHI REA ONACIPEHERTESTPRE ERVE THERELATIVEFREQUENCYATWHICHPLAINTESTELEMENT APPEARINTHECORRE PONDINGPLAINTESTINVERNAMCIPHERENCRYPTIONI PERFORMEDBYMEAN OFESCLU IVEORSORLOGICALOPERATIONPLAINTESTI SOREDWITHANENCRYPTIONKEYIFANENCRYPTIONKEYI CHO ENRANDOMLYANDI ATLEA TA LONGA THEPLAINTESTTOBEENCRYPTEDSORENCRYPTIONONETIMEPADI PROVABLYPERFECTLY ECURE

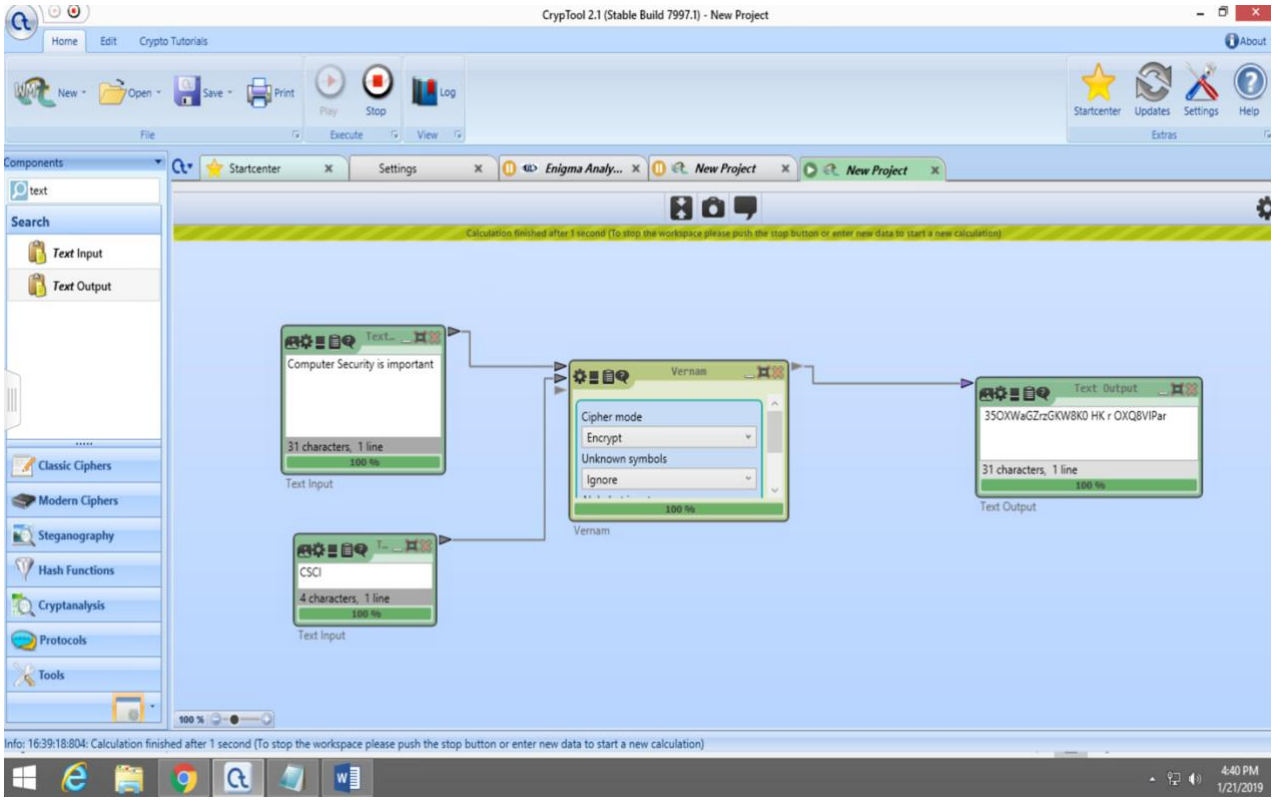
Screenshot:



Task 4.1. Enigma:



Task 4.2 Vernam



Task 4.3 Vigenere