

# Homework 1

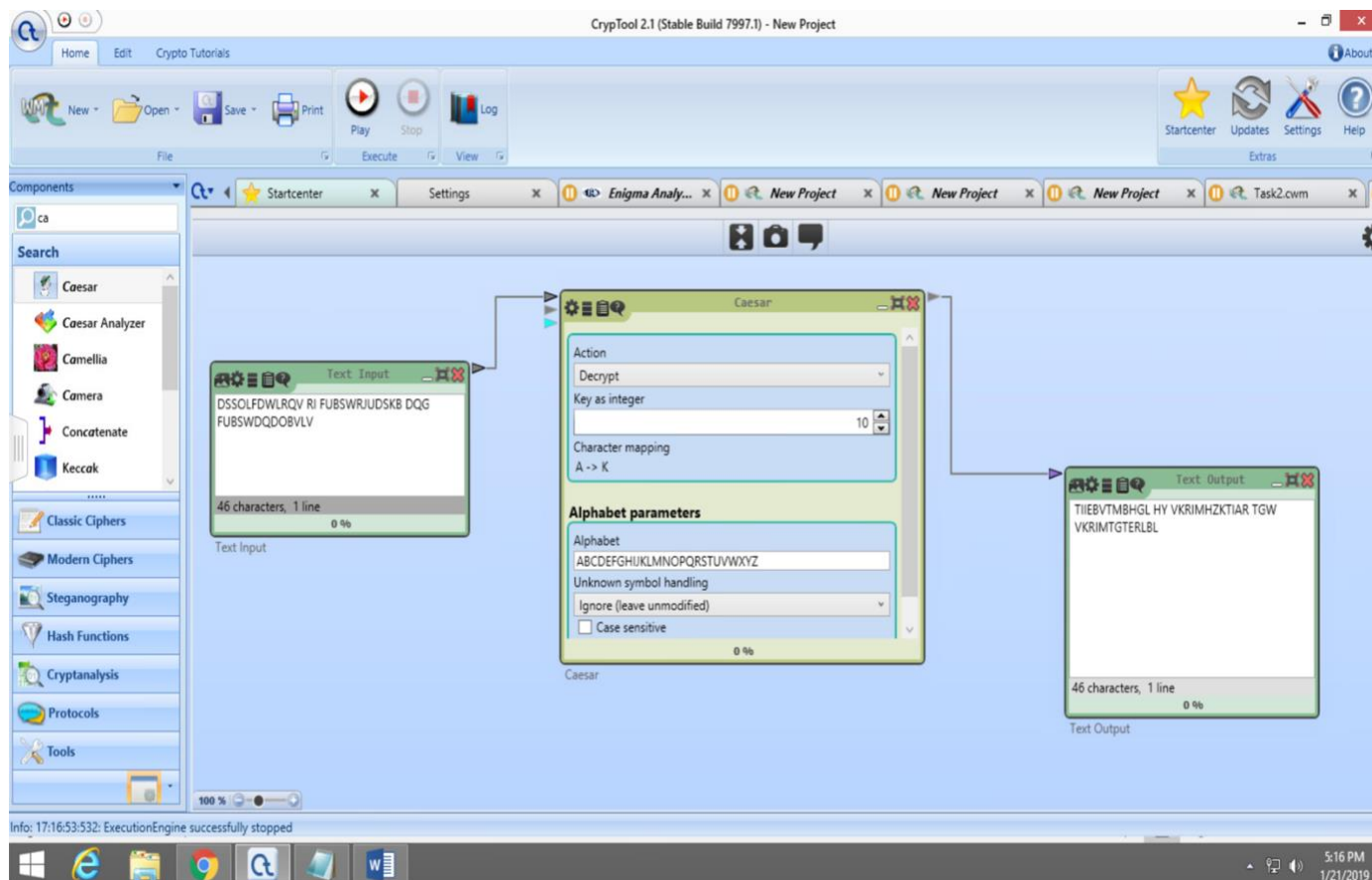
## Applied Cryptography

Mukesh Dangi

**Task 1.1:** Decrypt following text with **K=10**

Plain Text: TIIEBVTMBHGL HY VKRIMHZKTIAR TGW VKRIMTGTERLBL

Screenshot:

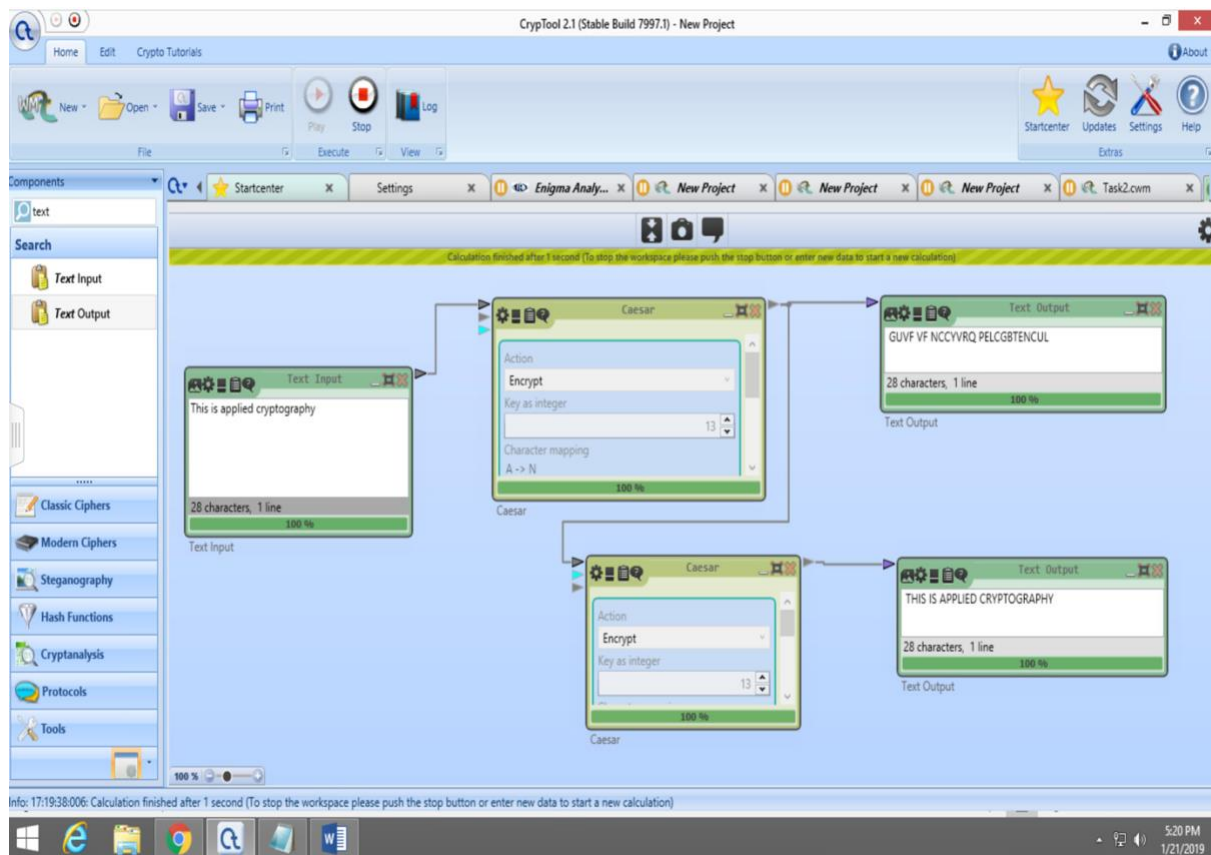


**Task 1.2:** K=13, double encryption with Caesar Cipher

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:



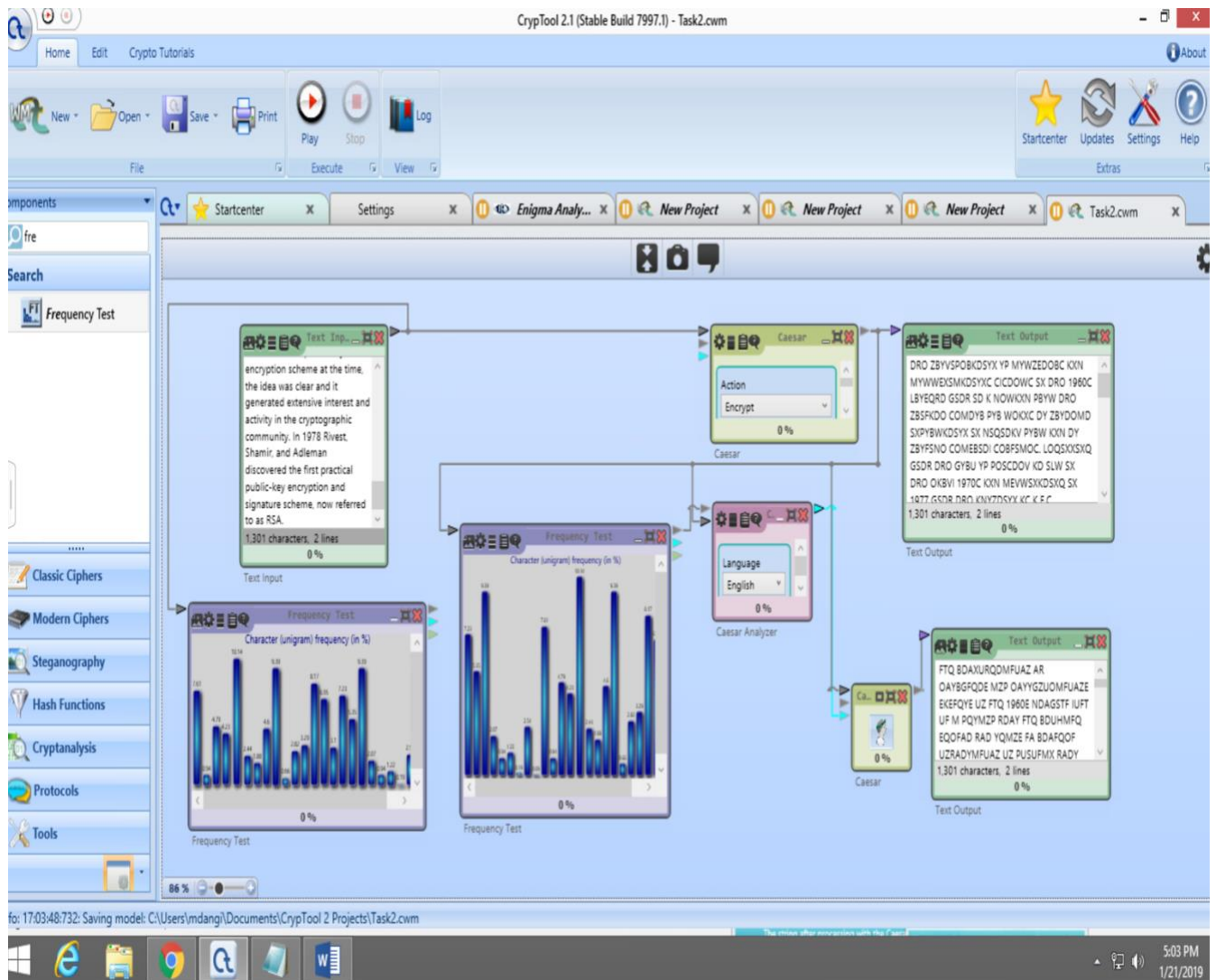
**Task 1.3:** If we take key=2 then to get a full circled or same cipher text as input, we need to encrypt the input text 13 times. In this encryption, we shift every letter by 2 next of it and there are 26 letters, we need 13 tries to get the same output as Task 1.2

## 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  
PONDINGPLAINTESTINVERNAMCIPHERENCRIPTIONI PERFORMEDBYMEAN OFESCLU  
IVEORSORLOGICALOPERATIONPLAINTESTI  
SOREDWITHANENCRIPTIONKEYIFANENCRIPTIONKEYI CHO ENRANDOMLYANDI ATLEA TA  
LONGA THEPLAINTESTTOBEENCRYPTEDSORENCRIPTIONONETIMEPADI  
PROVABLYPERFECTLY ECURE

## Screenshot:

Calculation finished after 1 second (To stop the workspace please push the stop button or enter new data to start a new calculation)

Input of the ciphertext:

```
lvzoo. Xzvhi' h xrksvi uzooh rm gsv xzgvtilb lu
hfyhgrfgrimlmizokszvgrx xrksvih (r.v. vzis
vovnmvg uiln gsv kozrmgvcg drooyv ivkozwv
drgs z frnjfv vovnmvg uiln gsv hlkzv lu
xrksvigvcgh).Uli gsrh izvilm, z xrksvigvcg
kivhvievh gsv ivozgrev uivfvmxb zgdsxrs
kozmvgvcg vovnmvgh zkkvzi rm gsv
xliivhklmwrmt kozrmgvcg. RmEvimzn xrksvi,
vmxibkgrim rh kvulinvw yb nvzmh lu vCxoofhrev-
U(CLI) oltrozo lkvizarl (kozmoyco rh CL)vw
613 characters, 1 line
```

Attack type:

- Algorithm: Hillclimbing CPU
- Fasters: 10

Language:

- Language: English
- Use roman: ☒

Output of the plaintext:

```
RECALLS AR CIPHER FALL IN THE CATEGORY OF SUBSTITUTION MONOALPHABETIC CIPHER
THE ELEMENTS FROM THE PLAINTEXT WILL BE REPLACED WITH A UNIQUE ELEMENT FROM THE
CIPHERTEXT. FORTH REA ON A CIPHERTEXT THE ERVE
THE RELATIVE FREQUENCY AT WHICH PLAINTEXT ELEMENT APPEAR IN THE CORRE
PONDING PLAINTEXT INVERNAM CIPHER ENCRYPTION. PERFORMED BY MEAN OF ESCLU
IVORS OR LOGICAL OPERATION PLAINTEXT
SORED WITH AN ENCRYPTION KEY (AN ENCRYPTION KEY) CHO ENRANDOMLY AND I AT LEA TA
504 characters, 1 line
```

Output of the plaintext alphabet:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
27 characters, 1 line
```

Output of the key:

```
qjwmutrapomkijgkldobh
27 characters, 1 line
```

Info: 16:18:25:285: Calculation finished after 1 second (To stop the workspace please push the stop button or enter new data to start a new calculation)

## Task 4.1. Enigma:

Enigma model: Enigma I / M3

Initial rotor setting: CSCI

Rotors used:

- Rotor 1 (fastest/right)
- I (since 1930)

Enigma processing: 0 %

Text Input:

```
Computer Security is important
31 characters, 1 line
```

Text Output:

```
Kvtnuxk Dfhrwgt gv pznvovcr
31 characters, 1 line
```

Info: 16:34:56:249: ExecutionEngine successfully stopped

## Task 4.2 Vernam

The screenshot shows the CrypTool 2.1 (Stable Build 7997.1) - New Project window. The interface includes a menu bar (Home, Edit, Crypto Tutorials), a toolbar with icons for New, Open, Save, Print, Play, Stop, and Log, and a sidebar with components like Text Input, Text Output, Classic Ciphers, Modern Ciphers, Steganography, Hash Functions, Cryptanalysis, Protocols, and Tools. The main workspace displays a workflow for the Vernam cipher. It starts with a 'Text Input' block containing the text 'Computer Security is important' (31 characters, 1 line, 100% completion). This is connected to a 'Vernam' block, which is configured with 'Cipher mode' set to 'Encrypt', 'Unknown symbols' set to 'Ignore', and 'Shift key' set to 'CSCI' (4 characters, 1 line, 100% completion). The output of the 'Vernam' block is connected to a 'Text Output' block, which displays the encrypted text '35OXWwGZrGKW8K0 HK r OXQ8VIPar' (31 characters, 1 line, 100% completion). The status bar at the bottom indicates 'Info: 16:39:18:804: Calculation finished after 1 second (To stop the workspace please push the stop button or enter new data to start a new calculation)'.

## Task 4.3 Vigenere

The screenshot shows the CrypTool 2.1 (Stable Build 7997.1) - New Project window. The interface is similar to the previous task, but the 'Components' sidebar now shows 'Vigenere' and 'Vigenere Analyzer'. The main workspace displays a workflow for the Vigenere cipher. It starts with a 'Text Input' block containing the text 'Computer Security is important' (31 characters, 1 line, 0% completion). This is connected to a 'Vigenere' block, which is configured with 'Encrypt' selected, 'Shift value (integer)' set to '2,18,2,8', 'Shift key (multiple letters)' set to 'CSCI', and 'Shift key' set to 'CSCI' (0% completion). The output of the 'Vigenere' block is connected to a 'Text Output' block, which displays the encrypted text 'EGOXWLGZ UWECTAVG KK KURGTBCFV' (31 characters, 1 line, 0% completion). The status bar at the bottom indicates 'Info: 16:42:21:567: ExecutionEngine successfully stopped'.