

CSCI-20 Programming and Algorithms I

Crypto Machine Project



Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

WANT A REPLY?
 "Answer by WESTERN UNION"
 or similar phrases may be
 included without charge:

5 5
 4 6
 2 3
 3 7
 4 6
 2 6
 4 9

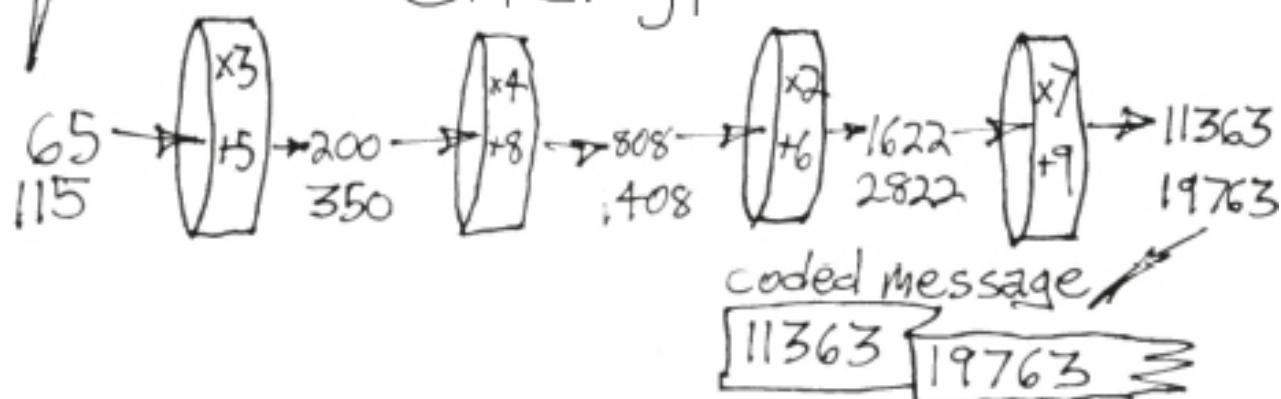
266705 431825 427985 155345 451025 128465
 397265 431825 443345 401105 393425 451025 128465
 451025 431825 128465
 389585 443345 408785 427985 416465 128465
 470225 431825 454865 443345 128465
 308945 458705 378065 420305 451025 408785 427985 393425 182225

A secret message
 $\begin{array}{c} 4 \\ \downarrow \\ 65 \end{array}$ $\begin{array}{c} 115 \\ \downarrow \\ 115 \end{array}$

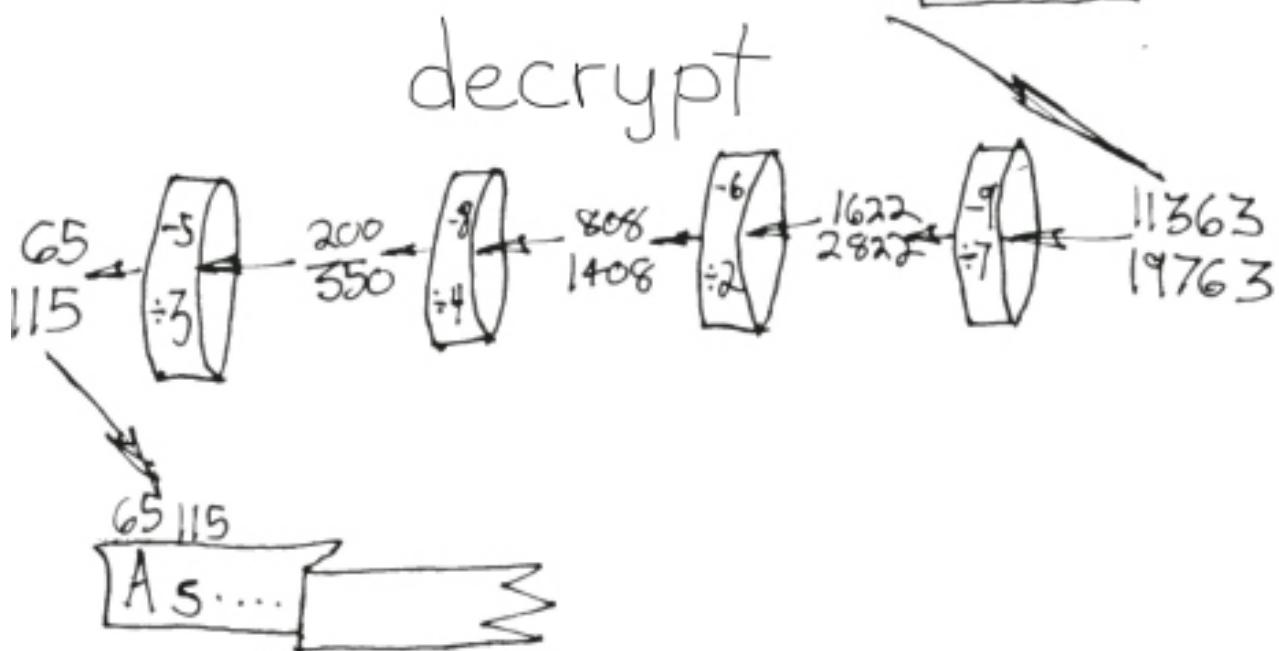
crypto-
rotors

3	5
4	8
2	6
7	9

encrypt



decrypt



Museum of Anacronistic Computation
Phineas Farington, Director

Kathy. Have you had a look at the latest acquisition? On Tuesday an anonymous donor brought by a small box of items. After some research we determined that the original owner of the items was a spy who was active during the late 1940's during the early days of the Cold War.

Among the most intriguing of the items is a coded telegram and an encryption machine that uses cryptographic rotors placed alongside each other to encrypt and decrypt messages. The machine is broken beyond repair but our consultant produced a drawing of how it would have worked.

We're in the process of salvaging what we can from the device to display in our ever-growing "Al B. Frank Memorial Cryptographic Machines With Rotors Throughout History" wing of the museum. I would like you to create a computer simulation of the device that runs alongside the device itself. For simplicity, the simulation should allow guests to input a premade message when the simulation is activated rather than trying to encrypt/decrypt each key stroke. Our consultant is available to answer your questions.

Thanks Kathy!

-Phin