Scott Bebington

U21546216

COS 330 Practical Assignment 1

Using the two keys (memory words) cryptographic and network security, encrypt the following message:  
  
Be at the third pillar from the left outside the lyceum theatre tonight at seven. If you are distrustful bring two friends.

Assumptions:

Duplicate letters: I removed all duplicate letters, this was to avoid confusion as well as keeping the numbering of the letters easier.

Spacing and Punctuation: For spaces, I kept it the same format as in the document (Removed them), for full stops an xx is used in its place (Also the same as the document)

Padding: The same as the document, any open spaces at the end of the table are padded with x’s

Word truncation: As the special forces document specifies that 10 letter memory words are to be used, in the case of the second memory word (Network Security), all duplicate letters and spaces were removed as well as any letters going past 10 were removed leaving the word “networkscu”. For cryptography the same approach is used leaving the word “cryptogahi”

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Single cypher word list:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| trfhe | hxibi | xbrou | yrtyr | ndeae | thgxd | lrxhf | teati | srexi | rolta |
| ftinx | hllet | ineuf | xtihi | uovat | wxedm | tceso | ugstl | edmne | rfoxa |
| ptset | eustx |  |  |  |  |  |  |  |  |

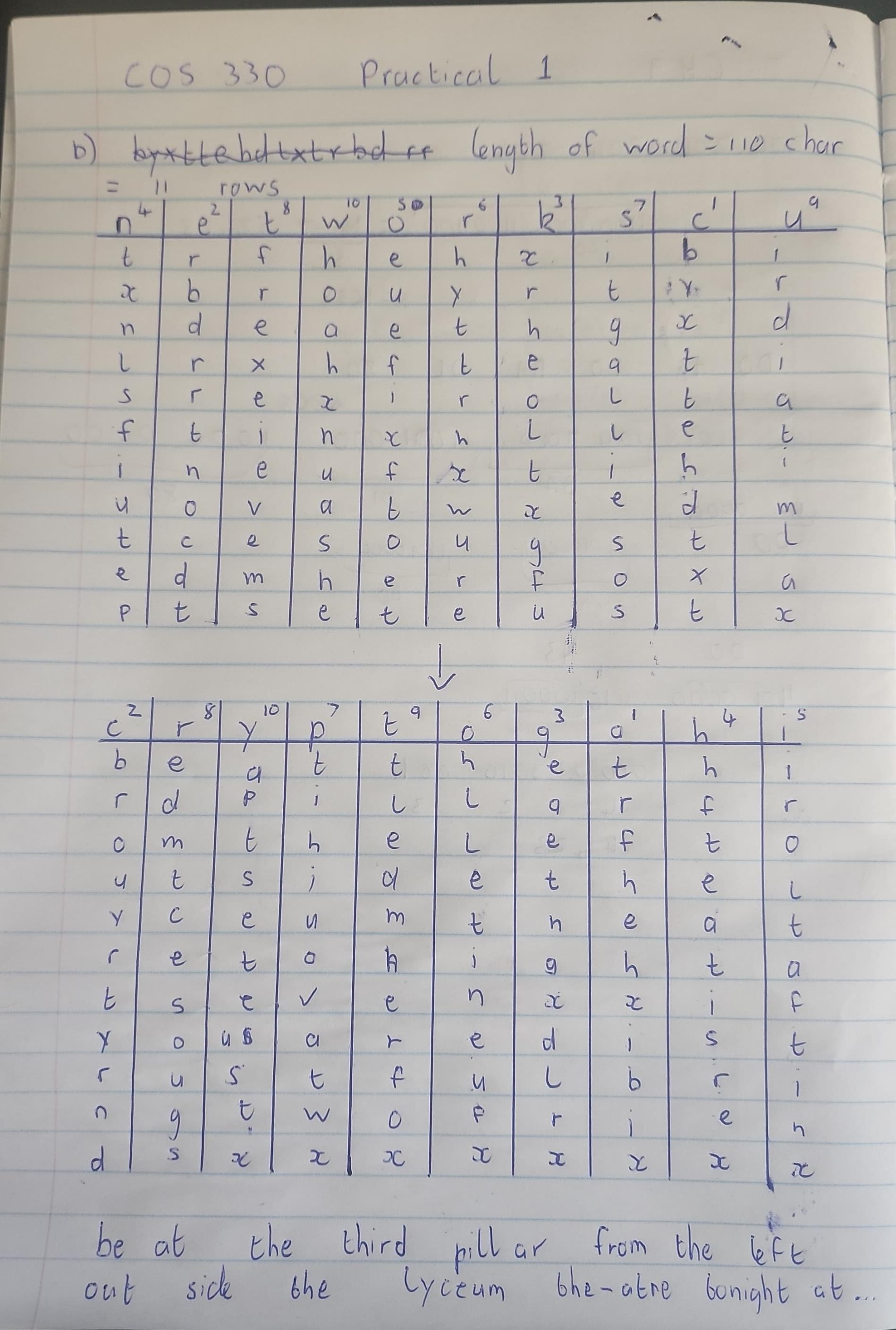
Single cypher final string:

Trfhehxibixbrouyrtyrndeaethgxdlrxhfteatisrexiroltaftinxhlletineufxtihiuovatwxedmtcesougstledmnerfoxaptseteustx

Double cypher word list:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| byxtt | ehdtx | trbdr | rtnoc | dtxrh | eoltx | gfutx | nlsfi | utepe | uefix |
| ftoet | hyttr | hxwur | eitga | llies | osfre | xeiev | emsir | diati | mlaxh |
| oahxn | uasne |  |  |  |  |  |  |  |  |

Double cypher final string:  
byxttehdtxtrbdrrtnocdtxrheoltxgfutxnlsfiutepeuefixftoethyttrhxwureitgalliesosfrexeievemsirdiatimlaxhoahxnuasne



1. Advantages: very simple to implement, using 2 memory words allows for an extra layer of encryption as apposed to a single memory word.

It is appropriate to use technique when only 2 parties are aware of the memory words and a quick hand written message needs to be encrypted and sent to the second party