CSCI/CSIS 631

Fall 2019

Homework 3

Solution

You can work this problem in one of two ways. Both are shown below.

a. First method: try all 26 keys. The results are:

key: A plaintext: TEBKFKQEBZLROPBLCERJXKBSBKQP

key: B plaintext: SDAJEJPDAYKQNOAKBDQIWJARAJPO

key: C plaintext: RCZIDIOCZXJPMNZJACPHVIZQZION

key: D plaintext: QBYHCHNBYWIOLMYIZBOGUHYPYHNM

key: E plaintext: PAXGBGMAXVHNKLXHYANFTGXOXGML

key: F plaintext: OZWFAFLZWUGMJKWGXZMESFWNWFL

K key: G plaintext: NYVEZEKYVTFLIJVFWYLDREVMVEKJ

key: H plaintext: MXUDYDJXUSEKHIUEVXKCQDULUDJI

key: I plaintext: LWTCXCIWTRDJGHTDUWJBPCTKTCIH

key: J plaintext: KVSBWBHVSQCIFGSCTVIAOBSJSBHG

key: K plaintext: JURAVAGURPBHEFRBSUHZNARIRAGF

key: L plaintext: ITQZUZFTQOAGDEQARTGYMZQHQZFE

key: M plaintext: HSPYTYESPNZFCDPZQSFXLYPGPYED

key: N plaintext: GROXSXDROMYEBCOYPREWKXOFOXDC

key: O plaintext: FQNWRWCQNLXDABNXOQDVJWNENWCB

key: P plaintext: EPMVQVBPMKWCZAMWNPCUIVMDMVBA

key: Q plaintext: DOLUPUAOLJVBYZLVMOBTHULCLUAZ

key: R plaintext: CNKTOTZNKIUAXYKULNASGTKBKTZY

key: S plaintext: BMJSNSYMJHTZWXJTKMZRFSJAJSYX

key: T plaintext: ALIRMRXLIGSYVWISJLYQERIZIRXW

key: U plaintext: ZKHQLQWKHFRXUVHRIKXPDQHYHQWV

key: V plaintext: YJGPKPVJGEQWTUGQHJWOCPGXGPVU

key: W plaintext: XIFOJOUIFDPVSTFPGIVNBOFWFOUT

key: X plaintext: WHENINTHECOURSEOFHUMANEVENTS

key: Y plaintext: VGDMHMSGDBNTQRDNEGTLZMDUDMSR

key: Z plaintext: UFCLGLRFCAMSPQCMDFSKYLCTCLRQ

Of these, the one with key X ("**WHEN IN THE COURSE OF HUMAN EVENTS**") is the only English plaintext, so it is the answer.

b. This approach uses the character frequencies from Figure 10-1. The frequency counts of the letters in the ciphertext are:

B 0.178571	C 0.035714	E 0.107143	F 0.035714
J 0.035714	K 0.142857	L 0.071429	O 0.035714
P 0.071429	Q 0.071429	R 0.071429	S 0.035714
T 0.035714	X 0.035714	Z 0.035714	

Putting this into the formula for ϕ on page 293, the values of ϕ are:

$\phi(0) = 0.036464$ $\phi(1) = 0.042643$ $\phi(2) = 0.035786$

$\phi(3) = 0.036571$ $\phi(4) = 0.034821$ $\phi(5) = 0.028250$

$\phi(6) = 0.040607$ $\phi(7) = 0.035071$ $\phi(8) = 0.040893$

$\phi(9) = 0.036679$ $\phi(10) = 0.047036$ $\phi(11) = 0.041714$

$\phi(12) = 0.037536$ $\phi(13) = 0.044107$ $\phi(14) = 0.036464$

$\phi(15) = 0.031214$ $\phi(16) = 0.037286$ $\phi(17) = 0.041571$

$\phi(18) = 0.032821$ $\phi(19) = 0.041571$ $\phi(20) = 0.026607$

$\phi(21) = 0.025143$ $\phi(22) = 0.040714$ $\phi(23) = 0.069464$

$\phi(24) = 0.043536$ $\phi(25) = 0.034429$

The index with the largest ϕ is 23, which corresponds to a key of X. Using this key, the message deciphers to **WHENINTHECOURSEOFHUMANEVENTS**, which is the answer.