

Worksheet Cryptography 3: Polyalphabetic Ciphers

1. Fill in the blanks below.

(a) Shift ciphers are vulnerable because

(b) Transposition ciphers are vulnerable because

2. Progressive Caesar Cipher (Sequential Shift)

(a) Using a private key of $A \rightarrow J$ (and sequential shift), encrypt the word
C O N S T I T U T I O N.

(b) Using a private key of $A \rightarrow D$, decrypt the ciphertext
W L J X P O Q D Z R G V T F V G I F Z

(c) What are some advantages of this cipher?

(d) What are some disadvantages of this cipher?

3. Vigenère Cipher

(a) Using the keyword UNION, encode the word CONSTITUTION.

(b) Using the keyword UNION, decode the ciphertext VVTZB ZEQUU NF

(c) What are some advantages of this cipher?

(d) What are some disadvantages of this cipher?

Optional Challenge: The following ciphertext was encoded using a Vigenère cipher with key AMENDMENT. What is the plaintext?

NAWBO PMRKS TEYOU RGBMQ SSSQE PXBQU HDDXR KEPMA DZCUH
UEIJL FLBNT FLRFA RFXNF SSWTI BPNQV ARDMA MIYIB IIEEU UF-
MAD YEAGE DXBEQ TEXSO VVEQH ORLMA