

HW # 5

Solution

1. (10 points) Decipher the following short English message using the Vigenere Cipher and the key “FAUST”.

BHIWO JRQAL MEMLH PEYHT XEWJX YMOKM MIXWM MEZSV YTBSM MEJGL
XEMKX XOHWZ TENZX

Please note that all spaces and punctuation characters have been removed from the message before encryption, and the letters of the ciphertext have been arranged for convenience and increased readability in the groups of five characters.

The result is

WHOEV ERWIS HESTO KEEPA SECRE TMUST HIDET HEFAC TTHAT HEPOS SESSE
SONEG OETHE

which reads as “Whoever wishes to keep a secret must hide the fact that he possesses one, Goethe.”

2. (10 points) Encrypt the message “Secrets travel fast in Paris” using the Playfair cipher (following the exact specification given in the Stallings book) using the key: NAPOLEON. Note: You should never use a password/key for a real cryptosystem that is so closely associated with the plaintext.

The setup of the Playfair cipher is as follows:

N	A	P	O	L
E	B	C	D	F
G	H	I/J	K	M
Q	R	S	T	U
V	W	X	Y	Z

The message is “SE|CR|ET|ST|RA|VE|LF|AS|TI|NP|AR|IS”.

The resulting ciphertext is: “QC|BS|DQ|TU|WB|NG|FM|PR|SK|AO|BW|SX”.

3. (10 points) Encrypt the message from question 2 using the Hill Cipher and the key

$$\begin{pmatrix} 3 & 12 \\ 19 & 5 \end{pmatrix}$$

If you use the Hill Cipher as defined in the Stallings book you would compute like this:

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 3 & 12 \\ 19 & 5 \end{pmatrix} \cdot \begin{pmatrix} 18 \\ 4 \end{pmatrix} = \begin{pmatrix} 102 \\ 362 \end{pmatrix} \equiv \begin{pmatrix} 24 \\ 24 \end{pmatrix} \pmod{26}$$

and the result is “YY CT GP WV ZL HD PA IM XL LK WH GI”

If you use the Hill Cipher as defined in the viewgraphs you would compute like this:

$$\begin{pmatrix} c_1 & c_2 \end{pmatrix} = \begin{pmatrix} 18 & 4 \end{pmatrix} \cdot \begin{pmatrix} 3 & 12 \\ 19 & 5 \end{pmatrix} = \begin{pmatrix} 130 & 236 \end{pmatrix} \equiv \begin{pmatrix} 0 & 2 \end{pmatrix} \pmod{26}$$

and the result is “AC RF JN ZZ ZW JM YB EM BI MX LH CE”