

CRYPTOGRAPHY HANDOUT

In each of the following problems, assume the coding scheme below:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	-1	2	-2	3	-3	4	-4	5	-5	6	-6	7	-7	8	-8
Q	R	S	T	U	V	W	X	Y	Z	blank	'	,	.	!	?
9	-9	10	-10	11	-11	12	-12	13	-13	14	-14	15	-15	16	-16

- (1) Use the matrix $M = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$ to encode the message: **ZAP!**

$$\begin{bmatrix} Z & A \\ P & ! \end{bmatrix} \rightarrow A = \begin{bmatrix} -13 & 1 \\ -8 & 16 \end{bmatrix} \rightarrow A \cdot M = \begin{bmatrix} -13 & 1 \\ -8 & 16 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} -21 & -10 \\ 64 & 40 \end{bmatrix}$$

- (2) The message $[-52, 42, 28, -21, -130, 106, -21, 17, 119, -98, 63, -51, -106, 87, 16, -15]$ was encoded using the matrix $M = \begin{bmatrix} 6 & -5 \\ -5 & 4 \end{bmatrix}$.

- (a) What is the matrix form of the message?

$$A \cdot M = \begin{bmatrix} -52 & 42 \\ 28 & -21 \\ -130 & 106 \\ -21 & 17 \\ 119 & -98 \\ 63 & -51 \\ -106 & 87 \\ 16 & -15 \end{bmatrix}$$

- (b) What matrix is needed for decoding the message?

$$M^{-1} = \frac{1}{6 \cdot 4 - (-5) \cdot (-5)} \cdot \begin{bmatrix} 4 & -(-5) \\ -(-5) & 6 \end{bmatrix} = (-1) \cdot \begin{bmatrix} 4 & 5 \\ 5 & 6 \end{bmatrix} = \begin{bmatrix} -4 & -5 \\ -5 & -6 \end{bmatrix}$$

- (c) What is the message?

$$A = (A \cdot M) \cdot M^{-1} = \begin{bmatrix} -52 & 42 \\ 28 & -21 \\ -130 & 106 \\ -21 & 17 \\ 119 & -98 \\ 63 & -51 \\ -106 & 87 \\ 16 & -15 \end{bmatrix} \cdot \begin{bmatrix} -4 & -5 \\ -5 & -6 \end{bmatrix} = \begin{bmatrix} -2 & 8 \\ -7 & -14 \\ -10 & 14 \\ -1 & 3 \\ 14 & -7 \\ 3 & -9 \\ -11 & 8 \\ 11 & 10 \end{bmatrix} \rightarrow \begin{bmatrix} D & O \\ N & ' \\ T & \\ B & E \\ & N \\ E & R \\ V & O \\ U & S \end{bmatrix}$$

The message is: **DON'T BE NERVOUS**