11. A cyber attack

Let us use the 2-dimensional affine enciphering function

$$f_E : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix} \mod 26 \tag{11.1}$$

to encipher the plaintext

N O A N S W E R

over the 26-letter alphabet with A $\leftrightarrow$ 0, B $\leftrightarrow$ 1, …, Z $\leftrightarrow$ 25. We begin by converting the plaintext to a sequence of column vectors over $\mathbb{Z}_{26}$, each vector of length 2.

$$\begin{pmatrix} \mathrm{N} \\ \mathrm{O} \end{pmatrix} \begin{pmatrix} \mathrm{A} \\ \mathrm{N} \end{pmatrix} \begin{pmatrix} \mathrm{S} \\ \mathrm{W} \end{pmatrix} \begin{pmatrix} \mathrm{E} \\ \mathrm{R} \end{pmatrix} \leftrightarrow \begin{pmatrix} 13 \\ 14 \end{pmatrix} \begin{pmatrix} 0 \\ 13 \end{pmatrix} \begin{pmatrix} 18 \\ 22 \end{pmatrix} \begin{pmatrix} 4 \\ 17 \end{pmatrix} \tag{11.2}$$

We then apply f_E to each column vector in turn. For the first vector we get:

$$f_E \begin{pmatrix} 13 \\ 14 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 13 \\ 14 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix} \mod 26 \tag{11.3}$$

$$\equiv \begin{pmatrix} 69 \\ 205 \end{pmatrix} \mod 26 \tag{11.4}$$

$$\equiv \begin{pmatrix} 17 \\ 23 \end{pmatrix} \mod 26 \tag{11.5}$$

$$\leftrightarrow \begin{pmatrix} \mathrm{Q} \\ \mathrm{W} \end{pmatrix} \tag{11.6}$$

For the subsequent three vectors we get:

$$f_E\begin{pmatrix}0\\13\end{pmatrix}=\begin{pmatrix}14\\2\end{pmatrix}\leftrightarrow\begin{pmatrix}\mathrm{O}\\\mathrm{C}\end{pmatrix} \tag{11.7}$$

$$f_E\begin{pmatrix}18\\22\end{pmatrix}=\begin{pmatrix}25\\18\end{pmatrix}\leftrightarrow\begin{pmatrix}\mathrm{Z}\\\mathrm{S}\end{pmatrix} \tag{11.8}$$

$$f_E\begin{pmatrix}4\\17\end{pmatrix}=\begin{pmatrix}8\\10\end{pmatrix}\leftrightarrow\begin{pmatrix}\mathrm{I}\\\mathrm{K}\end{pmatrix} \tag{11.9}$$

The ciphertext to be communicated to the receiver is thus:

Q W O C Z S I K

The deciphering function corresponding to (11.1) is:

$$f_D\colon\begin{pmatrix}x\\y\end{pmatrix}\mapsto\begin{pmatrix}2&3\\7&8\end{pmatrix}^{-1}\left(\begin{pmatrix}x\\y\end{pmatrix}-\begin{pmatrix}1\\2\end{pmatrix}\right)\qquad\mod 26 \tag{11.10}$$

$$=\begin{pmatrix}14&11\\17&18\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}16\\15\end{pmatrix} \tag{11.11}$$

This 2-dimensional cryptosystem over the 26-letter alphabet has a key space of size 98804160. Assuming it takes 1 second to apply f_D, for a given choice of deciphering key D, to a ciphertext to decide if the corresponding 'plaintext' is meaningful, then it would take over three years of continuous computing to run through all possible keys. If a user felt this was insufficiently secure, then a higher dimensional affine system and/or a larger alphabet could be used. For instance, an affine cryptosystem of dimension $k=3$ over a 103-letter alphabet has a key space of size 1411784169290494225596864. Assuming again 1 second to apply f_D and evaluate the output, it would take 4×10^{16} years of continuous computing to run through all possible keys. To place this number in some context, we note that the Earth is estimated to be only 4.5×10^{9} years old.

11.1 A secure cryptosystem in inexperienced hands

Algebra is the basis of secure cryptography. But algebra can also be used to exploit the inexperience of users. To illustrate the latter, suppose that we have intercepted the ciphertext

NHVGR!_ECTFMXSST_XFPOVMJB?ZSKRTCZ_GKJDDLGKQAMCXIROMTHOOTO
VHOVIDAPY_E_XBOFXKRDPXISI?YMTAAJZDPLW

which we know has been created using an affine cryptosystem

$$f_E\colon v\mapsto\mathbf{A}v+\mathbf{B}\qquad\mod 29 \tag{11.12}$$

of dimension $k=2$ over the alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ_?!

of 29 letters. We wrtie matrices in bold font in this section, so as to distinguish them from letters of the alphabet. Without any additional information about the ciphertext it would be quite difficult to determine the corresponding plaintext. However, suppose that we know the ciphertext was sent from Active Agent Karla, and that this inexperienced agent always signs off messages with:

AA_KARLA

This extra information provides tells us:

$$f_E\begin{pmatrix}\mathrm{A}\\ \mathrm{A}\end{pmatrix}=\begin{pmatrix}\mathrm{A}\\ \mathrm{A}\end{pmatrix},\ f_E\begin{pmatrix}0\\ 0\end{pmatrix}\equiv\begin{pmatrix}0\\ 0\end{pmatrix}\qquad \text{mod } 29 \tag{11.13}$$

$$f_E\begin{pmatrix}\_\\ \mathrm{K}\end{pmatrix}=\begin{pmatrix}\mathrm{J}\\ \mathrm{Z}\end{pmatrix},\ f_E\begin{pmatrix}26\\ 10\end{pmatrix}\equiv\begin{pmatrix}9\\ 25\end{pmatrix}\qquad \text{mod } 29 \tag{11.14}$$

$$f_E\begin{pmatrix}\mathrm{A}\\ \mathrm{R}\end{pmatrix}=\begin{pmatrix}\mathrm{D}\\ \mathrm{P}\end{pmatrix},\ f_E\begin{pmatrix}0\\ 17\end{pmatrix}\equiv\begin{pmatrix}3\\ 15\end{pmatrix}\qquad \text{mod } 29 \tag{11.15}$$

$$f_E\begin{pmatrix}\mathrm{L}\\ \mathrm{A}\end{pmatrix}=\begin{pmatrix}\mathrm{L}\\ \mathrm{W}\end{pmatrix},\ f_E\begin{pmatrix}11\\ 0\end{pmatrix}\equiv\begin{pmatrix}11\\ 22\end{pmatrix}\qquad \text{mod } 29 \tag{11.16}$$

Equation (11.13) tells us that

$$\mathbf{A0}+\mathbf{B}=\mathbf{0}\qquad \text{mod } 29 \tag{11.17}$$

and thus that the active agent has chosen $\mathbf{B}$ to be the zero vector $\mathbf{B}\equiv\mathbf{0}$. The deciphering function is thus:

$$f_D\colon v\mapsto \mathbf{A}^{-1}v\qquad \text{mod } 29 \tag{11.18}$$

Equations(11.15) and (11.16) can be combined into the following single matrix equation.

$$\mathbf{A}\begin{pmatrix}0&11\\ 17&0\end{pmatrix}\equiv\begin{pmatrix}3&11\\ 15&22\end{pmatrix}\qquad \text{mod } 29 \tag{11.19}$$

Multiplying both sides of equation (11.19) on the left by $\mathbf{A}^{-1}$, and multiplying both sides on the right by

$$\begin{pmatrix}3&11\\ 15&22\end{pmatrix}^{-1}\qquad \text{mod } 29 \tag{11.20}$$

yields the equation:

$$\begin{pmatrix}0&11\\ 17&0\end{pmatrix}\begin{pmatrix}3&11\\ 15&22\end{pmatrix}^{-1}\equiv\mathbf{A}^{-1}\qquad \text{mod } 29 \tag{11.21}$$

Since matrix multiplication is not commutative it is important to distinguish between multiplying on the right and multiplying on the left in these calculations.

To evaluate the inverse matrix (11.20) we note that:

$$5\times 22-15\times 11=-99\equiv 17\qquad \text{mod } 29 \tag{11.22}$$

We can use the Bézout identity to establish:

$$17^{-1}\equiv 12\qquad \text{mod } 29 \tag{11.23}$$

Equation (11.21) now yields

$$\mathbf{A}^{-1}=\begin{pmatrix}0&11\\ 17&0\end{pmatrix}12\begin{pmatrix}22&-11\\ -15&5\end{pmatrix}\qquad \text{mod } 29 \tag{11.24}$$

$$=\begin{pmatrix}21&19\\ 22&18\end{pmatrix}\qquad \text{mod } 29 \tag{11.25}$$

The reader should now use the deciphering function (11.18) to determine (at least a portion of) the plaintext. This worthwhile exercise will provide plenty of practice at modular arithmetic.