

**2.18** Let  $a, b, c, d, e, f$  be integers mod 26. Consider the following combination of the Hill and affine ciphers: Represent a block of plaintext as a pair  $(x, y)$  mod 26. The corresponding ciphertext  $(u, v)$  is

$$(x \ y) \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e \ f) \equiv (u \ v) \pmod{26}$$

Describe how to carry out a chosen plaintext attack on this system (with the goal of finding the key  $a, b, c, d, e, f$ ). You should state explicitly what plaintexts you choose and how to recover the key.

For a chosen plaintext attack, we will use the four plaintexts BA, AB, AZ, and ZA. Using BA = (1 0), we have

$$(1 \ 0) \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e \ f) \equiv (a+e \ b+f).$$

Similarly, for AB = (0 1), we have  $(0 \ 1) \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e \ f) \equiv (c+e \ d+f)$ .

Now, we have the quantities  $a+e, c+e, b+f,$  and  $d+f$ . Using ZA = (-1 0), we have

$$(-1 \ 0) \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e \ f) \equiv (-a+e \ -b+f).$$

Similarly, for AZ = (0 -1), we get  $(0 \ -1) \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e \ f) \equiv (-c+e \ -d+f)$ .

Using the quantities  $a+e$  and  $-a+e, c+e$  and  $-c+e$  we can determine the values for  $a, c,$  and  $e$ . Similarly, knowing the values of  $b+f, -b+f, d+f,$  and  $-d+f,$  we can determine the values of  $b, d,$  and  $f$ . So, using the plaintexts  $ab, ba, az,$  and  $za,$  we can find the values of  $a, b, c, d, e, f$ .