Question Suppose we have a ciphertext and we know that the cipher is an affine transform but not which one, how do we find the plaintext?

We use the frequency of occurrence of letters in English:

	A	B	C	D	E	F	G	H	I	J	K	L	M
%	7.8	1.3	2.9	4.4	13.1	2.8	1.4	5.9	6.8	<1	<1	3.6	2
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
%	7.3	8.2	2.2	<1	6.7	6.5	9.0	3.8	1.0	1.5	<1	1.5	<1

Theorem 16.5. *Let $a, b, c, d, e, f \in \mathbb{Z}$ and $n \in \mathbb{N}$. Take $\Delta = ad - bc$ and suppose that $\Delta \in \mathbb{N}$ and $(\Delta, n) = 1$. Then the system of congruences*

$$ax + by \equiv e \pmod{n}, \tag{16.1}$$
$$cx + dy \equiv f \pmod{n} \tag{16.2}$$

has a unique solution modulo n given by

$$x \equiv x_0 \pmod{n} \quad \text{and} \quad y \equiv y_0 \pmod{n},$$

with

$$x_0 = \Delta'(de - bf) \quad \text{and} \quad y_0 = \Delta'(af - ce),$$

where $\Delta' \in \mathbb{Z}$ satisfies $\Delta'\Delta \equiv 1 \pmod{n}$. In other words, if $\Delta = ab - bc$ satisfies $\Delta \in \mathbb{N}$ and $(\Delta, n) = 1$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} e \\ f \end{pmatrix} \pmod{n} \quad \Leftrightarrow \quad \begin{pmatrix} x \\ y \end{pmatrix} \equiv \Delta'\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} e \\ f \end{pmatrix} \pmod{n}$$

for $\Delta' \in \mathbb{Z}$ satisfying $\Delta'\Delta \equiv 1 \pmod{n}$.

Proof

$$\begin{aligned} d \times (16.1) - b \times (16.2) &\Rightarrow d(ax + by) - b(cx + dy) = de - bf \\ &\Rightarrow (ad - bc)x = de - bf \\ &\Rightarrow \Delta x = de - bf \\ &\Rightarrow \Delta'\Delta x = \Delta'(de - bf) = x_0 \\ &\Rightarrow x \equiv \Delta'\Delta x \pmod{n} \equiv x_0 \pmod{n} \end{aligned}$$

and

$$\begin{aligned} a \times (16.2) - c \times (16.1) &\Rightarrow a(cx + dy) - c(ax + by) = af - ce \\ &\Rightarrow (ad - bc)y = af - ce \\ &\Rightarrow \Delta y = af - ce \\ &\Rightarrow \Delta'\Delta y = \Delta'(af - ce) = y_0 \\ &\Rightarrow y \equiv \Delta'\Delta y \pmod{n} \equiv y_0 \pmod{n}. \end{aligned}$$