Example 16.2 (Deciphering).

	Q	X	P	E	H	U	W	K	H	R	U	B	L	V	H	D	V	B	ciphertext
$\to$	16	23	15	4	7	20	22	10	7	17	20	1	11	21	7	3	21	1	
$\to$	13	20	12	1	4	17	19	7	4	14	17	24	8	18	4	0	18	24	
$\to$	N	U	M	B	E	R	T	H	E	O	R	Y	I	S	E	A	S	Y	
$\to$	N	U	M	B	E	R	T	H	E	O	R	Y	I	S	E	A	S	Y	plaintext

Definition 16.3. If x is a plaintext letter and y is the corresponding ciphertext letter then, for any $c \in \mathbb{N}$ with $1 \le c \le 25$,

$$y \equiv x + c \pmod{26}$$

is called a *shift transformation*. For $b \in \mathbb{N}$ with $1 \le b \le 25$ and $(b, 26) = 1$,

$$y \equiv bx + c \pmod{26}$$

is called an *affine transformation*.

To encipher with a known affine transformation τ,

(1) divide the message into groups of 5 letters;

(2) change letters to numbers;

(3) apply τ;

(4) change numbers to letters.

To decipher, we reverse the process:

(1) change letters to numbers;

(2) apply τ^{-1};

(3) change numbers to letters;

(4) rearrange into words.

Note 16.4. Suppose that $\tau(x) \equiv bx + c \pmod{26}$ for some $b, c \in \mathbb{N}$ with $1 \le b, c \le 25$ and $(b, 26) = 1$. Suppose further that $b' \in \mathbb{N}$ satisfies $1 \le b' \le 25$, $(b', 26) = 1$ and $bb' \equiv 1 \pmod{26}$:

b	1	3	5	7	9	11	15	17	19	21	23	25
b'	1	9	21	15	3	19	7	23	11	5	17	25

Then $y \equiv b\tau^{-1}(y) + c \pmod{26}$. Hence

$$b'y \equiv b'\left[b\tau^{-1}(y) + c\right] \pmod{26} \equiv b'b\tau^{-1}(y) + b'c \pmod{26} \equiv \tau^{-1}(y) + b'c \pmod{26},$$

giving that $\tau^{-1}(y) \equiv b'[y - c] \pmod{26}$.

So if $y \equiv bx + c \pmod{26}$, then $x \equiv b'[y - c] \pmod{26}$.