Math 135 (Summer 2006)
Shift Ciphers and Modular Arithmetic

Example: Find the values of the function $f(x) = (x+3)\,\mathrm{MOD}\,7$ on the domain $\{0,1,2,3,4,5,6\}$. (Compare this with problem 5 in §2.1.) Find a formula for f^{-1}.

Solution: We see that f is given by

x	0	1	2	3	4	5	6
$f(x)$	3	4	5	6	0	1	2

As for f^{-1}, we observe that $0 \mapsto 4$, $1 \mapsto 5$, ..., $3 \mapsto 0$, etc., so that

$$f^{-1}(y) = (y+4)\,\mathrm{MOD}\,7.$$

Notice that it is equivalent to write $f^{-1}(y) = (y-3)\,\mathrm{MOD}\,7$.

We can use modular arithmetic to help "automate" the process of enciphering and deciphering Caesar-type $+k$ shift ciphers. Begin by writing down the numerical equivalents of the letters as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

If x denotes the plaintext numerical equivalent of a string, then a shift of $+k$ letters can be computed as

$$E_k(x) = (x+k)\,\mathrm{MOD}\,26$$

and if y denotes the ciphertext numerical equivalent, then the decipherment function (which is a shift by $-k$) is given by

$$D_k(y) = (y-k)\,\mathrm{MOD}\,26.$$

(As an aside, note that $D_k(y) = E_k^{-1}(y) = E_{-k}(y)$.)

Example: key $k = 7$; plaintext = `THURSDAY`; find the ciphertext

Solution: Using the letters-to-numerical equivalents chart above, we find

plaintext	T	H	U	R	S	D	A	Y
x	19	7	20	17	18	3	0	24
$x+7$	26	14	27	24	25	10	7	31
$(x+7)\,\mathrm{MOD}\,26$	0	14	1	24	25	10	7	5
ciphertext	A	O	B	Y	Z	K	H	F

Example: key $k = 11$; ciphertext = `QCTOLJ`; find the plaintext

Solution: Using the letters-to-numerical equivalents chart above, we find

ciphertext	Q	C	T	O	L	J
y	16	2	19	14	11	9
$y-11$	5	-9	8	3	0	-2
$(y-11)\,\mathrm{MOD}\,26$	5	17	8	3	0	24
plaintext	F	R	I	D	A	Y