Mathematics 124 (Winter 2009)
Permutations

Example. Consider the permutation

$$(1 \mapsto 4 \mapsto 2 \mapsto 5 \mapsto 1) \quad (3 \mapsto 3).$$

Determine p and q.

Solution. We have

x	1	2	3	4	5
$p(x)$					

and

x	1	2	3	4	5
$q(x)$					

Example. Use the permutation just defined to encipher `TYLER`.

Solution. Since

$$(1 \mapsto 4 \mapsto 2 \mapsto 5 \mapsto 1) \quad (3 \mapsto 3).$$

we find

x	T	Y	L	E	R
	1	2	3	4	5
$p(x)$					

and to decrypt we have

x					
	1	2	3	4	5
$q(x)$	T	Y	L	E	R

Example. Consider the following ciphertext.

```
ERLYT TMEEM THTAE UBLCE SEUOH IXSTA
```

The plaintext was encrypted by writing the original message row-wise in five columns. The columns were then permuted according to p. Determine the message.