（科目：　　）清华大学数学作业纸

编号：　　班级：　　姓名：

1.6、移位密码：

$e_k(x) = (x+k) \bmod 26$ ~~$e_k(x) = d$~~ $e_k = dy\,dx$.

$d_k(y) = (y-k) \bmod 26$.

即：~~$x+k = y$~~ $x+k = y-k+026\cdot n$, $n \in \mathbb{Z}$

即：$2k = 26\cdot n$, $n \in \mathbb{Z}$. $k = 13\cdot n$, $n \in \mathbb{Z}$. $0 < k \leq 25$

~~我们发现 $n=0, \pm 2$ 时, $e_k(x)$ 是同一个函数, $d_k(y)$ 也是同一个~~

~~$n = 0, \pm 1, \pm 3$,~~ ∴ $n = 0$ 或 1.

∴ $e_k(x) = (x+0)\ x \bmod 26$

$d_k(y) = x \bmod 26$

或 $e_k(x) = (x+13) \bmod 26$

$d_k(y) = (x-13) \bmod 26$.

1.7. $m = 30100$. 仿射密码密钥量.

~~gcd~~ $\varphi(m) = 35$. $35 \times 26 = 910$.

$m = 1225$

$\varphi(m) = 8$. $8 \times 26 = 208$.