CIS 3223 TMQ 3

Dr Anthony Hughes

Name: Solutions

Temple ID (last 4 digits:

6

1 (10 pts) Use the **modular exponentiation** algorithm to calculate $3^{25} \pmod{31}$.

$z = 1 \qquad 25 = 11001_2$

digit	power	z
1	3	3
0	9	3
0	$81 \equiv_{31} 19$	3
1	$361 \equiv_{31} 20$	$20 \times 3 = 60 \equiv_{31} 29$
1	$400 \equiv_{31} 28$	$28 \times 29 = 812 \equiv_{31} 6$

$-3 \times -2 \equiv_{31} 6$

2 (10 pts) Consider an RSA key set with $N = 77$ and $e = 7$.

What value of d should be used for the secret key? 53 (-1 for -7)

$N = 7 \times 11 \quad \varphi(N) = \varphi(7)\varphi(11) = 6 \times 10 = 60$

Want solns to $60x + 7y = 1$

a	b	q	r	Q
60	7	8	4	$\begin{bmatrix} 0 & 1 \\ 1 & -8 \end{bmatrix}$
7	4	1	3	$\begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & -8 \end{bmatrix} = \begin{bmatrix} 1 & -8 \\ -1 & 9 \end{bmatrix}$
4	3	1	1	$\begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & -8 \\ -1 & 9 \end{bmatrix} = \begin{bmatrix} -1 & 9 \\ 2 & -17 \end{bmatrix}$
3	1	3	0	$\begin{bmatrix} 0 & 1 \\ 1 & -3 \end{bmatrix}\begin{bmatrix} -1 & 9 \\ 2 & -17 \end{bmatrix} = \begin{bmatrix} 2 & -17 \\ -7 & 60 \end{bmatrix}$ check

$y = -7 \quad d = -7 + 60 = 53$

Could $e = 5$ be chosen? yes (no)

Justify your answer.

$\gcd(5, 60) = 5 \neq 1$