Name: ______________________________

1. (10 points) Consider an RSA key set with $p = 13$, $q = 17$, $n = 221$, and $e = 5$. Use the extended Euclidean algorithm to determine the decryption exponent d. **Show all steps of the computation.**

Solution: We need to find d such that $d \cdot e \equiv 1 \bmod \phi(n)$. $\phi(n) = (p-1)(q-1) = 192$. Using the extended Euclidean algorithm, we can find x and y such that $x \cdot e + y \cdot \phi(n) = 1$ and so $x \cdot e \equiv 1 \bmod \phi(n)$ and $d = x$:

a	b	r	q	s	t
				1	0
				0	1
192	5	2	38	1	-38
5	2	1	2	-2	77
2	1	0	2		

This gives $x = 77$ and $y = -2$; we can check this

$$77 \cdot 5 + (-2) \cdot 192 = 1.$$

Therefore, $d = 77$.

(continued on other side)

2. (5 points) Using the same key set as in problem #1, compute the encryption of the message $M = 4$. **Show all work.**

Solution: We need to compute $M^e \bmod n$ with $M = 4$, $e = 5$, and $n = 221$:

$$4^5 \bmod 221 = 1024 \bmod 221 = 1024 - 4 \cdot 221 = 140.$$

3. (5 points) Using the RSA key set $p = 11$, $q = 29$, $n = 319$, $e = 3$, and $d = 187$, verify that $S = 10$ is a valid signature for the message $M = 43$. **Show all work.**

Solution: To verify the signature, we compute $M' = S^e \bmod n$ and verify that $M' = M$:

$$M' = 10^3 \bmod 319 = 1000 \bmod 319 = 1000 - 3 \cdot 319 = 43 = M.$$