Solutions to the Attendance Quiz # 16 for Dr. Z.'s Number Theory Course for Oct. 31, 2013

1. For the following primes p and q (let $n = pq$) public key e, and encrypted message c

(i) Check that e is an OK key, i.e. that it is coprime to $\phi(n)$.

(ii) Find the deciphering key, d, such that $de \equiv 1 \pmod{\phi(n)}$

(iii) Suppose Alice sent you the encrypted message c. Check that this is an OK message (coprime to n), and if it is find her original message?, m

$$p = 5 \quad , \quad q = 7 \quad , \quad e = 5 \quad , \quad c = 9 \quad .$$

Sol. to 1.: (i) $n = 5 \cdot 7 = 35$, $\phi(35) = (5-1)(7-1) = (4)(6) = 24$. Since $gcd(5, 24) = 1$ it is an OK key.

(ii) $d = [5^{-1}]_{24} = 5$ (since $5 \cdot 5 = 25 \equiv 1 \pmod{24}$).

(iii) $gcd(9, 35) = 1$ (since $9 = 3^2$ and $35 = 5 \cdot 7$ so they don't share primes, in real life you would need to use the Euclidean algorithm, but here we can take shortcuts).

The original message m is $c^d \pmod{n}$, so

$$m = 9^5 \pmod{35} \quad .$$

$$9^1 \; modulo \; 35 = 9$$

$$9^2 \; modulo \; 35 = 81 \; modulo \; 35 = 11 \quad ,$$

$$9^4 \; modulo \; 35 = 11^2 \; modulo \; 35 = 121 \; modulo \; 35 = 16 \quad .$$

So

$$9^5 \; modulo \; 35 = 9^1 \cdot 9^4 \; modulo \; 35 = 9 \cdot 16 \; modulo \; 35 = 144 \; modulo \; 35 = 4 \quad .$$

Ans. to 1(iii): The original 'message' was 4.