CSE 5351 Homework 6

Due: Tuesday April 14

1. $\varphi(2400) = ?$
2. $19^{12362448602} \bmod 21 = ?$
3. What's the order of 2 in $\mathbb{Z}_{21}^*$?
4. In an RSA system, the public key of a user is $e = 31,\ N = 3599$. What is the private key of this user?
5. In a public-key system using RSA, you intercept a cipertext $c = 61$ sent to a user whose public key is $N = 155$ and $e = 7$. What is the plaintex m?
6. Fix the RSA modulus N, and assume there is an adversary/PPA A running in time t for which

$$\Pr\left[A\left(x^e \bmod N\right) = x : x \leftarrow_u \mathbb{Z}_N^* \right] = 0.01.$$

That is, A can correctly decrypt the ciphertext of a random message x with probability 0.01.

Using A as a subroutine, construct an adversary A' for which

$$\Pr\left[A'\left(x^e \bmod N\right) = x : x \leftarrow_u Z_N^* \right] \geq 0.99.$$

That is, A' can correctly decrypt a random challenge ciphertex with probability ≥ 0.99.

The running time of A' must be polynomial in t and $\|N\|$.

Hint: use the homomorphism property of RSA.