Math 4320 — Introduction to Algebra. Homework 3

Questions on RSA.

1. Suppose the public key is $N = 55$ and $s = 3$, and the secret key is $t = 27$.
   (a) Encrypt 12.
   (b) Decrypt 20.

2. Suppose the public key is $N = 187$ and $s = 3$, find the secret key.

3. Alice uses three different public keys N_1, N_2 and N_3 (all with $s = 3$), to send the same message x, an integer satisfying $0 \leq x < N_i$ for all i. Suppose Eve intercepts the three encrypted messages $x^3 \mod N_i$.
   (a) Explain an efficient way for Eve to find x if $\gcd(N_1, N_2, N_3) \neq 1$.
   (b) Explain an efficient way for Eve to find x if $\gcd(N_1, N_2, N_3) = 1$.
   Hint. Use the Chinese Remainder Theorem.

TRR