MATH 587/CSCE 557: HOMEWORK 8, DUE APR 12.

1. An RSA cryptosystem has public key $N = 35$ and $e = 7$. Messages are encrypted one letter at a time, converting letters to numbers by $A = 2, B = 3, ..., Z = 27$, space $= 28$.

(a) Showing your working, encrypt the message: BE GOOD.

(b) Find the decryption exponent d and decrypt the message: 20 23 26 7 15 16

(c) This choice of N and e has several weaknesses - name at least two different ones.

(d) Even if a good choice of N and e is made, the method of encrypting one letter at a time has weaknesses. Describe how we might find the plaintext if a very long ciphertext is given.

(e) Oscar intercepts the message $365, 0, 4845, 14930, 2608, 2608, 0$ from Alice to Bob. How do you think they are converting letters to numbers? Decrypt the message.

2. (a) Suppose Alice sends the same message x (e.g. her credit card number), encrypted, to three companies, all of which use the easy choice of $e = 3$ in their public key. Oscar intercepts these encrypted messages, i.e. $x^3 \pmod{N_1}, x^3 \pmod{N_2}, x^3 \pmod{N_3}$, where N_1, N_2, N_3 are the moduli used in the companies' public keys. There is a method (the Chinese Remainder Theorem) by which he can deduce the value of $x^3 \pmod{N_1 N_2 N_3}$. Why can he now compute x exactly? [Hint: how big is x^3 versus $N_1 N_2 N_3$?] This is why $e = 3$ is a poor choice in practice.

(b) A popular choice for e is 65537. Why is this a good choice in practice? [Hint: factor 65536.]