CSCI 3330: RSA by Hand

Do all computations by hand!

1 Key derivation

Suppose you have chosen primes $p = 11$ and $q = 17$, and you choose $e = 3$. What is your RSA public key?

2 Encryption

Suppose you encrypt $x = 4$ with the above key. What is the result? Is there a security problem when using a small e with a small x (relative to $n = p \times q$)? If c is your encrypted result, what is $\sqrt[e]{c}$?

3 Decrypting my ATM PIN code

Suppose you encounter an RSA public key ($n = 1257$, $e = 279$), and you wish to derive the corresponding private key. What are p and q? **Hint:** try factoring increasingly greater primes beginning with the smallest until you find a factor.

Using the Extended Euclidean Algorithm, you find that, given these p and q, the corresponding private exponent is $d = 3$. Suppose my ATM PIN code encrypted with this public key is 823. What is my ATM PIN code unencrypted? **Hint:** recall that in modular exponentiation,

$$x^d \ \% \ n = ((x^{d-k} \ \% \ n) \times x^k) \ \% \ n.$$

So, for example, if $d = 5$,

$$x^5 \ \% \ n = (((x \times x \ \% \ n) \times x \ \% \ n) \times x \ \% \ n) \times x \ \% \ n.$$

4 Malleability of RSA

Suppose I intercept an encrypted message $c = x^e \ \% \ n$ encrypted some public key (n, e), but I don't know the private key. I substitute the encrypted message c with $((c \times 2^e) \ \% \ n)$. If the original unencrypted message was x, what is the result of the substitute message when decrypted?