CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song

HW 5

Due: Friday, 9/28, 10pm

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Quick Computes

Simplify each expression using Fermat's Little Theorem.

(a) $3^{33} \pmod{11}$

(b) $10001^{10001} \pmod{17}$

(c) $10^{10} + 20^{20} + 30^{30} + 40^{40} \pmod{7}$

2 RSA Practice

Bob would like to receive encrypted messages from Alice via RSA.

(a) Bob chooses $p = 7$ and $q = 11$. His public key is (N, e). What is N?

(b) What number is e relatively prime to?

(c) e need not be prime itself, but what is the smallest prime number e can be? Use this value for e in all subsequent computations.

(d) What is $\gcd(e, (p-1)(q-1))$?

(e) What is the decryption exponent d?

(f) Now imagine that Alice wants to send Bob the message 30. She applies her encryption function E to 30. What is her encrypted message?

(g) Bob receives the encrypted message, and applies his decryption function D to it. What is D applied to the received message?

3 Squared RSA

(a) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where a is coprime to p, and p is prime. (Hint: Try to mimic the proof of Fermat's Little Theorem from the notes.)

(b) Now consider the RSA scheme: the public key is $(N = p^2q^2, e)$ for primes p and q, with e relatively prime to $p(p-1)q(q-1)$. The private key is $d = e^{-1} \pmod{p(p-1)q(q-1)}$. Prove that the scheme is correct for x relatively prime to both p and q, i.e. $x^{ed} \equiv x \pmod{N}$.

(c) Prove that this scheme is at least as hard to break as normal RSA; that is, prove that if this scheme can be broken, normal RSA can be as well. We consider RSA to be broken if knowing pq allows you to deduce $(p-1)(q-1)$. We consider squared RSA to be broken if knowing p^2q^2 allows you to deduce $p(p-1)q(q-1)$.