CS 70 Discrete Mathematics and Probability Theory
Spring 2018 Satish Rao and Babak Ayazifar

# HW 5

## Sundry

Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of homework party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

Please copy the following statement and sign next to it:

*I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.*

## 1 Breaking RSA

(a) Eve is not convinced she needs to factor $N = pq$ in order to break RSA. She argues: "All I need to know is $(p-1)(q-1)$... then I can find $d$ as the inverse of $e$ mod $(p-1)(q-1)$. This should be easier than factoring $N$." Prove Eve wrong, by showing that if she knows $(p-1)(q-1)$, she can easily factor $N$ (thus showing finding $(p-1)(q-1)$ is at least as hard as factoring $N$). Assume Eve has a friend Wolfram, who can easily return the roots of polynomials over $\mathbb{R}$ (this is, in fact, easy).

(b) When working with RSA, it is not uncommon to use $e = 3$ in the public key. Suppose that Alice has sent Bob, Carol, and Dorothy the same message indicating the time she is having her birthday party. Eve, who is not invited, wants to decrypt the message and show up to the party. Bob, Carol, and Dorothy have public keys $(N_1, e_1), (N_2, e_2), (N_3, e_3)$ respectively, where $e_1 = e_2 = e_3 = 3$. Furthermore assume that $N_1, N_2, N_3$ are all different. Alice has chosen a number $0 \leq x < \min\{N_1, N_2, N_3\}$ which indicates the time her party starts and has encoded it via the three public keys and sent it to her three friends. Eve has been able to obtain the three encoded messages. Prove that Eve can figure out $x$. First solve the problem when two of $N_1, N_2, N_3$ have a common factor. Then solve it when no two of them have a common factor. Again, assume Eve is friends with Wolfram as above.

*Hint*: The concept behind this problem is the Chinese Remainder Theorem: Suppose $n_1, \ldots, n_k$

are positive integers, that are pairwise co-prime. Then, for any given sequence of integers $a_1, ..., a_k$, there exists an integer $x$ solving the following system of simultaneous congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Furthermore, all solutions $x$ of the system are congruent modulo the product, $N = n_1 \cdots n_k$. Hence: $x \equiv y \pmod{n_i}$ for $1 \leq i \leq k \iff x \equiv y \pmod{N}$.

## 2 Squared RSA

(a) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where $a$ is relatively prime to $p$ and $p$ is prime.

(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, i.e. $x^{ed} \equiv x \pmod{N}$. You may assume that $x$ is relatively prime to both $p$ and $q$.

(c) Continuing the previous part, prove that the scheme is unbreakable, i.e. your scheme is at least as difficult to break as ordinary RSA.

## 3 Badly Chosen Public Key

Your friend would like to send you a message using the RSA public key $N = (pq, e)$. Unfortunately, your friend did not take CS 70, so your friend mistakenly chose $e$ which is *not* relatively prime to $(p-1)(q-1)$. Your friend then sends you a message $y = x^e$. In this problem we will investigate if it is possible to recover the original message $x$. Throughout this problem, assume that you have discovered an integer $a$ which has the property that $a^{(p-1)(q-1)} \equiv 1 \pmod{N}$, and for any positive integer $k$ where $1 \leq k < (p-1)(q-1)$, $a^k \not\equiv 1 \pmod{N}$.

(a) Show that for any integer $z$ which is relatively prime to $N$, $z$ can be written as $a^k \pmod{N}$ for some integer $0 \leq k < (p-1)(q-1)$. [*Hint*: Show that $1, a, a^2, \ldots, a^{(p-1)(q-1)-1}$ are all distinct modulo $N$. Think of the proof for Fermat's Little Theorem.]

(b) Show that if $k$ is any integer such that $a^k \equiv 1 \pmod{N}$, then $(p-1)(q-1) \mid k$.

(c) Assume that $y$ is relatively prime to $N$. By the first part, we can write $y \equiv a^\ell \pmod{N}$ for some $\ell \in \{0, \ldots, (p-1)(q-1)-1\}$. Show that if $k$ is an integer such that $(p-1)(q-1) \mid ek - \ell$, then $\tilde{x} := a^k$ satisfies $\tilde{x}^e \equiv y \pmod{N}$.

(d) Unfortunately the solution $\tilde{x}$ found in the previous part might not be the original solution $x$. Show that if $d := \gcd(e, (p-1)(q-1)) > 1$, then there are exactly $d$ distinct integers $x_1, \ldots, x_d$ which are all distinct modulo $N$ such that $x_i^e = y$, $i = 1, \ldots, d$. [*Hint*: You will probably find it helpful to use $a$ as a tool here.]

## 4 Quantum Factoring

We're pretty sure that classical computers can't break RSA (because it is hard to factor large numbers on them), but we know that quantum computers theoretically could. The fact that we will prove in this question is a key part of Shor's Algorithm, a quantum algorithm for factoring large numbers quickly.

(a) Let $N = pq$, for primes $p$ and $q$. Prove that, for all $a \in \mathbb{N}$, there are only four possible values for $gcd(a,N)$.

(b) Again, let $N = pq$. Using part (a), prove that, if $r^2 = 1 \mod N$ and $r \not\equiv \pm 1 \pmod{N}$ (i.e. $r$ is a "nontrivial square root of 1" mod $N$), then $gcd(r-1,N)$ is one of the prime factors of $N$. *Hint:* $r^2 = 1 \mod N$ *can be rewritten as* $r^2 - 1 = 0 \mod N$ *or* $(r+1)(r-1) = 0 \mod N$.

## 5 Polynomial Short Answer

For each of these questions, please provide a brief justification or explanation unless otherwise specified.

(a) Sanity checks (no justification needed):

(i) A degree $d$ nonzero polynomial in $\mathbb{R}$ has at most __ roots.

(ii) A degree $d$ nonzero polynomial in $GF(p)$ has at most min(__, $p$) roots.

(iii) $d$ points determine an at most __-degree polynomial.

(b) In a Galois Field, why does it make sense that we require $p$ to be a prime? (Hint: look at the properties of a field in note 8.)

(c) Use Lagrange interpolation to find a degree-2 polynomial that passes through these points in $GF(7)$: $(0,1),(5,0),(6,2)$.

(d) Using Fermat's Little Theorem, show that for every prime $p$, every polynomial over $GF(p)$ with degree $\geq p$ is equivalent to a polynomial of degree at most $p-1$. (Two polynomials are equivalent if they evaluate to the same value for every $x \in GF(p)$.

## 6 Rational Root Theorem

The rational root theorem states that for a polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

$a_0, \cdots, a_n \in \mathbb{Z}$, if $a_0, a_n \neq 0$, then for each rational solution $\frac{p}{q}$ (gcd$(p,q) = 1$) $p | a_0$ and $q | a_n$. Prove the rational root theorem.