CS 70 Spring 2019 | Discrete Mathematics and Probability Theory Course Notes | HW 5

1 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 $p(p-1)q(q-1)$.

Solution:

(a) We mimic the proof of Fermat's Little Theorem from the notes.
Let S be the set of all numbers between 1 and p^2-1 (inclusive) which are relatively prime to p. We can write

$$S = \{1, 2, \ldots, p-1, p+1, \ldots, p^2-1\}$$

Define the set

$$T = \{a, 2a, \ldots, (p-1)a, (p+1)a, \ldots, (p^2-1)a\}$$

We'll show that $S \subseteq T$ and $T \subseteq S$, allowing us to conclude $S = T$:

- $S \subseteq T$: Let $x \in S$. Since $\gcd(a, p) = 1$, the inverse of a exists $\pmod{p^2}$. For ease of notation, we use a^{-1} to denote the quantity $a^{-1} \pmod{p^2}$. We know $\gcd(a^{-1}, p) = 1$, because a^{-1} has an inverse $\pmod{p^2}$ too. Combining this with the fact that $\gcd(x, p) = 1$, we have $\gcd(a^{-1}x, p) = 1$. This tells us $a^{-1}x \in S$, so $a(a^{-1}x) = x \in T$.
- $T \subseteq S$: Let $ax \in T$, where $x \in S$. We know $\gcd(x, p) = 1$ because $x \in S$. Since $\gcd(a, p) = 1$ as well, we know the product xs cannot share any prime factors with p as well, i.e. $\gcd(xs, p) = 1$. This means $xs \in S$ as well, which proves the containment.

We now follow the proof of Fermat's Little Theorem. Since $S = T$, we have:

$$\prod_{s_i \in S} s_i \equiv \prod_{t_i \in T} t_i \pmod{p^2}$$

However, since we defined $T = \{a, 2a, \dots, (p-1)a, (p+1)a, \dots, (p^2-1)a\}$:

$$\prod_{t_i \in T} t_i \equiv \prod_{s_i \in S} a s_i \equiv a^{|S|} \prod_{s_i \in S} s_i \pmod{p^2}$$

We can now conclude $(\prod_{s_i \in S} s_i) \equiv a^{|S|}(\prod_{s_i \in S} s_i) \pmod{p^2}$.
Each $s_i \in S$ is coprime to p, so their product $\prod_{s_i \in S} s_i$ is as well. Then, we can multiply both sides of our equivalence with the inverse of $\prod_{s_i \in S} s_i$ to obtain $a^{|S|} \equiv 1 \pmod{p^2}$. Using HW4, 4(b), we know $|S| = p(p-1)$, which gives the desired result.

Alternate Solution: We can use Fermat's Little Theorem, combined with the Binomial Theorem, to get the result. Since $\gcd(a,p) = 1$ and p is prime, $a^{p-1} \equiv 1 \pmod{p}$, so we can write $a^{p-1} = \ell p + 1$ for some integer ℓ. Then,

$$(a^{p-1})^p = (\ell p + 1)^p = \sum_{i=0}^{p} \binom{n}{i} (\ell p)^i = 1 + p \cdot (\ell p) + \binom{p}{2} (\ell p)^2 + \cdots + (\ell p)^p,$$

and since all of the terms other than the first term are divisible by p^2, $a^{p(p-1)} \equiv 1 \pmod{p^2}$.

(b) By the definition of d above, $ed = 1 + kp(p-1)q(q-1)$ for some k. Look at the equation $x^{ed} \equiv x \pmod{N}$ modulo p^2 first:

$$x^{ed} \equiv x^{1+kp(p-1)q(q-1)} \equiv x \cdot (x^{p(p-1)})^{kq(q-1)} \equiv x \pmod{p^2}$$

where we used the identity above. If we look at the equation modulo q^2, we obtain the same result. Hence, $x^{ed} \equiv x \pmod{p^2 q^2}$.

(c) We consider the scheme to be broken if knowing p^2q^2 allows you to deduce $p(p-1)q(q-1)$. (Observe that knowing $p(p-1)q(q-1)$ is enough, because we can compute the private key with this information.) Suppose that the scheme can be broken; we will show how to break ordinary RSA. For an ordinary RSA public key $(N = pq, e)$, square N to get $N^2 = p^2q^2$. By our assumption that the squared RSA scheme can be broken, knowing p^2q^2 allows us to find $p(p-1)q(q-1)$. We can divide this by $N = pq$ to obtain $(p-1)(q-1)$, which breaks the ordinary RSA scheme. This proves that our scheme is at least as difficult as ordinary RSA.

Remark: The first part of the question mirrors the proof of Fermat's Little Theorem. The second and third parts of the question mirror the proof of correctness of RSA.

2 Breaking RSA

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).

Solution:

Let $a = (p-1)(q-1)$. If Eve knows $a = (p-1)(q-1) = pq - (p+q) + 1$, then she knows $p+q = pq - a + 1$ (note that $pq = N$ is known too). In fact, p and q are the two roots of polynomial $f(x) = x^2 - (p+q)x + pq$ because $x^2 - (p+q)x + pq = (x-p)(x-q)$. Since she knows $p+q$ and pq, she can give the polynomial $f(x)$ to Wolfram to find the two roots of $f(x)$, which are exactly p and q.

Alternate Solution: Consider the polynomial $r(x) = (x-p)(x-q)$. Evaluate the polynomial at three special points.

$$r(0) = N$$
$$r(1) = (p-1)(q-1)$$
$$r(N) = N(p-1)(q-1)$$

Use polynomial interpolation to find the polynomial that goes through the three points $(0,N)$, $(1,(p-1)(q-1))$, $(N,N(p-1)(q-1))$, and then ask Wolfram for the roots of the polynomial.

3 Polynomial Practice

(a) If f and g are non-zero real polynomials, how many roots do the following polynomials have at least? How many can they have at most? (Your answer may depend on the degrees of f and g.)

   (i) $f+g$

   (ii) $f \cdot g$

   (iii) f/g, assuming that f/g is a polynomial

(b) Now let f and g be polynomials over GF(p).

   (i) We say a polynomial $f = 0$ if
   $$\forall x, f(x) = 0$$
   . If $f \cdot g = 0$, is it true that either $f = 0$ or $g = 0$?

   (ii) If $\deg f \geq p$, show that there exists a polynomial h with $\deg h < p$ such that $f(x) = h(x)$ for all $x \in \{0,1,...,p-1\}$.

   (iii) How many f of degree *exactly* $d < p$ are there such that $f(0) = a$ for some fixed $a \in \{0,1,\ldots,p-1\}$?

(c) Find a polynomial f over GF(5) that satisfies $f(0) = 1, f(2) = 2, f(4) = 0$. How many such polynomials are there?

Solution:

(a) (i) It could be that $f+g$ has no roots at all (example: $f(x) = 2x^2 - 1$ and $g(x) = -x^2 + 2$), so the minimum number is 0. However, if the highest degree of $f+g$ is odd, then it has to cross the x-axis at least once, meaning that the minimum number of roots for odd degree polynomials is 1 (we did not look for this case when grading). On the other hand, $f+g$ is a polynomial of degree at most $m = \max(\deg f, \deg g)$, so it can have at most m roots. The one exception to this expression is if $f = -g$. In that case, $f+g = 0$, so the polynomial has an infinite number of roots!

(ii) A product is zero if and only if one of its factors vanishes. So if $f(x) \cdot g(x) = 0$ for some x, then either x is a root of f or it is a root of g, which gives a maximum of $\deg f + \deg g$ possibilities. Again, there may not be any roots if neither f nor g have any roots (example: $f(x) = g(x) = x^2 + 1$).

(iii) If f/g is a polynomial, then it must be of degree $d = \deg f - \deg g$ and so there are at most d roots. Once more, it may not have any roots, e.g. if $f(x) = g(x)(x^2+1)$, $f/g = x^2 + 1$ has no root.

(b) (i) **Example 1:** $x^{p-1} - 1$ and x are both non-zero polynomials on $GF(p)$ for any p. x has a root at 0, and by Little Fermat, $x^{p-1} - 1$ has a root at all non-zero points in $GF(p)$. So, their product $x^p - x$ must have a zero on all points in $GF(p)$.
Example 2: To satisfy $f \cdot g = 0$, all we need is $(\forall x \in S, f(x) = 0 \vee g(x) = 0)$ where $S = \{0, \ldots, p-1\}$. We may see that this is not equivalent to $(\forall x \in S, f(x) = 0)) \vee (\forall x \in S, g(x) = 0)$.
To construct a concrete example, let $p = 2$ and we enforce $f(0) = 1, f(1) = 0$ (e.g. $f(x) = 1 - x$), and $g(0) = 0, g(1) = 1$ (e.g. $g(x) = x$). Then $f \cdot g = 0$ but neither f nor g is the zero polynomial.

(ii) Little Fermat tells us that $x^s \equiv x \cdot x^{(s-1) \bmod (p-1)} \pmod p$ (note that we have to factor one x out to account for the possibility that $x = 0$), and since $(s-1) \bmod (p-1) \le p-2$, writing $f(x) = \sum_{k=0}^{n} a_k x^k$, we have that $h(x) = a_0 + \sum_{k=1}^{n} a_k x \cdot x^{(k-1) \bmod (p-1)}$ is a polynomial of degree $\le p-1$ with $f(x) = h(x)$.

(iii) We know that in general each of the $d+1$ coefficients of $f(x) = \sum_{k=0}^{d} c_k x^k$ can take any of p values. However, the conditions $f(0)$ and $\deg f = d$ impose constraints on the constant coefficient $f(0) = c_0 = a$ and the top coefficient $x_d \neq 0$. Hence we are left with $(p-1) \cdot p^{d-1}$ possibilities.

(c) We know by part (b) that any polynomial over GF(5) can be of degree at most 4. A polynomial of degree ≤ 4 is determined by 5 points (x_i, y_i). We have assigned three, which leaves $5^2 = 25$ possibilities. To find a specific polynomial, we use Lagrange interpolation:

$$\Delta_0(x) = 2(x-2)(x-4) \qquad \Delta_2(x) = x(x-4) \qquad \Delta_4(x) = 2x(x-2),$$

and so $f(x) = \Delta_0(x) + 2\Delta_2(x) = 4x^2 + 1$.

4 Old secrets, new secrets

In order to share a secret number s, Alice distributed the values $(1, p(1)), (2, p(2)), \dots, (n+1, p(n+1))$ of a degree n polynomial p with her friends $\text{Bob}_1, \dots, \text{Bob}_{n+1}$. As usual, she chose p such that $p(0) = s$. Bob_1 through Bob_{n+1} now gather to jointly discover the secret. Suppose that for some reason Bob_1 already knows s, and wants to play a joke on $\text{Bob}_2, \dots, \text{Bob}_{n+1}$, making them believe that the secret is in fact some fixed $s' \neq s$. How could he achieve this? In other words, what value should he report in order to make the others believe that the secret is s'?

Solution:

We know that in order to discover s, the Bobs would compute

$$s = y_1 \Delta_1(0) + \sum_{k=2}^{n+1} y_k \Delta_k(0), \tag{1}$$

where $y_i = p(i)$. Bob_1 now wants to change his value y_1 to some y_1', so that

$$s' = y_1' \Delta_1(0) + \sum_{k=2}^{n+1} y_k \Delta_k(0). \tag{2}$$

Subtracting Equation 1 from 2 and solving for y_1', we see that

$$y_1' = (\Delta_1(0))^{-1} \left(s' - s\right) + y_1,$$

where $(\Delta_1(0))^{-1}$ exists, because $\deg \Delta_1(x) = n$ with its n roots at $2, \dots, n+1$ (so $\Delta_1(0) \neq 0$).