CS70: Homework #5

Abhijay Bhatnagar

September 28, 2018

Problem 1: Quick Computes

Simplify each expression using Fermat's Little Theorem.

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

Solution: $5 \pmod{11}$.

$$\begin{aligned} 3^{33} \pmod{11} &\equiv (3^3)^{11} \pmod{11} \\ &\equiv 27^{11} \pmod{11} \\ &\equiv 27 \pmod{11} \\ &\equiv 5 \pmod{11} \end{aligned}$$

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

Solution: $5 \pmod{17}$.

$$\begin{aligned} 10001^{10001} \pmod{17} &\equiv 10001^{10000+1} \pmod{17} \\ &\equiv (10001^{625^{17-1}}) \cdot 10001 \pmod{17} \\ &\equiv (1) \cdot 10001 \pmod{17} \\ &\equiv 5 \pmod{17} \end{aligned}$$

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

Solution: $1 \pmod{7}$.

$$\begin{aligned} 10^{10} + 20^{20} + 30^{30} + 40^{40} \pmod{7} &\equiv 3^{10} + 6^{20} + 2^{30} + 5^{40} \pmod{7} \\ &\equiv 3^4 + 6^2 + 2^0 + 5^4 \pmod{7} \\ &\equiv 9^2 + 36 + 1 + 25^2 \pmod{7} \\ &\equiv 4 + 1 + 1 + 4^2 \pmod{7} \\ &\equiv 22 \pmod{7} \\ &\equiv 1 \pmod{7} \end{aligned}$$

Problem 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?

Solution: N=77

(b) What number is e relatively prime to?

Solution: e is relatively prime to (7-1)(11-1)= 60.

(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.

Solution: Smallest value for $e = 7$.

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

Solution: $\gcd(e, (p-1)(q-1)) = 1$

(e) What is the decryption exponent d?

Solution:

$$\begin{aligned} d &= e^{-1} \pmod{60} \\ &= 7^{-1} \pmod{60} \\ &= -17 \pmod{60} \\ &= 43 \pmod{60} \end{aligned}$$

(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?

Solution: $E(30) = 30^7 \pmod{77} = 2 \pmod{77}$ (Using extended Euclid's.)

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

Solution: $D(2) = 2^{43} \pmod{77} = 30 \pmod{77}$

Problem 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.)

Solution: We have to show $(\forall p \in \text{primes}, \forall a : gcd(p, a) = 1)(a^{p(p-1)} \equiv 1 \pmod{p^2})$.

Proof. Let S denote the set of nonzero integers which have an inverse mod p^2, i.e.

$$S = \{1, 2, ..., p^2 - 1\}/\{p, 2p, ..., (p-1)p\}$$

Note: S will have exactly $(p^2 - 1) - (p - 1) = p^2 - p$ terms. Now, consider the sequence

$$S' = a^p, 2a^p, ..., (p^2 - 1)a^p \pmod{p^2}$$

. Since a and p are coprime, we know that a^p and p^2 must also be coprime (because greatest common prime factor of a and p is 1, and that doesn't change in a^p and p^2, and all other factors have unique prime factorization). However, each term with a coefficient that is a scalar multiple of p is not coprime, so let us redefine S' to exclude those elements.

$$S' = \{a^p, 2a^p, ..., (p^2 - 1)a^p\}/\{pa^p, 2pa^p, ..., (p-1)a^p\} \pmod{p^2}$$

From here, we know that every element in S' must be distinct. None of them are zero, and there are exactly $(p^2 - 1) - (p - 1) = p^2 - p$ terms $\implies S$ and S' contain the same elements mod p^2.

Now if both sets contain the same elements mod p^2, then the products must also be equivalent mod p^2.

$$\implies a^{(p^2-p)} \times \prod_{n \in S} n \equiv \prod_{n \in S} n \pmod{p^2}$$

Since each $n \in S$ is coprime to p^2, it must have an inverse mod p^2. Let us call this inverse S^{-1}. We can multiply both sides by S^{-1} to remove the product term.

$$\implies a^{(p^2-p)} \times \prod_{n \in S} n \times S^{-1} \equiv \prod_{n \in S} n \times S^{-1} \pmod{p^2}$$

$$\implies a^{p(p-1)} \equiv 1 \pmod{p^2}$$

$\square$

(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. $x^{ed} \equiv x \pmod N$.

Solution: To prove the statement, we have to prove:

$$\forall x \text{ relatively prime to } p \text{ and } q, (x^e)^d = x \pmod N \tag{1}$$

Proof. Consider the exponent, ed. By the definition of d, we know that $ed = 1 \pmod{p(p-1)q(q-1)}$; hence we can write $ed = 1 + kp(p-1)q(q-1)$, therefore:

$$x^{ed} - x = x^{1+kp(p-1)q(q-1)} - x = x(x^{kp(p-1)q(q-1)} - 1) \tag{2}$$

From (1), we want to show that this last expression is 0 mod N. We claim this is so because $x(x^{kp(p-1)q(q-1)} - 1)$ is divisible by p^2. To show this, let us consider 2 cases:

1.) x is not a multiple of p^2. In this case, since $x \neq 0 \pmod{p^2}$, we can use our results from (a) to deduce that $x^{kp(p-1)q(q-1)} - 1 = 0 \pmod{p^2}$, as desired.

2.) x is a multiple of p^2. In this case, since $x \neq 0 \pmod{p^2}$ is a multiple of x, it is trivially divisible by p^2.

By a symmetrical argument, the expression is also divisible by q^2, therefore it is divisible by both p^2 and q^2, and must also be divisible by their products, $p^2q^2 = N$. This implies the final expression in (2) $= 0 \pmod N$, which was the necessary condition for our proof. □

(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: The difficult of breaking RSA comes down to difficult of factoring, which is generally accepted to be *hard.* The difficult of breaking squared RSA is a question of figuring out the nontrivial factors of $N = p^2q^2$, which are $\{p, p, q, q\}$ (and combinations of those), which are also the prime factors of the normal RSA N. If we are able to find out the factors of squared RSA, it means we have deduced we have also found the factors of the normal RSA. Additionally, it means we've found $p(p-1)q(q-1)$. From there, we can easily (read: low complexity) divide by the $\sqrt{p^2q^2} = pq$ to get $(p-1)(q-1)$, which is solution to cracking the conventional RSA.