CS70 HW5

February 28, 2021

1 Quick Computes

(a) $3^{33} \equiv 5 \pmod{11}$.

Since gcd(3, 11) = 1 and 11 is a prime number. we have $3^{10} \equiv 1 \pmod{11}$, and $33 \equiv 3 \pmod{10}$, so the original answer is same to $3^3 = 27 \equiv 5 \pmod{11}$.

(b) $10001^{10001} \equiv 5 \pmod{17}$.

$10001 \equiv 5 \pmod{17}$. Since gcd(5, 17) = 1 and 17 is a prime number. we have $5^{16} \equiv 1 \pmod{17}$, and $10001 \equiv 1 \pmod{16}$, so the original answer is same to $5^1 = 5 \equiv 5 \pmod{17}$.

(c) $10^{10} + 20^{20} + 30^{30} + 40^{40} \equiv 1 \pmod{7}$.

$$\begin{aligned}10^{10} + 20^{20} + 30^{30} + 40^{40} &\equiv 3^4 + 6^2 + 2^0 + 5^4 \\ &= 81 + 36 + 1 + 625 \\ &= 743 \\ &\equiv 1 \pmod{7}\end{aligned}$$

2 RSA Practice

(a) N = p * q = 77;

(b) e relatively prime to (p-1)*(q-1) = 60;

(c) smallest prime number e is 7;

(d) $\gcd(e, (p-1)(q-1)) = 1$;

(e) $d = e^{-1} \pmod{60} \equiv 43 \pmod{60}$;

(f) The procedure is as following:

$$\begin{aligned} E(x) &= 30^7 \pmod{77} \\ &= 30 * 900^3 \\ &= 30 * 55^3 \\ &\equiv 2 \end{aligned}$$

(g) $D(E(x)) = x = 30$;

3 Squared RSA

(a) Claim : For any prime p and its square p^2, for any $a \in \{1, 2, \ldots, p^2 - 1\}$, we have $a^{p(p-1)} \equiv 1 \pmod{p^2}$

Proof. Define a Set S = $\{$s | s is prime to $p^2\}$, and from HW04 we learn that $\phi(p^2) = p * (p-1)$; And define a map T from S to S and $T = a * s, s \in S$ is a bijection. Looping in two ways, $\prod S_i \equiv a^{|S| = \phi(p^2) = p*(p-1)} \prod S_i \pmod{p}^2$. Thus dividing each side of $\prod S_i$, we obtain $a^{p(p-1)} \equiv 1 \pmod{p^2}$. □

(b) We wanna prove that $x^{ed} \equiv x \pmod{N}$.

Proof. By the definition of ed, we have $ed \equiv 1 \pmod{p(p-1)q(q-1)}$;hence we can write $ed = 1 + kp(p-1)q(q-1)$ for some integer k, and therefore

$$x^{ed} - x = x(x^{kp(p-1)q(q-1)} - 1)$$

Since we know from part (a), that $x^{kp(p-1)} \equiv 1 \pmod{p^2}$, same as $x^{kq(q-1)} \equiv 1 \pmod{q^2}$. So the expression $(x^{kp(p-1)q(q-1)} - 1)$ is both the multiple of p^2 and q^2. Since $gcd(p, q) \neq 1$, $(x^{kp(p-1)q(q-1)} - 1)$ must be multiple of $p^2q^2 = N$.

□

(c) Claim: If this scheme can be broken, normal RSA can be as well.

Proof. If knowing p^2q^2, we can deduce $p(p-1)q(q-1)$. Then we can obtain pq since $pq = \sqrt{p^2q^2}$, we can also obtain $(p-1)(q-1)$, since $(p-1)(q-1) = p(p-1)q(q-1)/pq$. Therefore, if this scheme can be broken, normal RSA can be as well. □