CS 70 Discussion 3B: tinyurl.com/frank-discussion 7/7/2020

Public: N, e

Private: p, q, d

p, q prime

$N = pq$

$d = e^{-1} \bmod (p-1)(q-1)$

2 min alone
5 min break
15 min disc

1 (a) What's wrong w/ $e=2$?

By defn., e must be coprime w/ $(p-1)(q-1)$

However, we know p, q are primes > 3

Therefore, $p-1$ and $q-1$ are even numbers.

Hence, $GCD(e, (p-1)(q-1)) = 2$, not 1 as desired.

(b) Condition on p, q st $e=3$ is valid exponent.

$p, q \equiv 2 \pmod 3$

$p, q \not\equiv 0 \pmod 3$

otherwise p, q would not be prime!

$p, q \not\equiv 1 \pmod 3$

$p-1, q-1 \equiv 0 \pmod 3$

$e = 3$

then $GCD(e, (p-1)(q-1)) = 3 \neq 1$

(c) $p=5, q=17, e=3$

Public key = ?

public key: (N, e)

$N = pq = 85$

$\boxed{(85, 3)}$

(d) Private key?

$d = e^{-1} \pmod{(p-1)(q-1)}$

$d = 3^{-1} \pmod{(16)(4)}$

$d = 3^{-1} \bmod 64$

$64 \times 2 = 128$
$+ 1$
$129 \leftarrow$ divisible by 3

$43(3) = 129$

$43(3) = 129 = 64(2) + 1$

$\boxed{d = 43}$

(e) Alice wants to send $x = 10$.

$E(x) = ?$

$E(x) = x^e \pmod N$

$E(10) = 10^3 \pmod{85}$

$\equiv (100)(10) \pmod{85}$

$\equiv (15)(10) \pmod{85}$

$\equiv \boxed{65 \pmod{85}}$

$x^e \pmod N$

(f) Bob recieves $y = 24$

$D(y) = ?$

$D(y) = y^d \pmod N$

$D(24) = 24^{43} \pmod{85} = a$

$\begin{cases} a \equiv ? \pmod 5 \\ a \equiv ? \pmod{17} \end{cases}$

$24^{43} \pmod 5$ $\quad 24^{43} \pmod{17}$

5:34

[2] Show to make RSA w/ 3 primes p, q, r work.

1 min alone
5 min break
10 min disc

5:50

[3] (a) Eve sees $(\overbrace{p_1 q_1}^{N_1}, 7)$ and $(\underbrace{p_1 q_2}_{N_2}, 7)$. Can she break the encryption?

3 min alone

Key: It is slow to do prime factorization of a number, but fast to run the Euclid GCD algorithm

$$\gcd(p_1 q_1, p_1 q_2) = \boxed{p_1}$$

division is also a quick algorithm

Eve can then use division to find q_1, q_2, and the exponent d as well. ∎

(b) Eve sees $(p_1 q_1, 3)$, $(p_2 q_2, 3)$, $(p_3 q_3, 3)$. Can she break encryption?

No, because now $N_1 = p_1 q_1$, $N_2 = p_2 q_2$, and $N_3 = p_3 q_3$ share no common divisors. ∎

$$\begin{cases} x < N_1 \\ x < N_2 \\ x < N_3 \end{cases}$$

$$x^3 < N_1 N_2 N_3$$

(c) Say secret x remains constant, e stays $= 3$, but use same N values as before. How can Eve figure out x?

$e = 3 \quad N_1, N_2, N_3$

$p_1 q_1 \quad p_2 q_2 \quad p_3 q_3$

$$\begin{cases} x^3 \equiv a_1 \pmod{N_1} \\ x^3 \equiv a_2 \pmod{N_2} \\ x^3 \equiv a_3 \pmod{N_3} \end{cases}$$

$\Downarrow$ CRT

$$x^3 = a_4 \pmod{N_1 N_2 N_3}$$

$\boxed{\text{cube root of } a_4 \text{ is } x}$