Basic Crypto

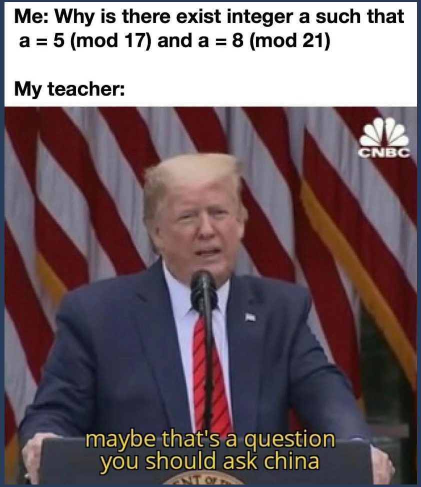
Axel Nilsson

RSA

- Randomly select two large prime numbers p and q
- Calculate N = p * q
- Calculate phi(N) = (p-1) * (q-1)
- Select e such that p-1 and q-1 are relatively prime to e. Same as if phi(N) and e are relatively prime
- Calculate d from ed = 1 (mod phi(N))
- Encryption: m^e = c (mod N)
- Decryption: c^d = m (mod N)

CRT - Chinese remainder theorem

- $x = a1 \ (\mathrm{mod}\ m1)$ …. $x = ak \ (\mathrm{mod}\ mk)$
- Construct $m = m1*m2*...*mk$
- Define: $z1 = m/m1$ … $zk = m/mk$
- Calculate $y1 = z1^{\wedge}-1 \ (\mathrm{mod}\ m1)$ … $yk = zk^{\wedge}-1 \ (\mathrm{mod}\ mk)$
- $X = a1*y1*z1 + …. + ak*yk*zk \ (\mathrm{mod}\ m)$



Me: Why is there exist integer a such that a = 5 (mod 17) and a = 8 (mod 21)

My teacher:

End of the boring, let’s solve some challs!

- Some tips for tools that can be useful
  - pow(a, b, m) = a^b mod m
  - long_to_bytes - from Crypto.Util.number
  - sagemath
  - http://factordb.com/