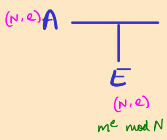

$m^e \bmod N$

$N = pq$

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

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

$(m^e)^d \bmod N \equiv m \pmod N$

WTS $m^{ed} \equiv m \bmod pq$

$ed \equiv 1 \bmod (p-1)(q-1)$

$\Rightarrow ed = k(p-1)(q-1) + 1$

Show $m^{k(p-1)(q-1)+1} \equiv m \bmod pq$

$m^{p-1} \equiv 1 \bmod p$ $\quad$ $m^{q-1} \equiv 1 \bmod q$

$(m^{p-1})^k \equiv 1^k \equiv 1 \bmod p$ $\quad$ $(m^{q-1})^k \equiv 1^k \equiv 1 \bmod q$

$m^{k(p-1)} \equiv 1 \bmod p$ $\quad$ $m^{k(q-1)} \equiv 1 \bmod q$

$(m^{p-1})^{q-1} \bmod p \equiv 1^{q-1} \bmod p$

$(m^{q-1})^{p-1} \bmod q \equiv 1 \bmod q$ (mod q FLT)

$m^{k(p-1)(q-1)} - 1 \equiv 0 \bmod p$ $\quad$ $m^{k(p-1)(q-1)} - 1 \equiv 0 \bmod q$

$m^{k(p-1)(q-1)} \equiv 1 \bmod pq$

$m^{k(p-1)(q-1)+1} \equiv m \bmod pq$ ∎

$7(-8) + 60(1) = 4$

$7(9) + 60(-1) = 3$

$7(-17) + 60(2) = 1$

$7^{-1} \equiv -17 \equiv 43 \bmod 60$

$\gcd(60, 7)$

$= \gcd(7, 4)$

$= \gcd(4, 3)$

$= \gcd(3, 1)$

$1 = 4 - 3(1)$

$= 4 - (7 - 4(1))$

$= 4(2) - 7(1)$

$= (60 - 7(8)) \cdot 2 + 7(-1)$

$= 60(2) + 7(-16) + 7(-1)$

$= 60(2) + 7(-17)$

$-17 \equiv 43 \bmod 60$

7) 60 (8
56
4) 7 (1
4
3) 4 (1
3
1

60
−17
43

3 (RSA w/ 1 prime)

$m^{k(p-1)+1} \equiv m \bmod p$ by FLT

$(m^e)^d \equiv m$

$ed = k(p-1) + 1$

$ed \bmod P = 1$

$d \equiv e^{-1} \bmod (p-1) \equiv 67^{-1} \equiv 3 \bmod 100$

$67 \times 3 = 201$

$100 \times 2 = 200$

$(m^e)^d \equiv m \bmod p$

$35^3 \bmod 101$

$\equiv 35^2 \cdot 35 \bmod 101$

$\equiv 13 \cdot 35 \bmod 101$

$\equiv \boxed{51} \bmod 101$

$35^2 \equiv 1225 \equiv 13 \bmod 101$

1225
1212
13

455
404
51

35
13
105
35x
455

$51^{67} \bmod 101 \equiv 35 \bmod 101$

$x \equiv 0 \bmod m_1$

$x \equiv 0 \bmod m_2$

$x \equiv 0 \bmod m_1 m_2$

$ed = k(p-1) + 1$

$\Rightarrow ed \equiv 1 \bmod (p-1)$

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 04B

1 RSA Practice

Consider the following RSA schemes and solve for asked variables.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key d? Calculate the exact value.

(b) If the receiver gets 4, what was the original message?

(c) Encode your answer from part (b) to check its correctness.

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?

77

(b) What number is e 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.

7

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

1

(e) What is the decryption exponent d?

$d = 7^{-1} \mod 60$

$d \equiv 43 \mod 60$

(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?

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

3 RSA Lite

Woody misunderstood how to use RSA. So he selected prime $P = 101$ and encryption exponent $e = 67$, and encrypted his message m to get $35 = m^e \bmod P$. Unfortunately he forgot his original message m and only stored the encrypted value 35. But Carla thinks she can figure out how to recover m from $35 = m^e \bmod P$, with knowledge only of P and e. Is she right? Can you help her figure out the message m? Show all your work.

4 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p, q, r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$.