# DIS 04B : RSA

- Send memes
- how are you?
  - ↳ i'm currently vibing.

RSA meme

## review

Eve

$$\text{Alice} \xRightarrow{\boxed{\text{msg}}} \text{Bob}$$

Setup: Bob picks two big primes $p, q$.
& $e$ (small), $\gcd(e, (p-1)(q-1)) = 1$.

Also releases $\boxed{(N = pq, e)}$, ← public

computes $d = e^{-1} \pmod{(p-1)(q-1)}$.
↳ private.

Encryption: $A \xrightarrow{x} B$, send $E(x) = x^e \pmod N$

Decryption: B gets $y = E(x)$, does $D(y) = y^d \pmod N$
$\equiv x^{ed} \equiv x \pmod N$.

## 1 RSA Practice

icebreaker: what keeps you going during these virtual times? what do you look forward to?

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?

(b). $D(4) = 4^9 \pmod{55}$

$= 14 \pmod{55}$

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

(c). $14^9 \equiv 4 \pmod{55}$

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

$\equiv 9^{-1} \pmod{4 \cdot 10}$

$\text{egcd}(40, 9) = \text{egcd}(9, 4)$

$= \text{egcd}(4, 1)$

$1 = 9 - 2(4)$

$1 = 9 - 2(40 - 4 \cdot 9) = 9 \cdot 9 - 2 \cdot 40$

$\Rightarrow \boxed{d = 9}$

## 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 $N$?

$N = pq = 77$

(b) What number is $e$ relatively prime to?

$(p-1)(q-1) = 60.$

(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.

$2 \mid 60,\ 3 \mid 60,\ 5 \mid 60, \Rightarrow \boxed{7}$. $\boxed{e = 7}$.

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

1.

(e) What is the decryption exponent $d$? 43?

$d \equiv 7^{-1} \pmod{60}$ $\quad 301 = 7 \cdot \boxed{43}$.

$7d \equiv 1 \pmod{60}$

$1, 61, \ldots, 301$

(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?

$30^7 \equiv 2$

$E(x) = x^e = x^7 \pmod{77}$

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

$2^{43} \equiv 30$

$D(y) = y^d \equiv y^{43} \pmod{77}$.

f)

$30^7 \pmod{77}$

$\equiv 30 \cdot (30^2)^3$

$\equiv 30 (53)^3$

$2^{43} \pmod{77}$

mod 7 $\quad$ mod 11

$2^{43} \equiv 2 \pmod 7$, $\quad 2^{43} \equiv 8 \pmod{11}$.

$x \equiv 2 \pmod 7$

$x \equiv 8 \pmod{11}$.

$x \equiv 8 \cdot 11 \cdot 2$ $\quad x = 8 + 11k \pmod 7$

$\equiv 30$.

$2 \equiv 8 + 4k$

$1 \equiv 4k \pmod 7$

$k = 2$.

## 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.

$d \equiv e^{-1} \pmod{P-1}$. $\leftarrow$

$W \xrightarrow{m^e} C$

$D(m^e) = (m^e)^d = m^{ed} \pmod{P}$

$\equiv m$

$\Rightarrow m^{ed-1} \equiv 1 \pmod{P}$

$\Leftrightarrow \underline{ed-1 \equiv 0 \pmod{p-1}}$

$d = 3 \Rightarrow m \equiv 51 \pmod{101}$.

FLT

$x^{p-1} \equiv 1 \pmod{p}$

$(x^{p-1})^2 \equiv 1 \equiv x^{2(p-1)}$

$\vdots$

$(x^{p-1})^k \equiv \underline{x^{k(p-1)}} \equiv 1$