RSA is a way for one person to receive encrypted messages from anyone.

To receive messages, I:

pick 2 prime numbers p, q

$m = pq$

$\phi(m) = \phi(p)\phi(q) = (p-1)(q-1)$

e coprime to $\phi(m)$.

Publish publically m and e.

⚠ e should be coprime to $\underline{\underline{\phi(m)}}$!

To send me a message, encode it as a string of numbers, send number x by sending. $x^e \bmod m$

(x should be smaller than m; to send a long message break it into chunks!),

Meanwhile, I compute d = multiplicative inverse of e modulo $\phi(m)$.

$$(x^e)^d = x \bmod m.$$

Exercise 2-(2). Establish a public key (m, e) then have a partner transmit a message.

Exercise 1

Primitive root.

If $\mathbb{K}$ is a finite field $g \in \mathbb{K}^\times$ is a primitive root if every element of $\mathbb{K}^\times$ can be written as g^a for some a.

In Diffie-Hellman p, g — g is a primitive root in $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$,

Naive way to check if g is a primitive root — list out all powers of g and check that you get everything.

$g \in \mathbb{K}^\times$ is a primitive root $\iff$ $g^d \neq 1$ for and d a prpr divisor of $|\mathbb{K}^\times|$

$|\mathbb{K}^\times| = |\mathbb{K}| - 1$

$\left(g^{|K^\times|} = 1 \quad \text{always} \right).$

Exercise 2 – (2)

2 – (3).

---

(2) – $p = 31$ $\quad |\mathbb{F}_p^\times| = p-1 = 30$

proper divisors are 2, 3, 5, 6, 10, 15

try $K=2$.

$2^2 = 4 \qquad 2^3 = 8 \qquad 2^5 = 32 \equiv 1 \mod 31$

Not a primitive root!

try $k = 3$

$3^2 = 9 \quad 3^3 = 27 \quad 3^5 = 26 \quad 3^6 = \ldots$

all powers are in $\mathbb{F}_{31} = \mathbb{Z}/31\mathbb{Z}$

so compute mod 31.