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 \( e. \) \( \Delta e \) should be co-prime to \( \phi(M). \)

To send me a message, encode it as a string of numbers, send number \( x \) by sending \( x^e \mod M \) (\( x \) should be smaller than \( m \); to send a long message, break it into chunks).

Meanwhile, I compute \( d = \text{multiplicative inverse of} \ e \mod \phi(M). \)

\[
(x^e)^d = x \mod M.
\]
Exercise 2 (2). Establish a public key $(C, m, e)$ then have a partner transmit a message.

Exercise 1

Primitive root.

If $K$ is a finite field, $g \in K^*$ is a primitive root if every element of $K^*$ can be written as $g^a$ for some $a$. 
In Diffie-Hellman $p, g$, $g$ is a primitive root in $\mathbb{Z}/p\mathbb{Z} = F_p$.

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

$g \in \mathbb{K}^x$ is a primitive root $\iff$

$g^d \neq 1$ for all $d$ a power of $|\mathbb{K}| - 1$.
Exercise 2 - (2)

2 - (2).

(2) - $p = 31$

$\mathbb{F}_{p^4}^x \mid = p - 1 = 30$

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

Try $k = 2$.

$2^2 = 4 \quad 2^3 = 8 \quad 2^5 = 32 = 1 \pmod{31}$

Not a primitive root!
try } K = 3 \)

\[ 3^2 = 9 \quad 3^3 = 27 \quad 3^5 = 243 \quad 3^6 = \ldots \]

All powers are in } F_{3^6} = \mathbb{Z}/3^6 \mathbb{Z} \)

so compute mod 3^6.