For positive n, we say integers a and b are congruent mod n and write

divides

$$a \equiv b \pmod{n}$$

if $n \mid (a-b)$. Alternatively, $a \equiv b \pmod{n}$ iff $a \% n = b \% n$.

Is $32 \equiv 2 \pmod{5}$?

$32 \equiv 7 \pmod{5}$?

Come up w/ one T example and one F example w/ different n.

T

$21 \equiv 27 \pmod{6}$

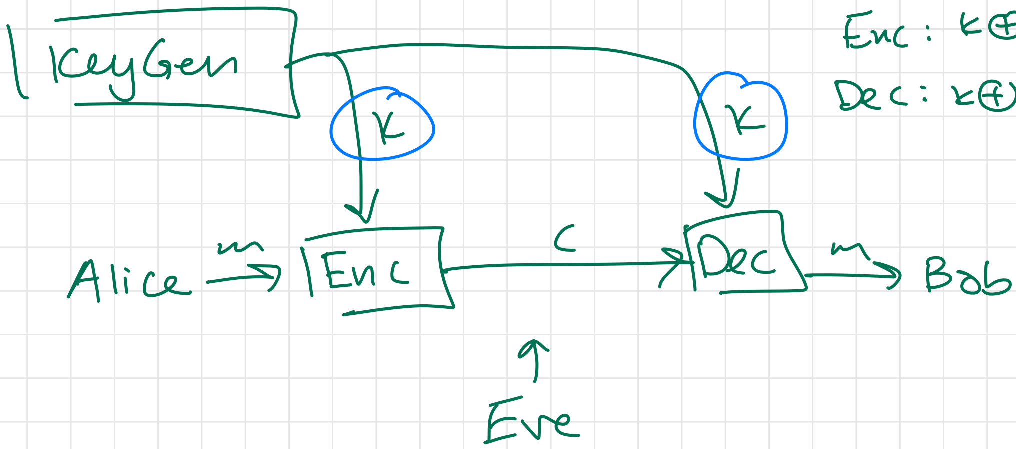
$6 \mid 21-27=6$ ✓

Encryption

one-time pad:
random k

Enc: $k \oplus m$

Dec: $k \oplus c$

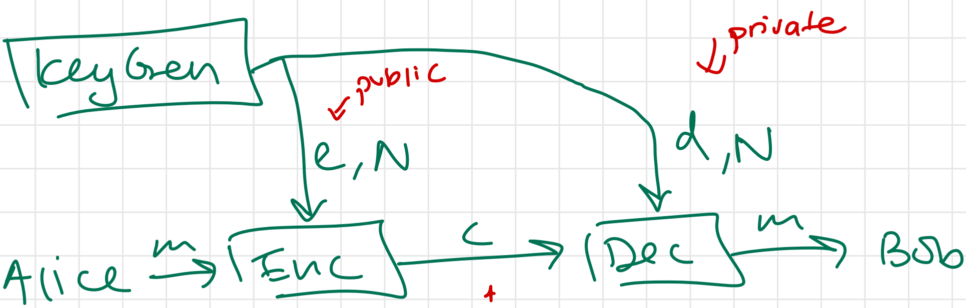


① Correctness: for all k, m

$$\mathrm{Dec}(k, \mathrm{Enc}(k,m)) = m$$

② Security: whatever is ~~knowable~~ efficiently computable about m given c is also ~~knowable~~ efficiently computable without c.

RSA Encryption scheme



Eve

keyGen:

random primes p, q

$\boxed{N = p \cdot q}$

totient phi $\phi(N)$

e, d s.t. $e \cdot d \equiv 1 \pmod{\overbrace{(p-1)(q-1)}^{\phi(N)}}$

return e, d, N

$Enc(e, m \in \{0, 1, \ldots, N-1\})$

return $m^e \% N$

$Dec(d, c \in \{0, 1, \ldots, N-1\})$

return $c^d \% N$

Questions:

- how big can m be? $N-1$

$N = 2^{2048}$ 2048 bits $\underbrace{1101 \cdots 1}_{2048 \text{ bits}}$

encode 256 chars

~ tweet

m 0

- how do we compute e, d?

for any prime e there is a d (and vice versa)

e = random prime $\{0, 1, \ldots, (p-1)(q-1)\}$

d = multiplicative inverse of e mod $(p-1)(q-1)$

↑ fast compute

- correctness — assume
- security

Eve's perspective: c, N, e

Could get d if had p, q

p, q are only factors of N other than 1

```
getpq(N):
  i = 2
  while i doesn't evenly divide N:
      i++
  p = i
  q = N/p
```

×

$O(\sqrt{N}) \longrightarrow O(\sqrt{2^n}) = O((2^n)^{1/2}) = \boxed{O(2^{n/2})}$

Size of N is $\log_2 N = n$

$N = 2^n$