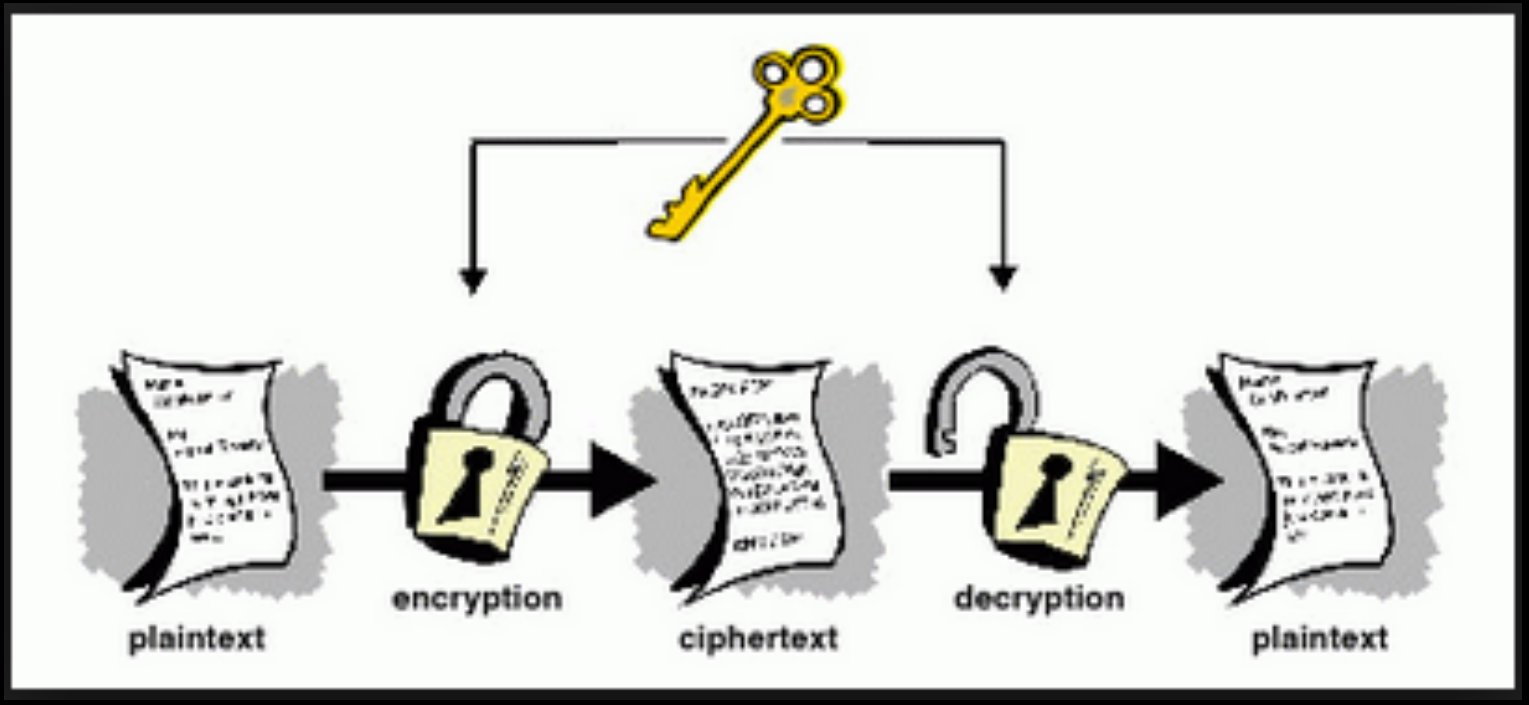
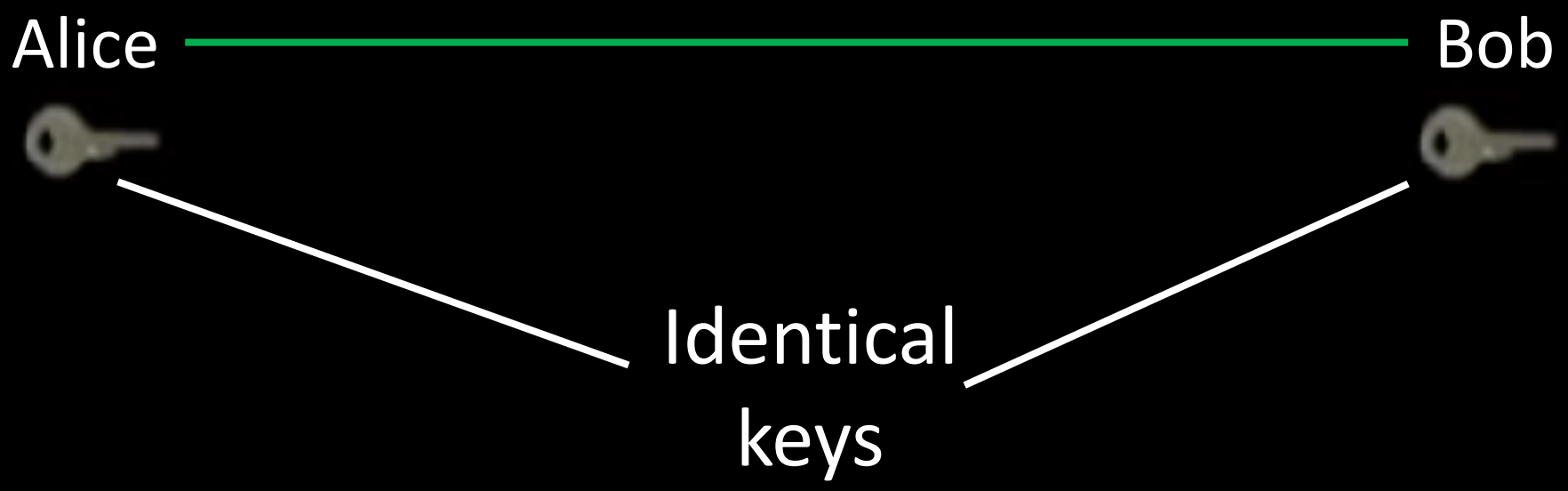
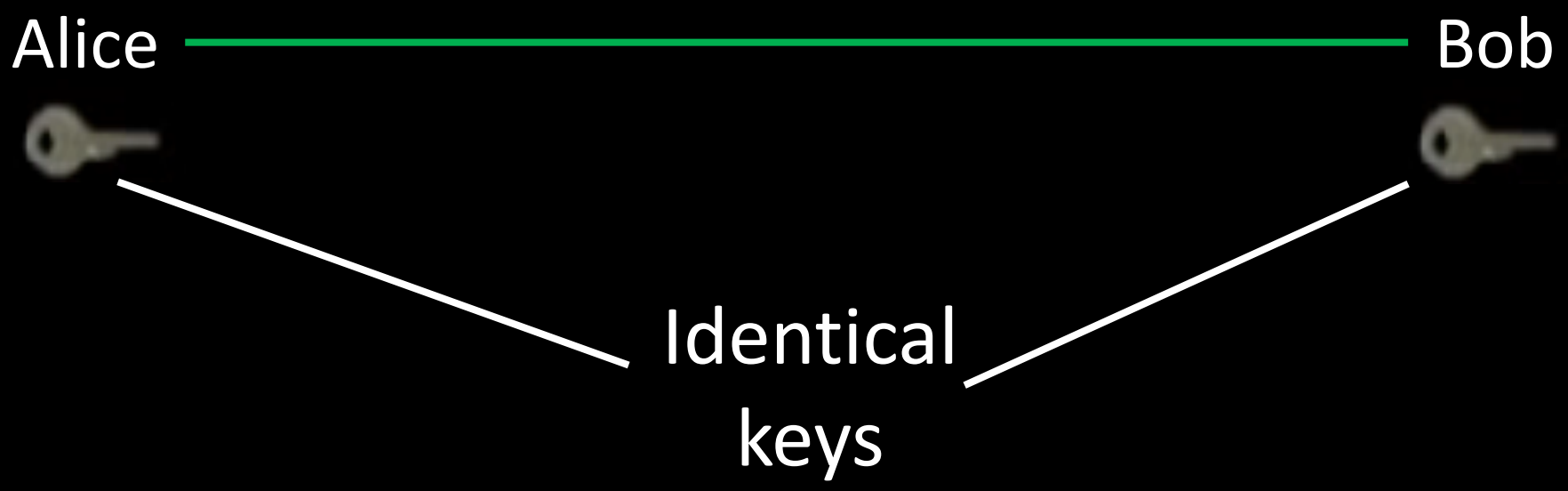
How secure is RSA: Mathematical Approach

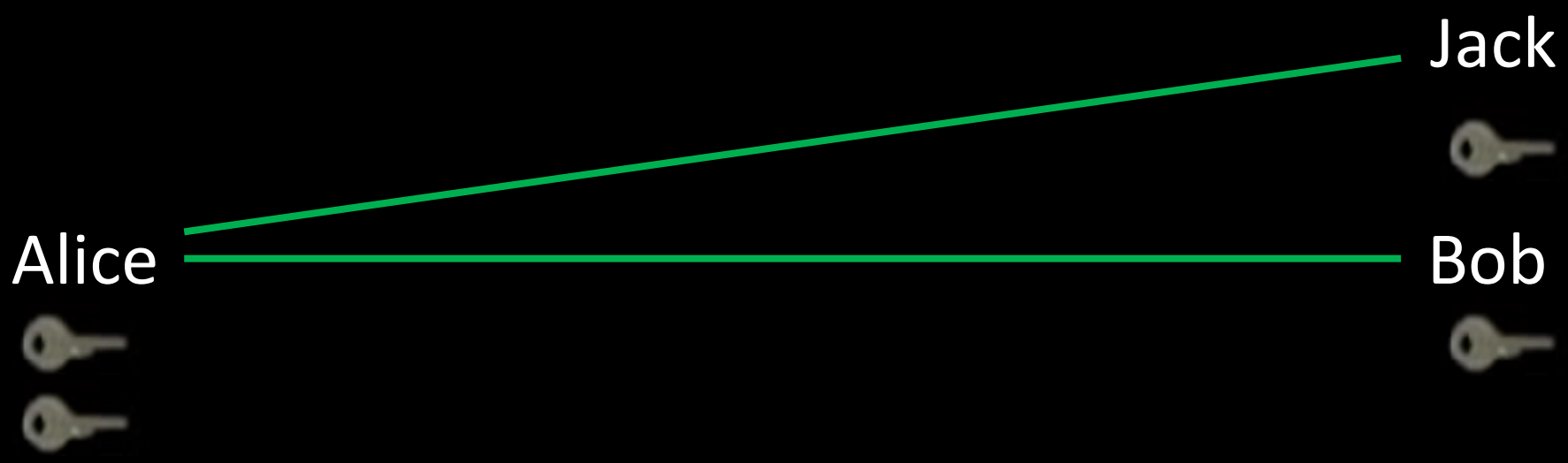
By: Rana Khalil
Supervised by: Dr. Monica Nevins

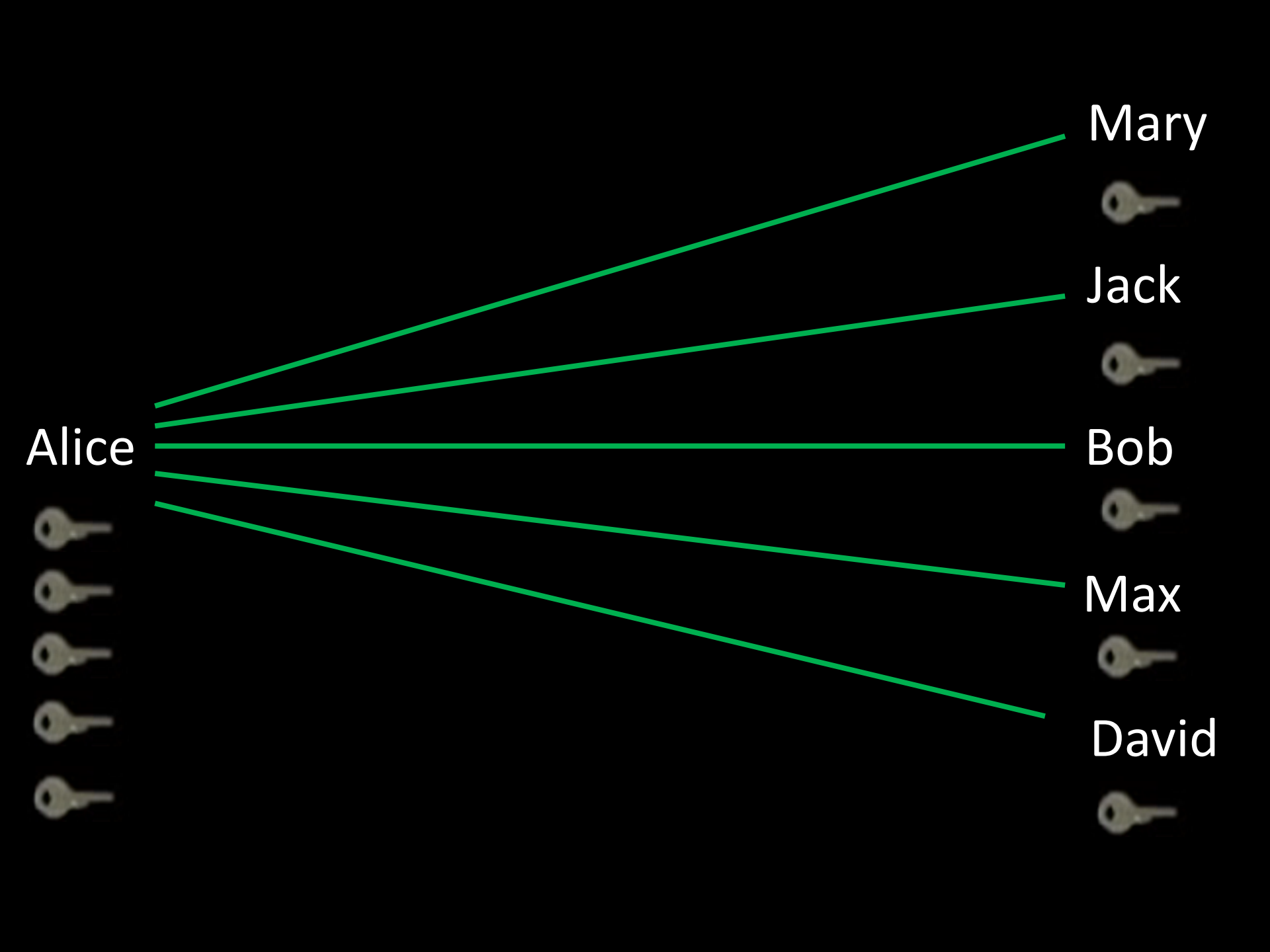
Symmetric Key Cryptography




Alice
Bob
Identical
keys


Alice
Bob
Identical
keys


Jack
Alice
Bob


Mary
Jack
Alice
Bob
Max
David

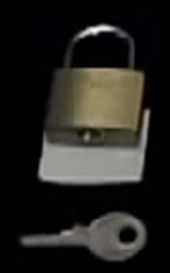
Asymmetric Key Cryptography

Alice

Bob

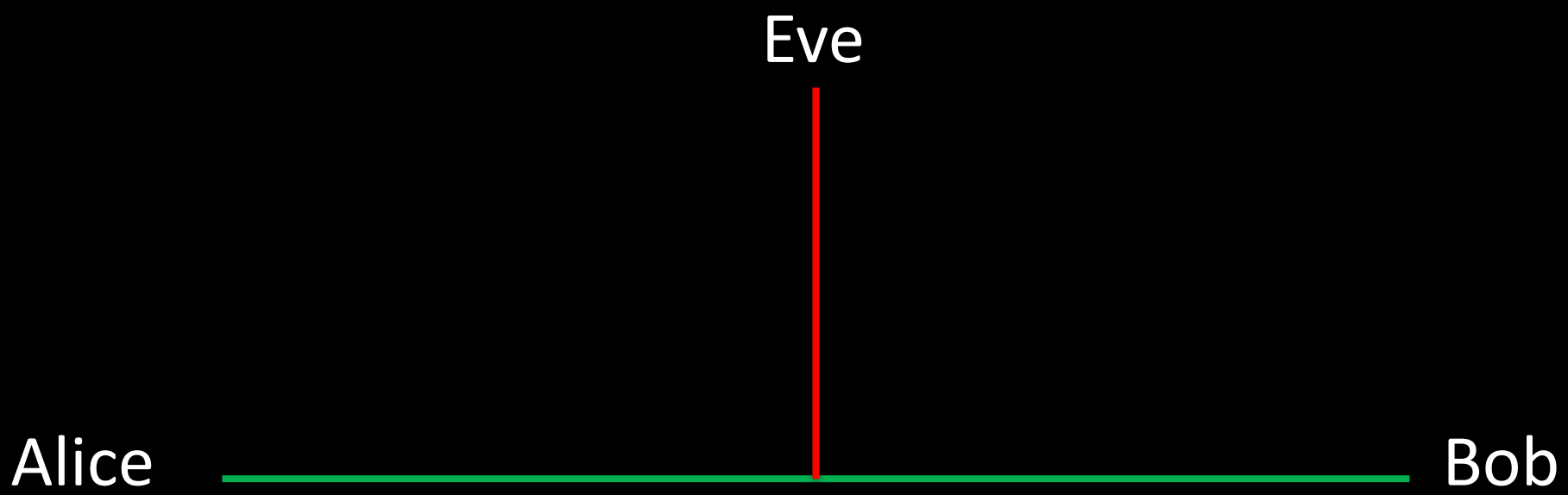
Alice Bob

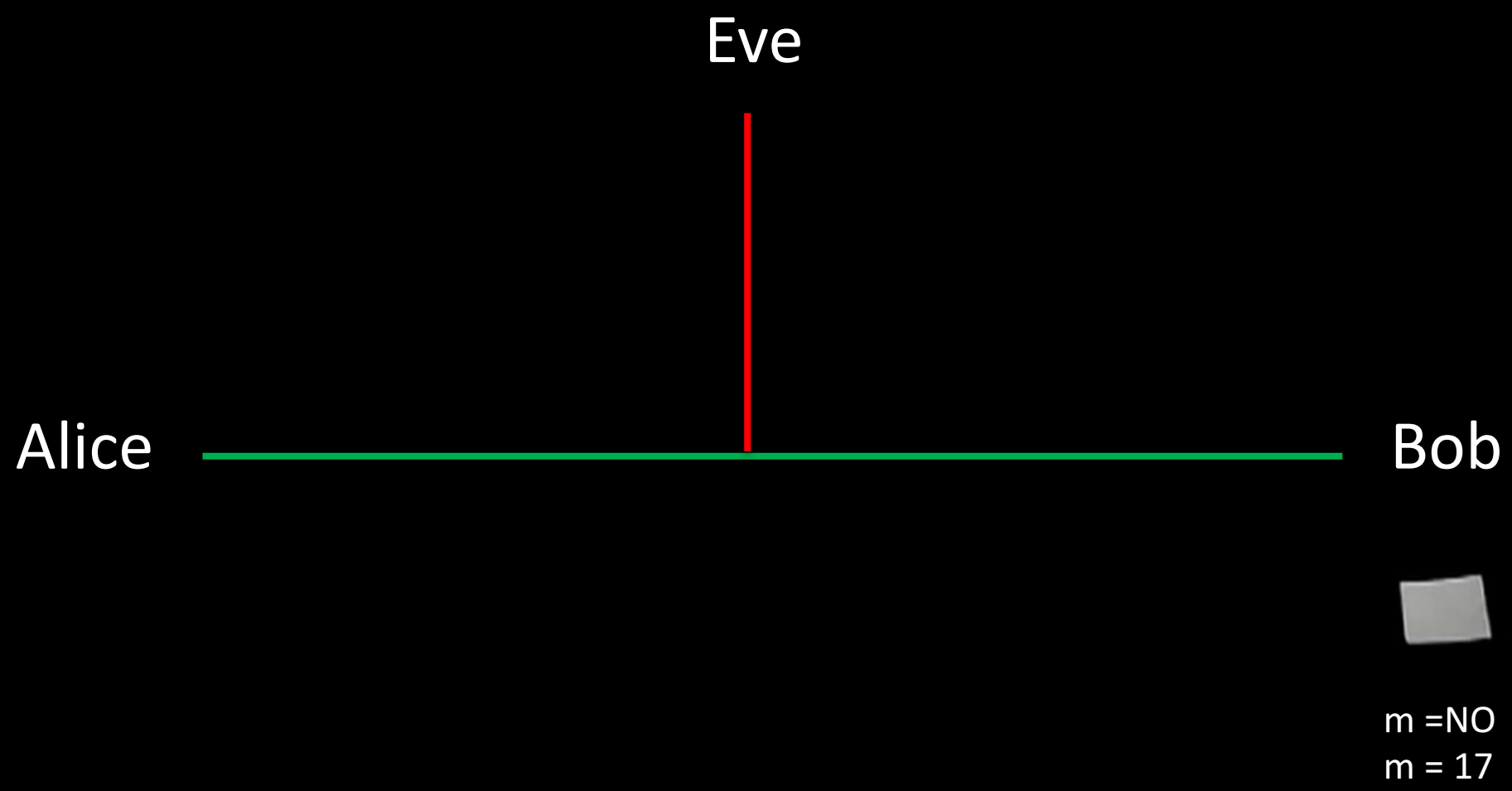
Alice Bob



Alice Bob

RSA




Eve
Alice
Bob
m =NO
m = 17

Eve

Alice

Bob

p1 = 3
p2 = 11
N = 3* 11 = 33

m =NO
m = 17

Eve

Alice

Bob

p1 = 3
p2 = 11
N = 3* 11 = 33

$\Phi(n) = (p1 – 1) (p2 -1)$
$= 2 * 10 = 20$

m =NO
m = 17

Eve

Alice

Bob

p1 = 3
p2 = 11
N = 3* 11 = 33

$\Phi(n) = (p1 – 1) (p2 -2)$
$= 2 * 10 = 20$

e = 3

m =NO
m = 17

Eve

Alice

Bob

p1 = 3
p2 = 11
N = 3* 11 = 33
Φ(n) = (p1 – 1) (p2 -2)
= 2 * 10 = 20
e = 3

$$ed \equiv 1 \; mod \; \Phi(n)$$

$$3d = 1 \bmod 20$$

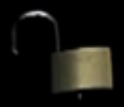
$$d = 7$$

m =NO
m = 17

Eve

N = 33
e = 3

Alice



N = 33
e = 3

Bob

m =NO
m = 17

Eve

N = 33
e = 3

Alice

Bob

N = 33
e = 3

m =NO
m = 17

$$m^e \; mod \; n \equiv c$$

$$17^3 mod \; 33 \equiv 29$$

Eve

n = 33
e = 3
c = 29

Alice

Bob

c =29

m = 17

$$m \equiv c^d \bmod N$$

$$m \equiv 29^7 \bmod 33$$

m = 17

EQUAL!

How Hard is factoring?

Let N be 1024 digits long

- In order to find a factor you need to search

$$\sqrt{N} \sim 512 \text{ digits}$$

How Hard is factoring?

Let N be 1024 digits long

- In order to find a factor you need to search

$$\sqrt{N} \sim 512 \text{ digits}$$

- $\mathbf{10^{512}}$ numbers

How Secure is RSA?

- National Security Agency (NSA) – Access to classified information
- Lenstra et al.
  - Prime factor in common
  - Among 4.7 million 1024-bit RSA moduli collected, more than 12500 have a single prime factor in common!

How Secure is RSA?

- National Security Agency (NSA) – Access to classified information
- Lenstra et al.
  - Prime factor in common
  - Among 4.7 million 1024-bit RSA moduli collected, more than 12500 have a single prime factor in common!
  - Probability is $\frac{1}{2^{459}} \approx 0$!