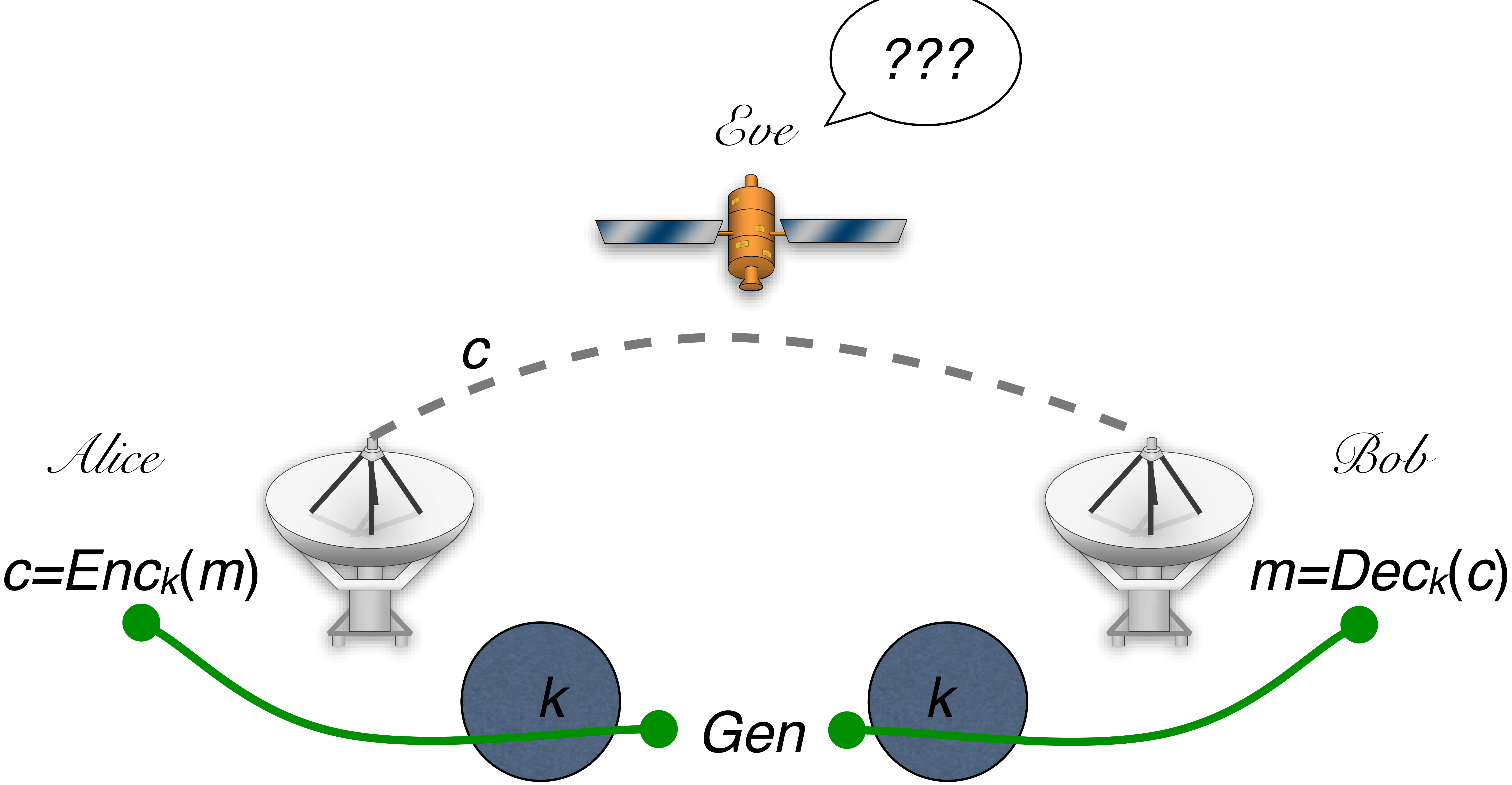
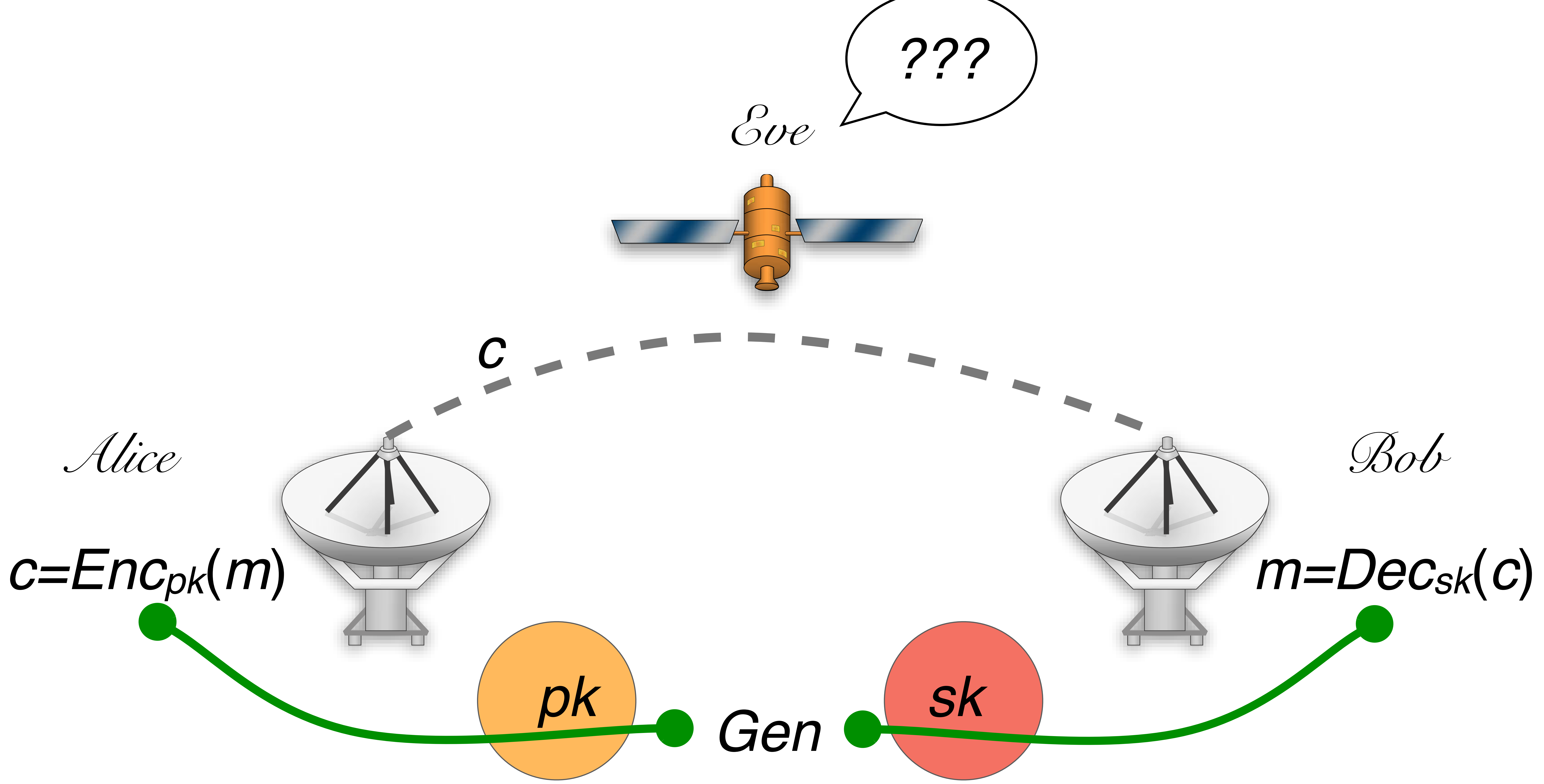
2550 Intro to cybersecurity

L12: Crypto: PKC

Ran Cohen/abhi shelat

Revisit our model for Encryption


???
Eve
c
Alice
Bob
c=Enc_k(m)
m=Dec_k(c)
k
k
Gen


???
Eve
c
Alice
Bob
c=Encpk(m)
m=Decsk(c)
pk
Gen
sk

public key encryption

Gen Enc Dec

3 algorithms

Gen (key generation)

$$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$$

Enc (encryption)

$$c \leftarrow \mathsf{Enc}_{pk}(m) \text{ for } pk \in \mathcal{K}, m \in \mathcal{M}$$

Dec (decryption)

public key encryption

Gen Enc Dec

3 algorithms

Gen (key generation)

$$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$$

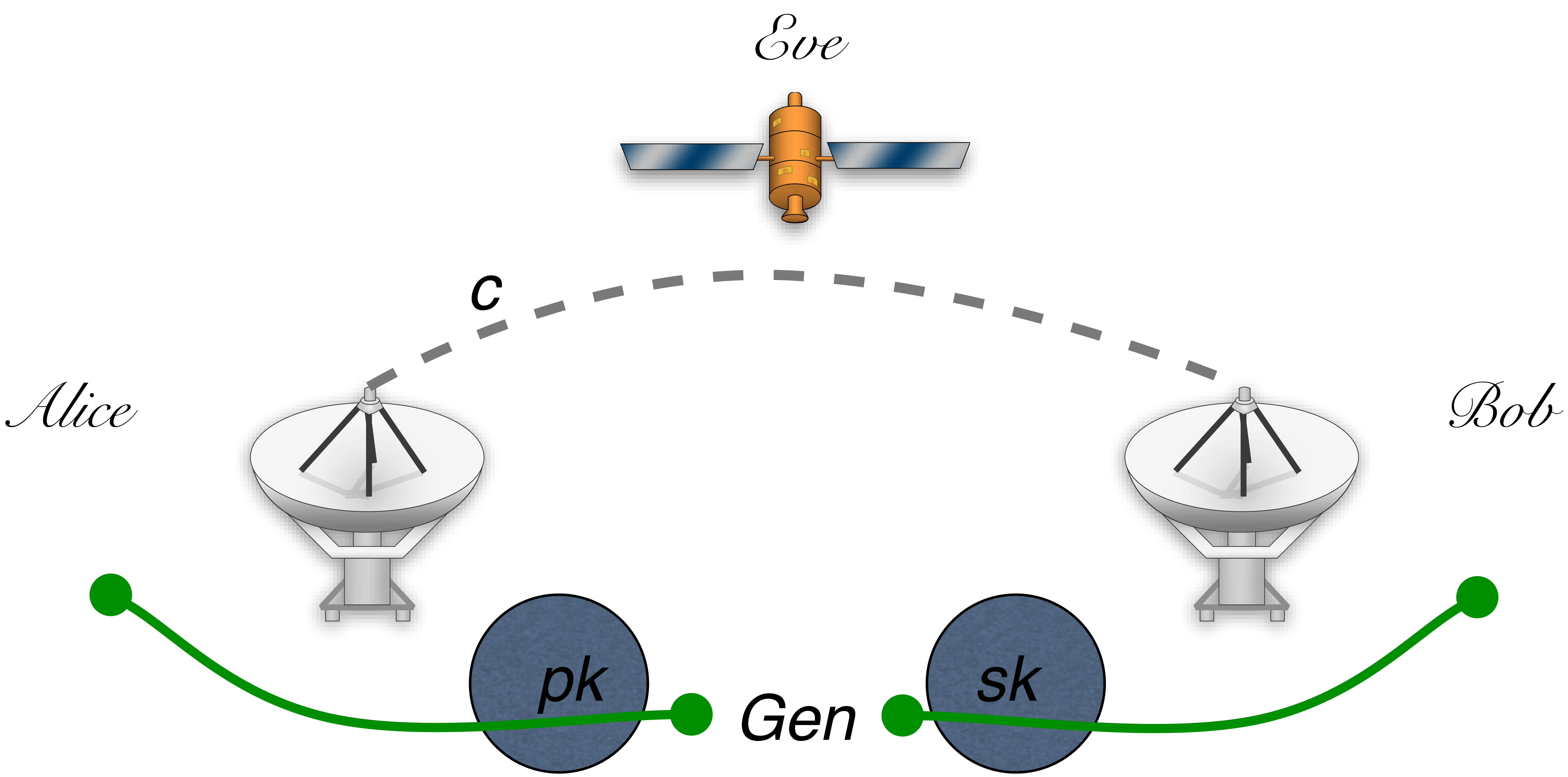
Enc (encryption)

$$c \leftarrow \mathsf{Enc}_{pk}(m) \text{ for } pk \in \mathcal{K}, m \in \mathcal{M}$$

Dec (decryption)

$$\forall m \in \mathcal{M}, (pk, sk) \leftarrow \mathsf{Gen}(1^n)$$

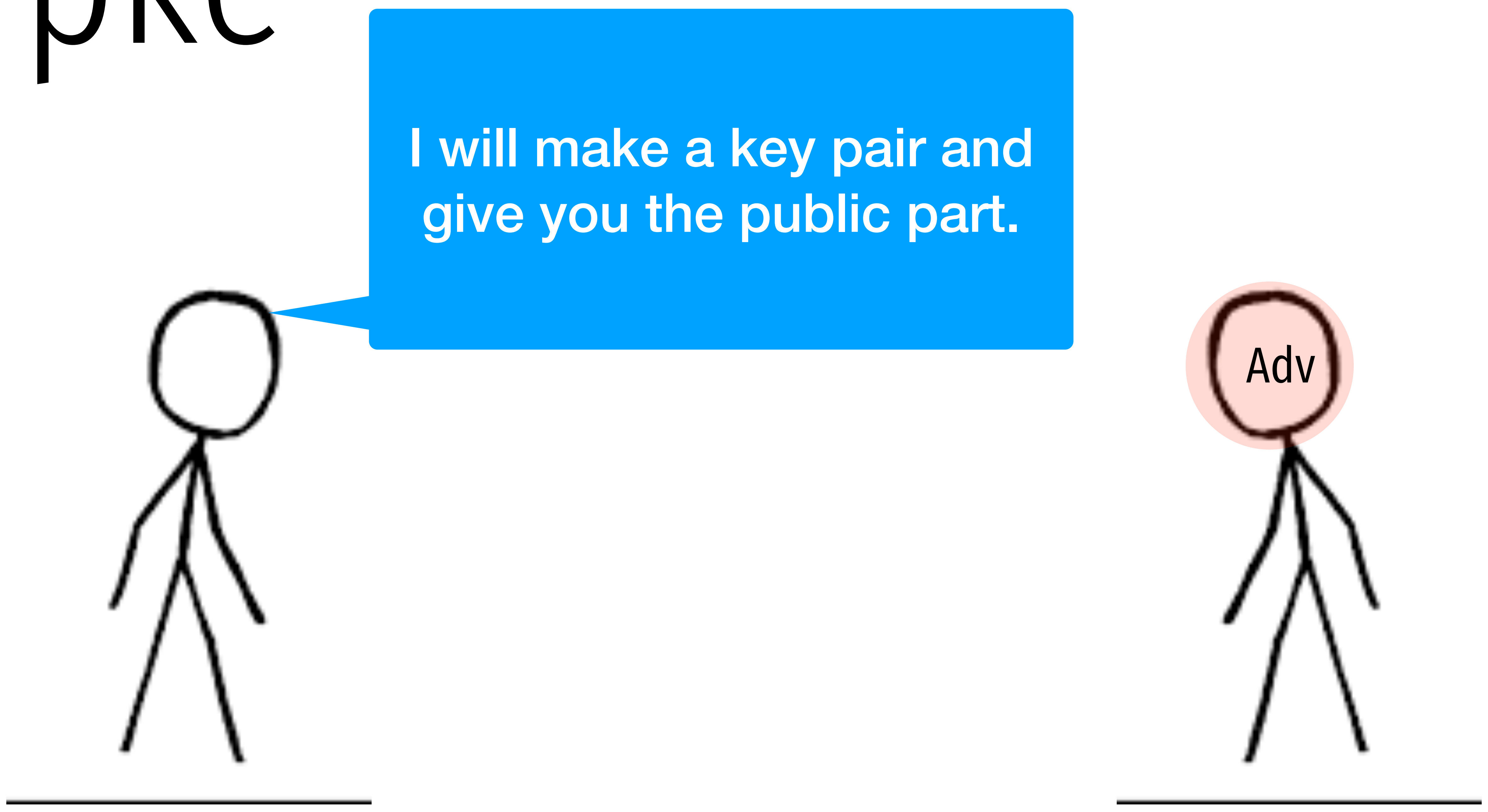
$$\Pr[\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m] = 1$$



"for any pair of messages m_1, m_2,
Eve cannot tell whether $c = Enc_{pk}(m_i)$."

IND-CPA security for pke

(weakest notion of security)

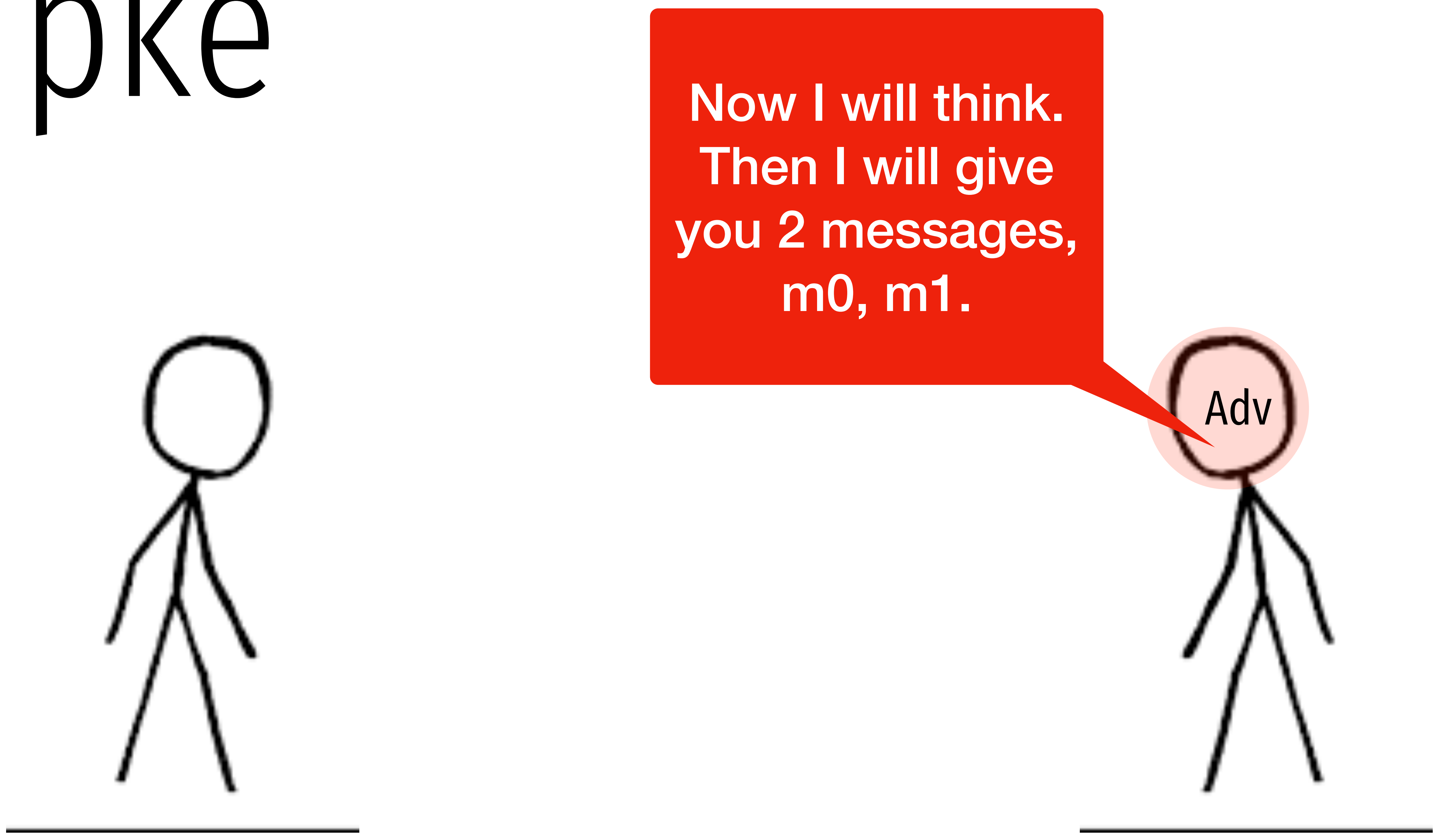


$pk, sk \leftarrow \mathsf{gen}(1^n)$

pk

IND-CPA security for pke

(weakest notion of security)



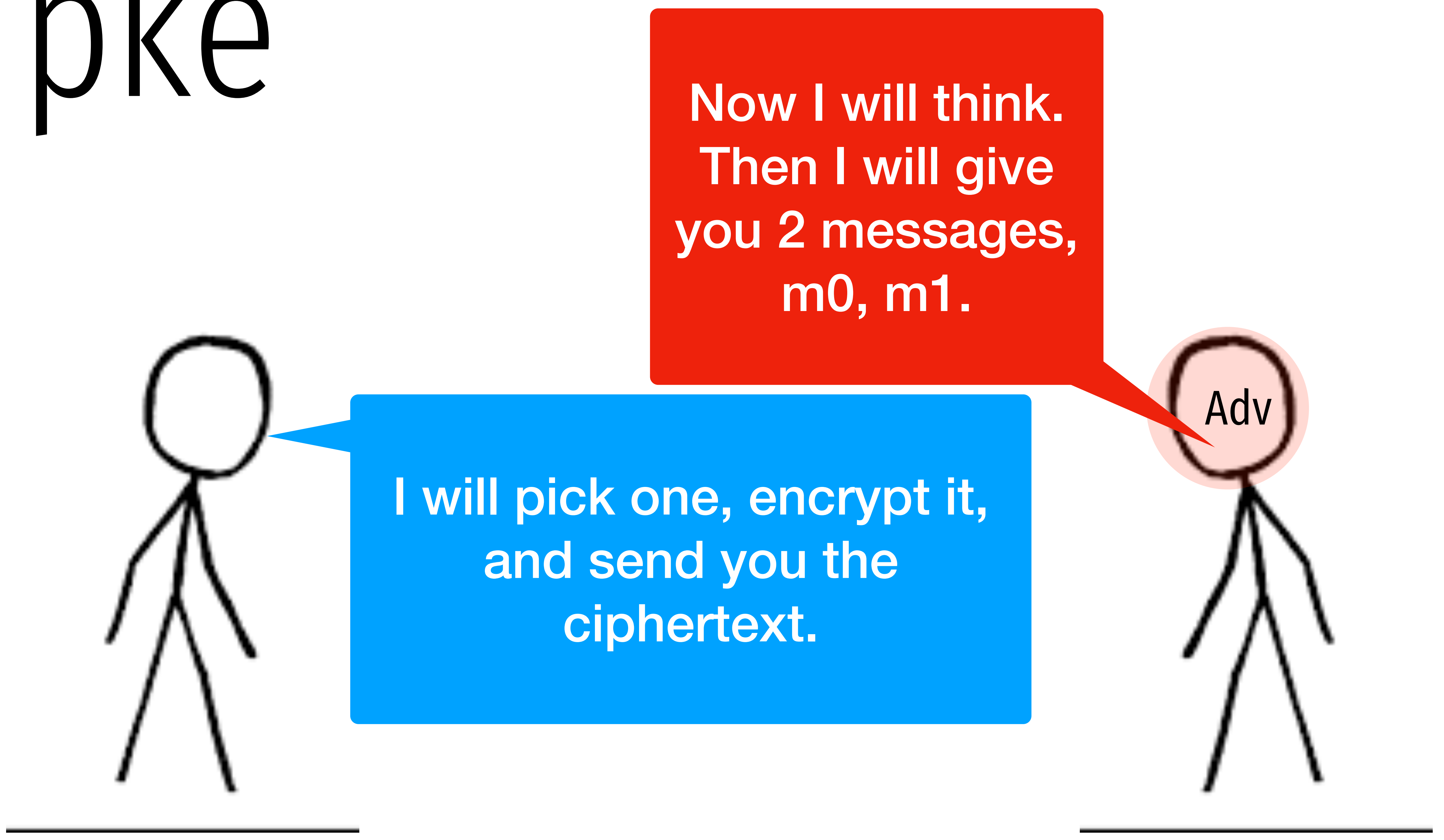
$pk, sk \leftarrow \mathsf{gen}(1^n)$

pk

$m_0, m_1 \leftarrow A(pk)$

IND-CPA security for pke

(weakest notion of security)



$pk, sk \leftarrow \mathsf{gen}(1^n)$

pk

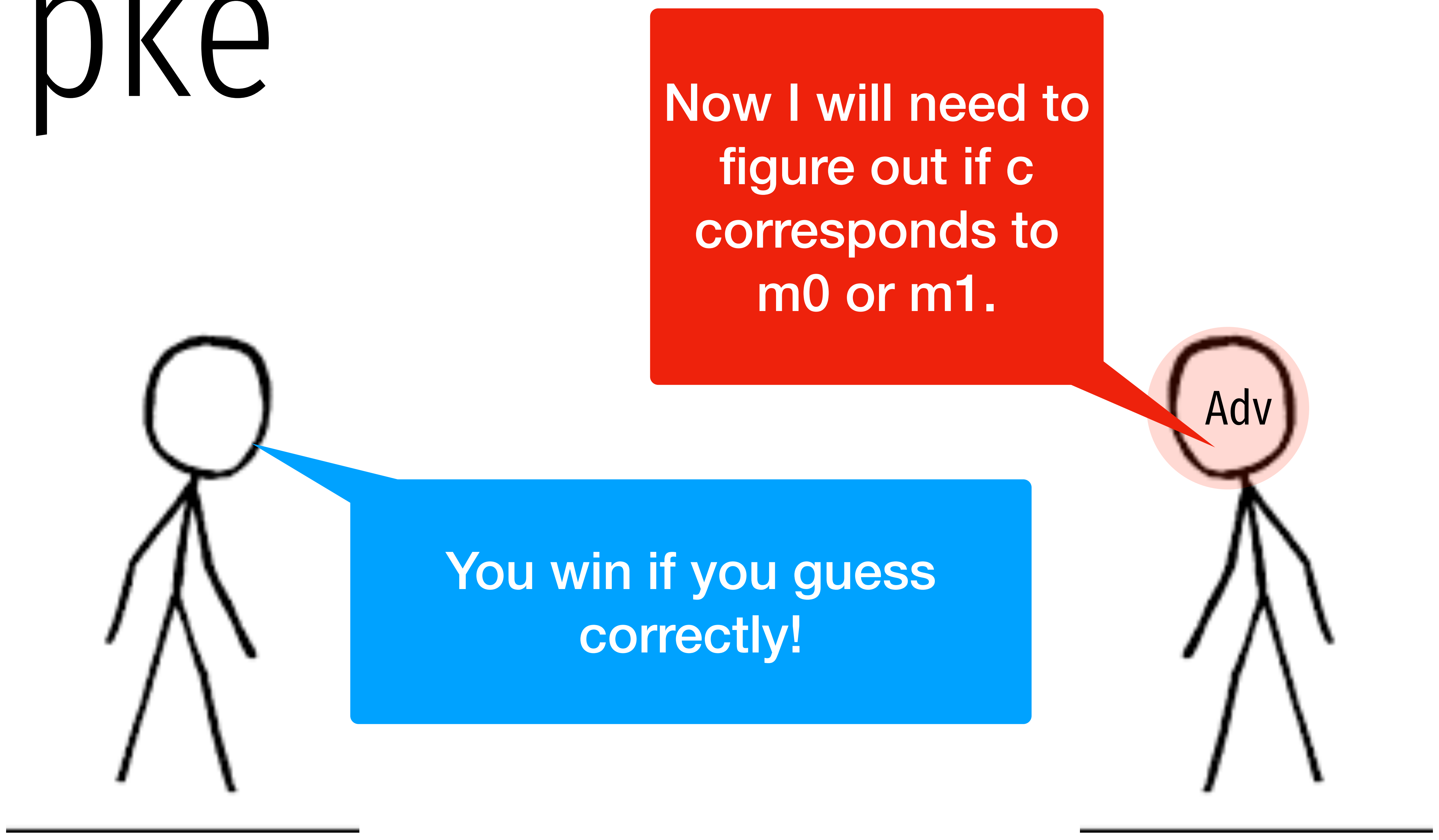
$m_0, m_1 \leftarrow A(pk)$

$b \leftarrow \{0,1\}$

$c \leftarrow \mathsf{enc}_{pk}(m_b)$

IND-CPA security for pke

(weakest notion of security)



$pk, sk \leftarrow \mathsf{gen}(1^n)$

pk

$m_0, m_1 \leftarrow A(pk)$

$b \leftarrow \{0,1\}$

$c \leftarrow \mathsf{enc}_{pk}(m_b)$

$b' \leftarrow A(pk, m_0, m_1, c)$

IND-CPA security for pke

(weakest notion of security)

$$
\begin{aligned}
pk, sk &\leftarrow \mathsf{gen}(1^n) \\
m_0, m_1 &\leftarrow A(pk) \\
b &\leftarrow \{0,1\} \\
c &\leftarrow \mathsf{enc}_{pk}(m_b) \\
b' &\leftarrow A(pk, m_0, m_1, c)
\end{aligned}
$$

$$\Pr[b = b'] = 1/2 + \epsilon(n)$$

How to build public key encryption?

Basic Number theory

$$a \bmod p$$

$17 \bmod 11$

$135433238 \bmod 11$

$$a \bmod p$$

17 mod 11 =6

135433238 mod 11 =6

$$\begin{array}{r|l} & 12312112 \quad R\,6 \\ 11 & 135433238 \end{array}$$

11
25
22
34
33
13
11
23
22
12
11
13
11
28

Basic number theory

Modular arithmetic

Claim 28.1. *For* $n > 0$ *and* $a, b \in \mathbb{Z}$*,*

1. $(a \bmod n) + (b \bmod n) = (a + b) \bmod n$

2. $(a \bmod n)(b \bmod n) \bmod n = ab \bmod n$

Modular Exponentiation $(a, x, n) \to a^x \bmod n$

$$7^{19} \bmod 31$$

Modular Exponentiation

$$(a, x, n) \to a^x \bmod n$$

Algorithm 2: ModularExponentiation(a, x, n)

Input: $a, x \in [1, n]$

$r \leftarrow 1$
while $x > 0$ **do**
    if x *is odd* **then**
        $r \leftarrow r \cdot a \bmod n$
    $x \leftarrow \lfloor x/2 \rfloor$
    $a \leftarrow a^2 \bmod n$
Return r

Modular Exponentiation

$$(a, x, n) \to a^x \bmod n$$

$$a^x \bmod n = \prod_{i=0}^{\ell} x_i a^{2^i} \bmod n$$

Algorithm 2: ModularExponentiation(a, x, n)

```
Input: a, x ∈ [1, n]
r ← 1
while x > 0 do
    if x is odd then
        r ← r · a mod n
    x ← ⌊x/2⌋
    a ← a^2 mod n
Return r
```

Greatest Common Divisor

```
GCD(A,B)  =  GCD(              )
```

Greatest Common Divisor

`GCD(6809,1639)`

Greatest Common Divisor

GCD(6809,1641)

$6809 = 4 \cdot 1641 + 245 \quad (-643, 2668)$

$1641 = 6 \cdot 245 + 171 \quad (96, -643$

$245 = 1 \cdot 171 + 74 \quad (-67, 96)$

$171 = 2 \cdot 74 + 23 \quad (29, -67)$

$74 = 3 \cdot 23 + 5 \quad (-9, 29)$

$23 = 4 \cdot 5 + 3 \quad (2, -9)$

$5 = 1 \cdot 3 + 2 \quad (-1, 2)$

$3 = \boxed{1} \cdot 2 + 1 \quad (1, -1)$

$2 = 2 \cdot 1 + 0 \quad (0, 1)$

given (a,b), finds (x,y) s.t.
ax + by = gcd(a,b)

Algorithm 1: ExtendedEuclid(a, b)

Input: (a, b) s.t $a > b \geq 0$

Output: (x, y) s.t. $ax + by = \gcd(a, b)$

if $a \bmod b = 0$ **then**

  Return $(0, 1)$

else

  $(x, y) \leftarrow$ `ExtendedEuclid` $(b, a \bmod b)$

  Return $(y, x - y(\lfloor a/b \rfloor))$

---

groups

$$(G, \bigoplus)$$

closure

associativity

identity

inverse

groups

$(G, \oplus)$

closure	$a, b \in G \implies a \oplus b \in G$
associativity	$a, b, c \in G \implies (a \oplus b) \oplus c = a \oplus (b \oplus c)$
identity	$\exists i \in G \; s.t. \; \forall a \in G, \; i \oplus a = a$
inverse	$\forall a \in G. \; \exists a^{-1} \in G \; s.t. \; a \oplus a^{-1} = i$

example of groups

$$(\mathbb{Z}_n, +)$$

Example of groups

$$(\mathbb{Z}_n, \star)$$

$$\{a \mid \gcd(a,n) = 1\}$$

multiplicative group, mod n

$$\mathbb{Z}_n^\star$$

verify

$$\mathbb{Z}_n^\star \qquad \{a \mid \gcd(a,n) = 1\}$$

is a group

closure

associativity

identity

inverse?

Euler totient

Euler totient

$\phi(15) =$

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15$$

Euler totient

$$|\mathbb{Z}_n^\star| = \Phi(n)$$

prime $\quad \Phi(p) = p - 1$

product of 2 primes $\quad \Phi(n) = (p-1)(q-1)$

Euler theorem

$$\forall a \in \mathbb{Z}_n^{\star},\ a^{\Phi(n)} = 1 \bmod n$$

Examples

$$7^{30} \bmod 31 =$$

1	2	4	8	16
7	18	14	10	7

Examples

$$2^8 \bmod 15 =$$

Euler's theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 19 20 21 22 23 24 25 26 27 28 29 30

Euler's theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 19 20 21 22 23 24 25 26 27 28 29 30

$1a$ $2a$ $3a$ $4a$ $5a$ $6a$ $7a$ $8a$ $9a$ $10a$ $11a$ $12a$ $13a$ $14a$ $15a$ $16a$ $17a$ $19a$ $20a$ $21a$ $22a$ $23a$ $24a$ $25a$ $26a$ $27a$ $28a$ $29a$ $30a$

Euler's theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$

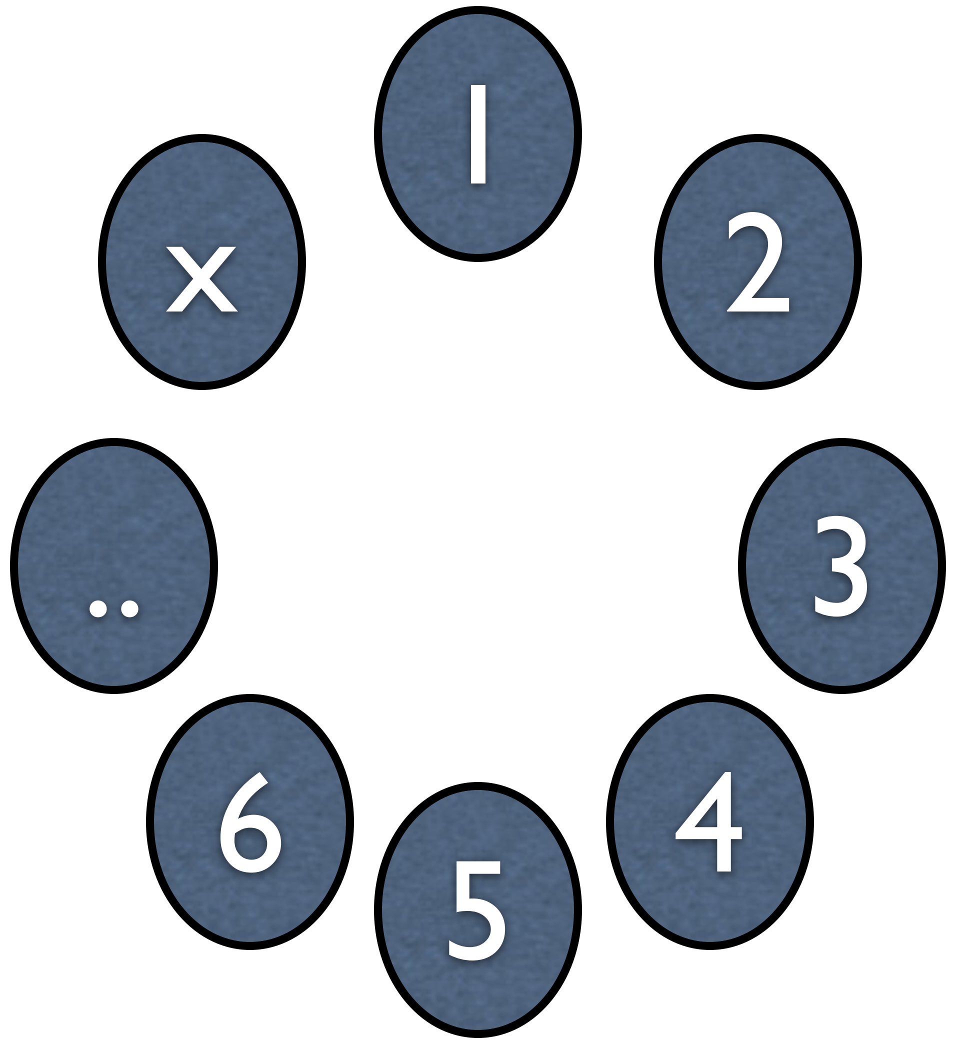
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 19 20 21 22 23 24 25 26 27 28 29 30

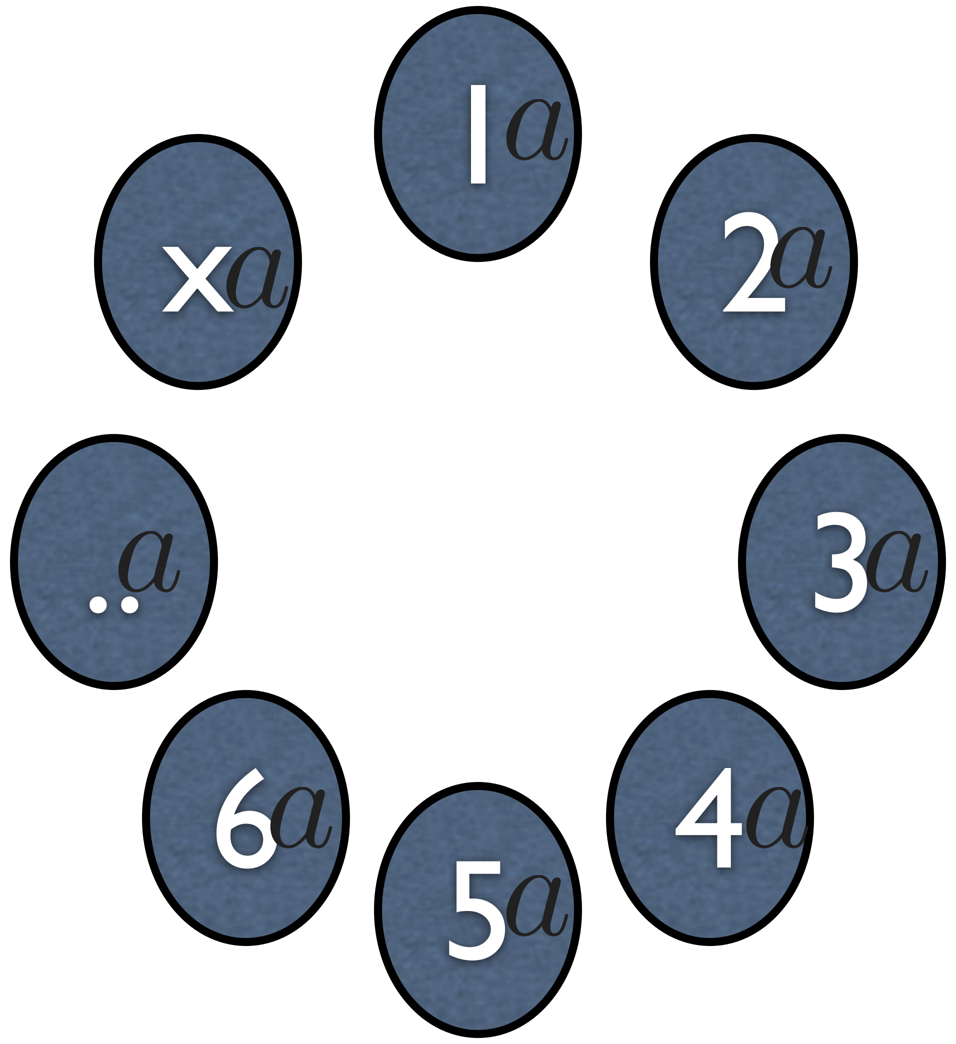
$1a$ $2a$ $3a$ $4a$ $5a$ $6a$ $7a$ $8a$ $9a$ $10a$ $11a$ $12a$ $13a$ $14a$ $15a$ $16a$ $17a$ $19a$ $20a$ $21a$ $22a$ $23a$ $24a$ $25a$ $26a$ $27a$ $28a$ $29a$ $30a$

3 6 9 12 15 18 21 24 27 30 2 5 8 11 14 17 20 23 26 29 1 4 7 10 13 16 19 22 25

Euler theorem

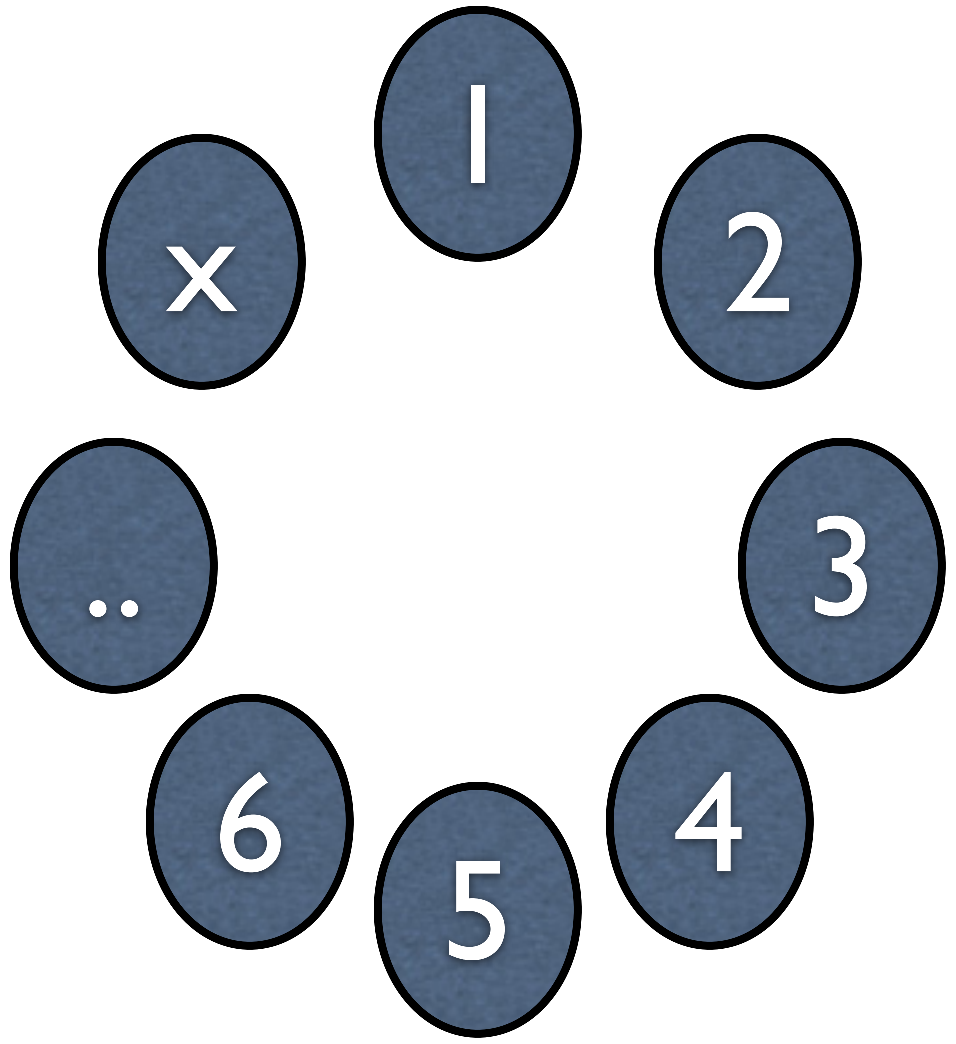
$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$

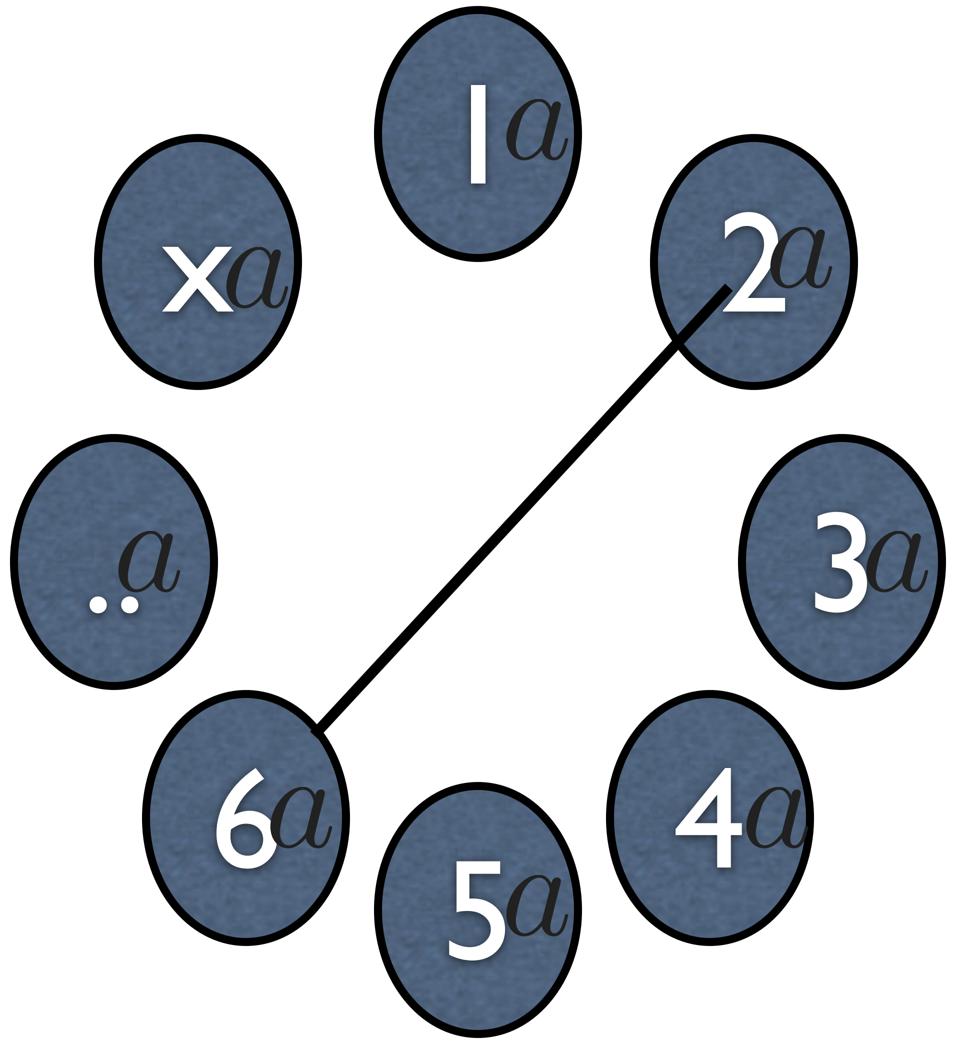




Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$





argue: all are distinct

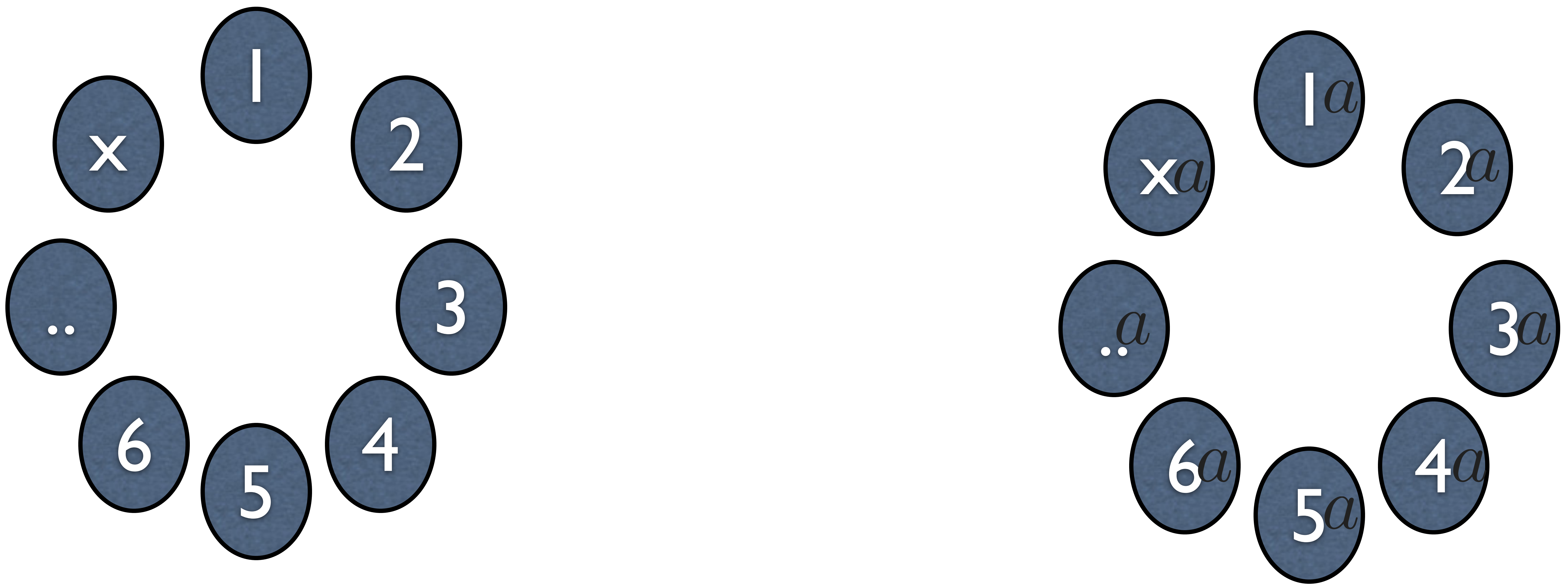
spse two are equal.

multiply by a^{-1}

this implies 2=6!

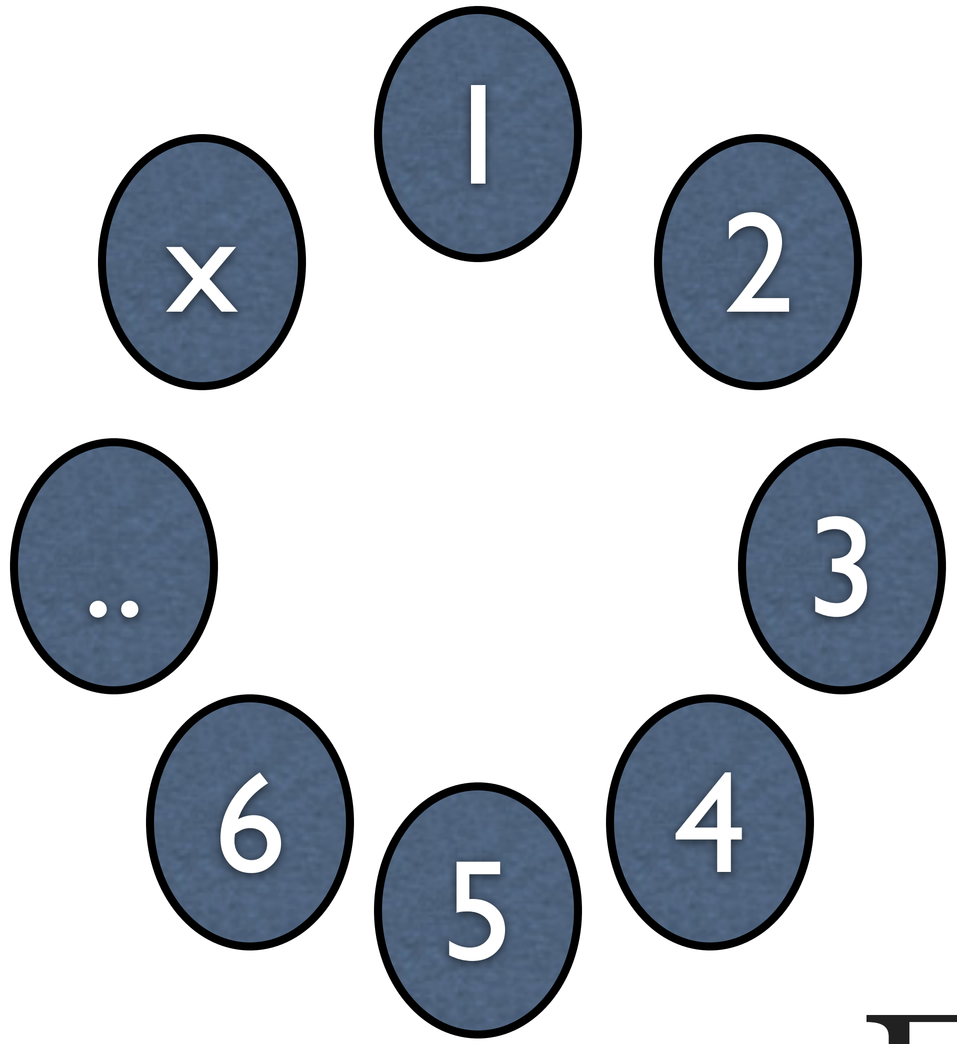
Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$

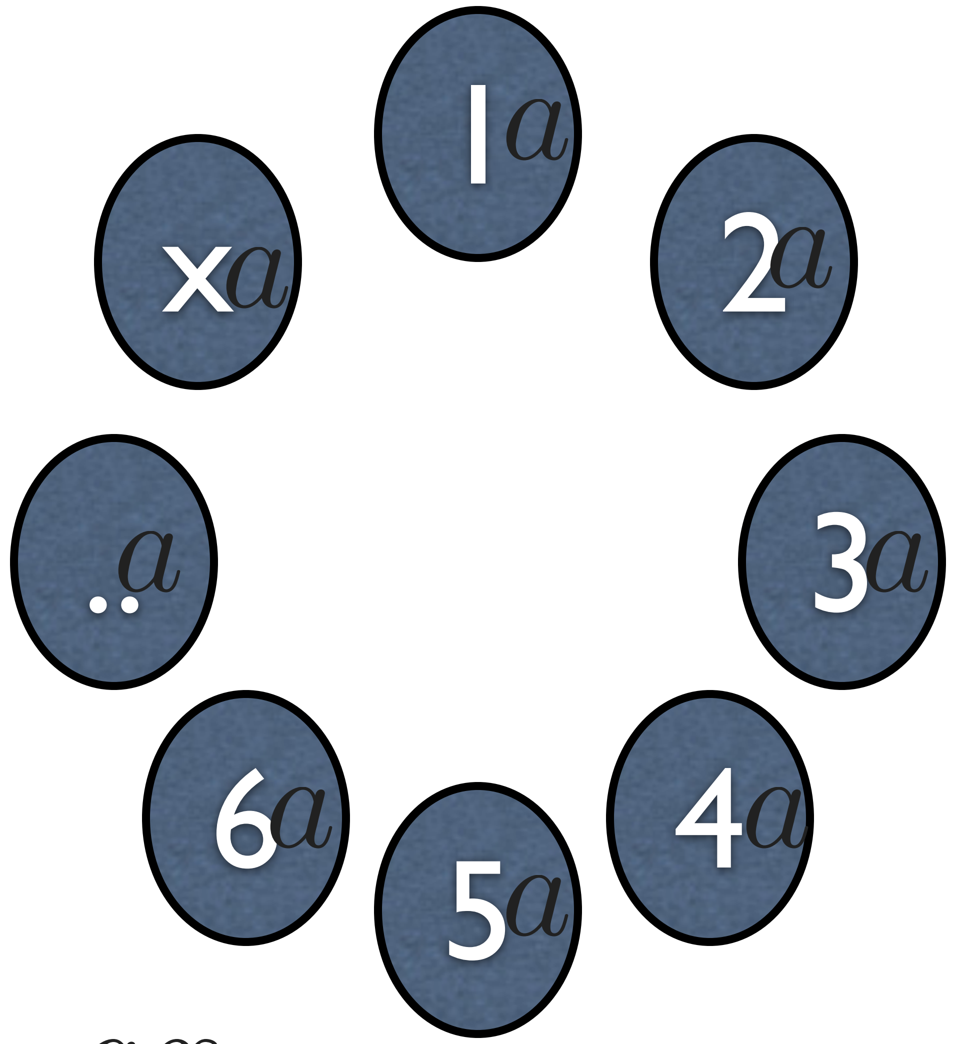


Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$



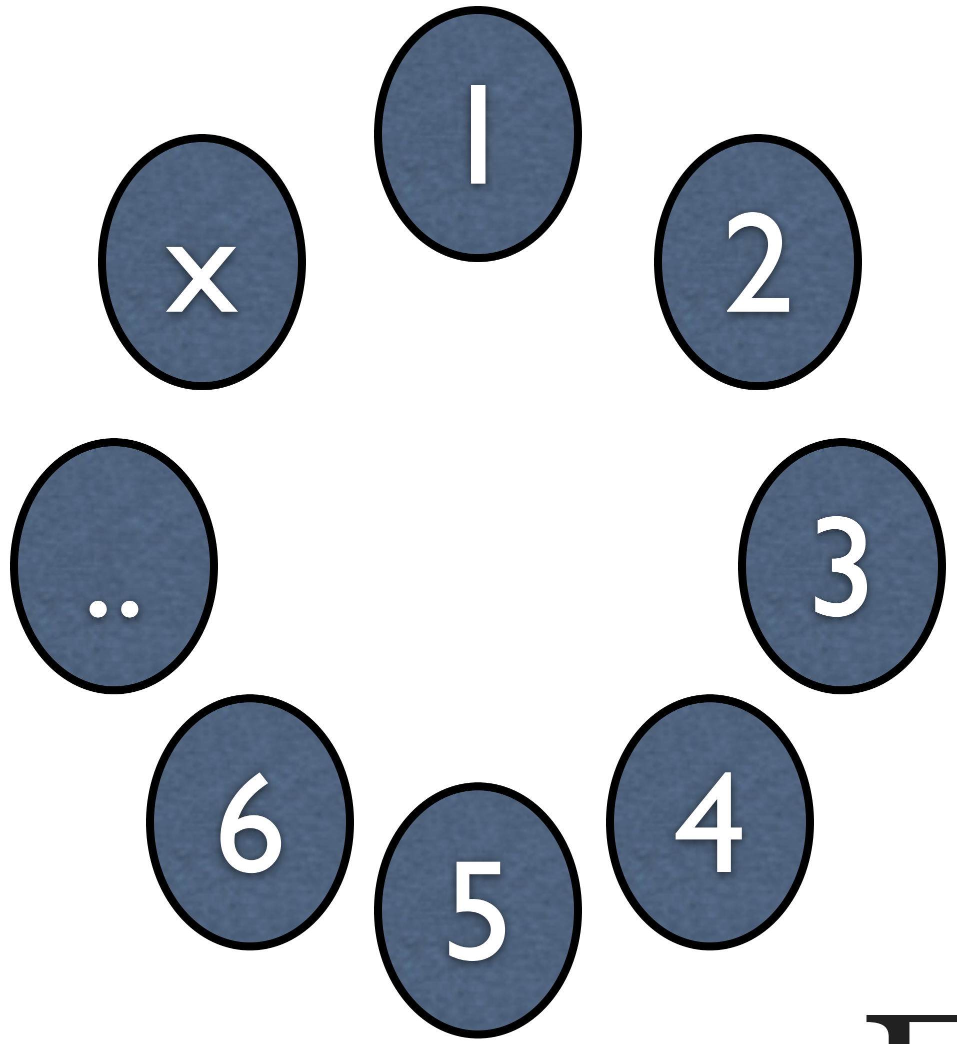
$$\prod_{x \in Z_N^\star} x$$

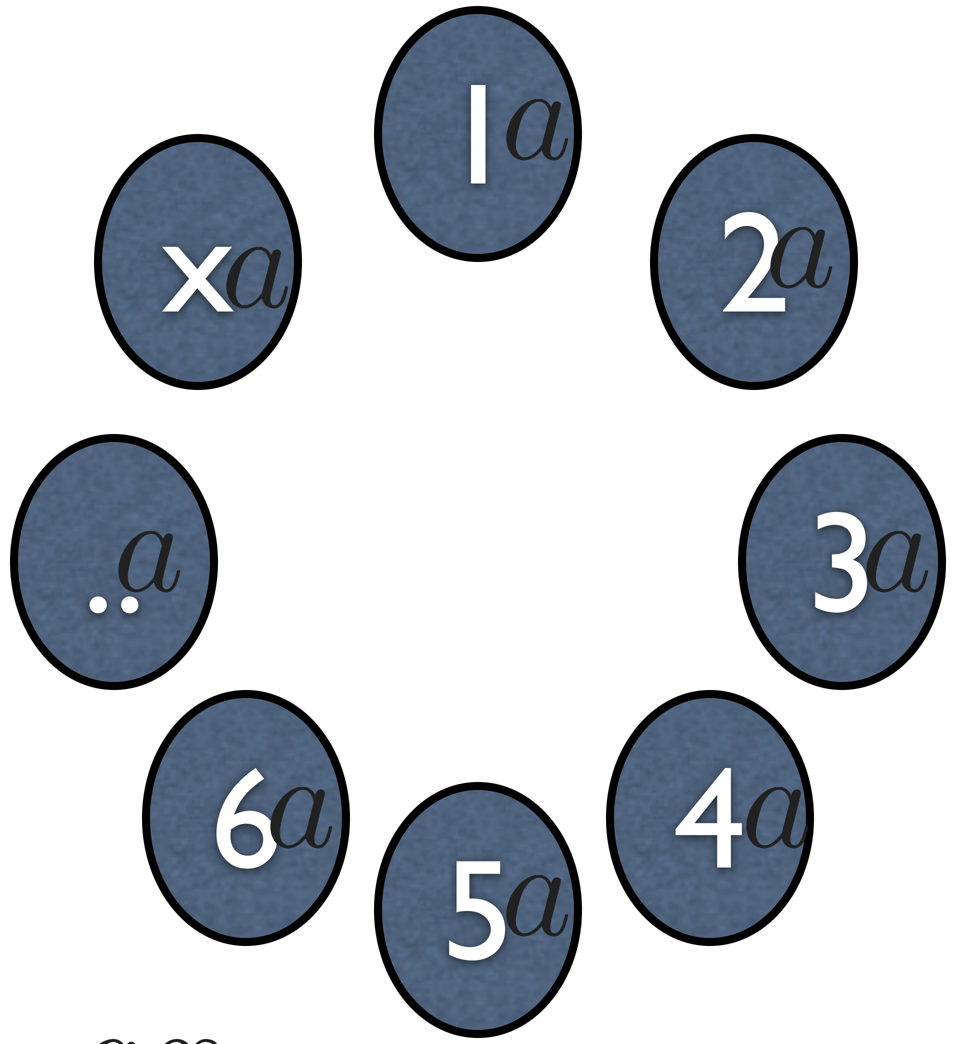


$$\prod_{x \in Z_N^\star} ax$$

Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$

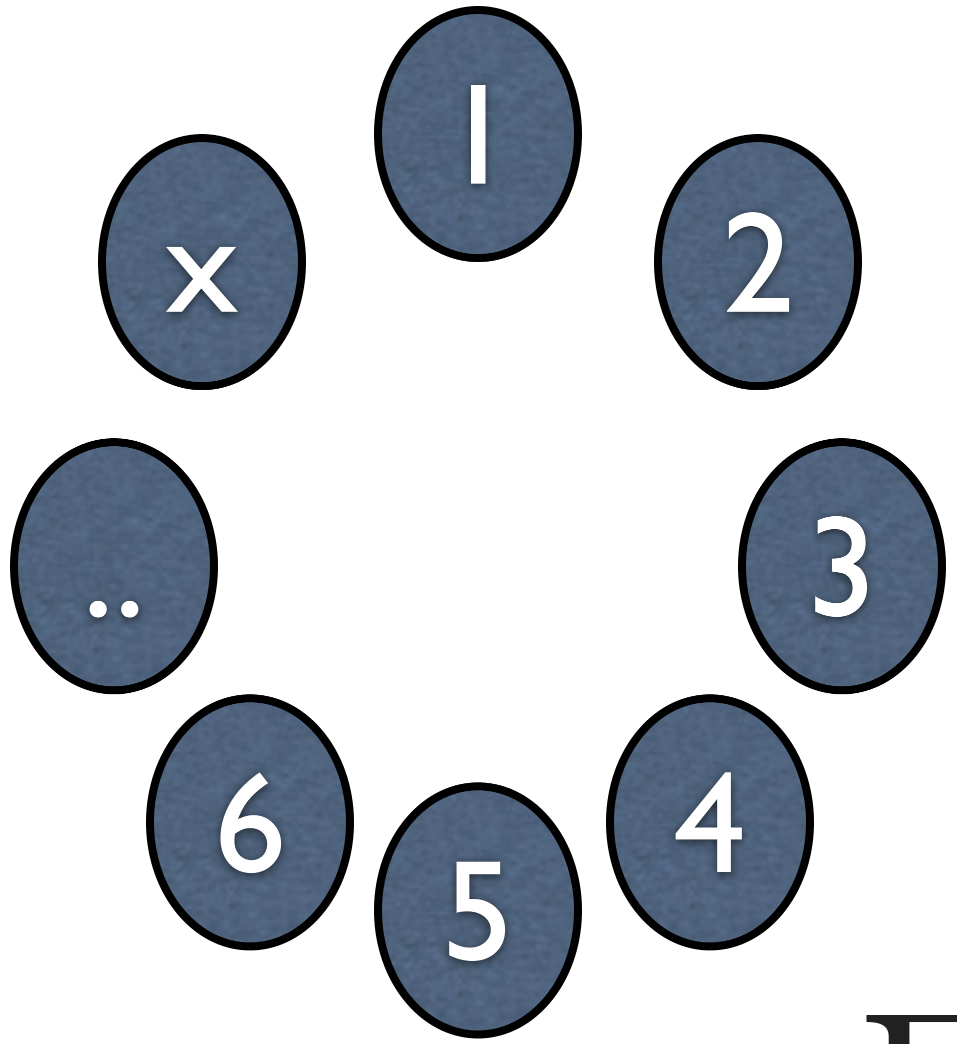


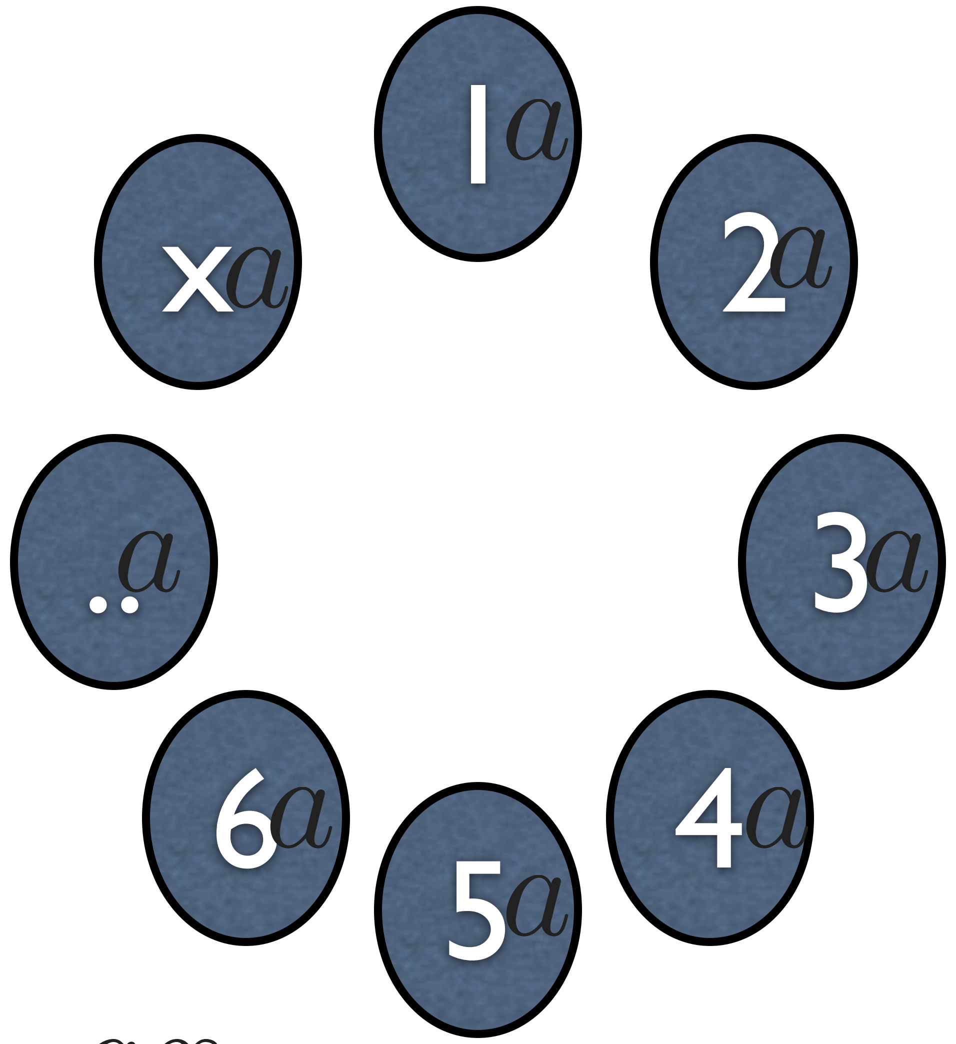


$$\prod_{x \in Z_N^\star} x = \prod_{x \in Z_N^\star} ax$$

Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$



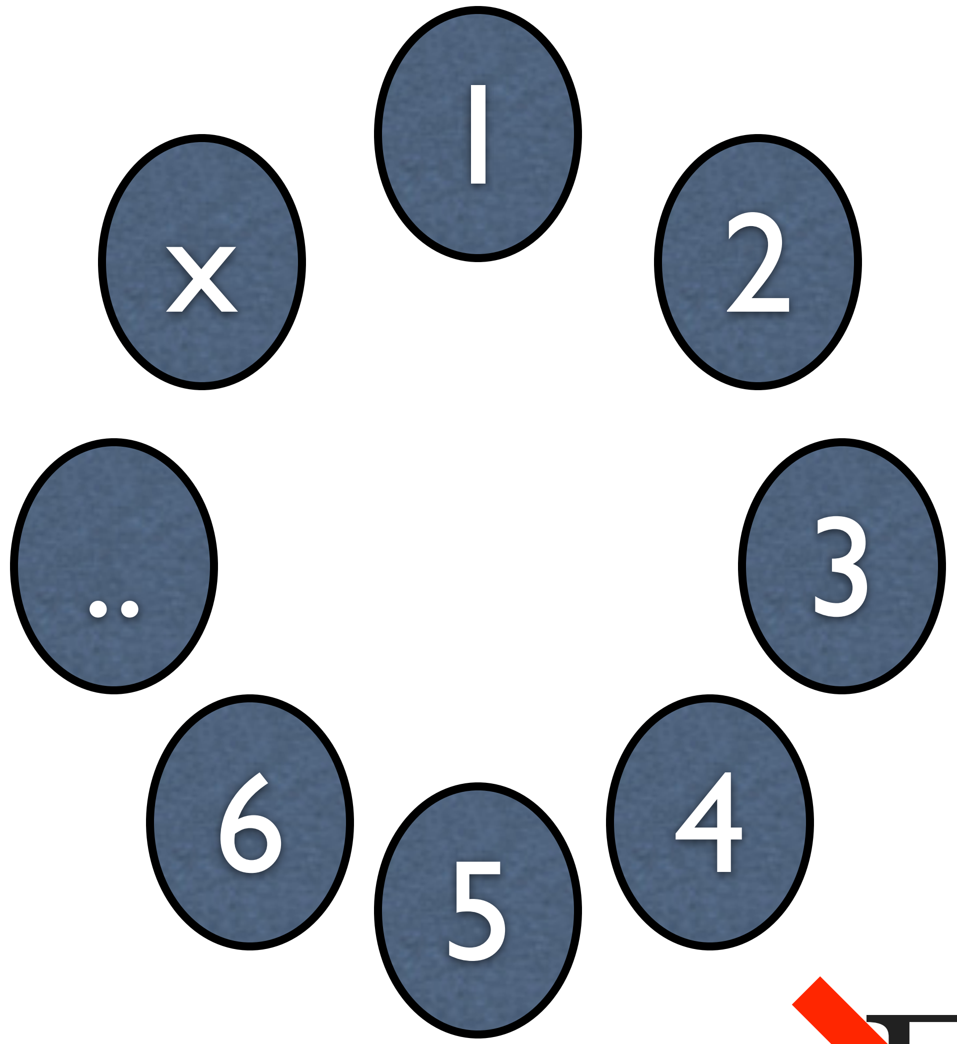


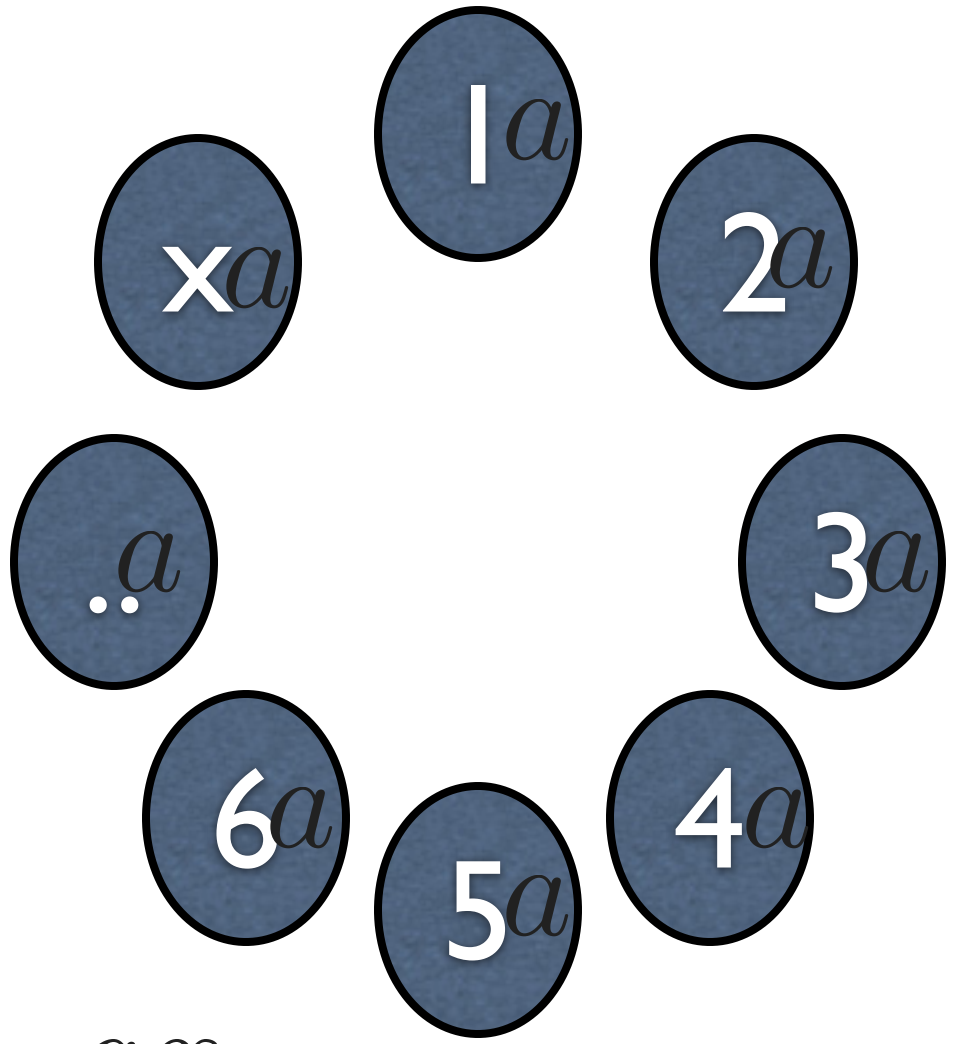
$$\prod_{x \in Z_N^\star} x = \prod_{x \in Z_N^\star} ax$$

$$a^{\Phi(N)} \prod_{x \in Z_N^\star} x$$

Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$





$$\cancel{\prod_{x\in Z_N^\star}} x = \prod_{x\in Z_N^\star} ax$$

$$a^{\Phi(N)} \cancel{\prod_{x\in Z_N^\star}} x$$

Implications of Euler

$$a^{10\phi(N)} \bmod N =$$

$$a^{k\phi(N)+1} \bmod N =$$

compute

$$11^{30^{2021}} \bmod 23$$

(show your work)

“Textbook” RSA (insecure)

Pick N = p*q where p,q are primes.

“Textbook” RSA (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \bmod \phi(N)$

“Textbook” RSA (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \mod \phi(N)$

$\text{Enc}_{N,e}(m) = m^e \mod N$

$\text{Dec}_{N,d}(c) = c^d \mod N$

"Textbook" RSA (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \bmod \phi(N)$

$\mathsf{Enc}_{N,e}(m) = m^e \mod N$

$\mathsf{Dec}_{N,d}(c) = c^d \mod N$

$$(m^e)^d \bmod N =$$

Example of Textbook RSA

$m=5$

“Textbook” RSA (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \bmod \phi(N)$

$\text{Enc}_{N,e}(m) = m^e \mod N$

$\text{Dec}_{N,d}(c) = c^d \mod N$

Why is it insecure against IND-CPA attack?

pkcs1.5

ENC$_{pk}$(m)

PICK r AS A RANDOM STRING WITH NO 0S

(TYPICALLY 8 BYTES)

$$c \leftarrow (0||2||r||0||m)^e \bmod N$$

"PADDING ORACLE" ATTACK AGAINST THIS SCHEME

Example

RSA-OAEP+

GEN(1^n)

$$f, f^{-1} \leftarrow \text{TRAPDOOR OWP}()$$

ENC$_{pk}$(m)

$$r \leftarrow U_n$$
$$s \leftarrow R_1(r) \oplus m \;||\; R_2(r||m)$$
$$t \leftarrow R_3(s) \oplus r$$
$$c \leftarrow f(s||t)$$

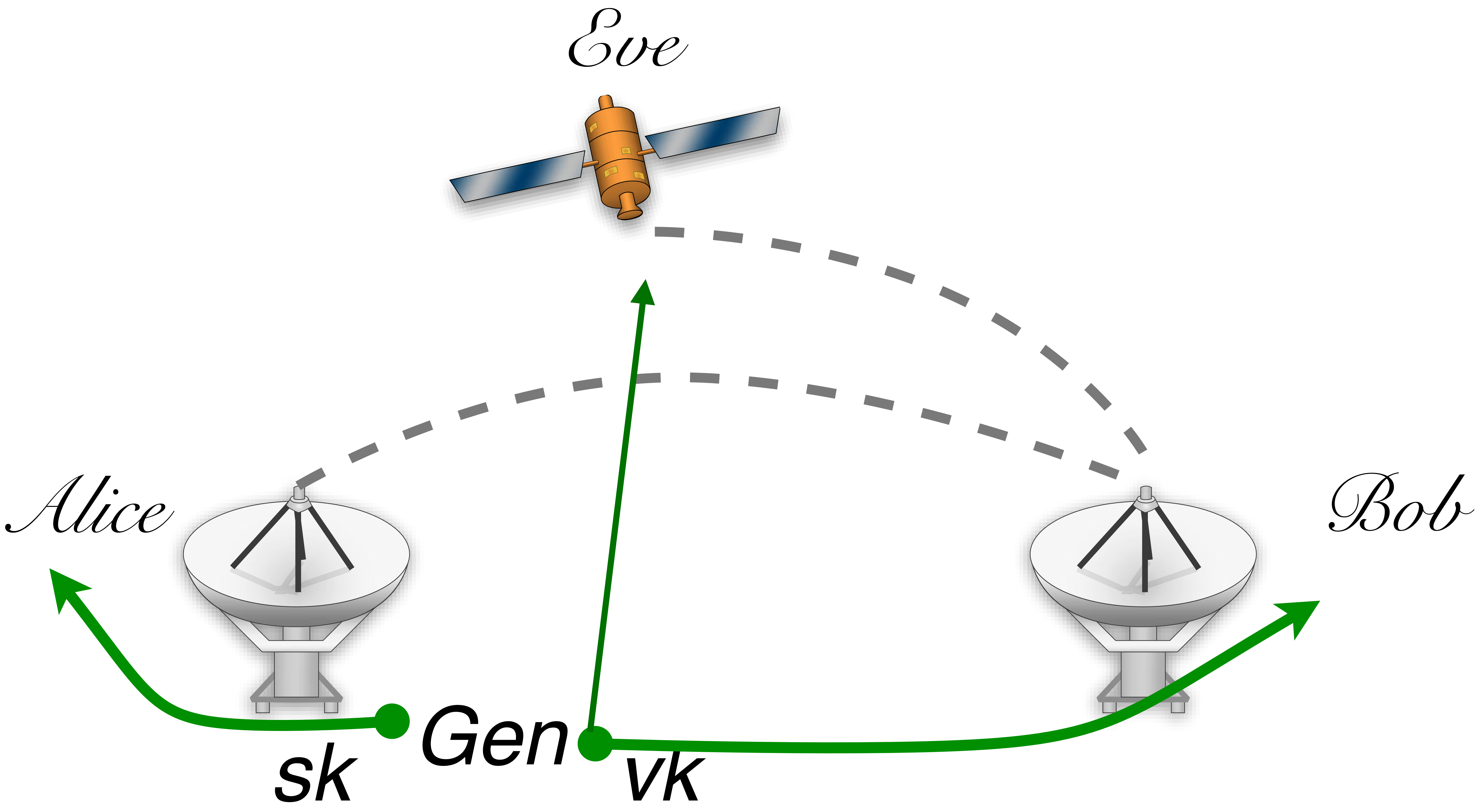
$$R_1 : \{0,1\}^{k_0} \rightarrow \{0,1\}^n$$
$$R_2 : \{0,1\}^{n+k_0} \rightarrow \{0,1\}^{k_1}$$
$$R_3 : \{0,1\}^{n+k_1} \rightarrow \{0,1\}^{k_0}$$

DEC$_{sk}$(c)

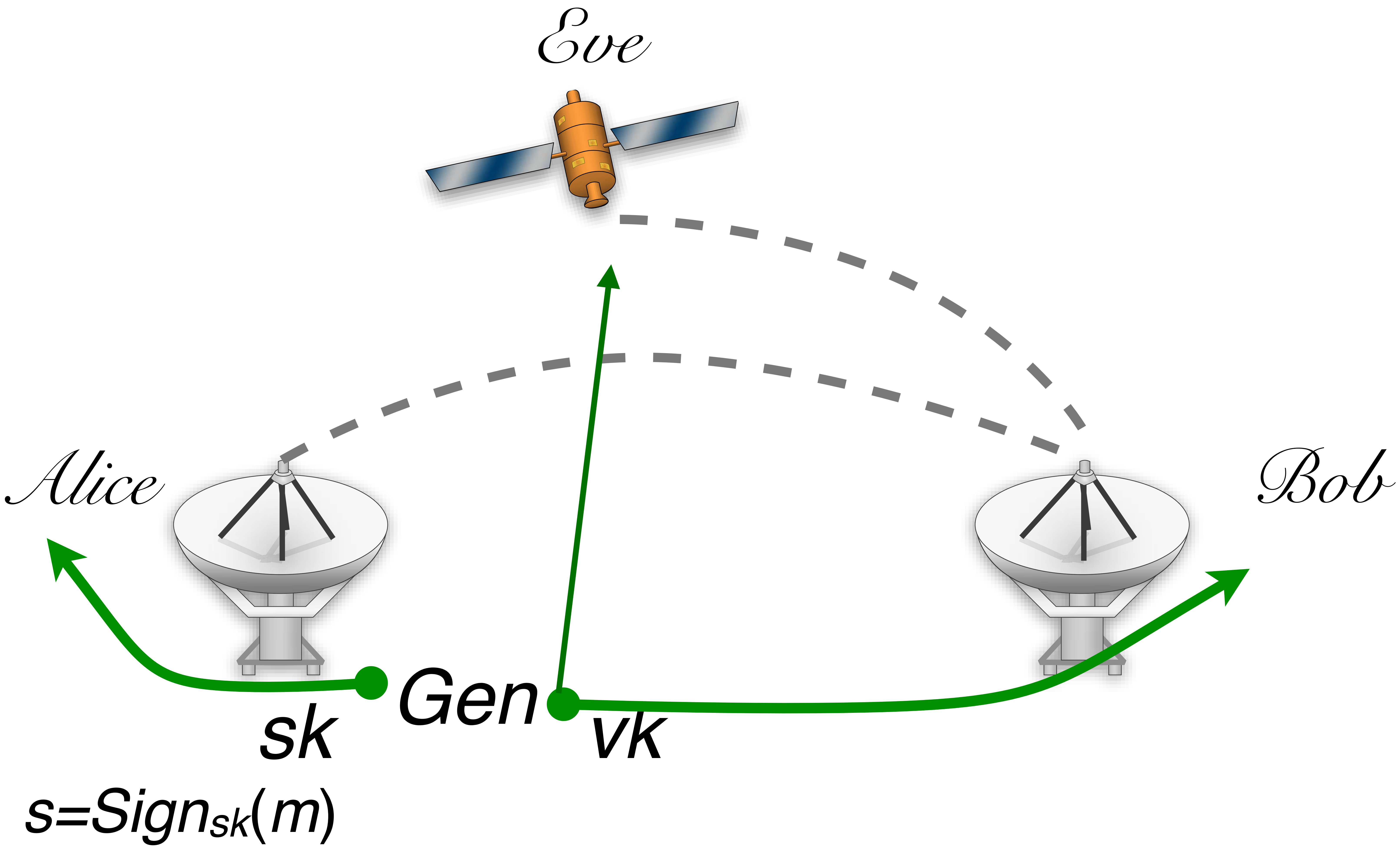
$$(s = (s_1, s_2), t) \leftarrow f^{-1}(c)$$
$$r \leftarrow R_3(s) \oplus t$$
$$m \leftarrow R_1(r) \oplus s_1$$
$$R_2(r||m) \stackrel{?}{=} s_2$$

OUTPUT m ELSE FAIL

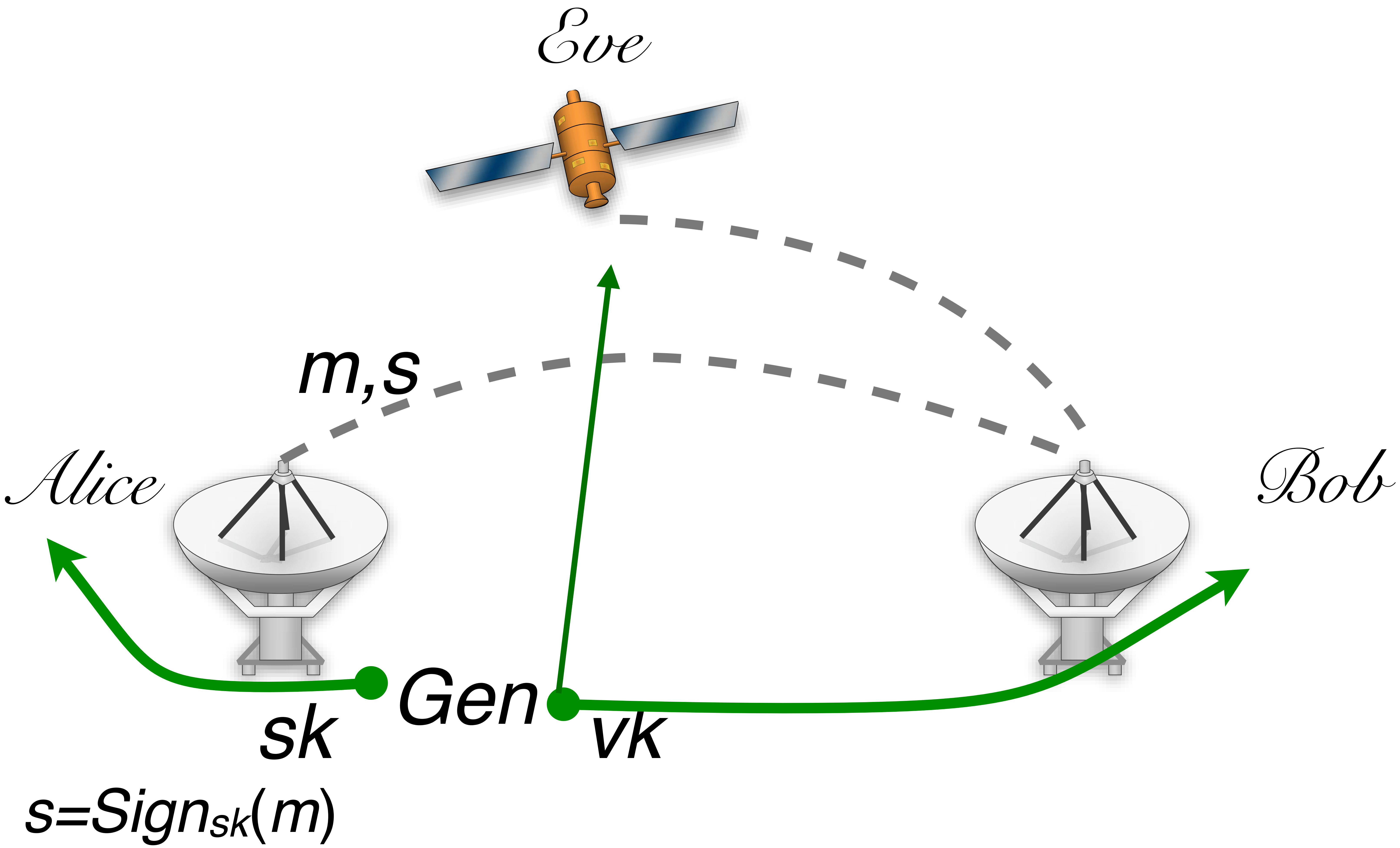
Public key digital signature



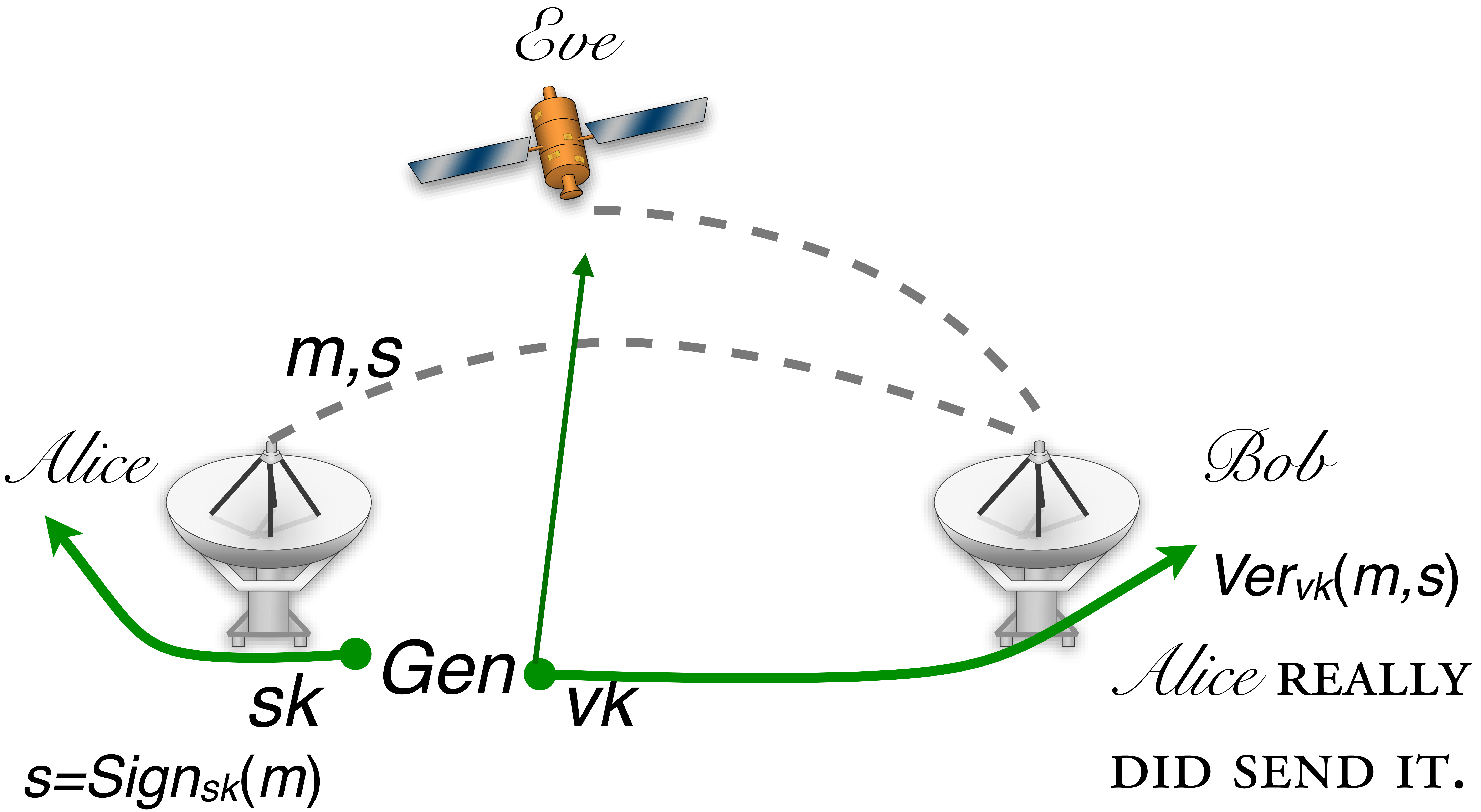
Public key digital signature



Public key digital signature



Public key digital signature



Public key digital signature

MESSAGE SPACE $\{\mathcal{M}\}_n$

$Gen(1^n)$

$Sign_{sk}(m)$

$Ver_{vk}(m,s)$

Public key digital signature

MESSAGE SPACE $\{\mathcal{M}\}_n$

$Gen(1^n)$ GENERATES A KEY PAIR sk, vk

$Sign_{sk}(m)$

$Ver_{vk}(m,s)$

Public key digital signature

MESSAGE SPACE $\{\mathcal{M}\}_n$

$Gen(1^n)$ GENERATES A KEY PAIR sk, vk

$Sign_{sk}(m)$ GENERATES A SIGNATURE s FOR $m \in \mathcal{M}_n$

$Ver_{vk}(m,s)$

Public key digital signature

MESSAGE SPACE $\{\mathcal{M}\}_n$

Gen(1^n) GENERATES A KEY PAIR *sk,vk*

Sign$_{sk}$(m) GENERATES A SIGNATURE *s* FOR $m \in \mathcal{M}_n$

Ver$_{vk}$(m,s) ACCEPTS OR REJECTS A MSG,SIG PAIR

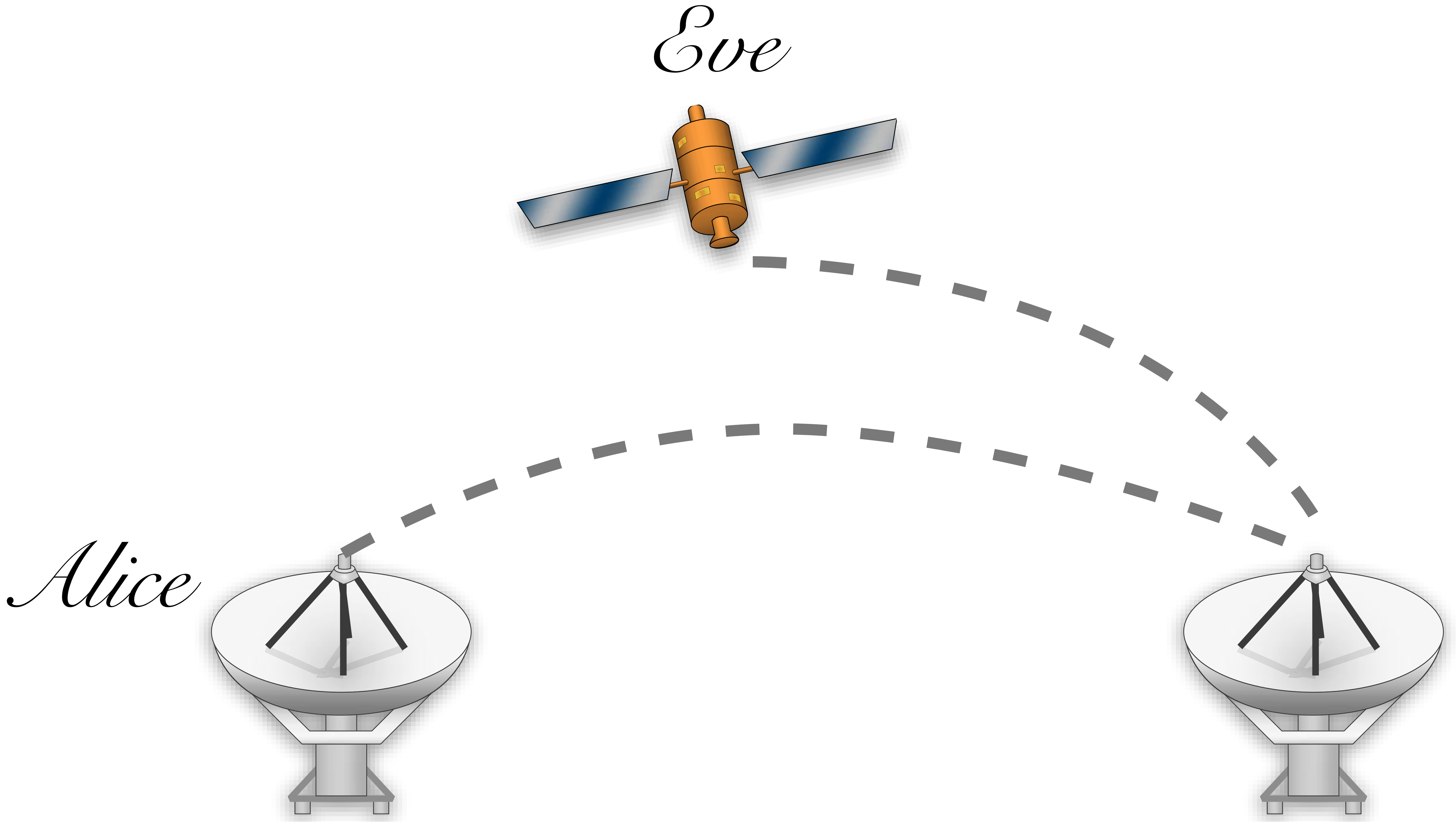
$$\Pr[k \leftarrow Gen(1^n) : Ver_{vk}(m, Sign_{sk}(m)) = 1] = 1$$

existential unforgability

"EVEN WHEN GIVEN A SIGNING ORACLE,

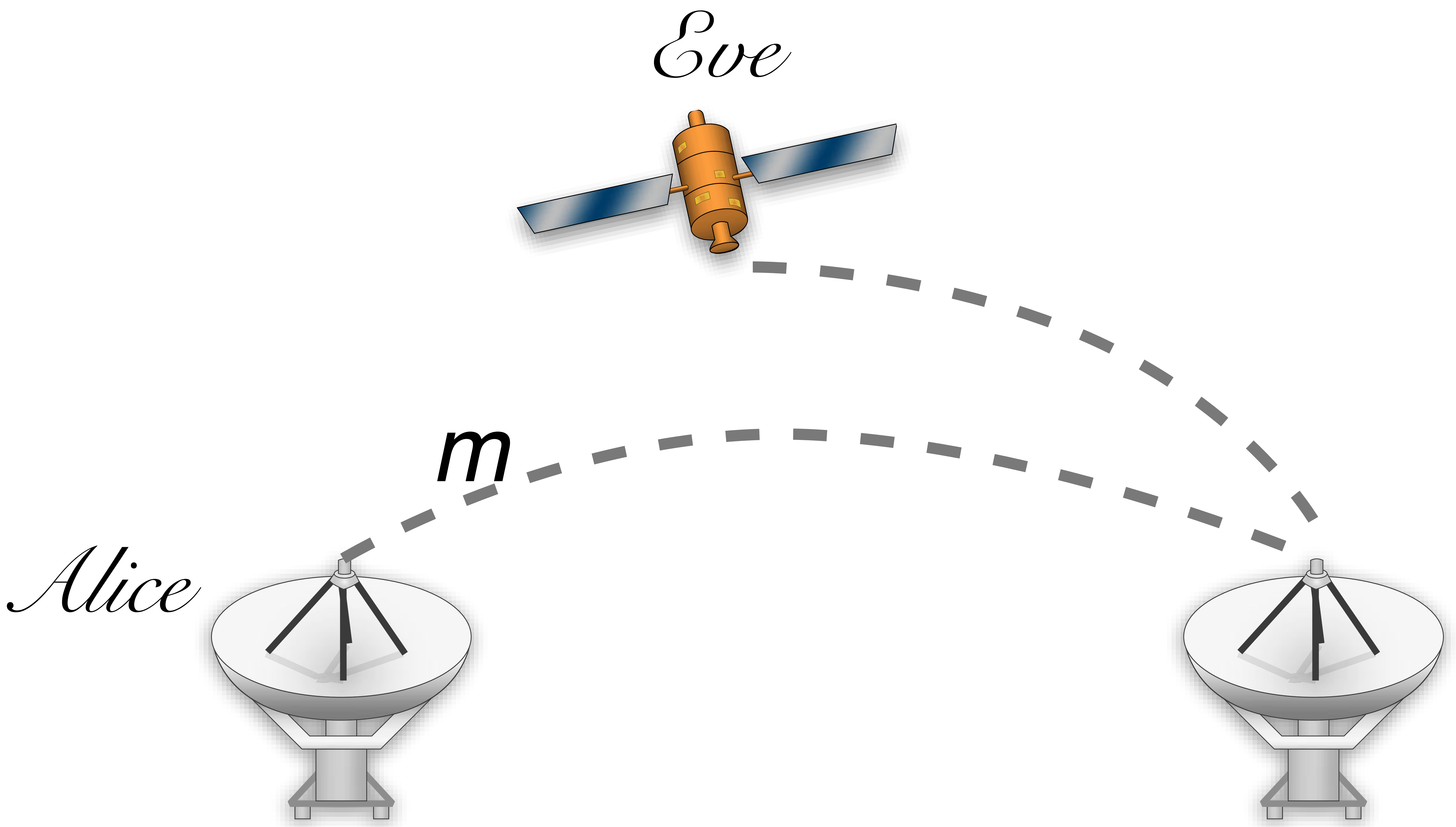
AN ADVERSARY CANNOT FORGE A SIGNATURE FOR

ANY MESSAGE OF ITS CHOOSING"

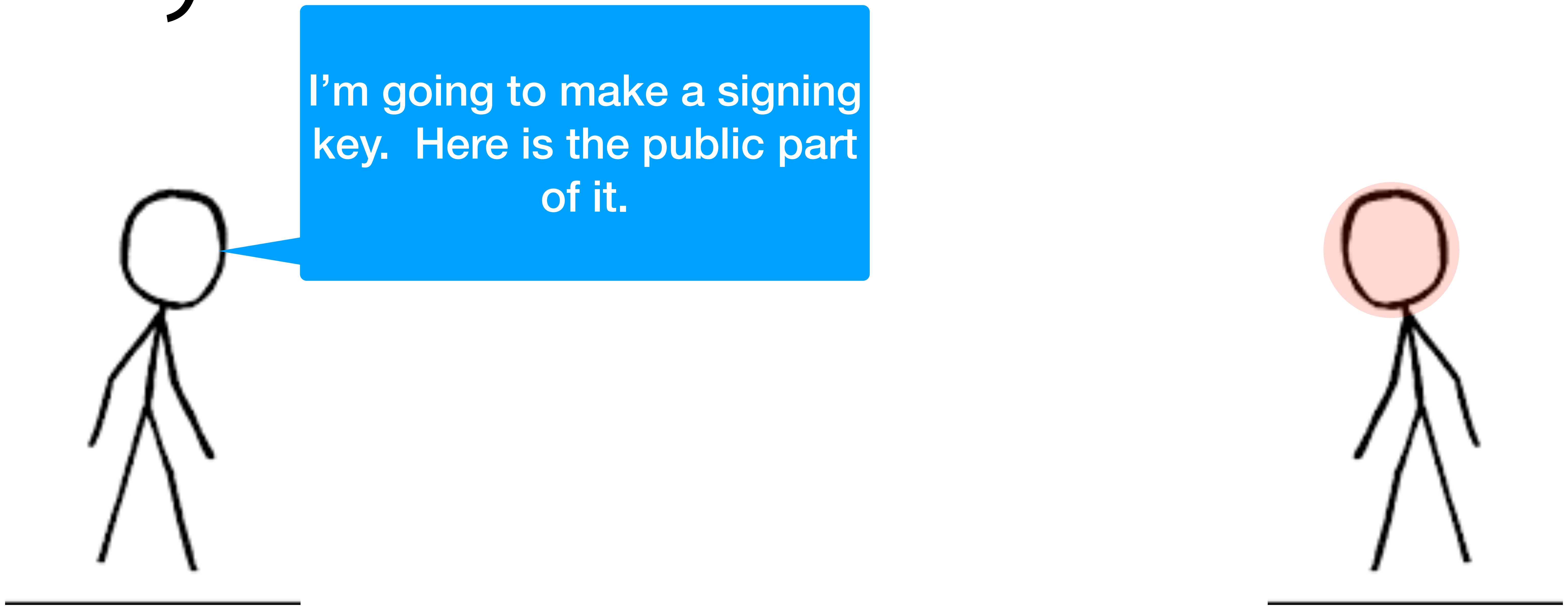


existential unforgability

"EVEN WHEN GIVEN A SIGNING ORACLE,
AN ADVERSARY CANNOT FORGE A SIGNATURE FOR
ANY MESSAGE OF ITS CHOOSING"



Signature security



$$(vk, sk) \leftarrow \mathrm{Gen}(1^n)$$

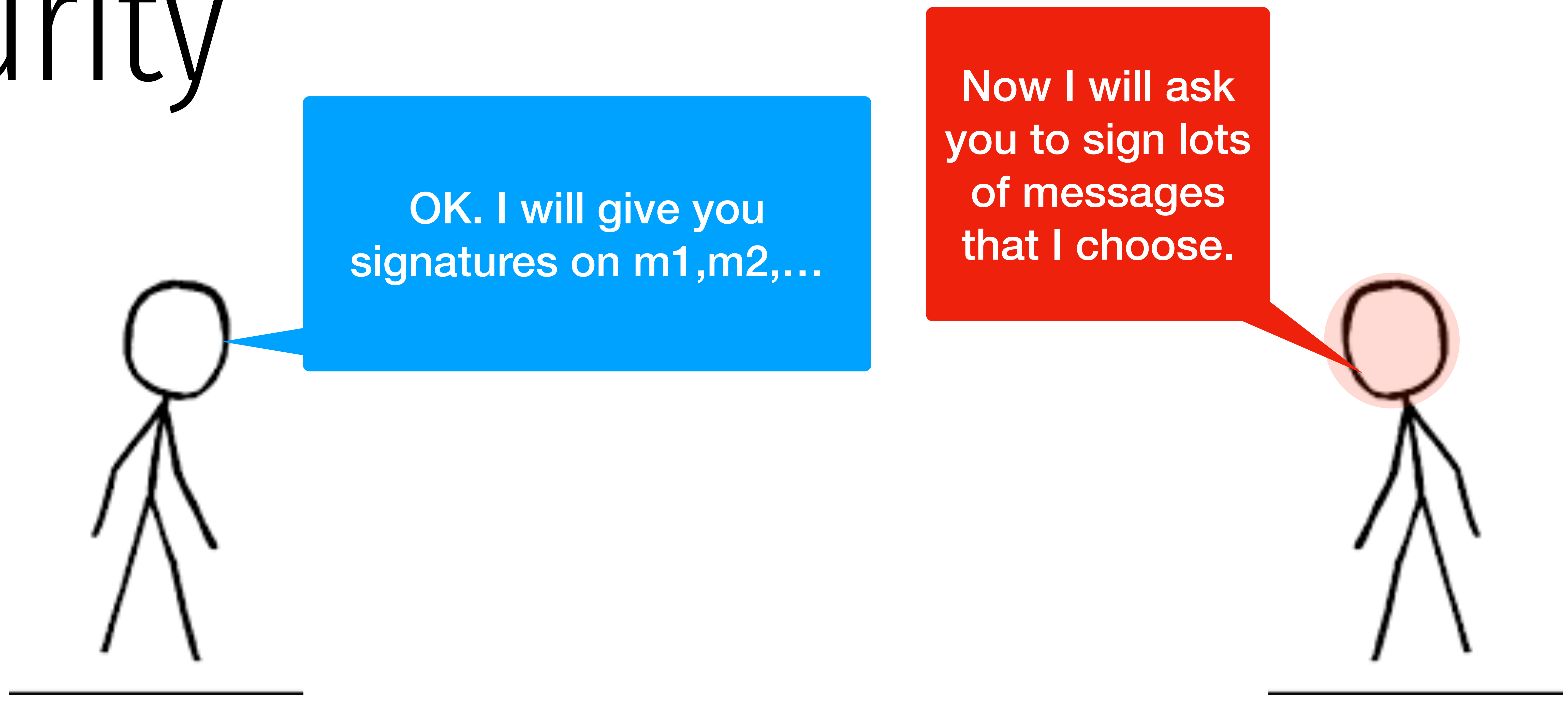
Signature security

$(vk, sk) \leftarrow \mathrm{Gen}(1^n)$

$m_0, m_1, \ldots$

vk

Signature security



$(vk, sk) \leftarrow \mathrm{Gen}(1^n)$

vk

$s_i \leftarrow \mathsf{Sign}_{sk}(m_i)$

Signature security

Now I will try to create a new (signature, message) pair…one that I didn't receive from yoiu. signature on a new message

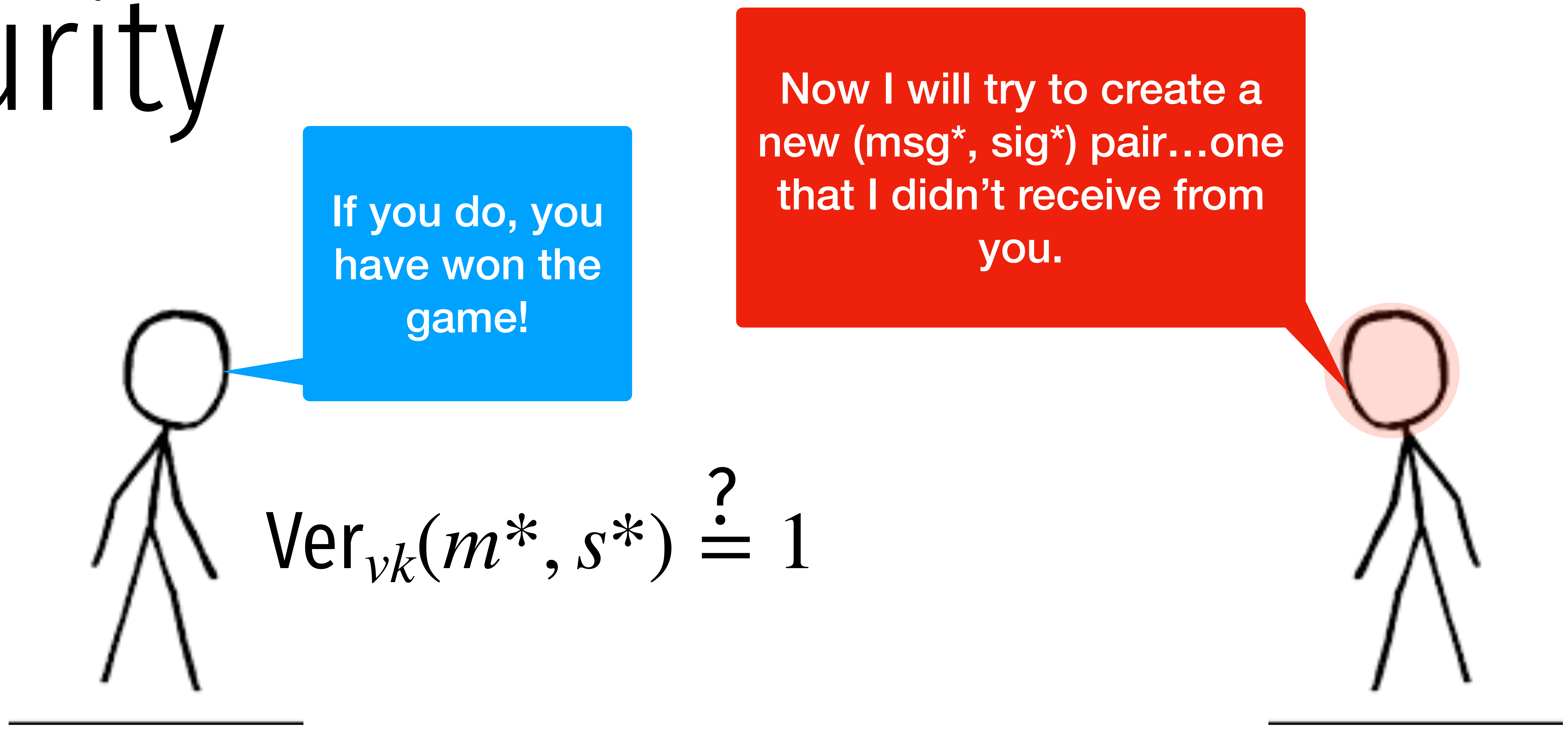
$(vk, sk) \leftarrow \mathsf{Gen}(1^n)$

vk

$s_i \leftarrow \mathsf{Sign}_{sk}(m_i)$

$s_1, s_2, \ldots$

Signature security



$$\mathsf{Ver}_{vk}(m^*, s^*) \stackrel{?}{=} 1$$

FOR ALL NON-UNIFORM PPT A

$$\Pr\left[\begin{array}{l}(vk, sk) \leftarrow Gen(1^n); (m, s) \leftarrow A^{Sign_{sk}(\cdot)} : \\ \quad Ver_{vk}(m, s) = 1, \\ \quad \text{AND } A \text{ DIDN'T QUERY } m\end{array}\right] < \mu(n)$$

Textbook RSA Signatures (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \bmod \phi(N)$

Sign((sk=d, N) m):

Compute the signature: $\sigma \leftarrow m^d \bmod N$

Verify((pk=e, N), σ, m):

$$m \stackrel{?}{=} \sigma^e \bmod N$$

RSA Signatures in GPG

Sign((sk, N) m):

Compute the padding: $z \leftarrow 00 \cdot 01 \cdot FF \cdots FF \cdot 00 \cdot \mathsf{ID}_H \cdot H(m)$

Compute the signature: $\sigma \leftarrow z^{sk} \bmod N$