2550 Intro to cybersecurity

Public key Crypto

abhi shelat

Recap

Revisit our model for Encryption

Symmetric key enc has 1 major drawback.

Bob

Carol

Dave

Alice

Evan

George

Francis

Symmetric key enc has 1 major drawback.

$k_{ba}, k_{bc}, k_{bd}, k_{be}, k_{bf}, k_{bg}$
Bob

$k_{ca}, k_{cb}, k_{cd}, k_{ce}, k_{cf}, k_{cg}$
Carol

$k_{da}, k_{db}, k_{dc}, k_{de}, k_{df}, k_{dg}$
Dave

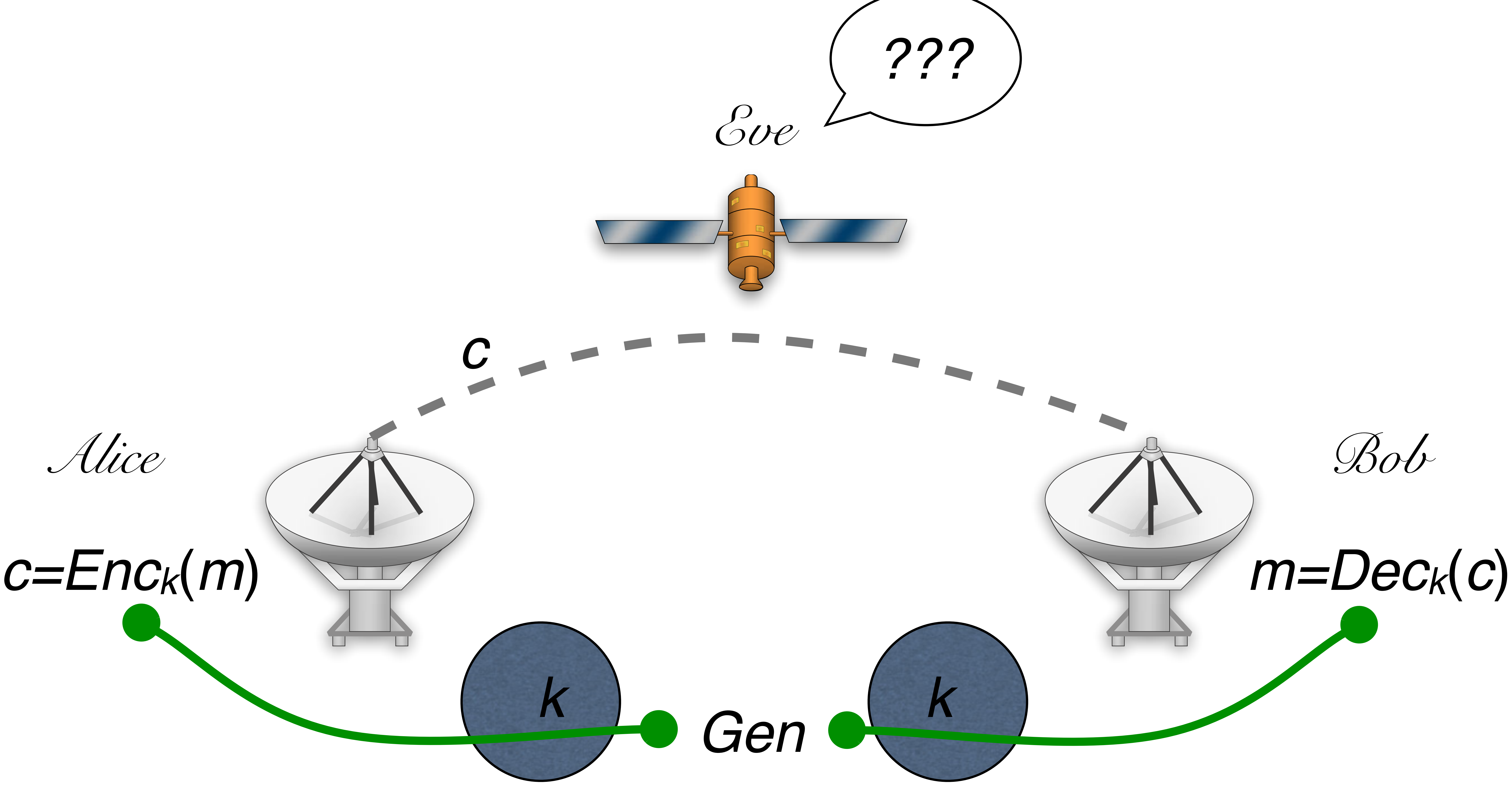
Alice
$k_{ab}, k_{ac}, k_{ad}, k_{ae}, k_{af}, k_{ag}$

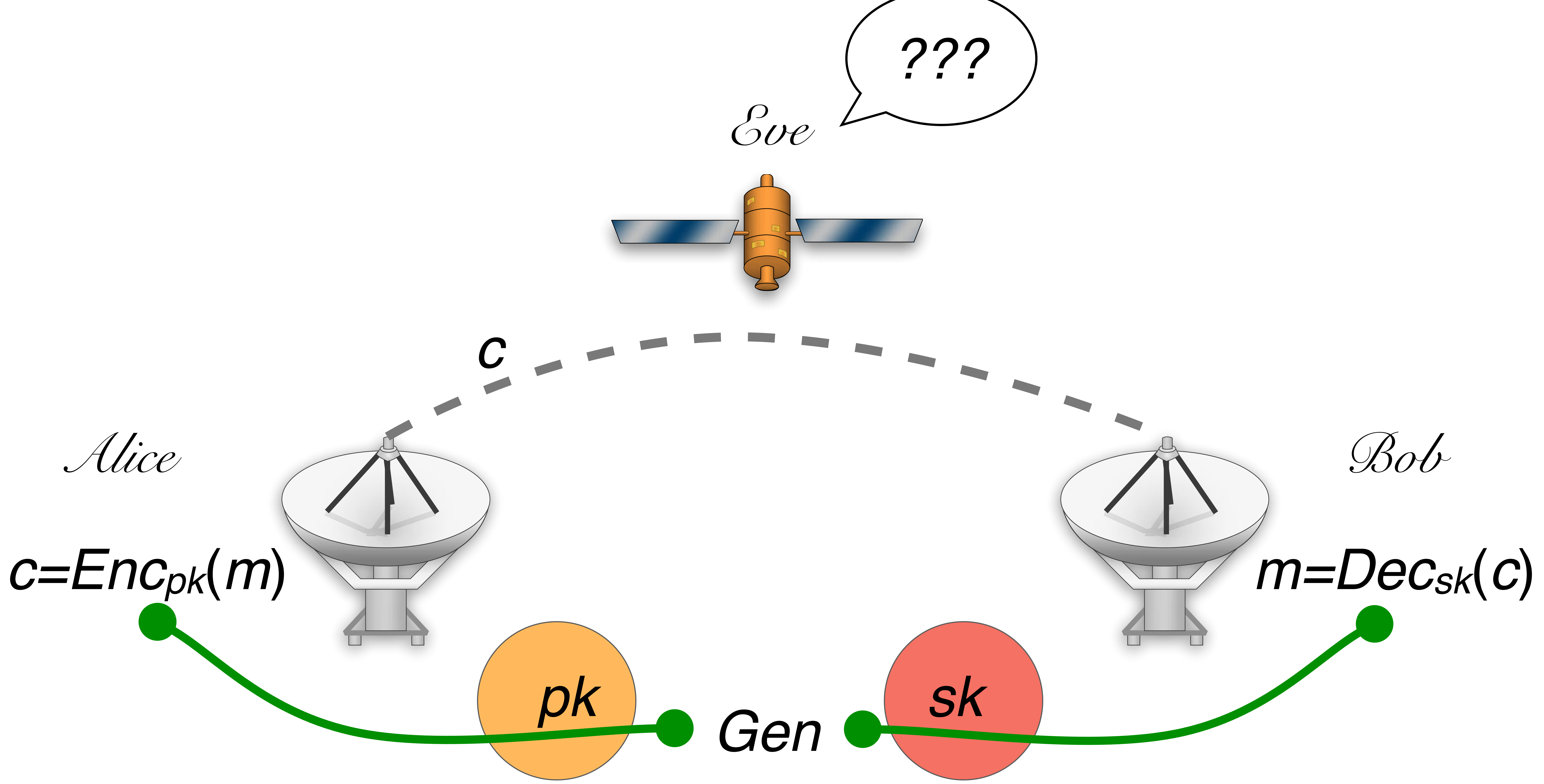
$O(n^2)$ keys to manage!

Evan
$k_{ea}, k_{eb}, k_{ec}, k_{ed}, k_{ef}, k_{eg}$

George
$k_{ga}, k_{gb}, k_{gc}, k_{gd}, k_{ge}, k_{gf}$

Francis
$k_{fa}, k_{fb}, k_{fc}, k_{fd}, k_{fe}, k_{fg}$


???
Eve
c
Alice
Bob
c=Enck(m)
m=Deck(c)
k
Gen
k



Pk can be used to encrypt.

sk can be used to decrypt.

PKC key enc

sk_b

Bob

sk_c

Carol

sk_d

Dave

Alice

sk_a

$pk_a, pk_b, pk_c, pk_d, pk_e, pk_f, pk_g$

Are publicly posted

Evan

sk_e

George

sk_g

Francis

sk_f

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)

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

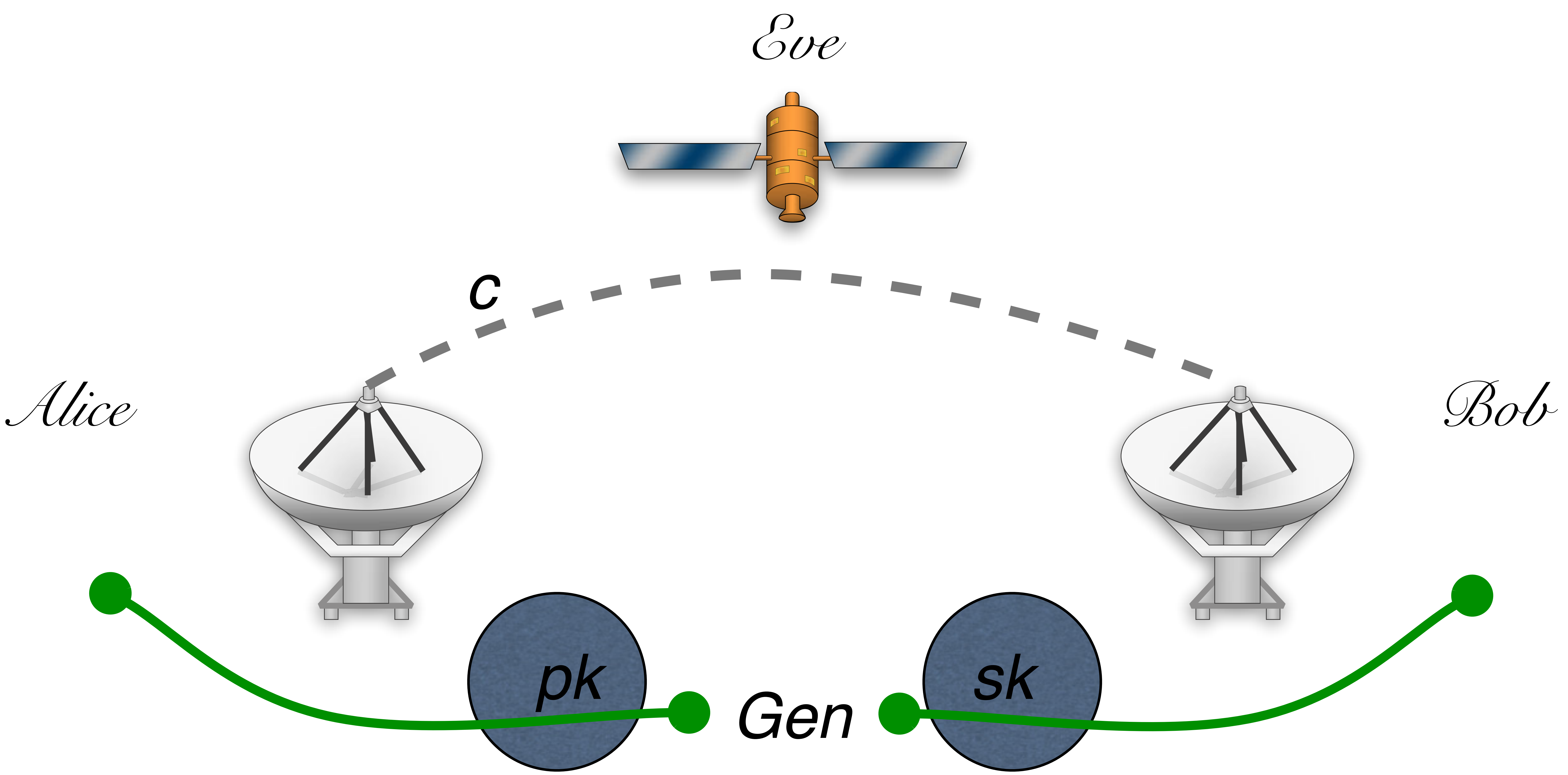
Enc (encryption)

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

Dec (decryption)

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

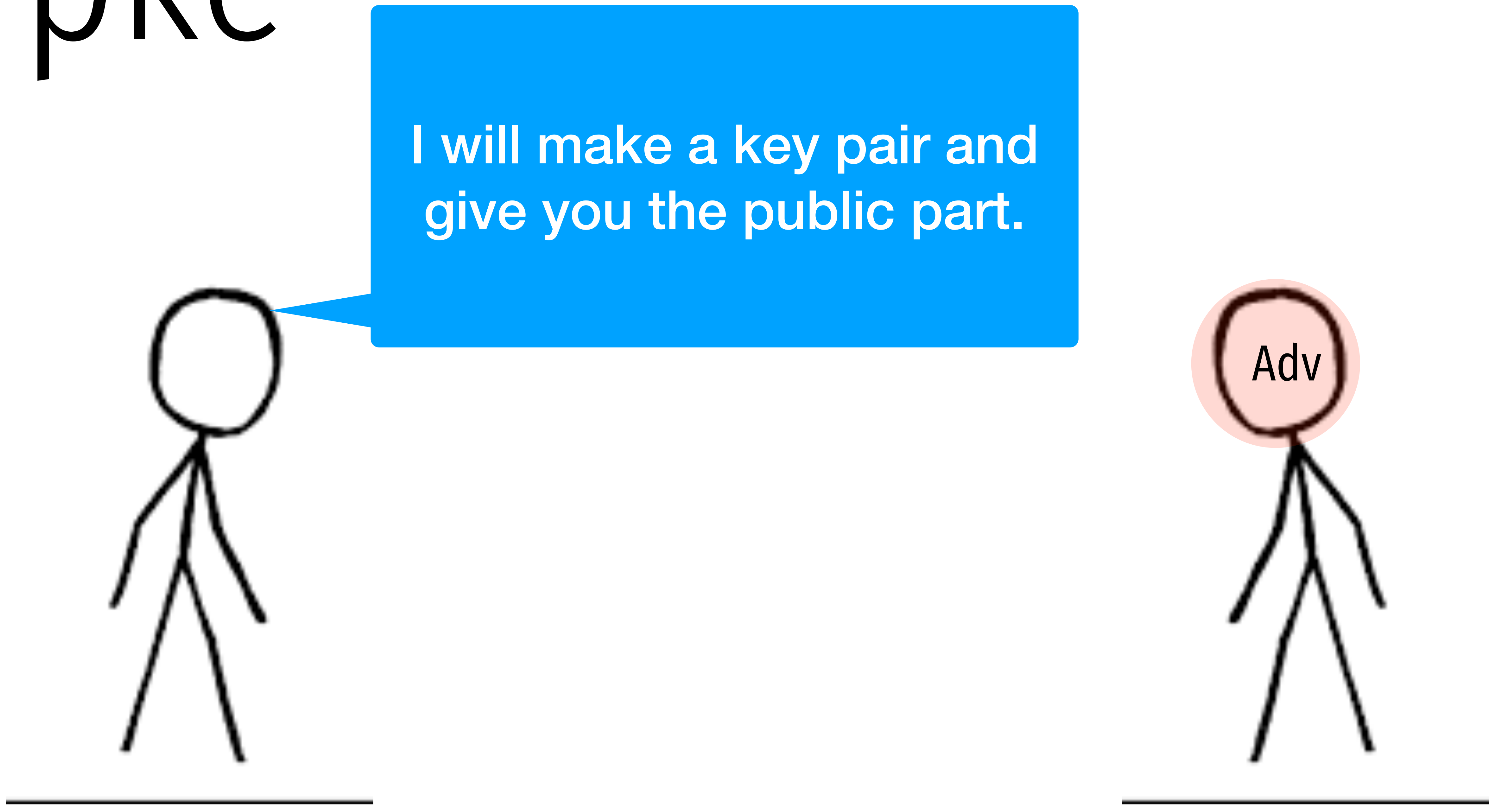
$$\Pr[\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m] = 1$$



"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)

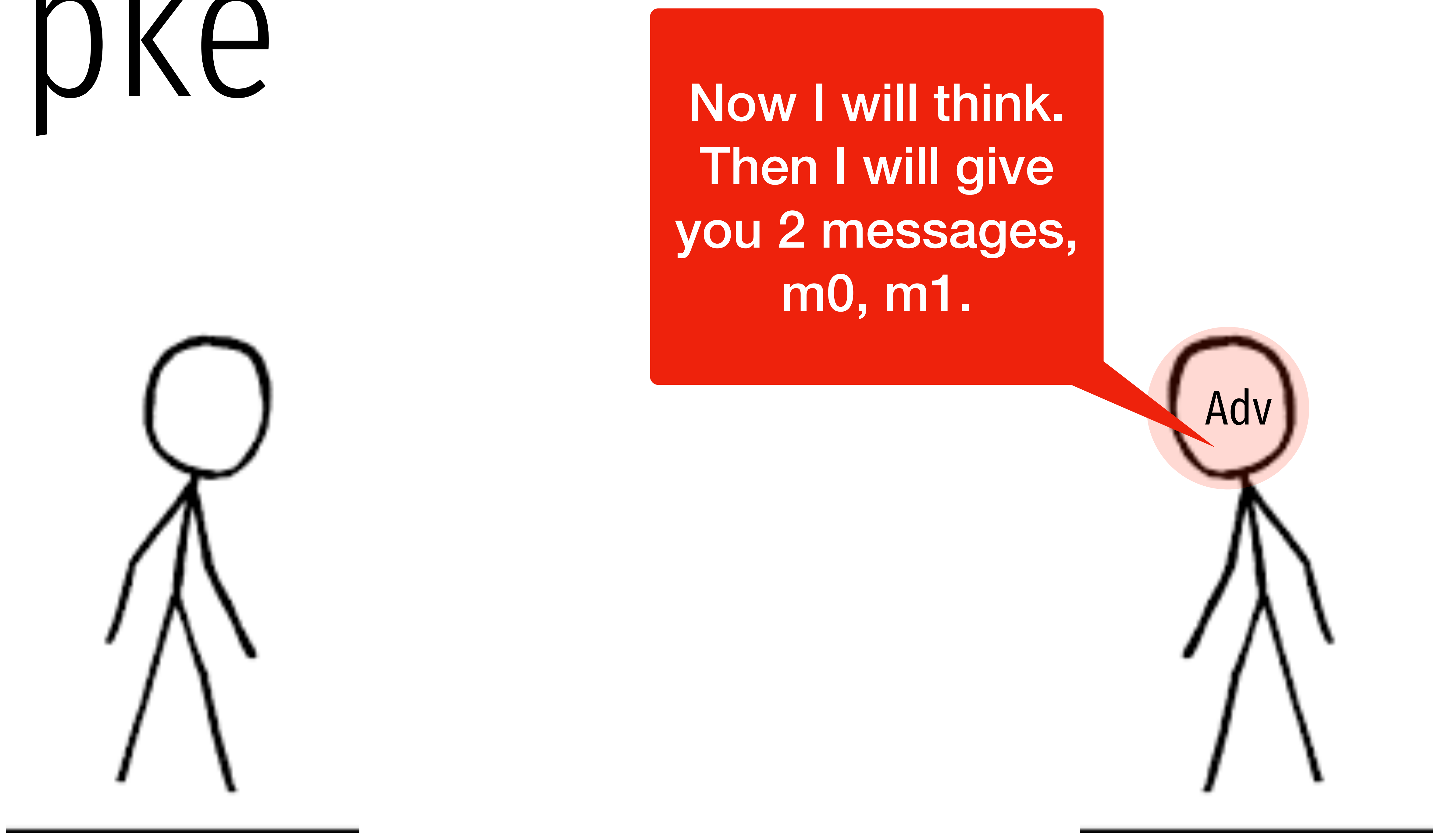


$pk, sk \leftarrow \mathsf{gen}(1^n)$

pk

IND-CPA security for pke

(weakest notion of security)



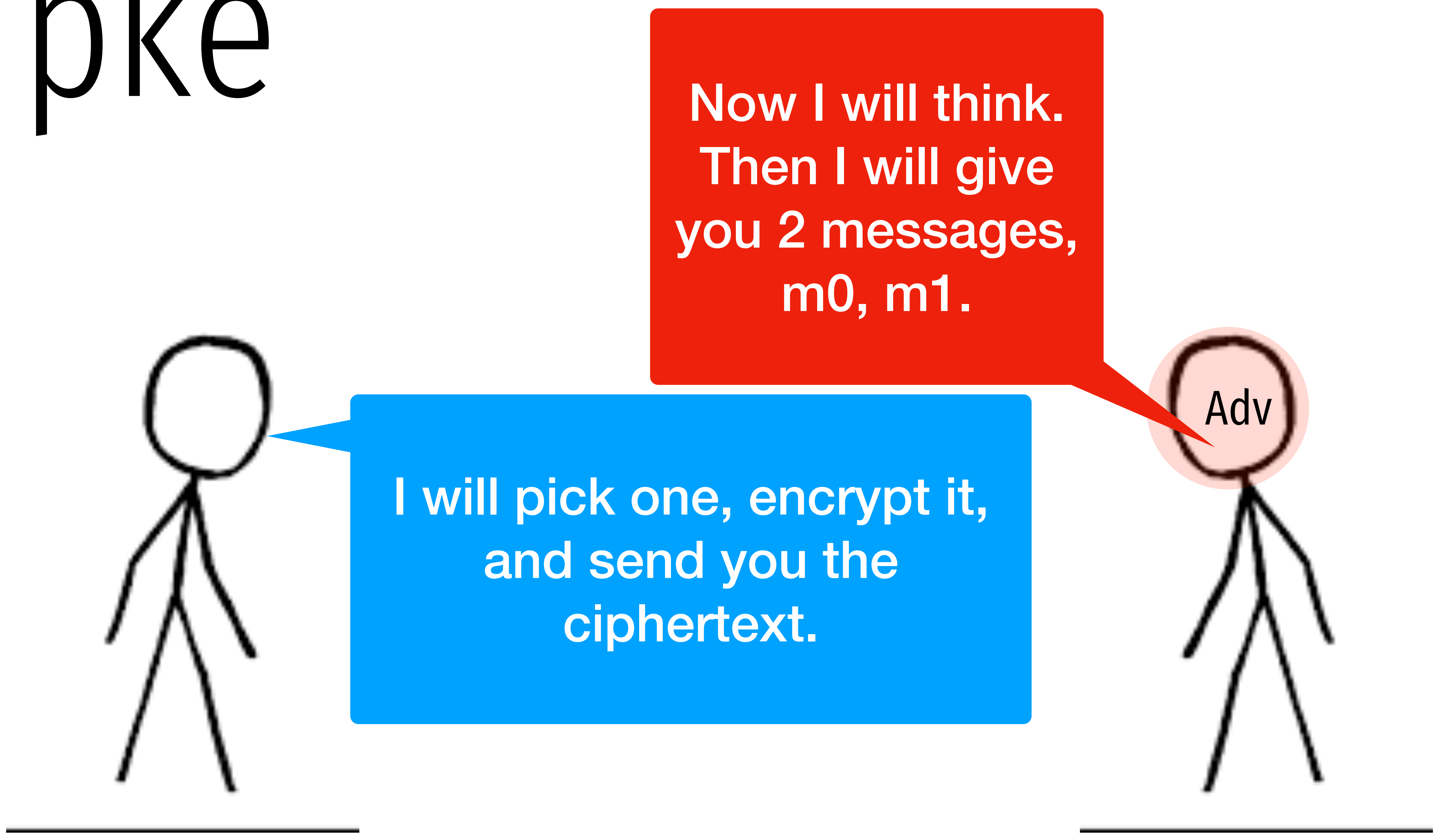
$pk, sk \leftarrow \mathsf{gen}(1^n)$

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

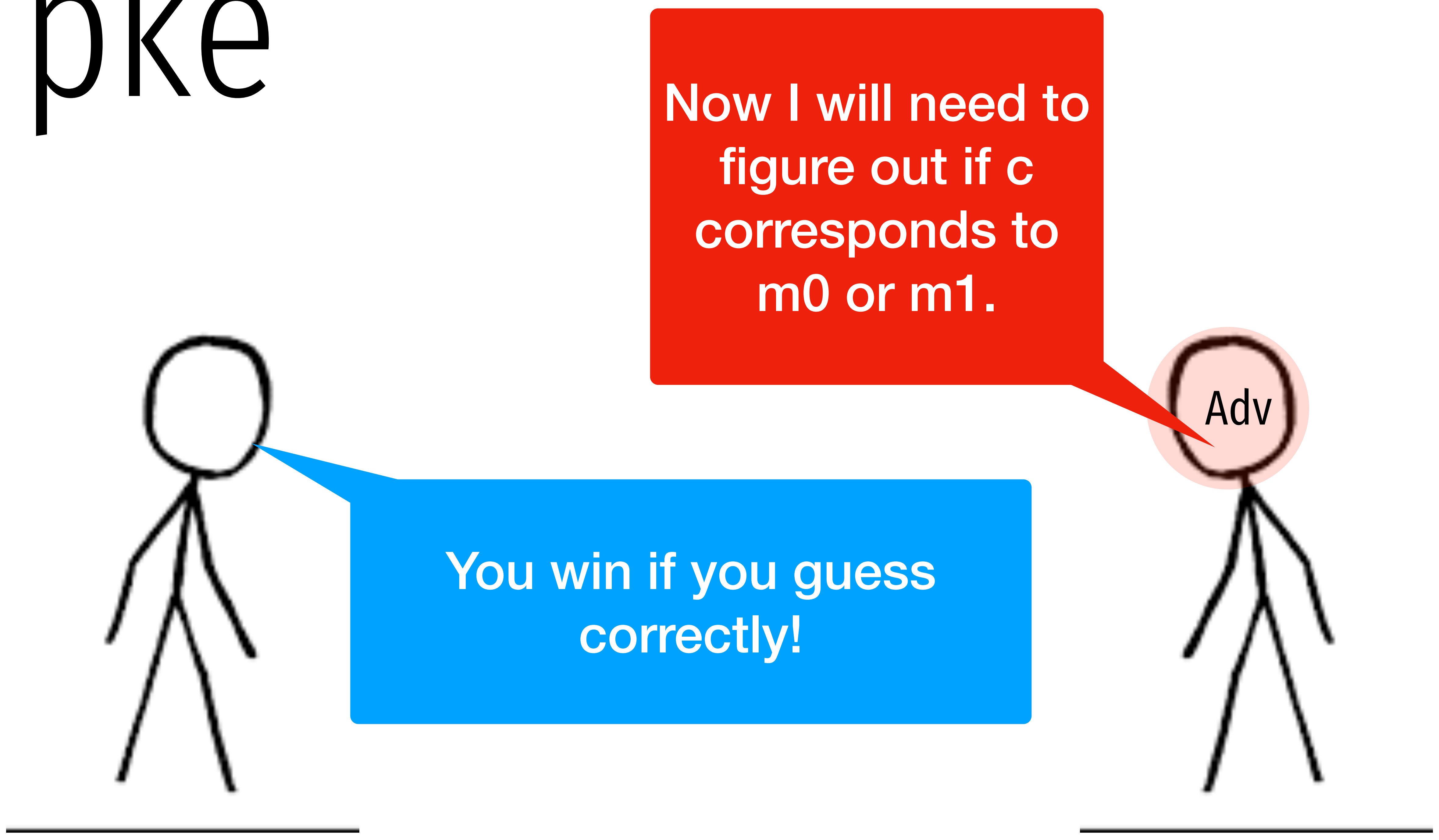
$m_0, m_1 \leftarrow A(pk)$

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

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

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

Modular Exponentiation

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

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

$$\underbrace{7 \cdot 7 \cdots 7}_{19 \text{ times}}$$

Modular Exponentiation

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

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

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

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

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

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

$7^1 \quad 7^2 \quad 7^4 \quad 7^8 \quad 7^{16}$ (mod 31)

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

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

7^1	7^2	7^4	7^8	7^{16}	(mod 31)
7	18	14	10	7	

Modular Exponentiation

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

Algorithm 2: ModularExponentiation(a, x, n)

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

```
r ← 1
while x > 0 do
    if x is odd then
        r ← r · a mod n
    x ← ⌊x/2⌋
    a ← a² mod 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: $a, x \in [1, n]$

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

Greatest Common Divisor

```
GCD(6809,1641)
```

Greatest Common Divisor

GCD(6809,1641)

GCD(1641, 245)

GCD(245, 171)

GCD(171, 74)

GCD(74, 23)

GCD(23, 5)

GCD(5, 3)

GCD(3, 2)

GCD(2, 1)

$6809 = 4 \cdot 1641 + 245$

$1641 = 6 \cdot 245 + 171$

$245 = 1 \cdot 171 + 74$

$171 = 2 \cdot 74 + 23$

$74 = 3 \cdot 23 + 5$

$23 = 4 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = \boxed{1} 2 + 1$

$2 = 2 \cdot 1 + 0$

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 mod b = 0 then
    Return (0, 1)
else
    (x, y) ← ExtendedEuclid (b, a mod b)
    Return (y, x − y(⌊a/b⌋))
```

Greatest Common Divisor

GCD(6809,1641)

		$6809 = 4 \cdot 1641 + 245$	$(-643, 2668)$
GCD(1641, 245)		$1641 = 6 \cdot 245 + 171$	$(96, -643)$
GCD(245, 171)		$245 = 1 \cdot 171 + 74$	$(-67, 96)$
GCD(171, 74)		$171 = 2 \cdot 74 + 23$	$(29, -67)$
GCD(74, 23)		$74 = 3 \cdot 23 + 5$	$(-9, 29)$
GCD(23, 5)		$23 = 4 \cdot 5 + 3$	$(2, -9)$
GCD(5, 3)		$5 = 1 \cdot 3 + 2$	$(-1, 2)$
GCD(3, 2)	`(1, 0 - 1*1 )`	$3 = \boxed{1} \cdot 2 + 1$	$(1, -1)$
GCD(2, 1)	`(0,1)`	$2 = 2 \cdot 1 + 0$	$(0, 1)$

Greatest Common Divisor

`GCD(6809,1641)`		$6809 = 4 \cdot 1641 + 245$
GCD(1641, 245)		$1641 = 6 \cdot 245 + 171$
GCD(245, 171)		$245 = 1 \cdot 171 + 74$
GCD(171, 74)		$171 = 2 \cdot 74 + 23$
GCD(74, 23)		$74 = 3 \cdot 23 + 5$
GCD(23, 5)		$23 = 4 \cdot 5 + 3$
GCD(5, 3)		$5 = 1 \cdot 3 + 2$
GCD(3, 2)		$3 = \boxed{1} \cdot 2 + 1$
GCD(2, 1)	`(0,1)`	$2 = 2 \cdot 1 + 0$

Greatest Common Divisor

```
GCD(6809,1641)
```

GCD(1641, 245)

GCD(245, 171)

GCD(171, 74)

GCD(74, 23)

GCD(23, 5)

GCD(5, 3)

GCD(3, 2) `(1, 0 - 1*1 )`

GCD(2, 1) `(0,1)`

$6809 = 4 \cdot 1641 + 245$

$1641 = 6 \cdot 245 + 171$

$245 = 1 \cdot 171 + 74$

$171 = 2 \cdot 74 + 23$

$74 = 3 \cdot 23 + 5$

$23 = 4 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = \boxed{1} \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

Greatest Common Divisor

GCD(6809,1641)		$6809 = 4 \cdot 1641 + 245$
GCD(1641, 245)		$1641 = 6 \cdot 245 + 171$
GCD(245, 171)		$245 = 1 \cdot 171 + 74$
GCD(171, 74)		$171 = 2 \cdot 74 + 23$
GCD(74, 23)		$74 = 3 \cdot 23 + 5$
GCD(23, 5)		$23 = 4 \cdot 5 + 3$
GCD(5, 3)		$5 = 1 \cdot 3 + 2$
GCD(3, 2)	(1,-1)	$3 = \boxed{1} \cdot 2 + 1$
GCD(2, 1)	(0,1)	$2 = 2 \cdot 1 + 0$

Greatest Common Divisor

GCD(6809,1641)

		$6809 = 4 \cdot 1641 + 245$
GCD(1641, 245)		$1641 = 6 \cdot 245 + 171$
GCD(245, 171)		$245 = 1 \cdot 171 + 74$
GCD(171, 74)		$171 = 2 \cdot 74 + 23$
GCD(74, 23)		$74 = 3 \cdot 23 + 5$
GCD(23, 5)		$23 = 4 \cdot 5 + 3$
GCD(5, 3)	(-1,2)	$5 = 1 \cdot 3 + 2$
GCD(3, 2)	(1,-1)	$3 = \boxed{1} \cdot 2 + 1$
GCD(2, 1)	(0,1)	$2 = 2 \cdot 1 + 0$

Greatest Common Divisor

GCD(6809,1641)		$6809 = 4 \cdot 1641 + 245$	(-643, 2668)
GCD(1641, 245)		$1641 = 6 \cdot 245 + 171$	(96, -643)
GCD(245, 171)		$245 = 1 \cdot 171 + 74$	(-67, 96)
GCD(171, 74)		$171 = 2 \cdot 74 + 23$	(29, -67)
GCD(74, 23)		$74 = 3 \cdot 23 + 5$	(-9, 29)
GCD(23, 5)	(2,-9)	$23 = 4 \cdot 5 + 3$	(2, -9)
GCD(5, 3)	(-1,2)	$5 = 1 \cdot 3 + 2$	(-1, 2)
GCD(3, 2)	(1,-1)	$3 = \boxed{1} \cdot 2 + 1$	(1, -1)
GCD(2, 1)	(0,1)	$2 = 2 \cdot 1 + 0$	(0, 1)

Greatest Common Divisor

GCD allows us to compute modular inverses.

`GCD(6809,1641)`

`6809*(-643) + 1641*2668 =`

Greatest Common Divisor

```
GCD(6809,1641)
```

GCD allows us to compute modular inverses.

```
6809*(-643) + 1641*2668 =   1

   -437818      437818
```

Euler totient

Euler totient

$\phi(15) =$

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

Euler totient

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

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

Example of groups

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

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

multiplicative group, mod n

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

Z*_15 = {1,2,4,7,8,11,13,14}

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

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

$$2^8 \bmod 15 =$$

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 $e \cdot d = 1 \bmod \phi(N)$

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

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

“Textbook” RSA (insecure)

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

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

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

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

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

Example of Textbook RSA

$m=5$

$PK = (N=143,\ e=7)$ $SK = (d=103)$

“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

RSA-OAEP+

GEN(1^n)

$f, f^{-1} \leftarrow$ 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)

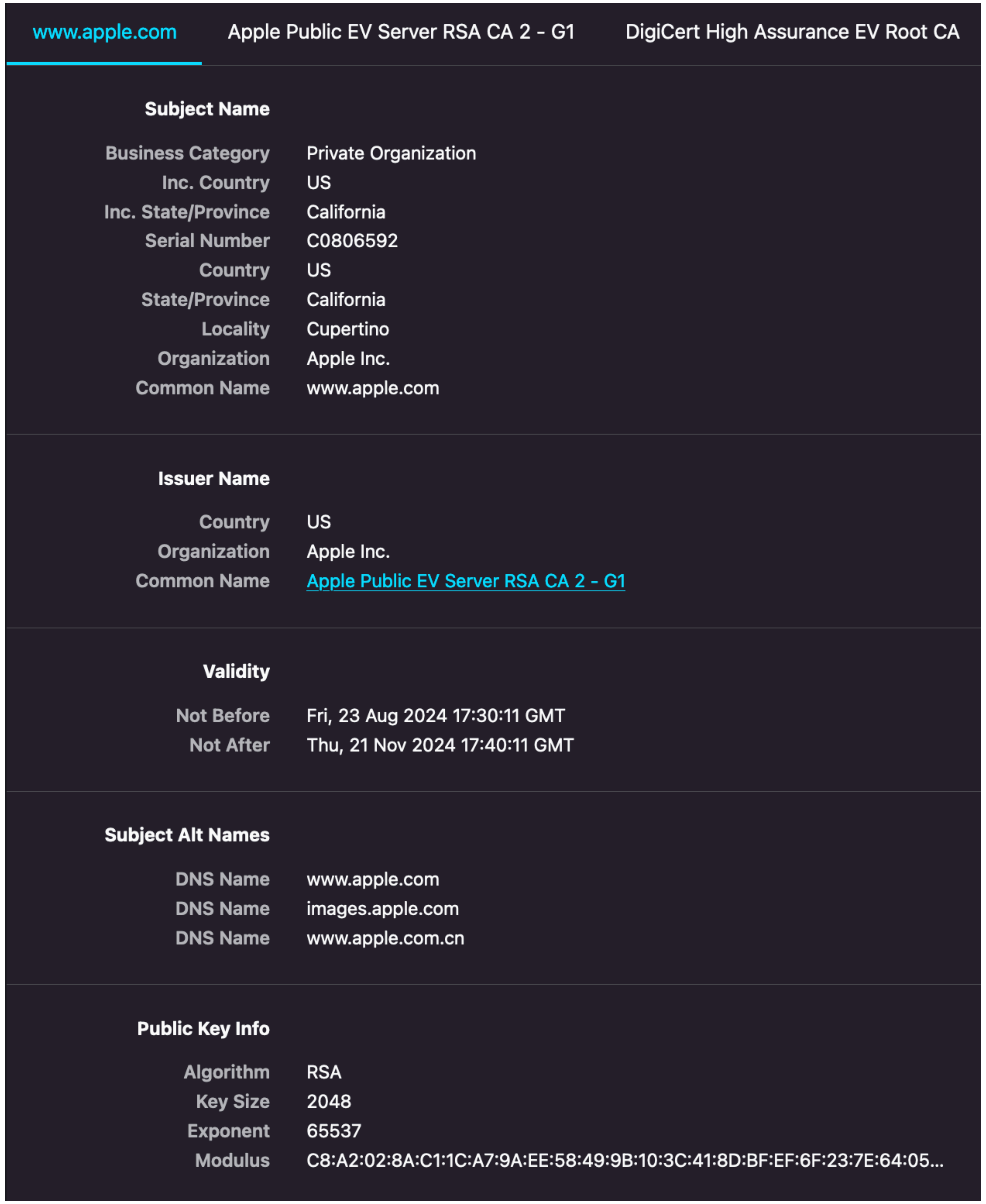
$(s = (s_1, s_2), t) \leftarrow f^{-1}(c)$

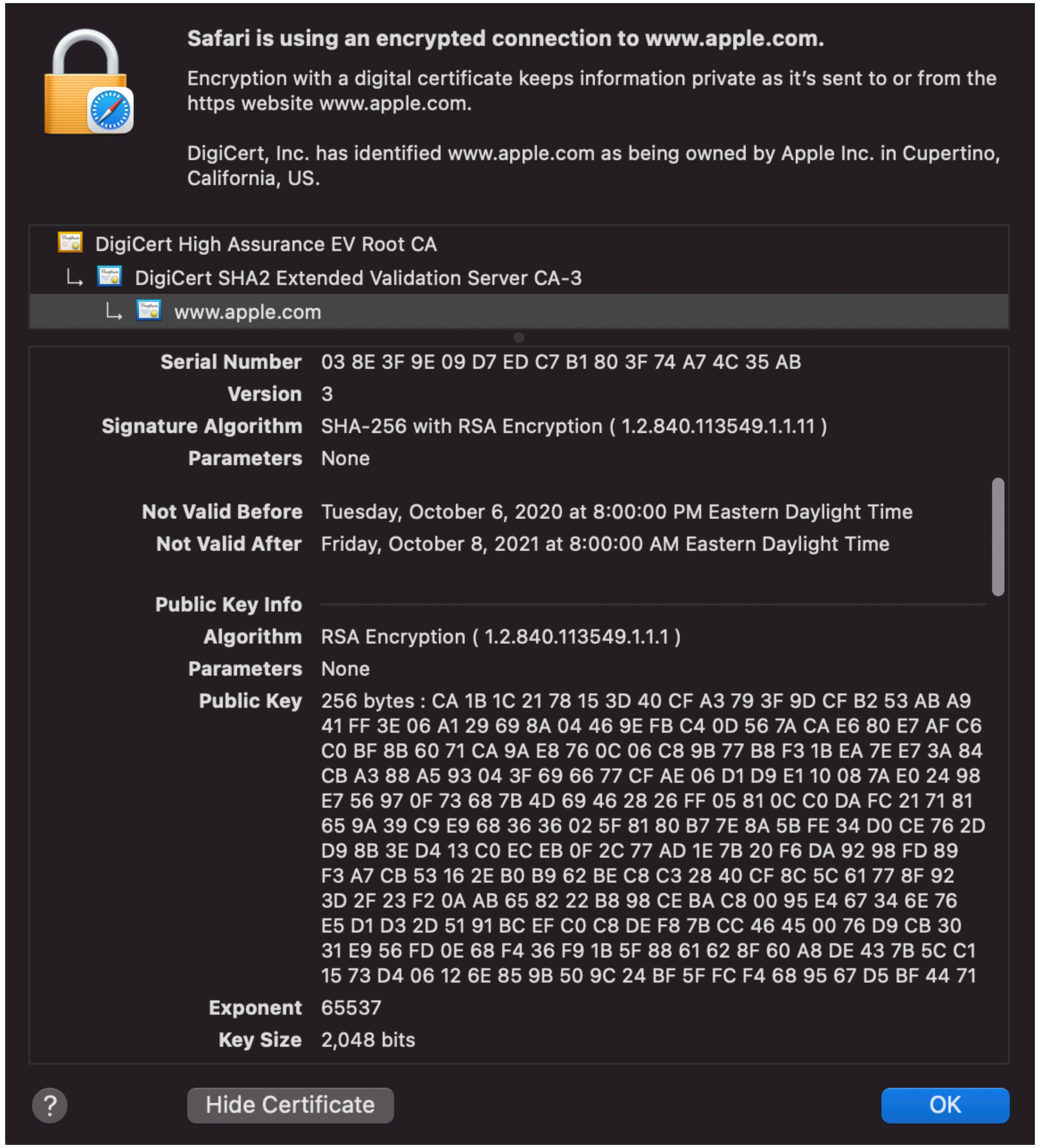
$r \leftarrow R_3(s) \oplus t$

$m \leftarrow R_1(r) \oplus s_1$

$R_2(r||m) \stackrel{?}{=} s_2$ OUTPUT m ELSE FAIL

Example: apple.com

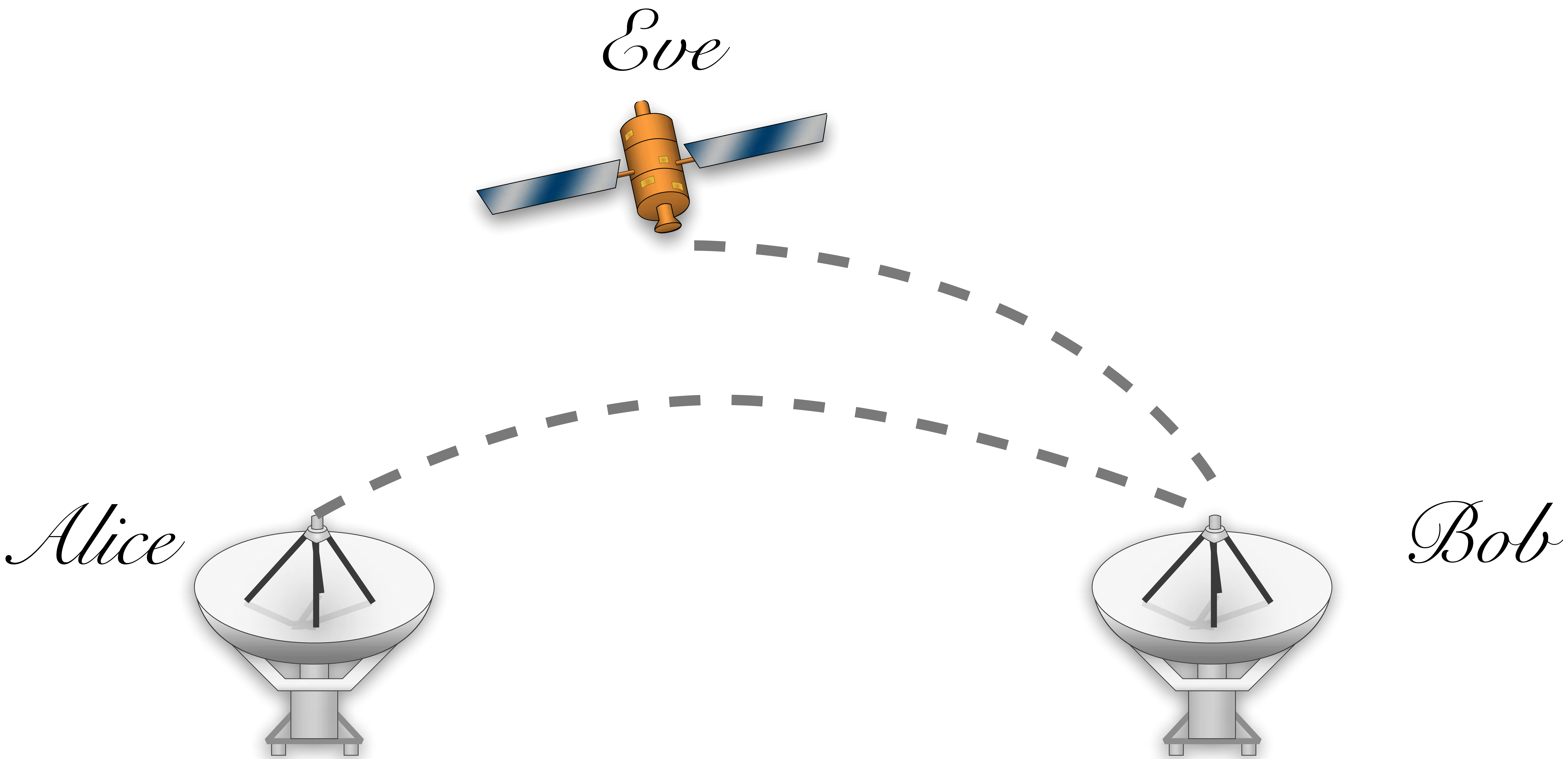




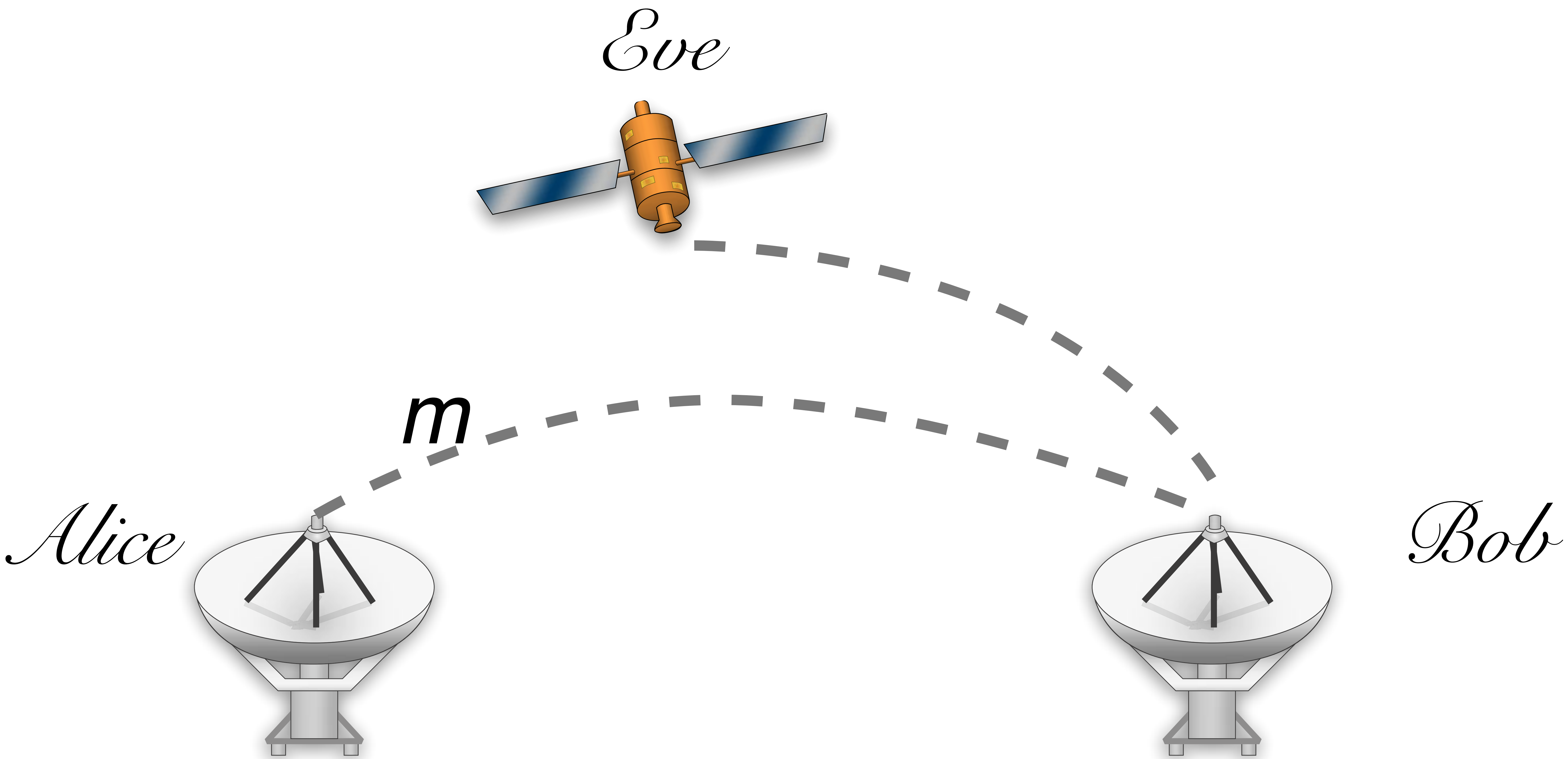
Very old problem

John Hancock

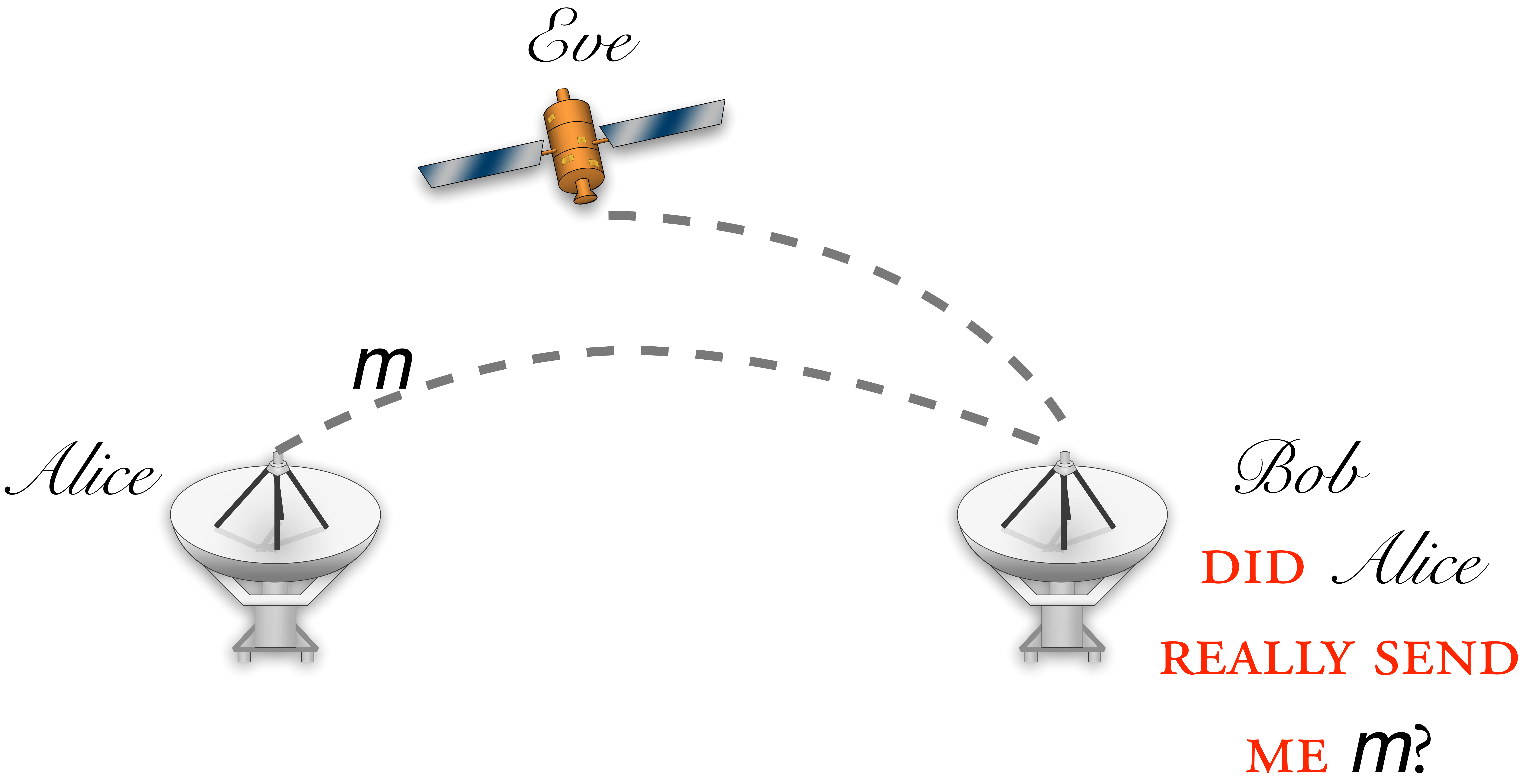
New Problem



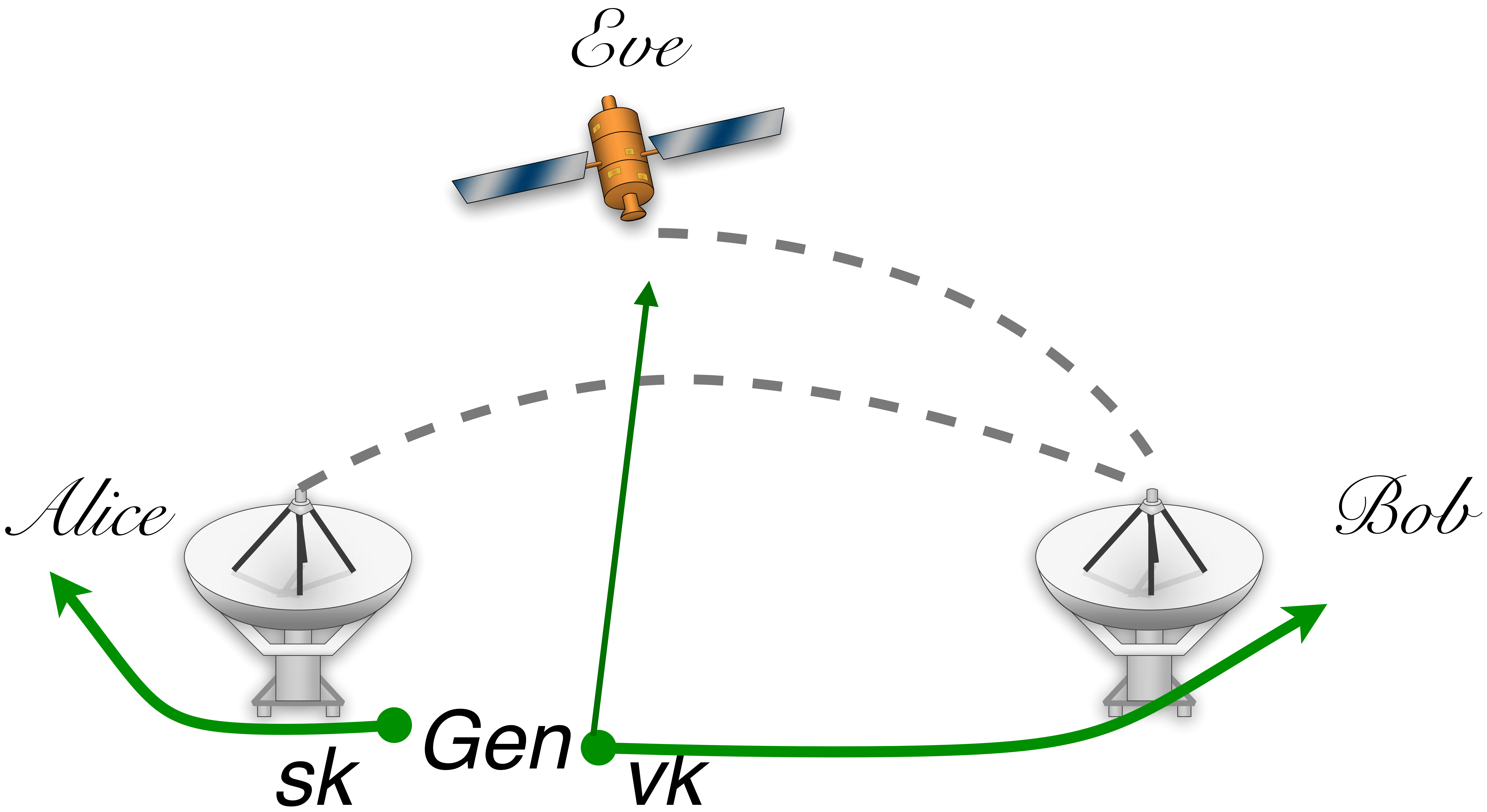
New Problem



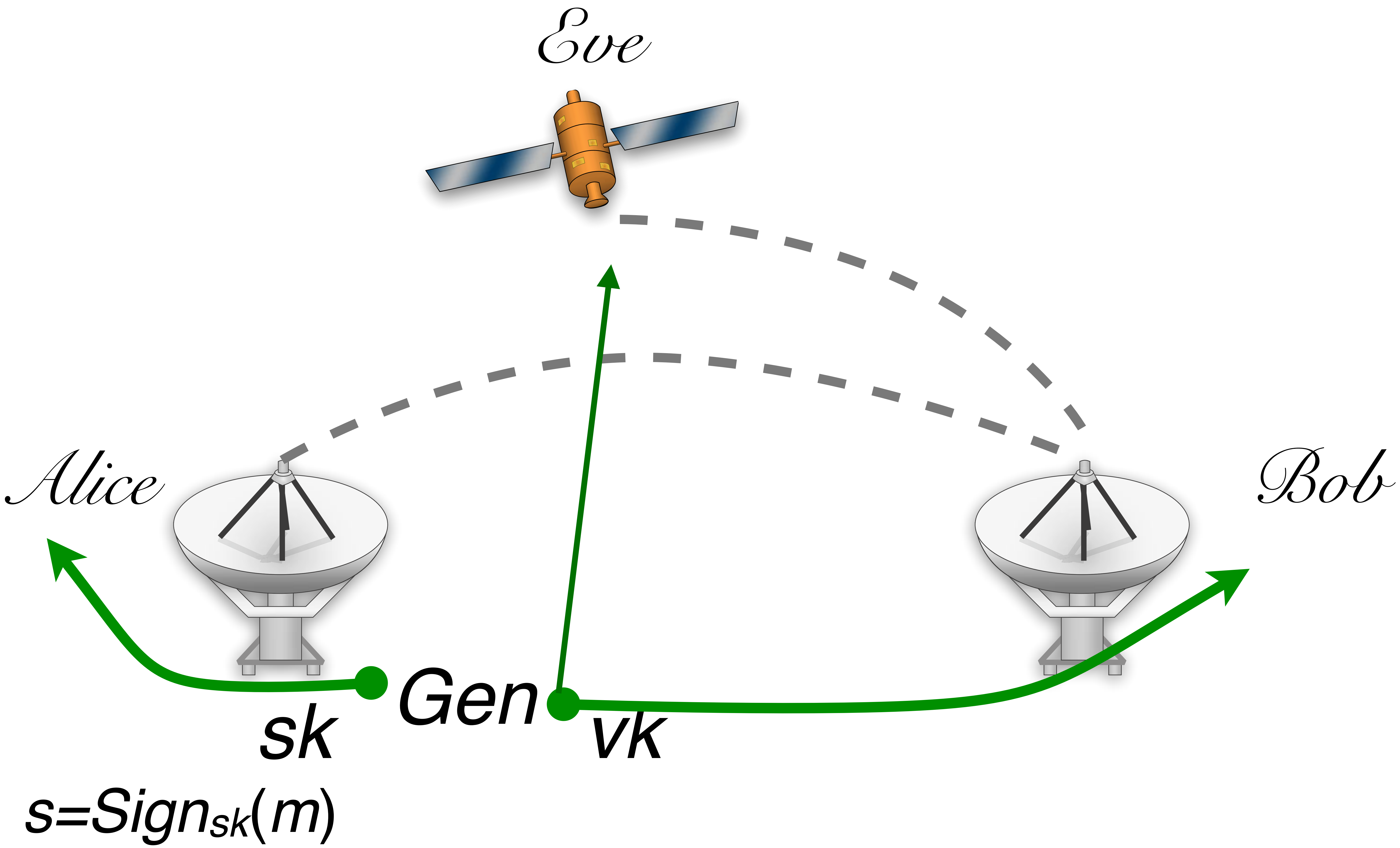
New Problem



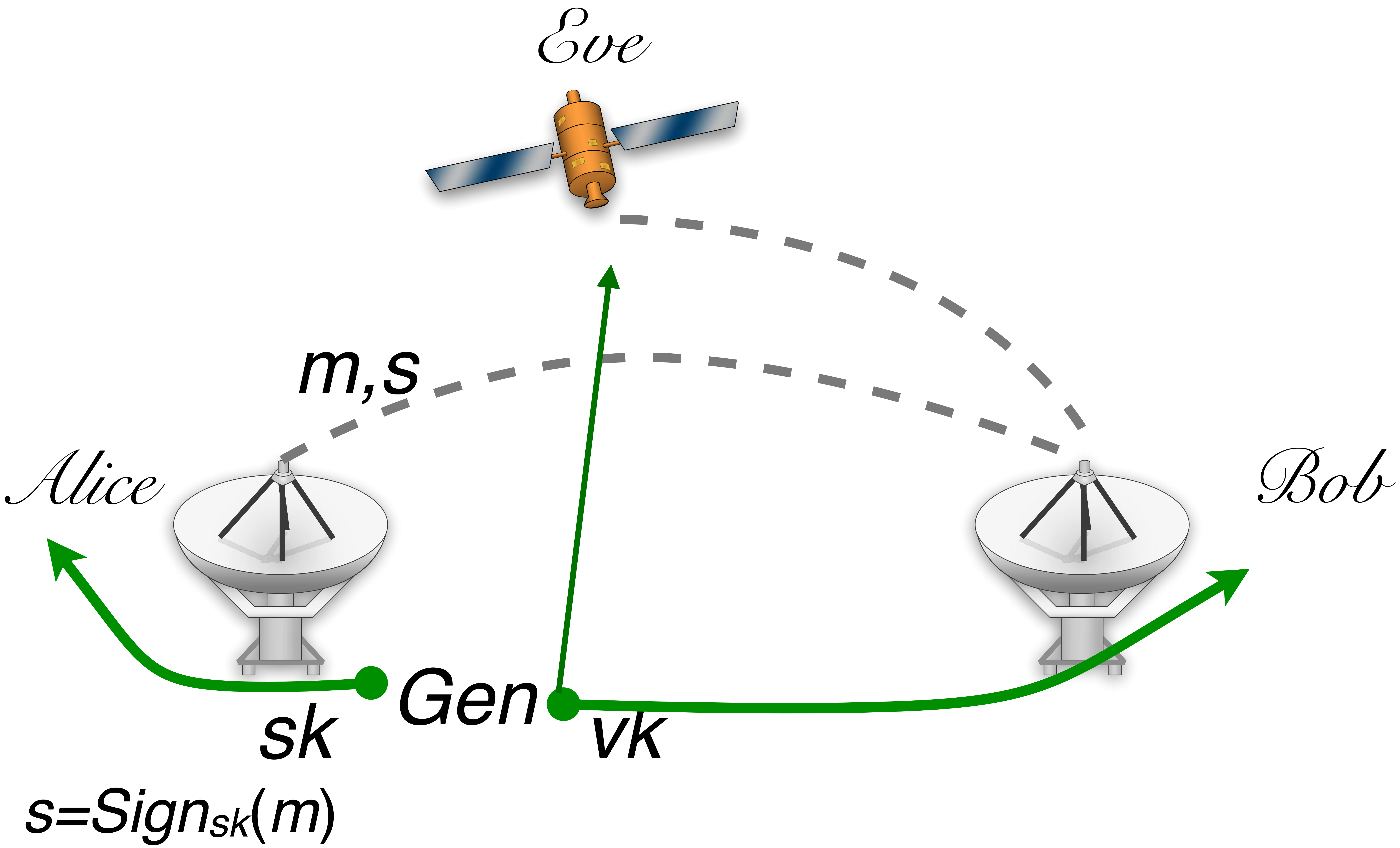
Public key digital signature



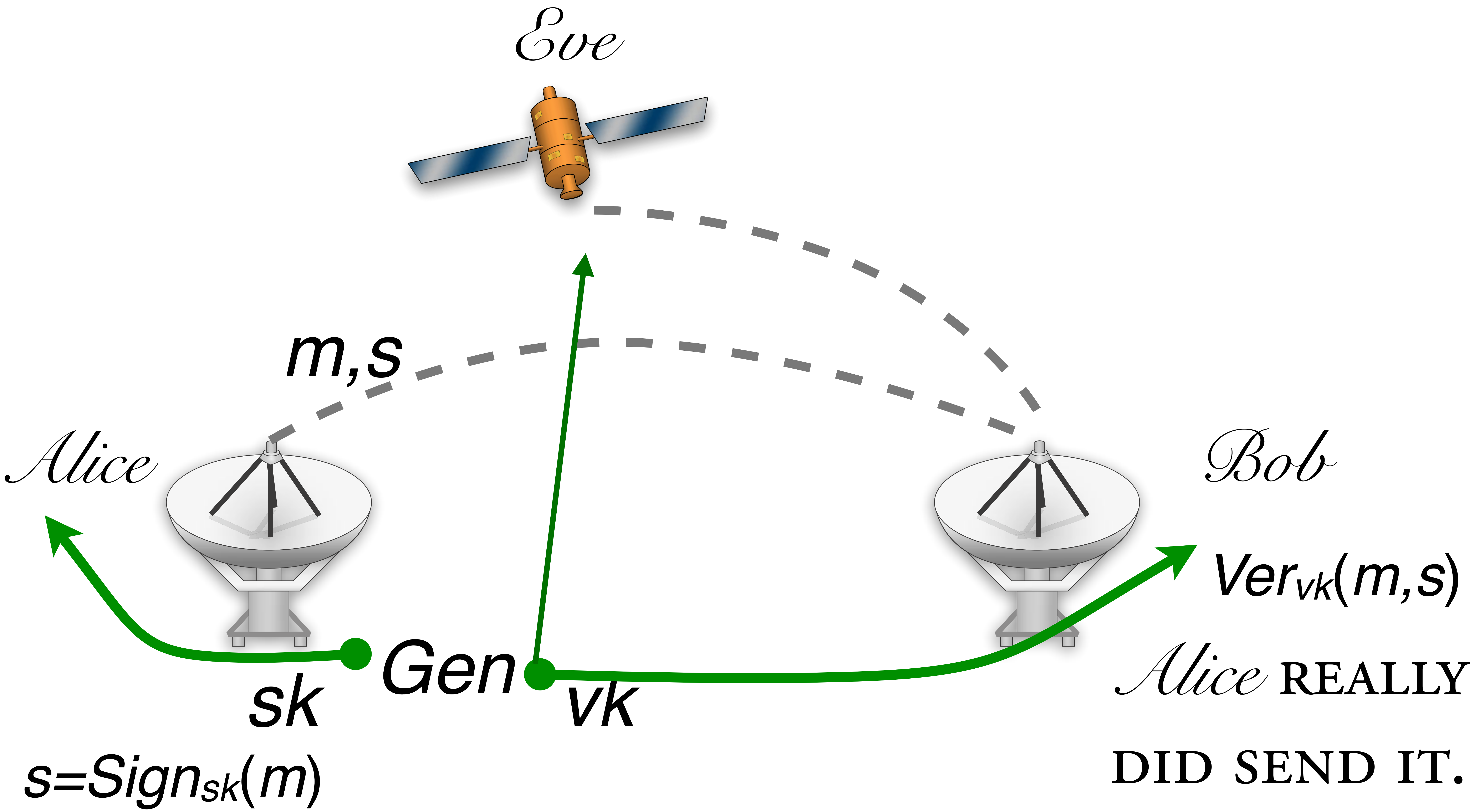
Public key digital signature



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

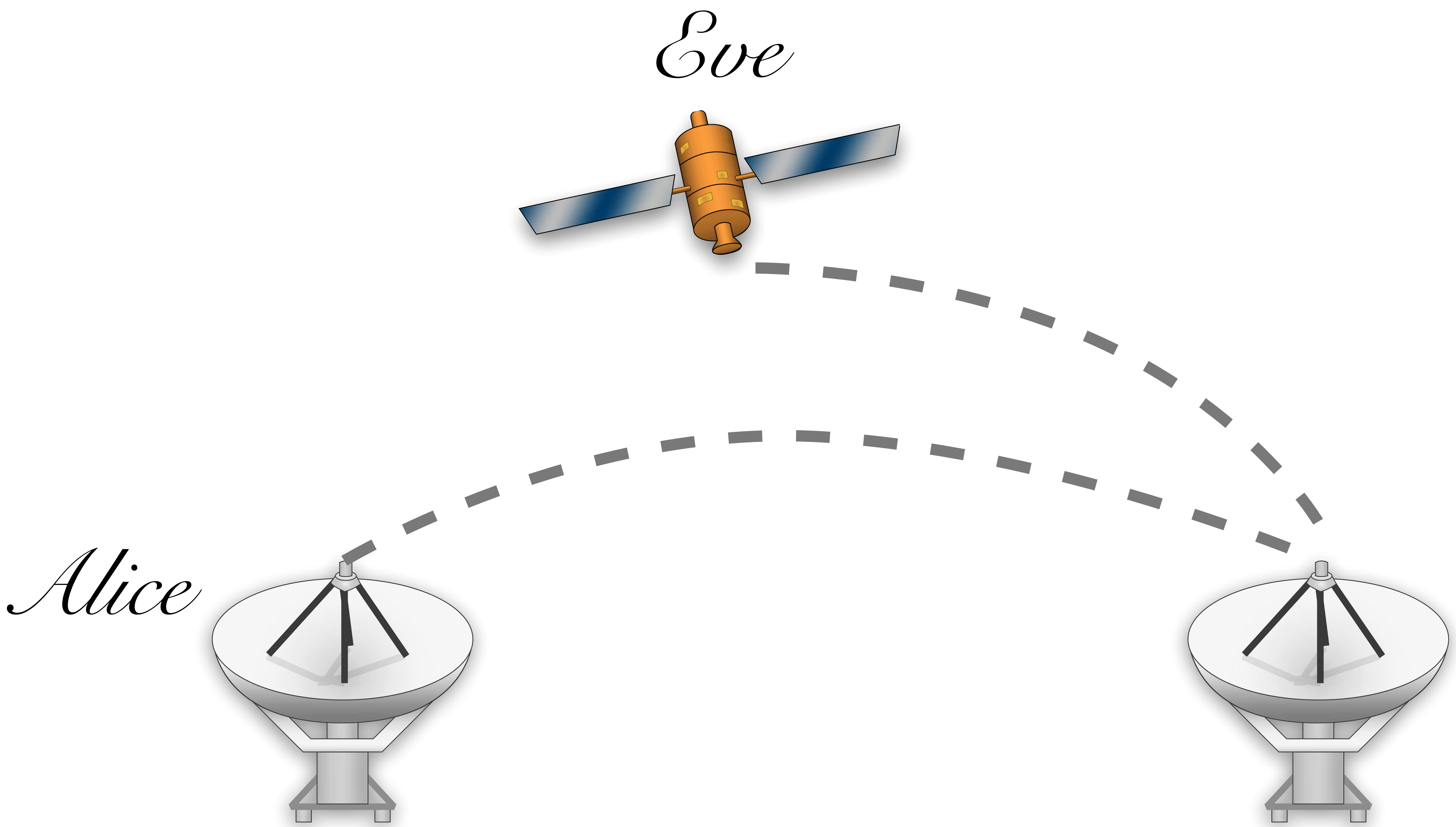
$$\Pr[k \leftarrow Gen(1^n) : Ver_{vk}(m, Sign_{sk}(m)) = 1] = 1$$

existential unforgability

“EVEN WHEN GIVEN A SIGNING ORACLE,

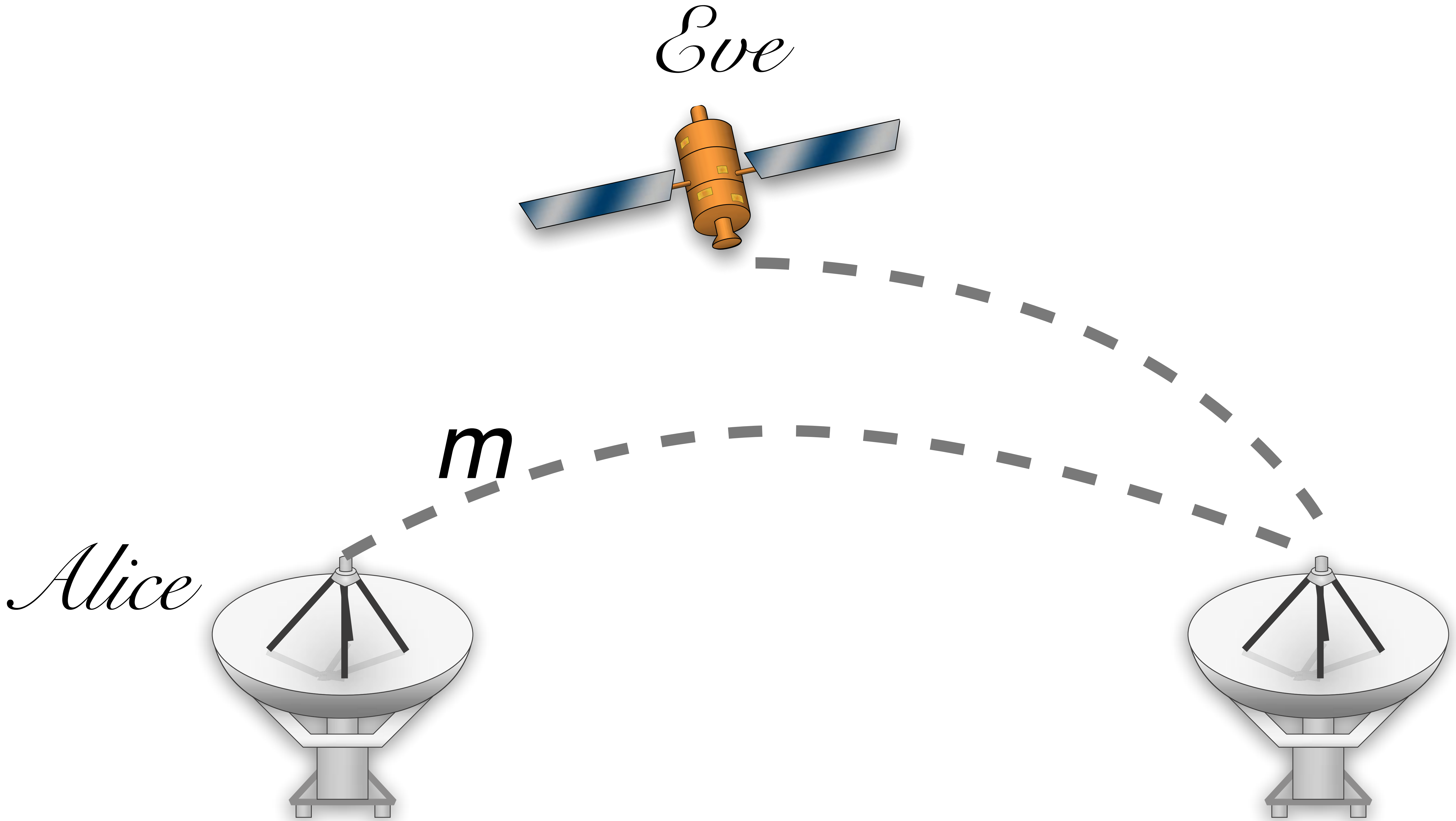
AN ADVERSARY CANNOT FORGE A SIGNATURE FOR

ANY MESSAGE OF ITS CHOOSING”

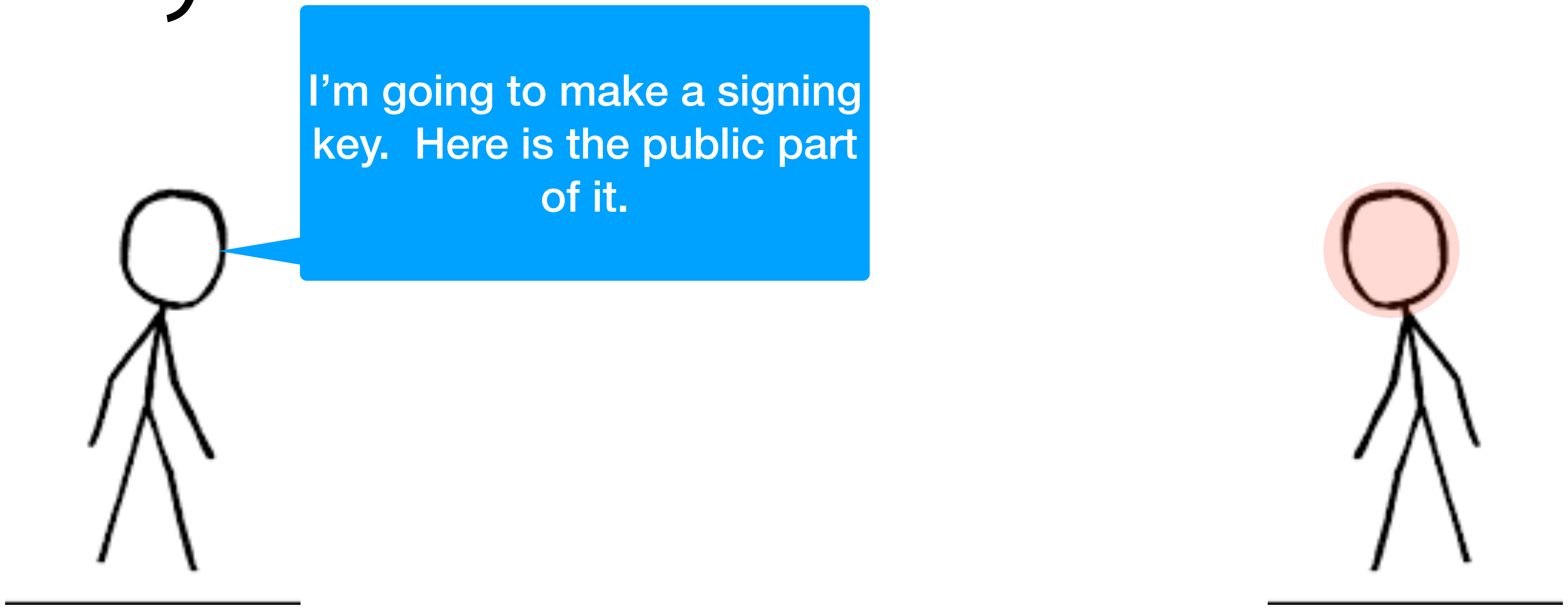


existential unforgability

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



Signature security



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

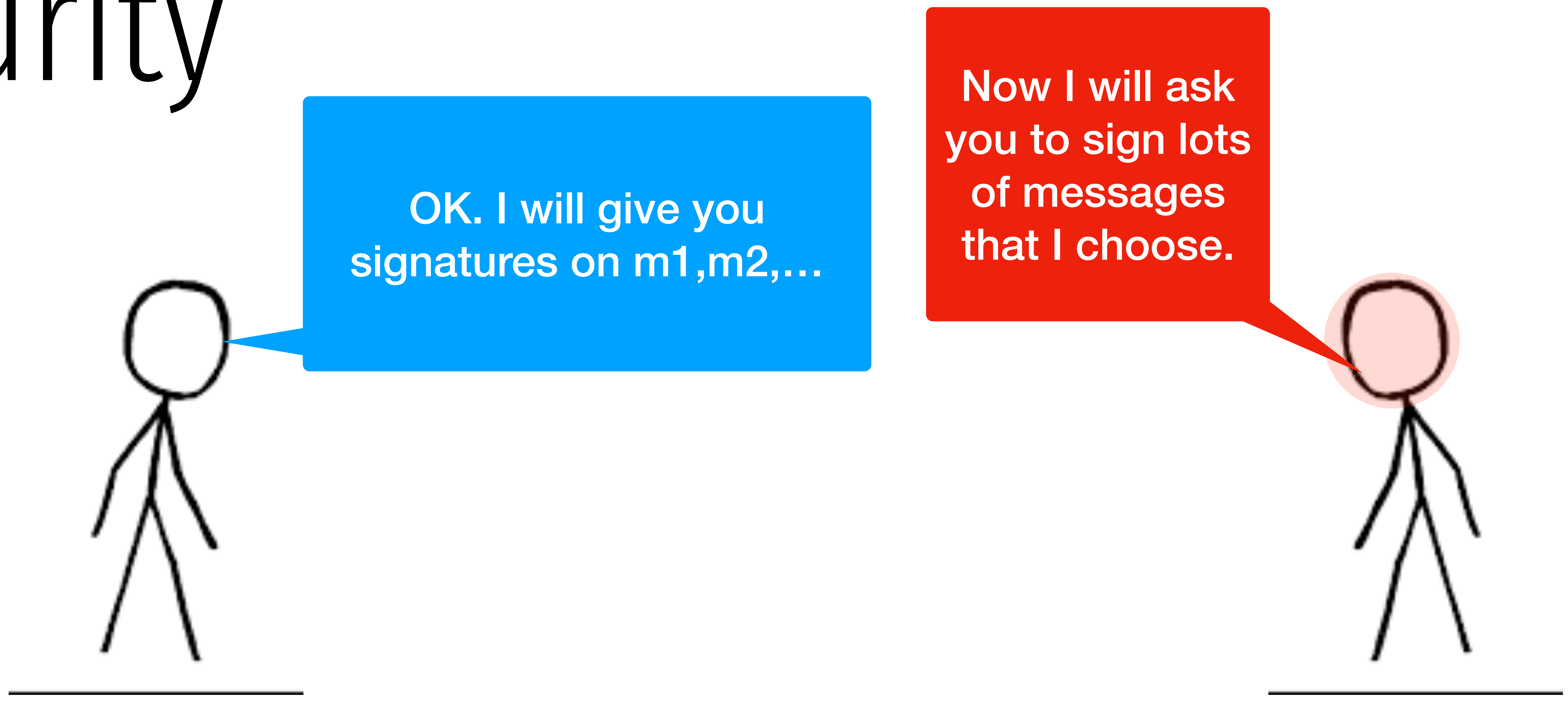
Signature security

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

$m_0, m_1, \ldots$

vk

Signature security

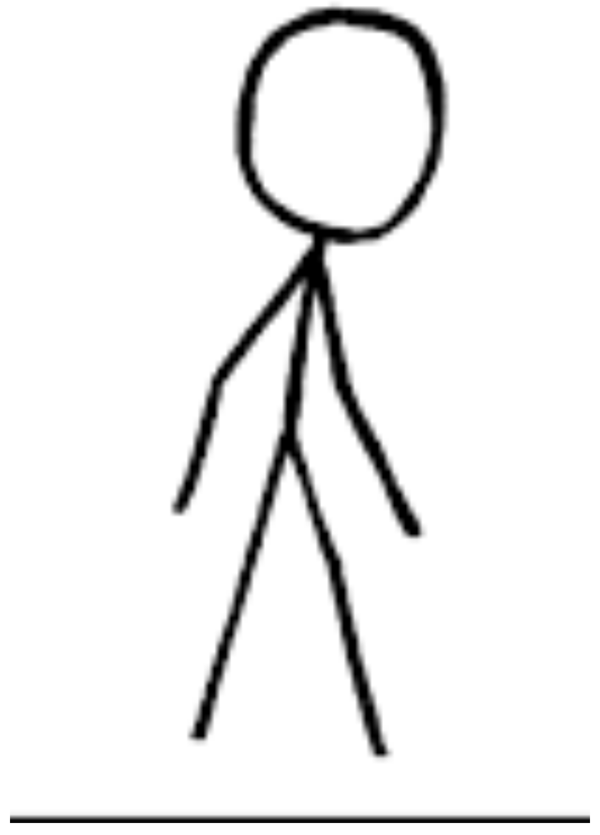


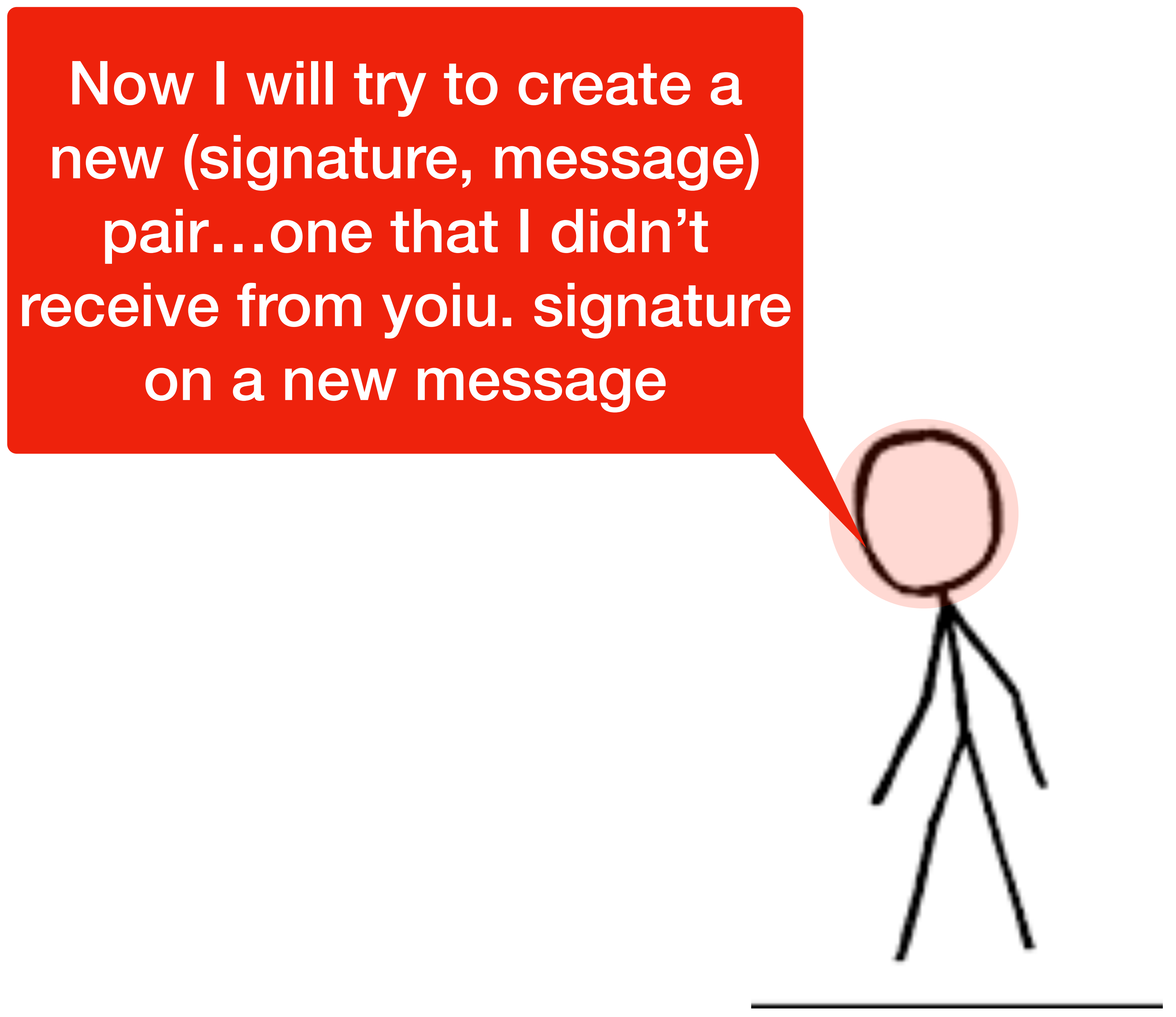
$$(vk, sk) \leftarrow \mathrm{Gen}(1^n)$$

$$vk$$

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

Signature security





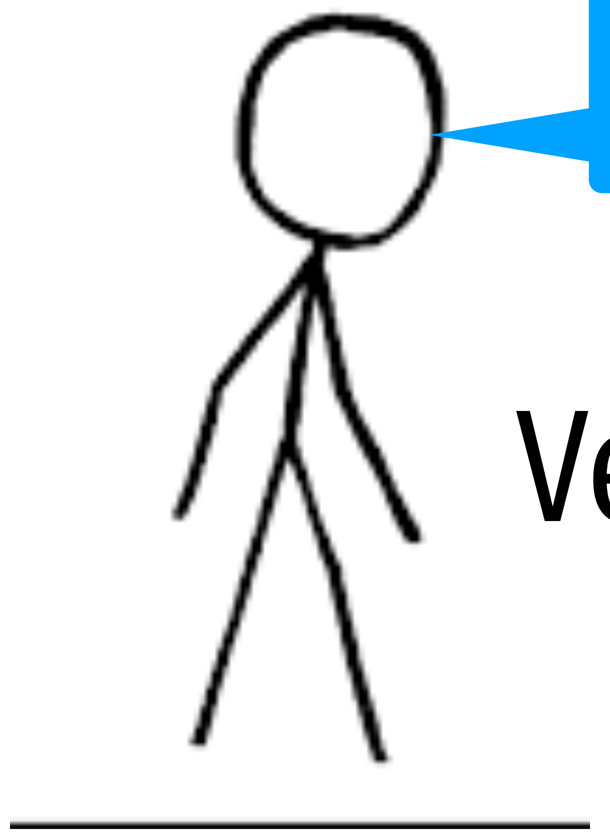
$(vk, sk) \leftarrow \text{Gen}(1^n)$

vk

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

$s_1, s_2, \ldots$

Signature security



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

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