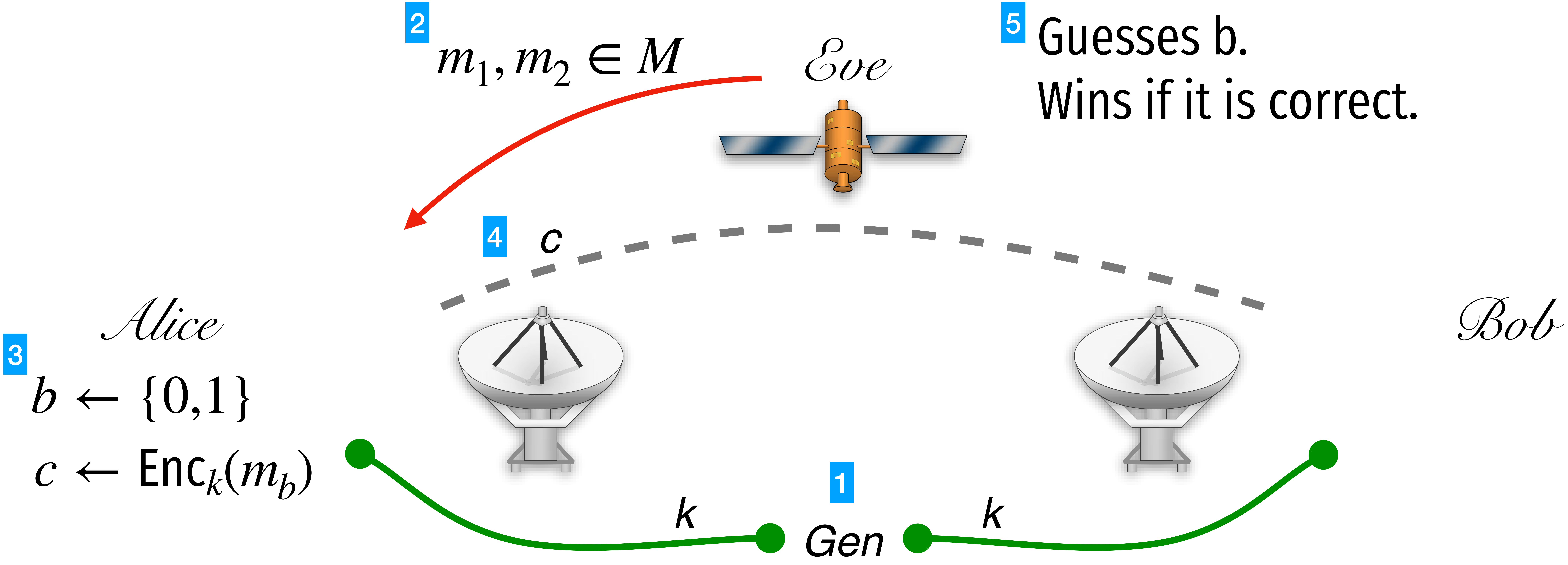
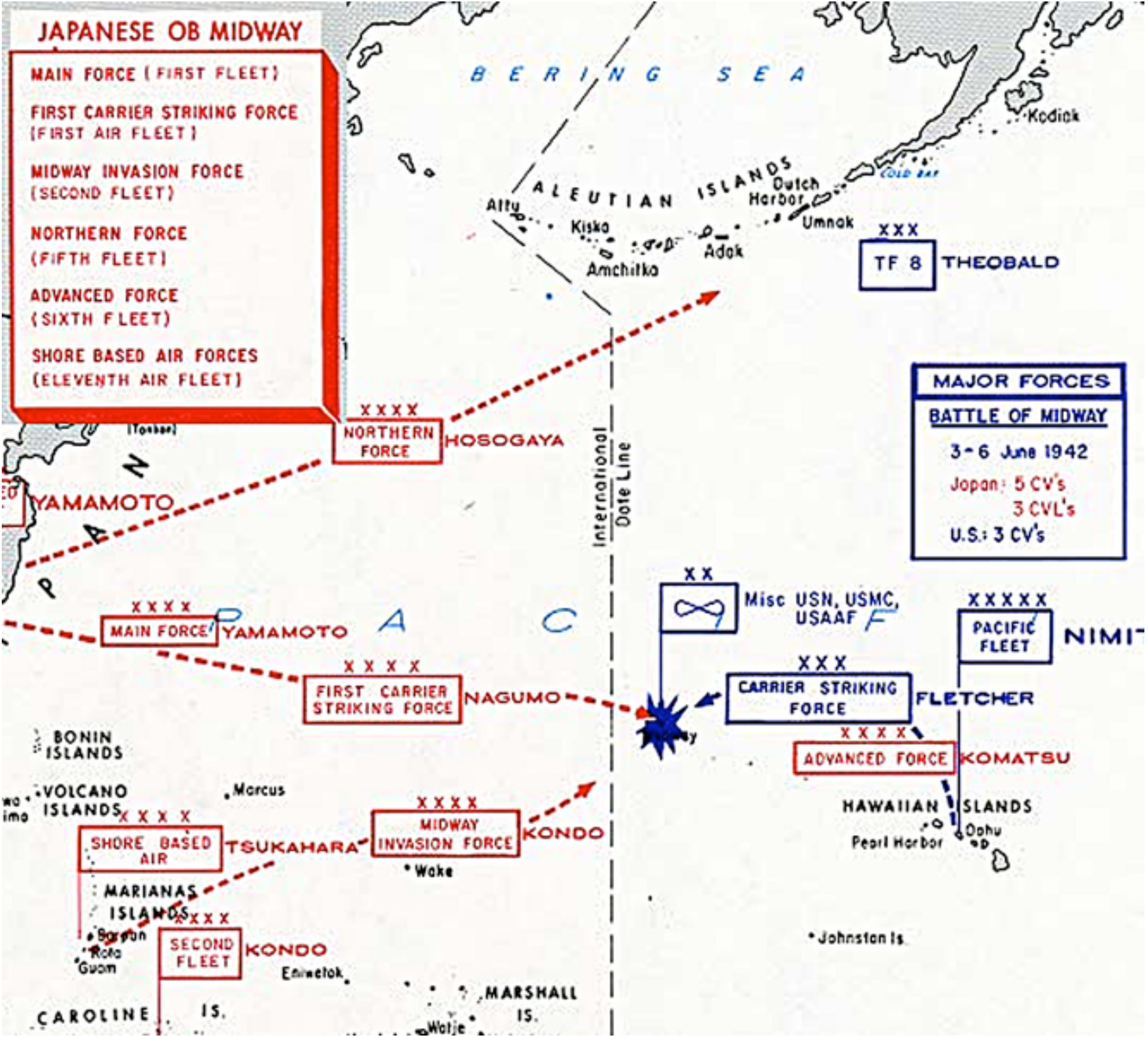
2550 Intro to cybersecurity

L10: Public key Crypto

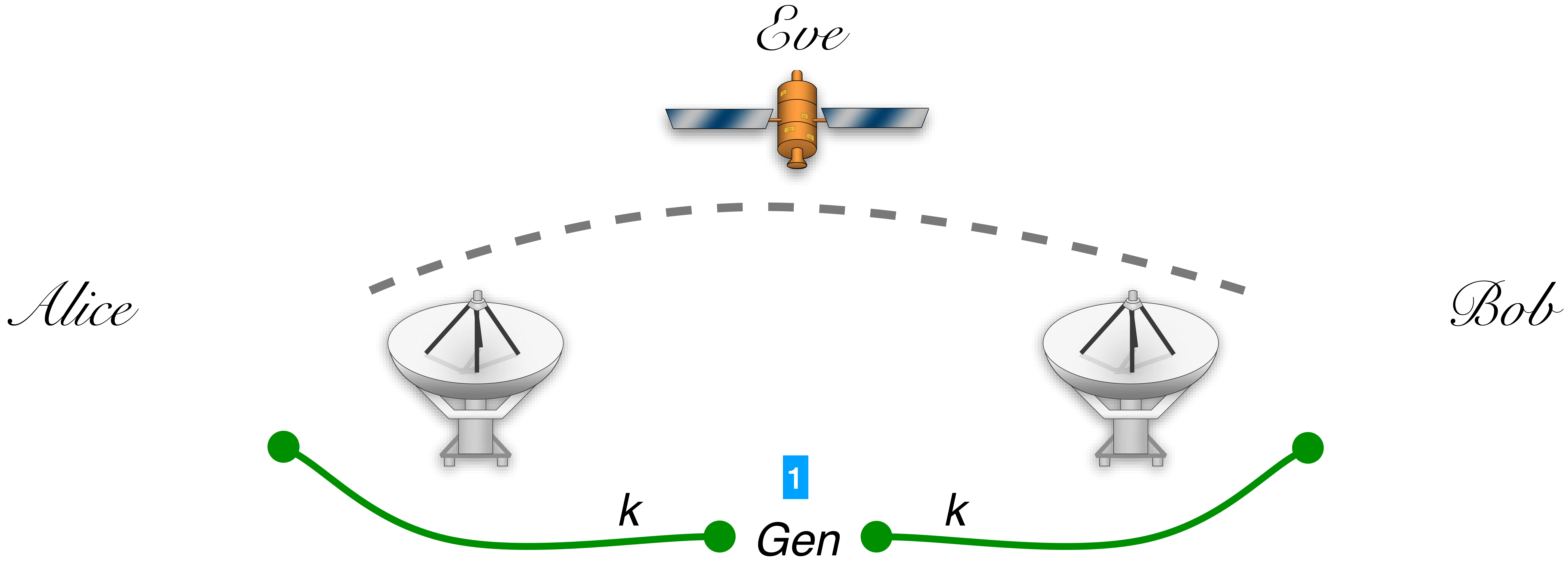
abhi shelat

Is this game strong enough to capture all feasible attacks?

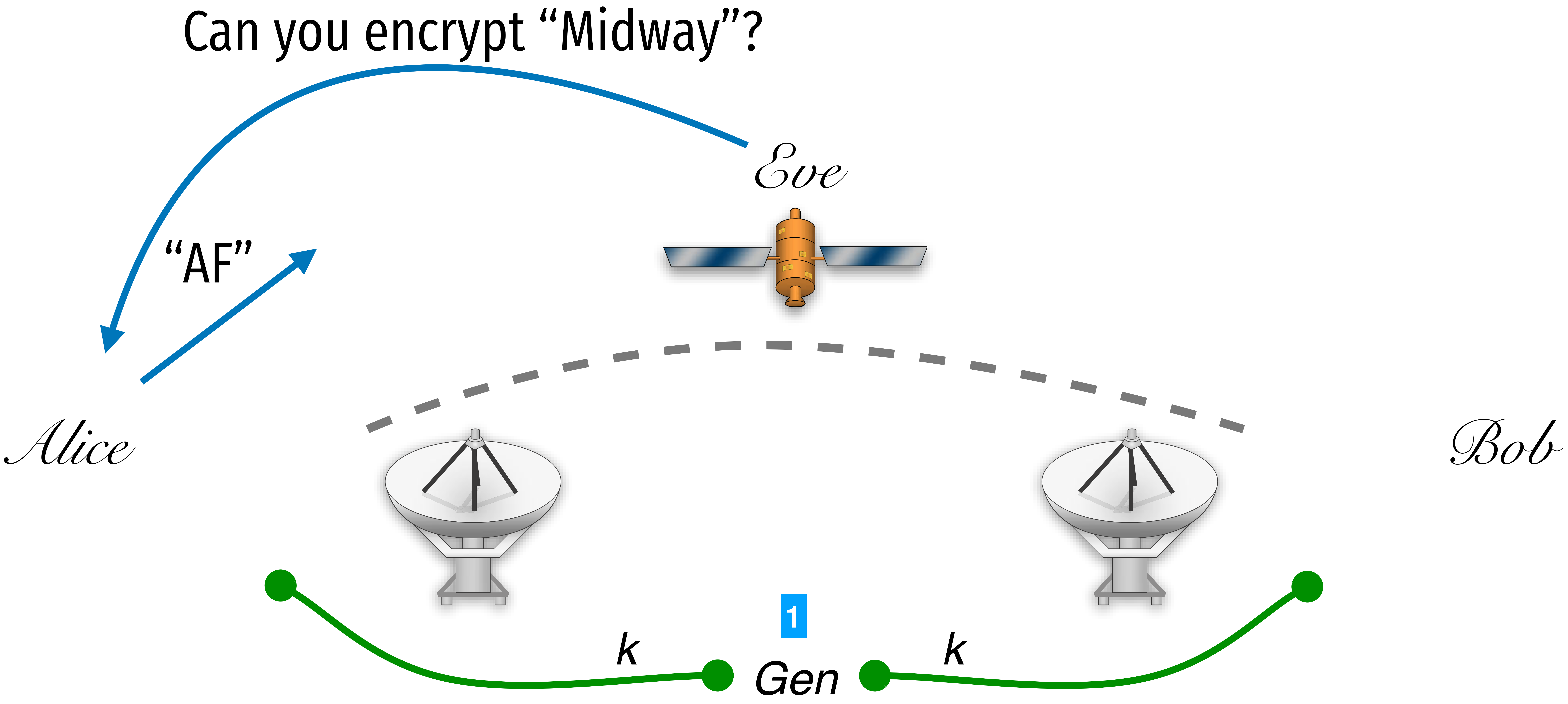



JAPANESE OB MIDWAY
MAIN FORCE (FIRST FLEET)
FIRST CARRIER STRIKING FORCE (FIRST AIR FLEET)
MIDWAY INVASION FORCE (SECOND FLEET)
NORTHERN FORCE (FIFTH FLEET)
ADVANCED FORCE (SIXTH FLEET)
SHORE BASED AIR FORCES (ELEVENTH AIR FLEET)
BERING SEA
Kodiak
Cold Bay
ALEUTIAN ISLANDS
Dutch Harbor
Attu
Kiska
Umnak
Adak
Amchitka
XXX
TF 8
THEOBALD
XXXX
NORTHERN FORCE
HOSOGAYA
YAMAMOTO
International Date Line
MAJOR FORCES
BATTLE OF MIDWAY
3 - 6 June 1942
Japan: 5 CV's
3 CVL's
U.S.: 3 CV's
XX
Misc USN, USMC, USAAF
XXXXX
PACIFIC FLEET
NIMIT
XXXX
MAIN FORCE
YAMAMOTO
P A C I F
XXXX
FIRST CARRIER STRIKING FORCE
NAGUMO
XXX
CARRIER STRIKING FORCE
FLETCHER
XXXX
ADVANCED FORCE
KOMATSU
BONIN ISLANDS
VOLCANO ISLANDS
Marcus
XXXX
SHORE BASED AIR
TSUKAHARA
XXXX
MIDWAY INVASION FORCE
KONDO
Wake
HAWAIIAN ISLANDS
Oahu
Pearl Harbor
MARIANAS ISLANDS
XXXX
SECOND FLEET
KONDO
Saipan
Rota
Guam
Eniwetok
Johnston Is
MARSHALL IS.
CAROLINE IS.
Wotje

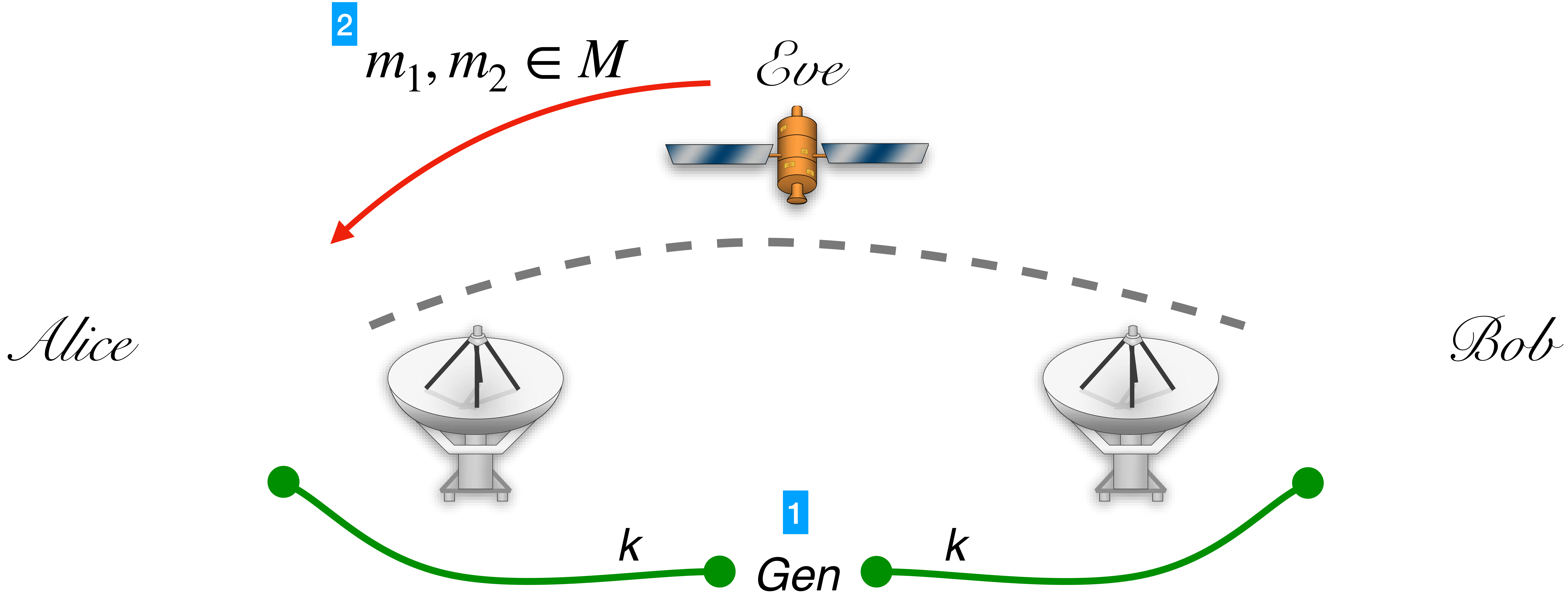
A summary of the attack



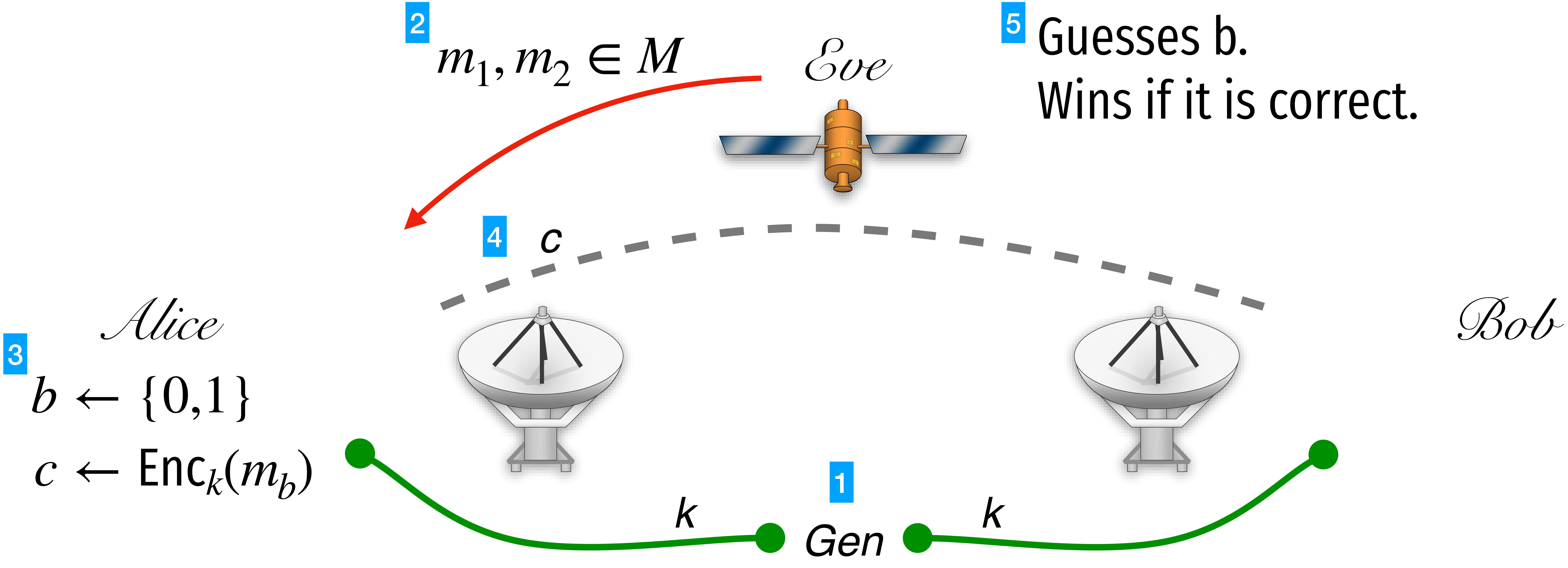
A summary of the attack



A summary of the attack

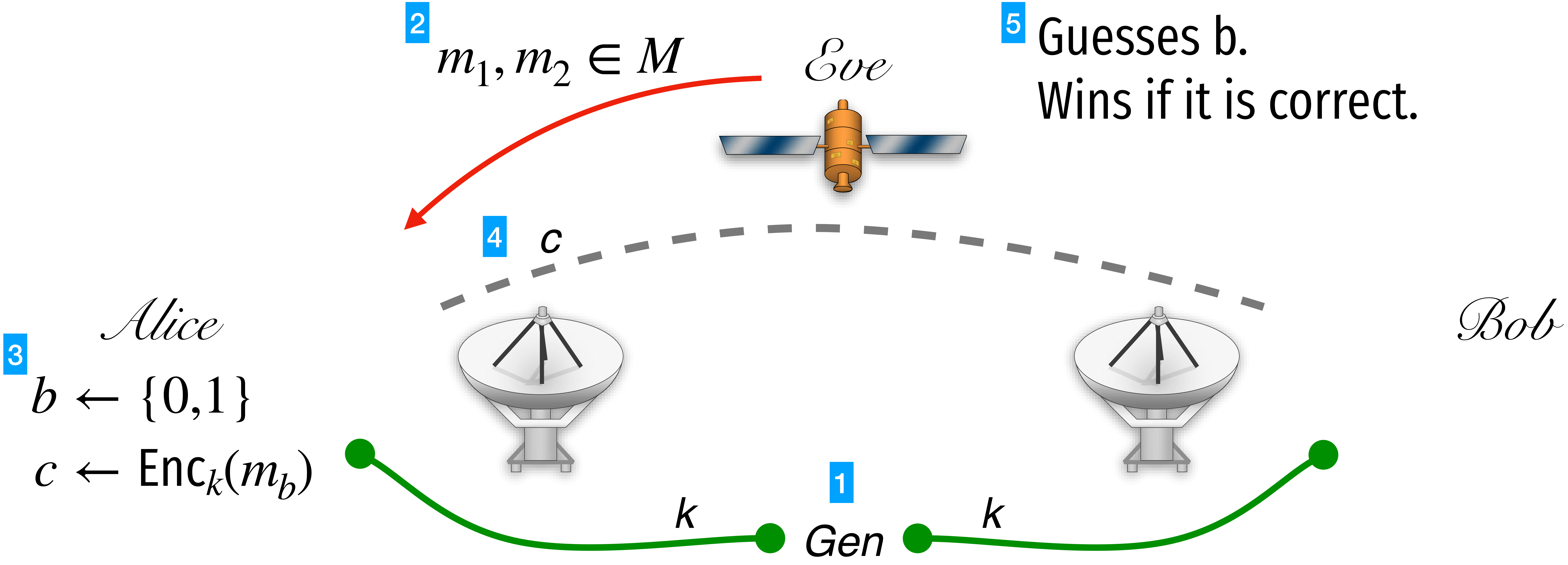


A summary of the attack



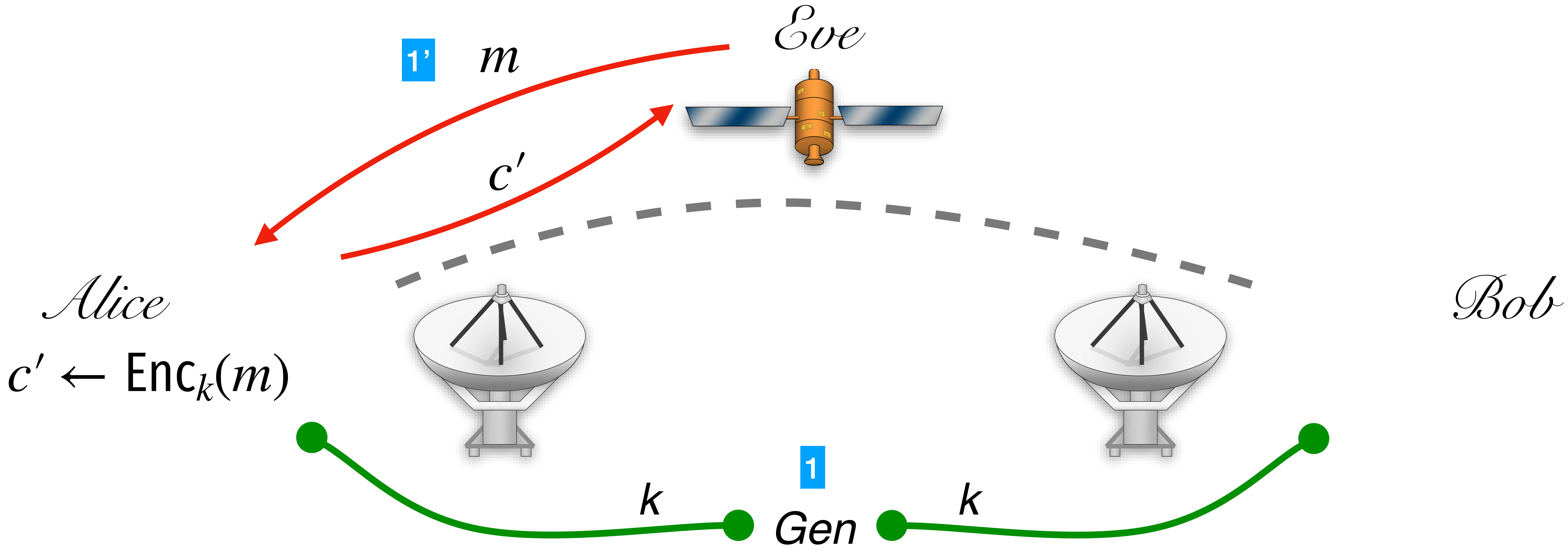
A summary of the attack

Eve was allowed to ask for encryptions of arbitrary messages before step2.

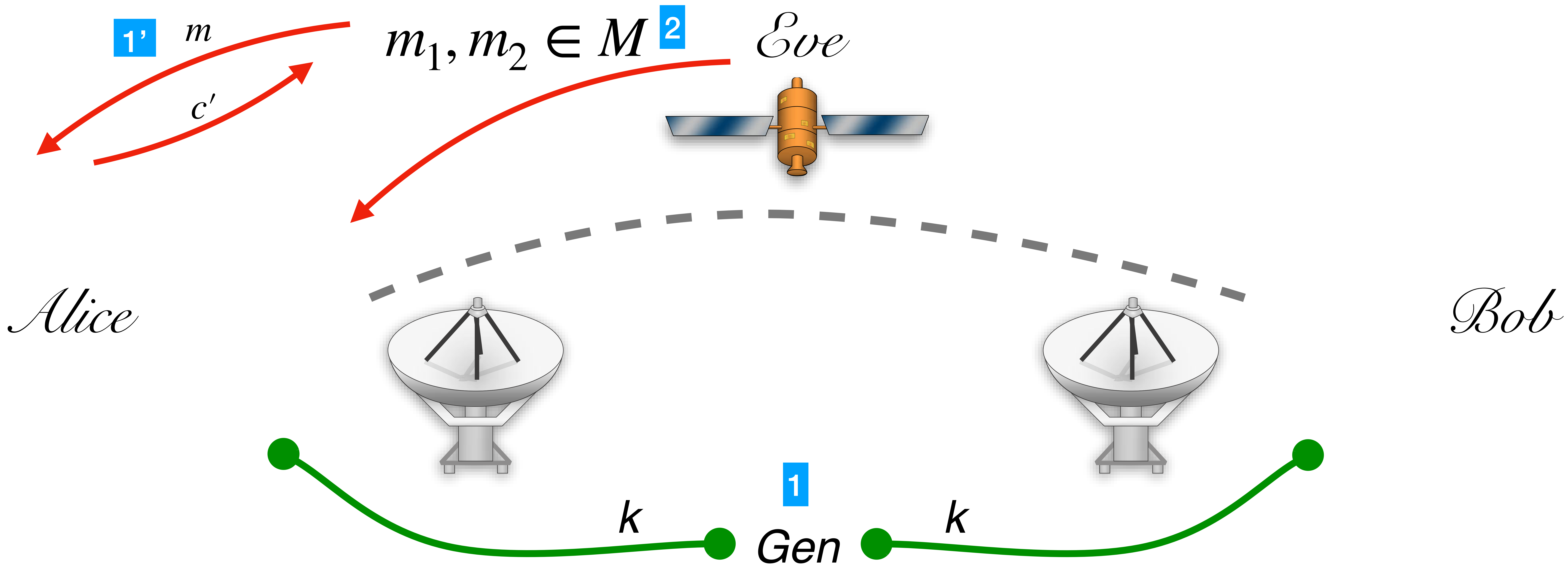


IND-CPA attack for Symmetric Enc

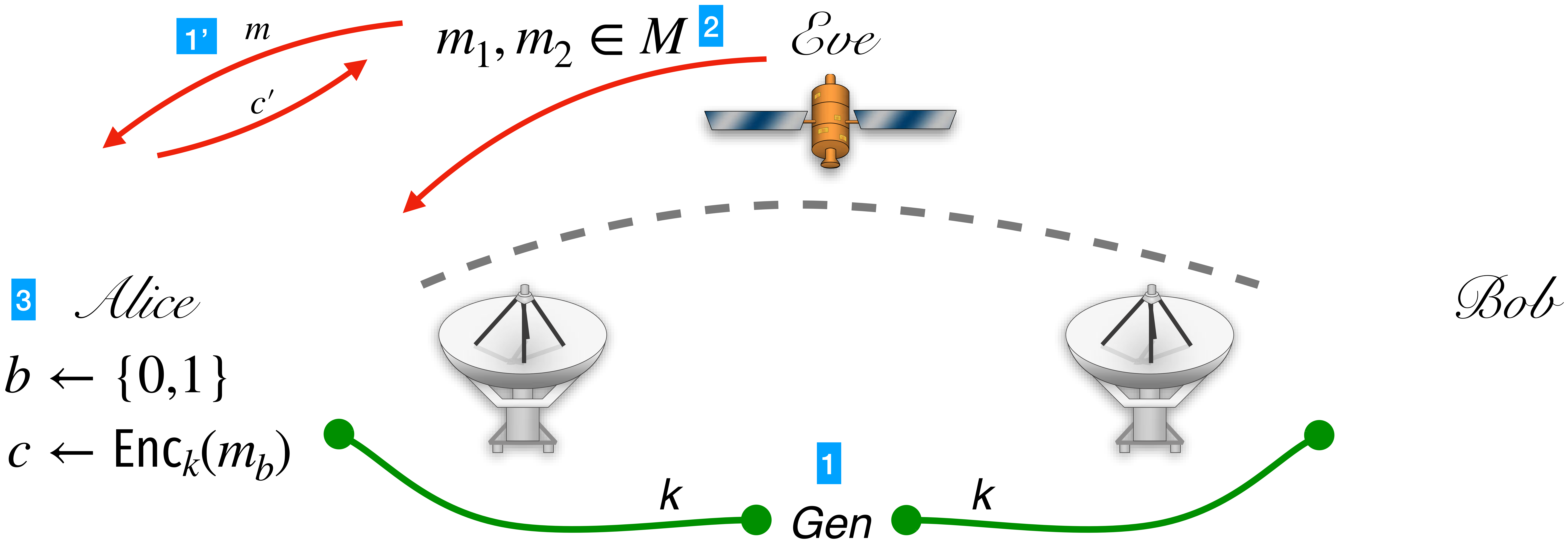
IND-CPA attack for Symmetric Enc



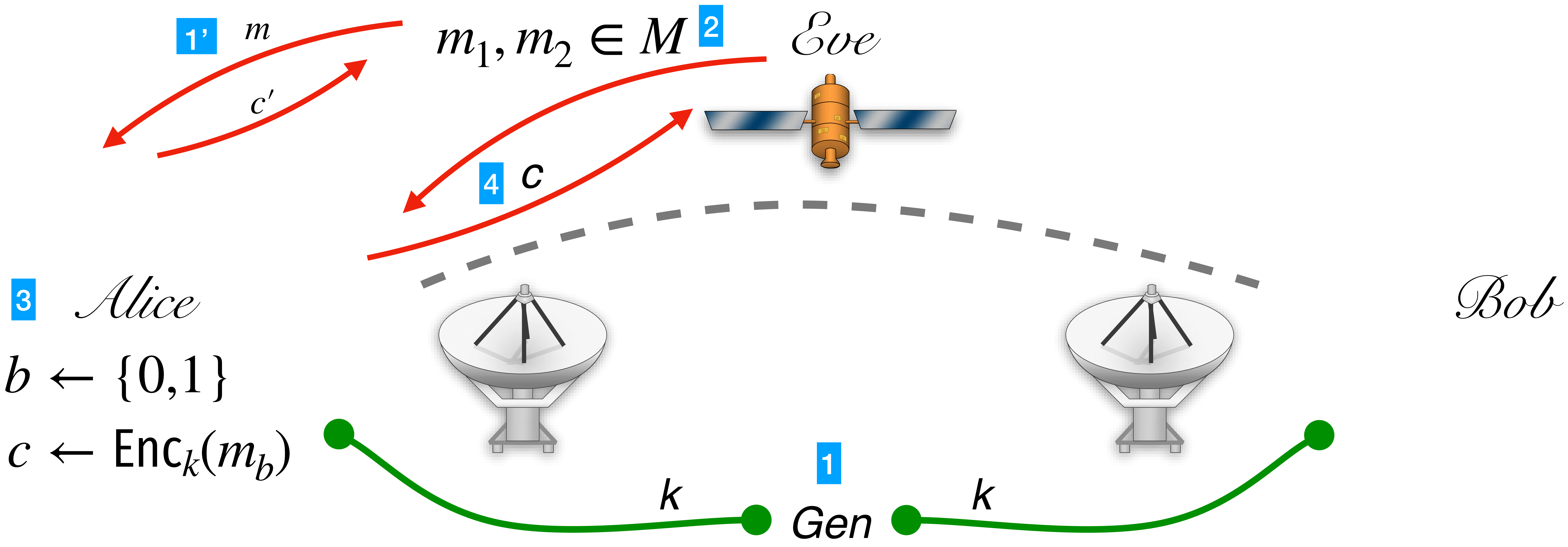
IND-CPA attack for Symmetric Enc



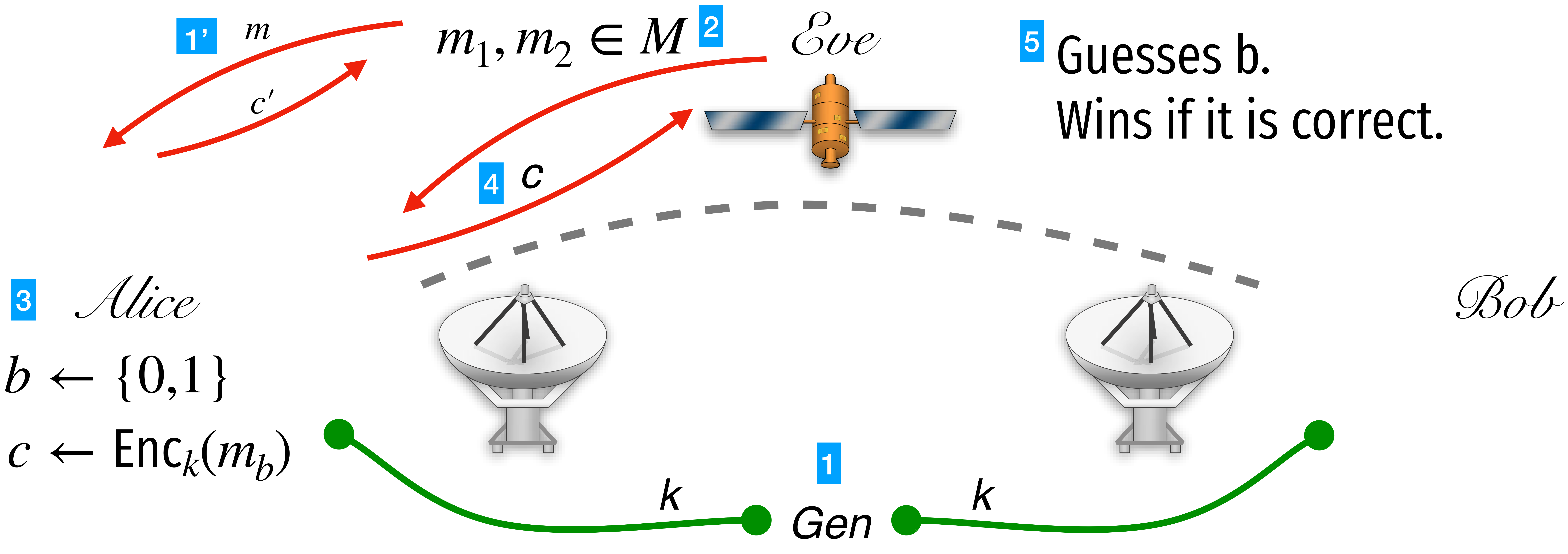
IND-CPA attack for Symmetric Enc



IND-CPA attack for Symmetric Enc



IND-CPA attack for Symmetric Enc



To satisfy IND-CPA, Enc must be randomized.

Enc(k, “hello”)

Enc(k, “hello”)

To satisfy IND-CPA, Enc must be randomized.

Enc(k, “hello”)

Enc(k, “hello”)

If the encryption of a message is always the same cipher text,
then the scheme CANNOT be IND-CPA secure!

Theorem: If One-way functions exist, Then IND-CPA secure symmetric encryption exists.

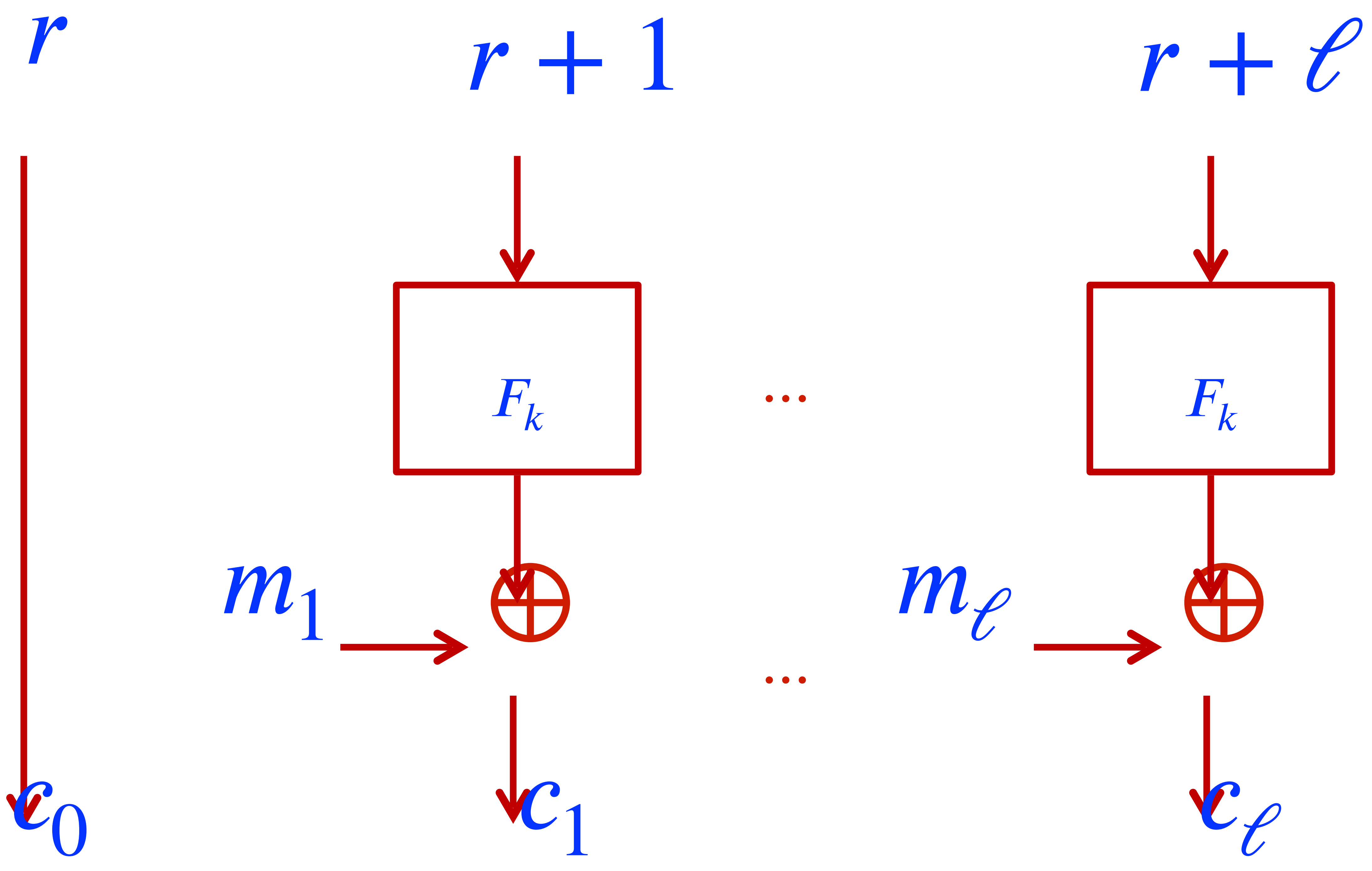
Example of IND-CPA: AES-CTR

Example of IND-CPA: AES-CTR

$$\mathrm{Enc}_k\left(m_1 \cdots m_\ell ; r\right)$$
$$= \left(r, F_k(r+1) \oplus m_1, F_k(r+2) \oplus m_2, \ldots, F_k\left(r+\ell\right) \oplus m_\ell\right)$$

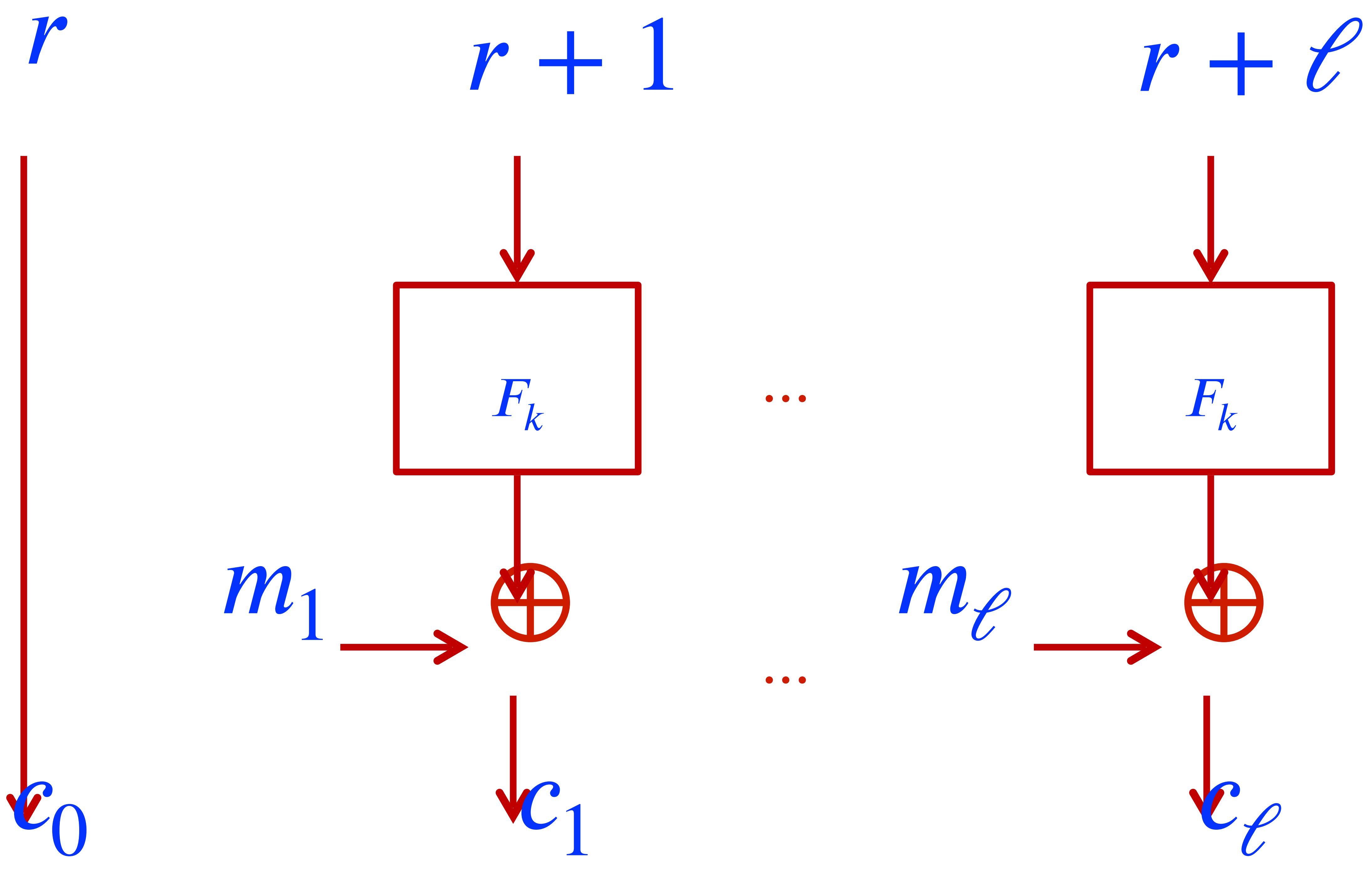
Example of IND-CPA: AES-CTR

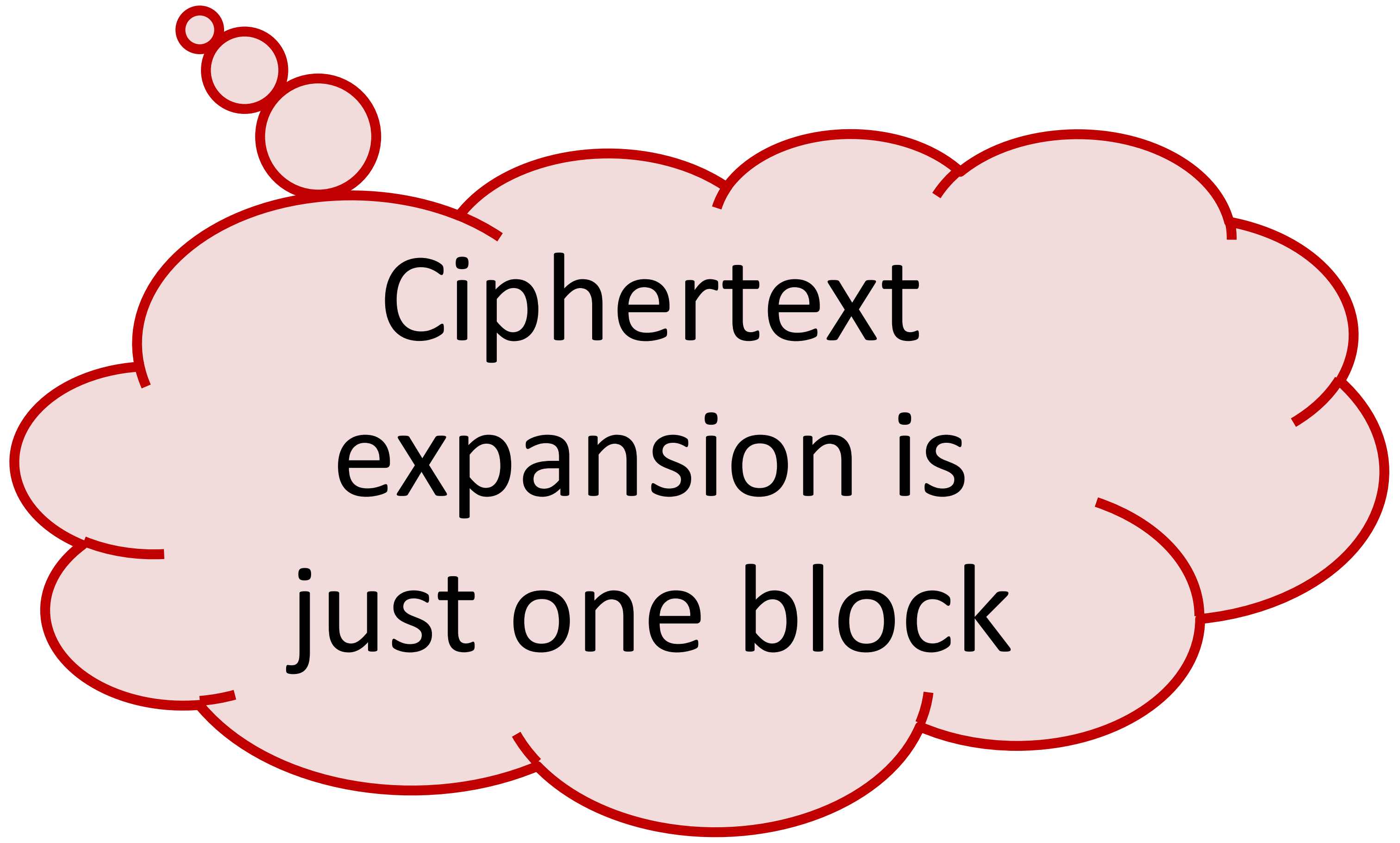
$$\mathrm{Enc}_k\left(m_1 \cdots m_\ell; r\right)$$
$$= \left(r, F_k(r+1) \oplus m_1, F_k(r+2) \oplus m_2, \ldots, F_k\left(r+\ell\right) \oplus m_\ell\right)$$



Example of IND-CPA: AES-CTR

$$\mathrm{Enc}_k\left(m_1 \cdots m_\ell; r\right)$$
$$= \left(r, F_k(r+1) \oplus m_1, F_k(r+2) \oplus m_2, \ldots, F_k\left(r+\ell\right) \oplus m_\ell\right)$$





How to use AES-CTR with openssl

```
$ openssl enc -aes-128-ctr -a
```

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

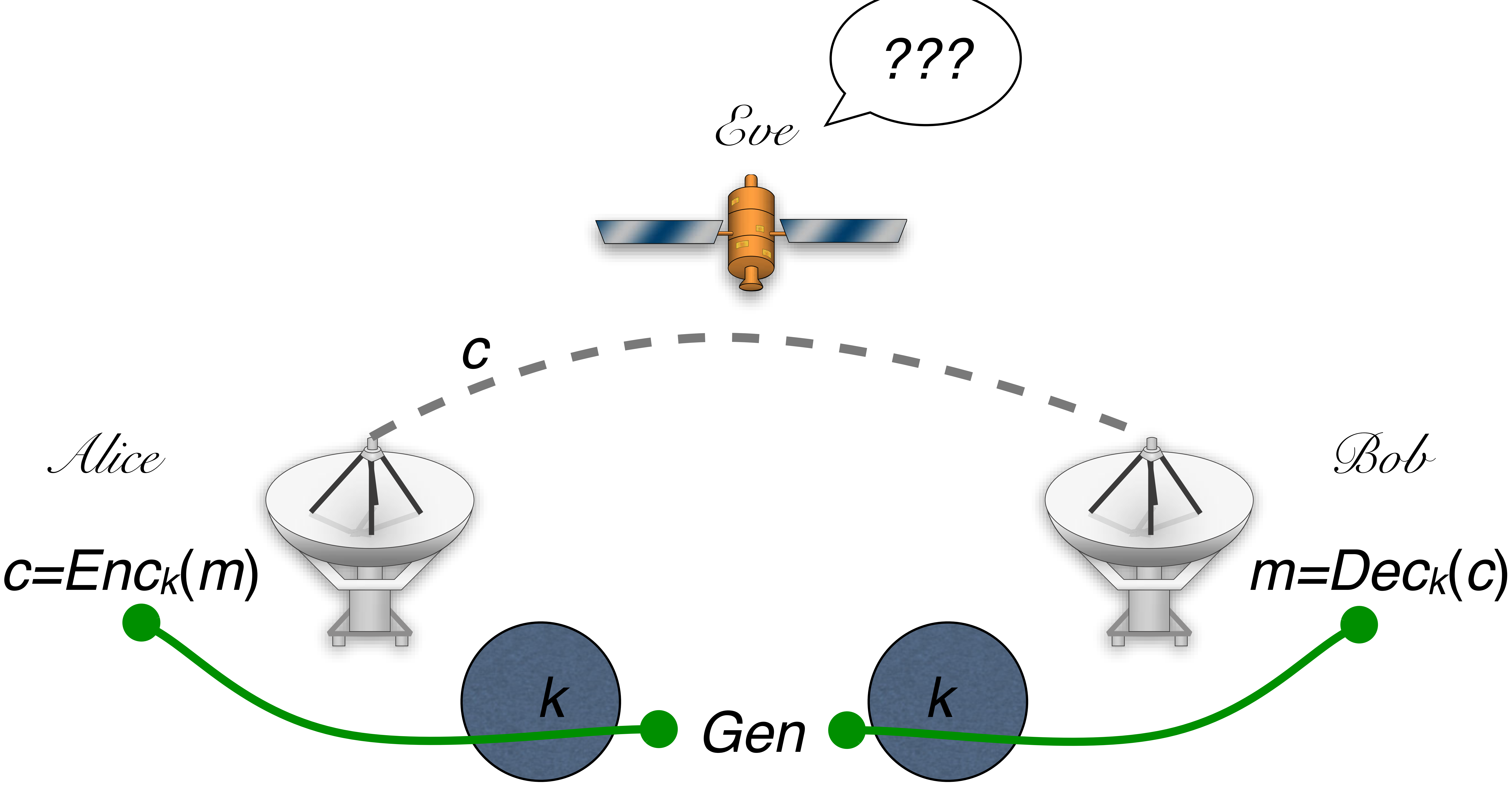
Alice
$k_{ab}, k_{ac}, k_{ad}, k_{ae}, k_{af}, k_{ag}$

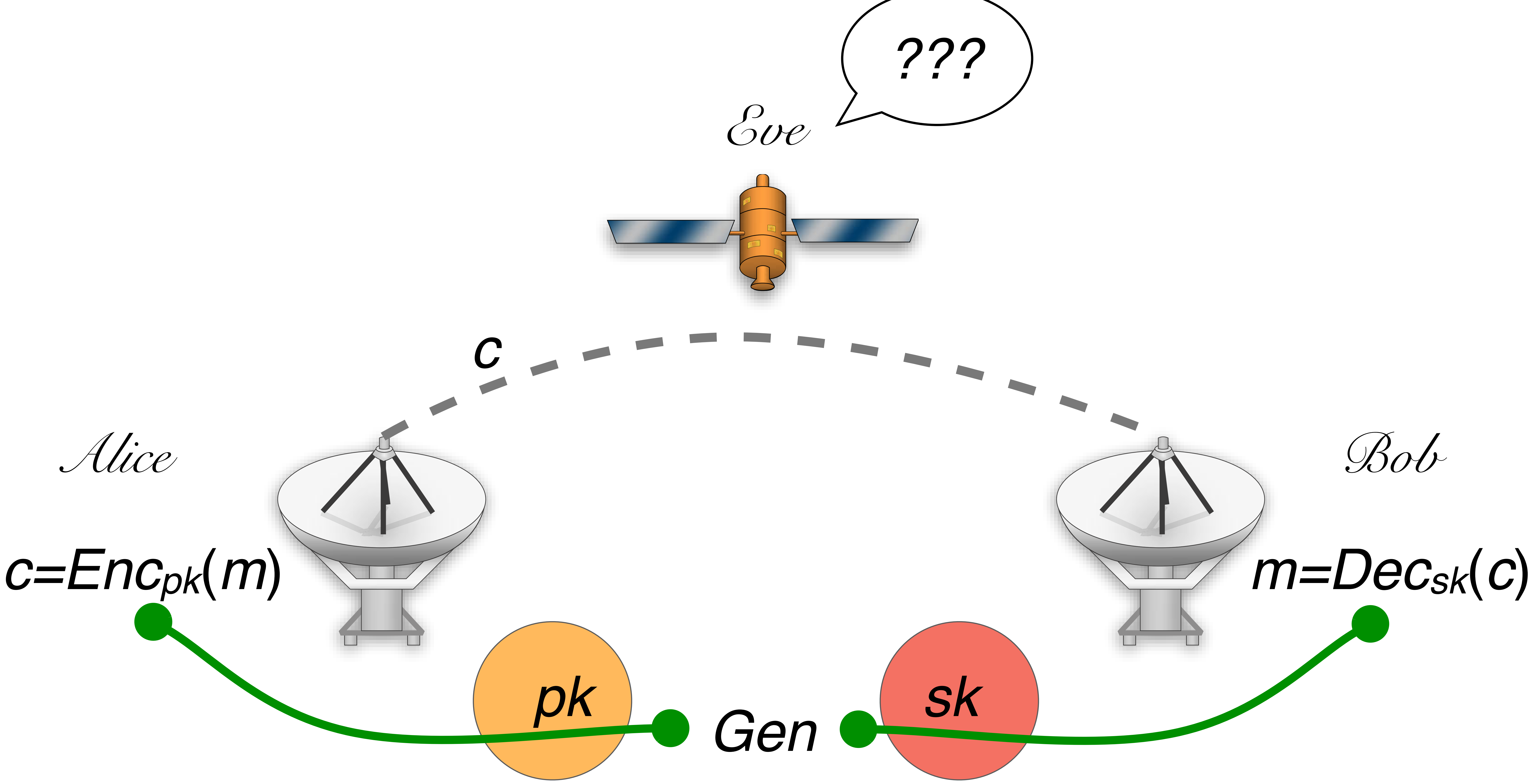
O(n^2) keys to manage!

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)

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

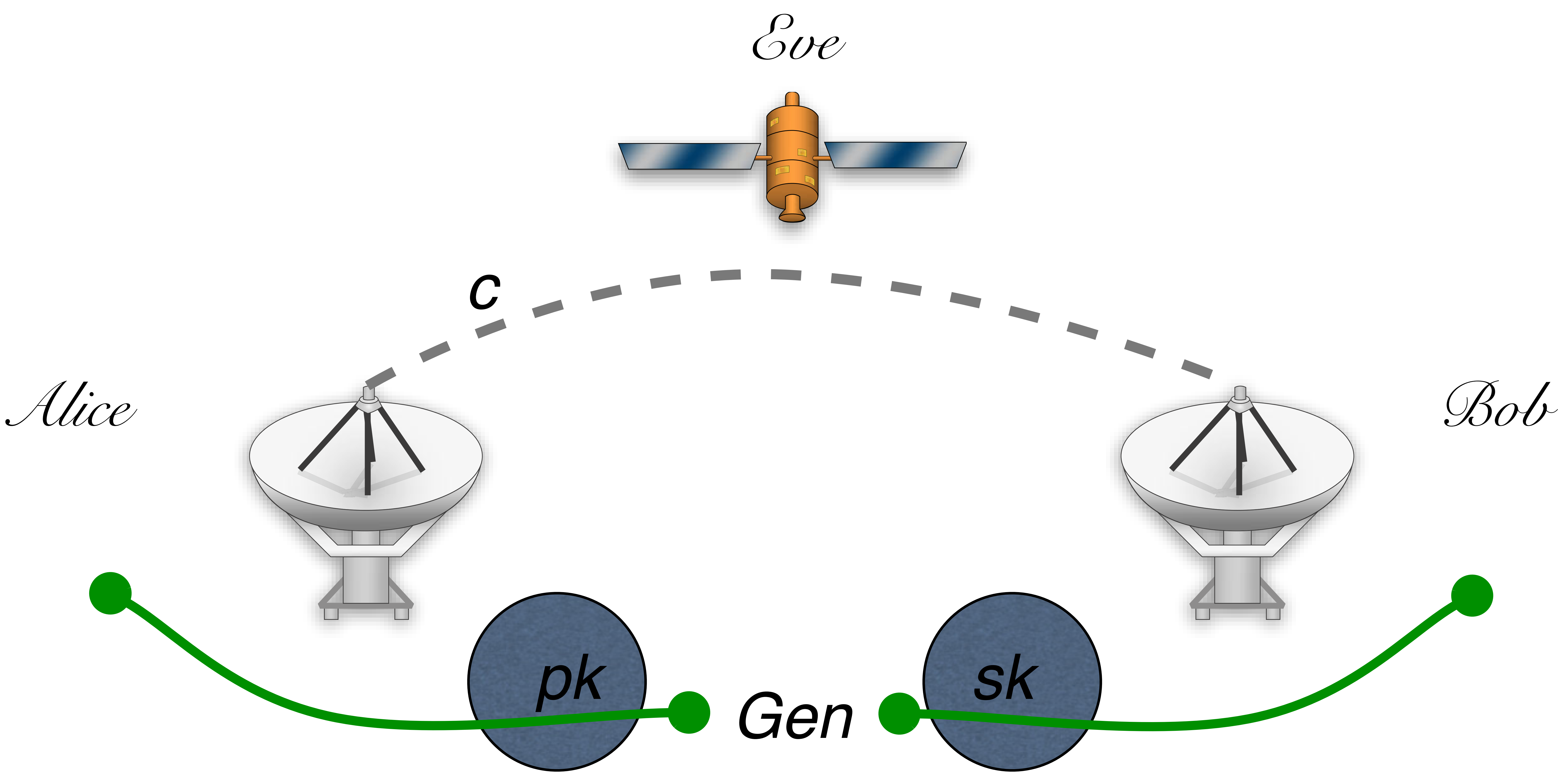
Enc (encryption)

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

Dec (decryption)

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

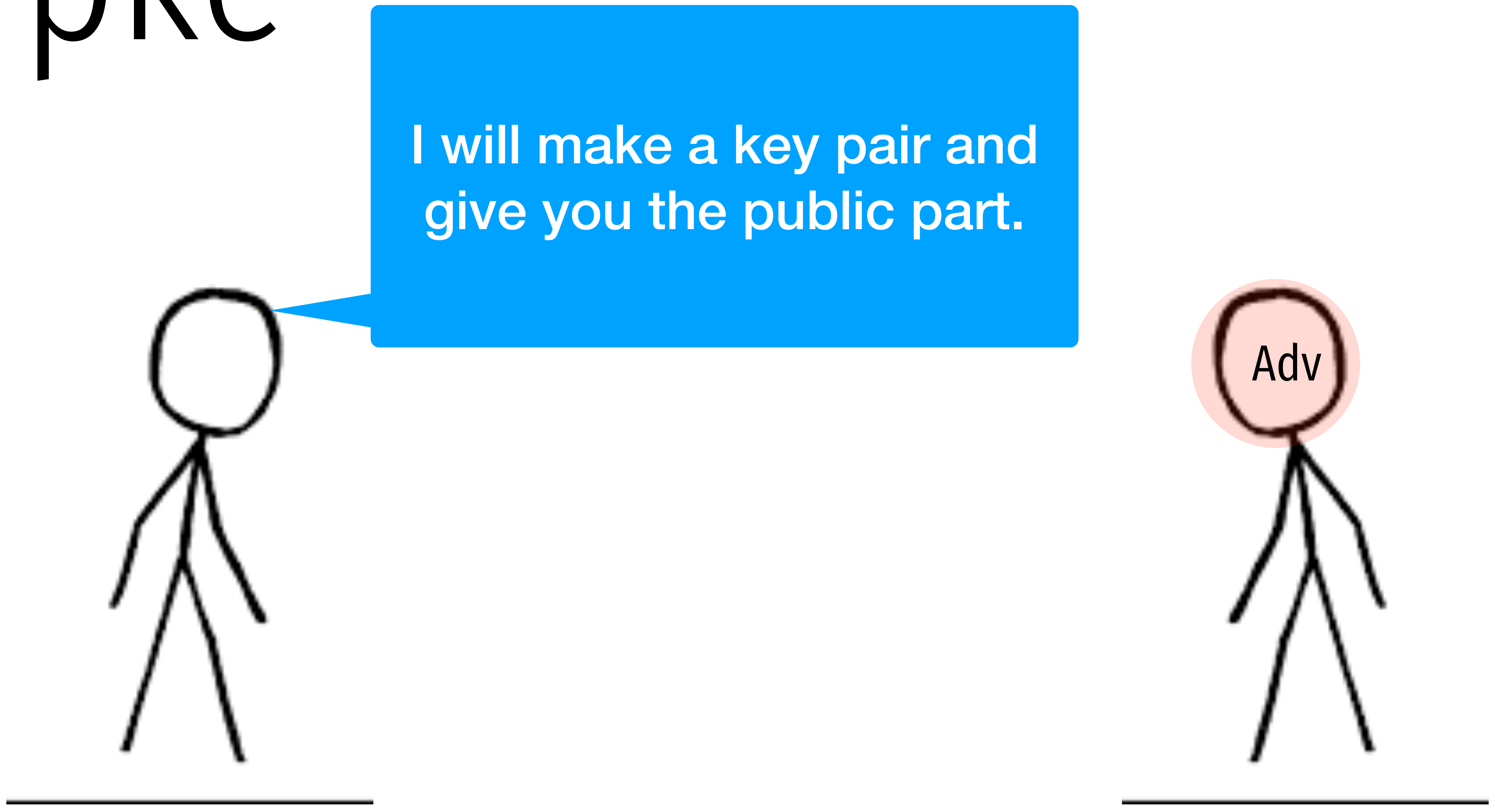
$$\Pr[\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m] = 1$$



“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)

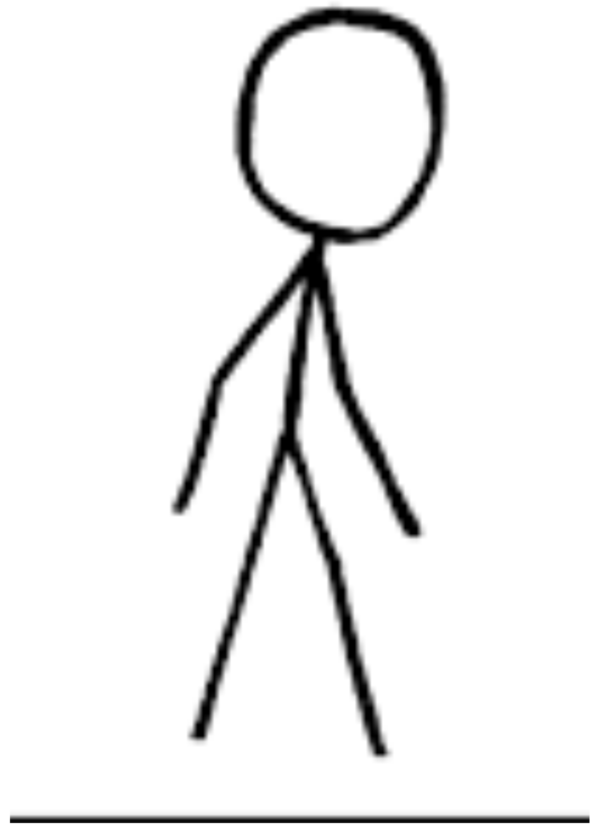


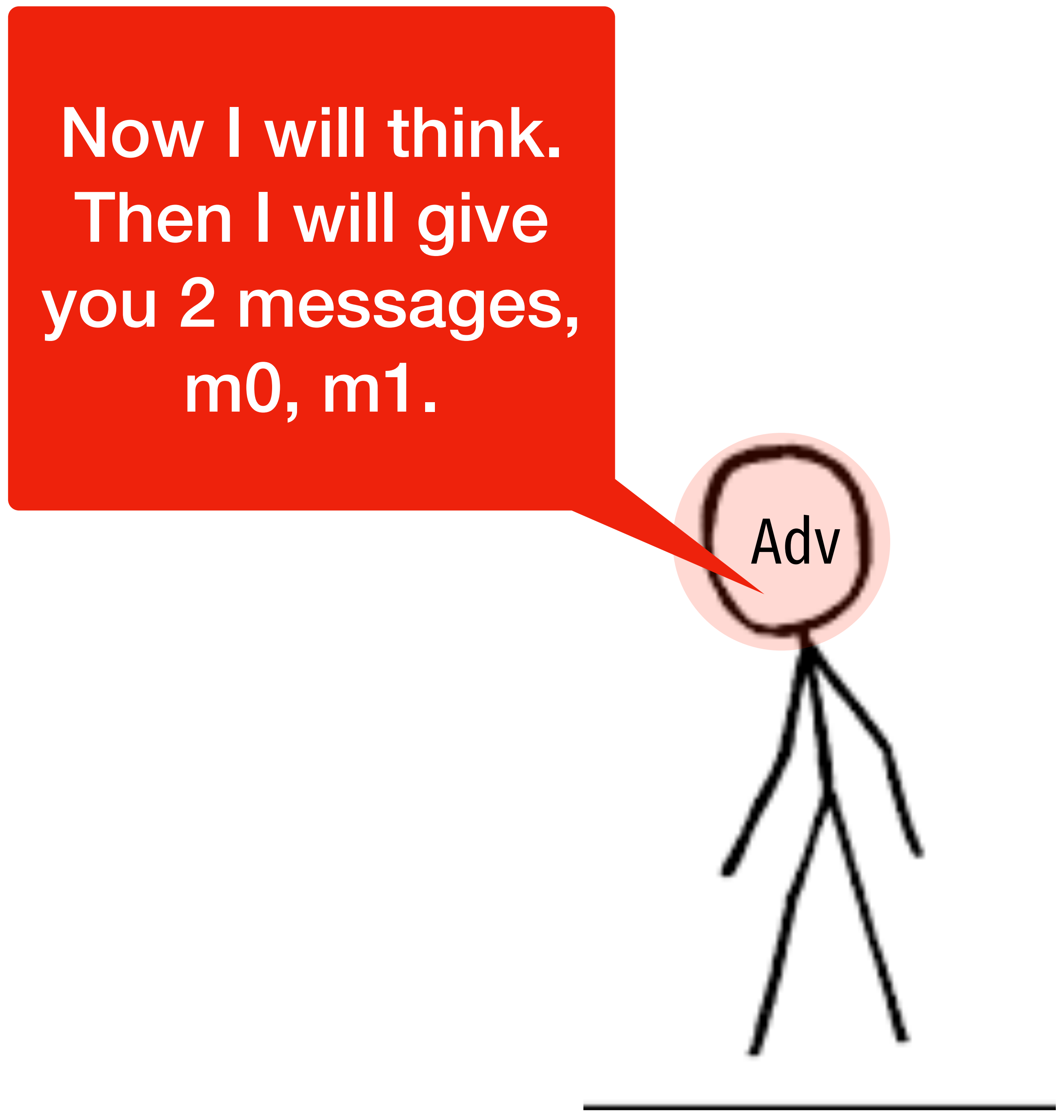
$pk, sk \leftarrow \mathsf{gen}(1^n)$

pk

IND-CPA security for pke

(weakest notion of security)





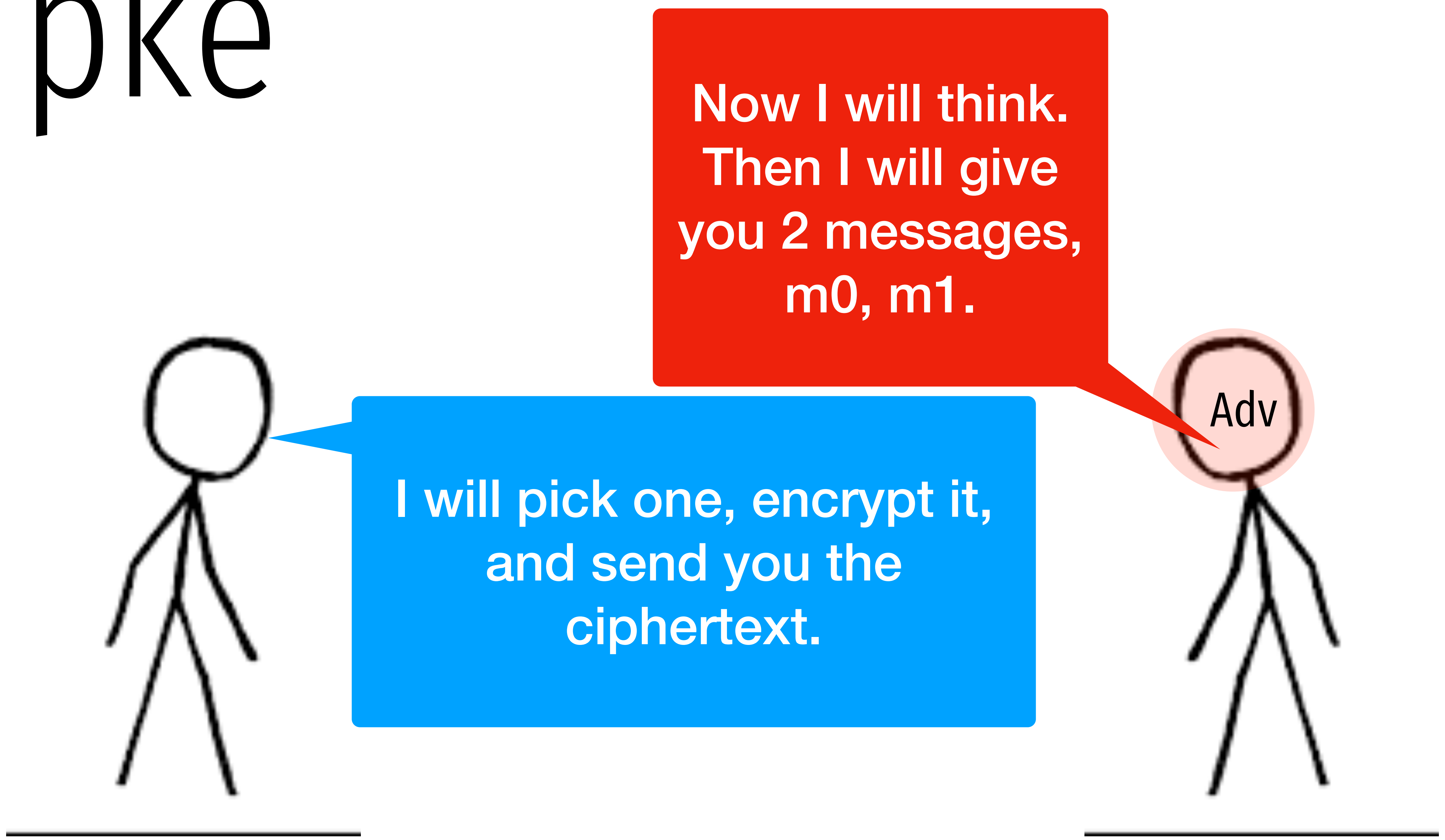
$pk, sk \leftarrow \mathsf{gen}(1^n)$

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

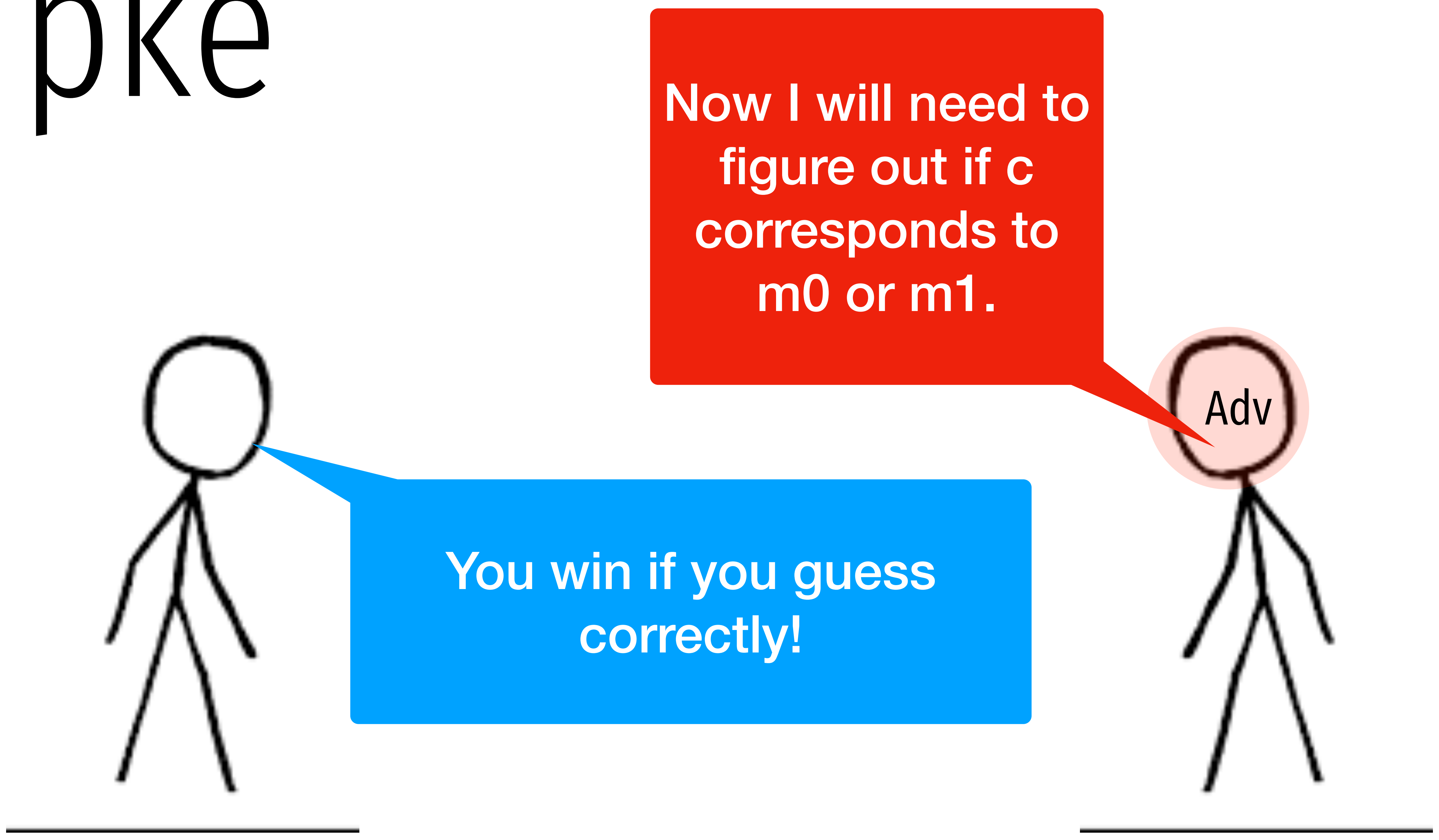
$m_0, m_1 \leftarrow A(pk)$

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

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

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

$$a \bmod p$$

$17 \bmod 11$

$135433238 \bmod 11$

$a \bmod p$

17 mod 11 =6

135433238 mod 11 =6

12312112 R6

11) 135 433 238

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

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

$7^{19} \bmod 31$

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

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

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

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

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 ∈ [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)

$6809 = 4 \cdot 1641 + 245$

$1641 = 6 \cdot 245 + 171$

$245 = 1 \cdot 171 + 74$

$171 = 2 \cdot 74 + 23$

$74 = 3 \cdot 23 + 5$

$23 = 4 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

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

$2 = 2 \cdot 1 + 0$

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

  Return $(0, 1)$

else

  $(x, y) \leftarrow \texttt{ExtendedEuclid}\,(b, a \bmod b)$

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

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) $\quad 6809 = 4 \cdot 1641 + 245$

GCD(1641, 245) $\quad 1641 = 6 \cdot 245 + 171$

GCD(245, 171) $\quad 245 = 1 \cdot 171 + 74$

GCD(171, 74) $\quad 171 = 2 \cdot 74 + 23$

GCD(74, 23) $\quad 74 = 3 \cdot 23 + 5$

GCD(23, 5) $\quad 23 = 4 \cdot 5 + 3$

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

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

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

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(6809,1641)
```

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

Greatest Common Divisor

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

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

 -4378187       4378188
```

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

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

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

“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)

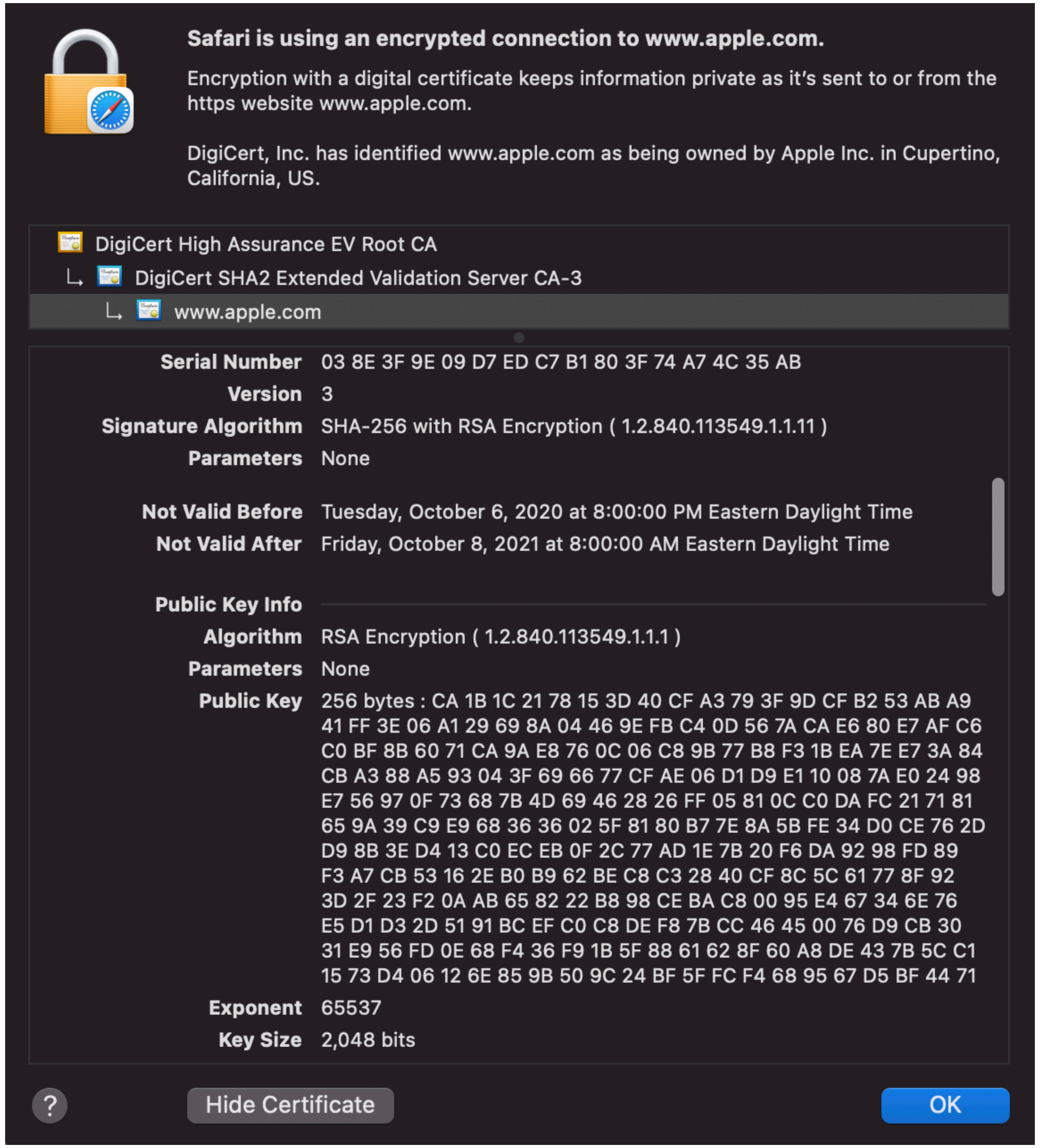
$(s = (s_1, s_2), t) \leftarrow f^{-1}(c)$

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

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

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

Example: apple.com

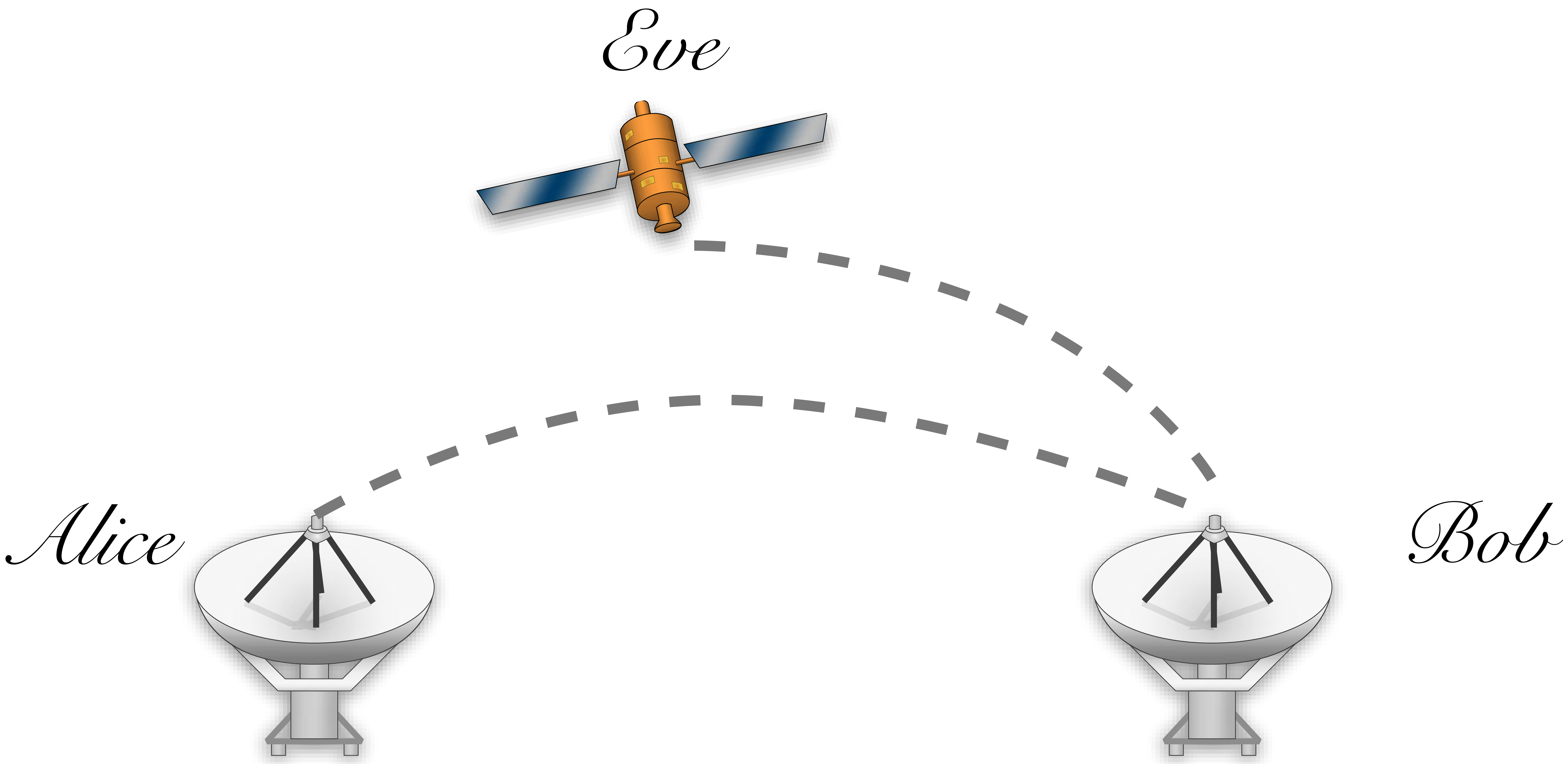


Very old problem

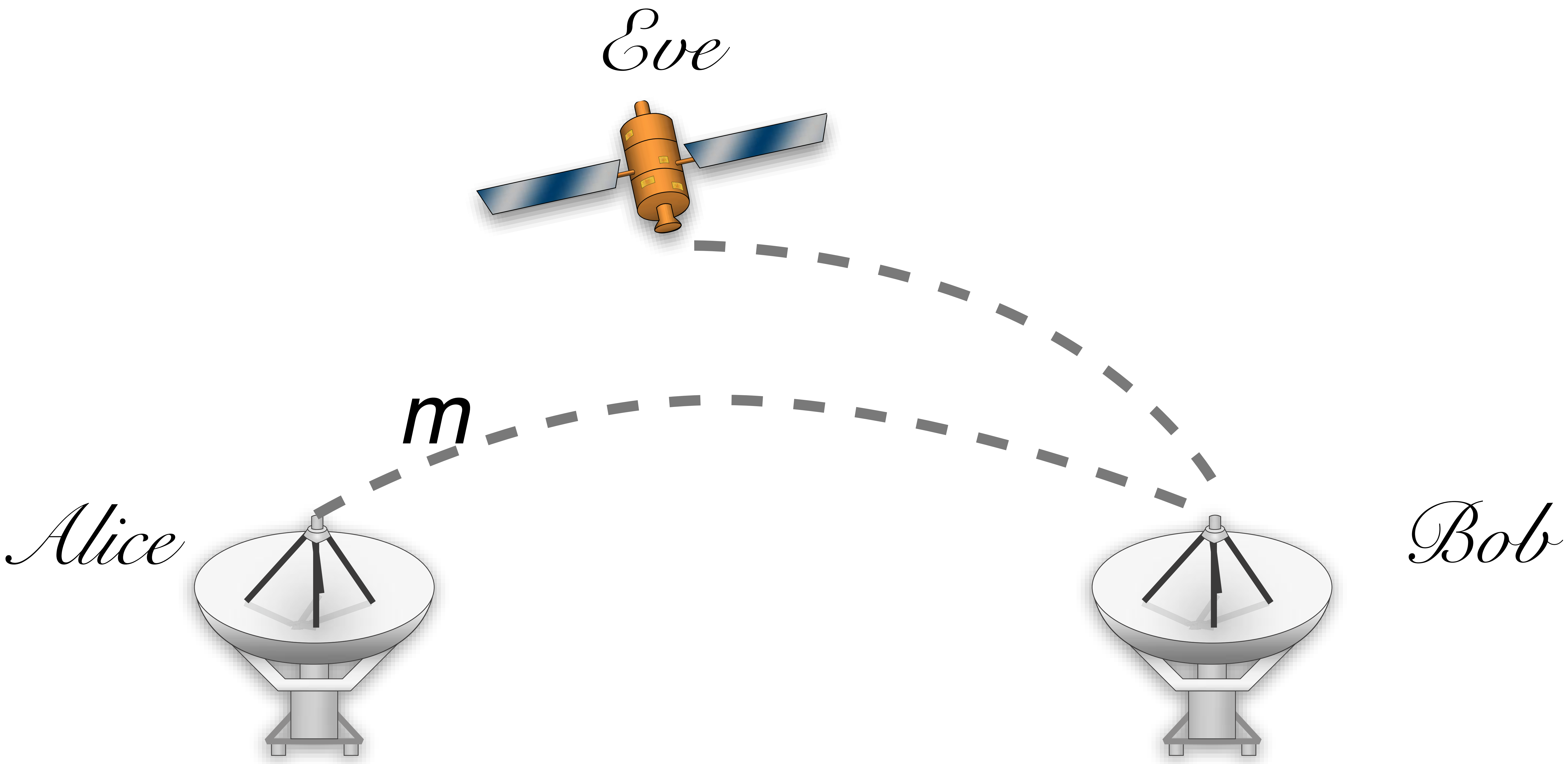
John Hancock


ΚΟΡΑΣ

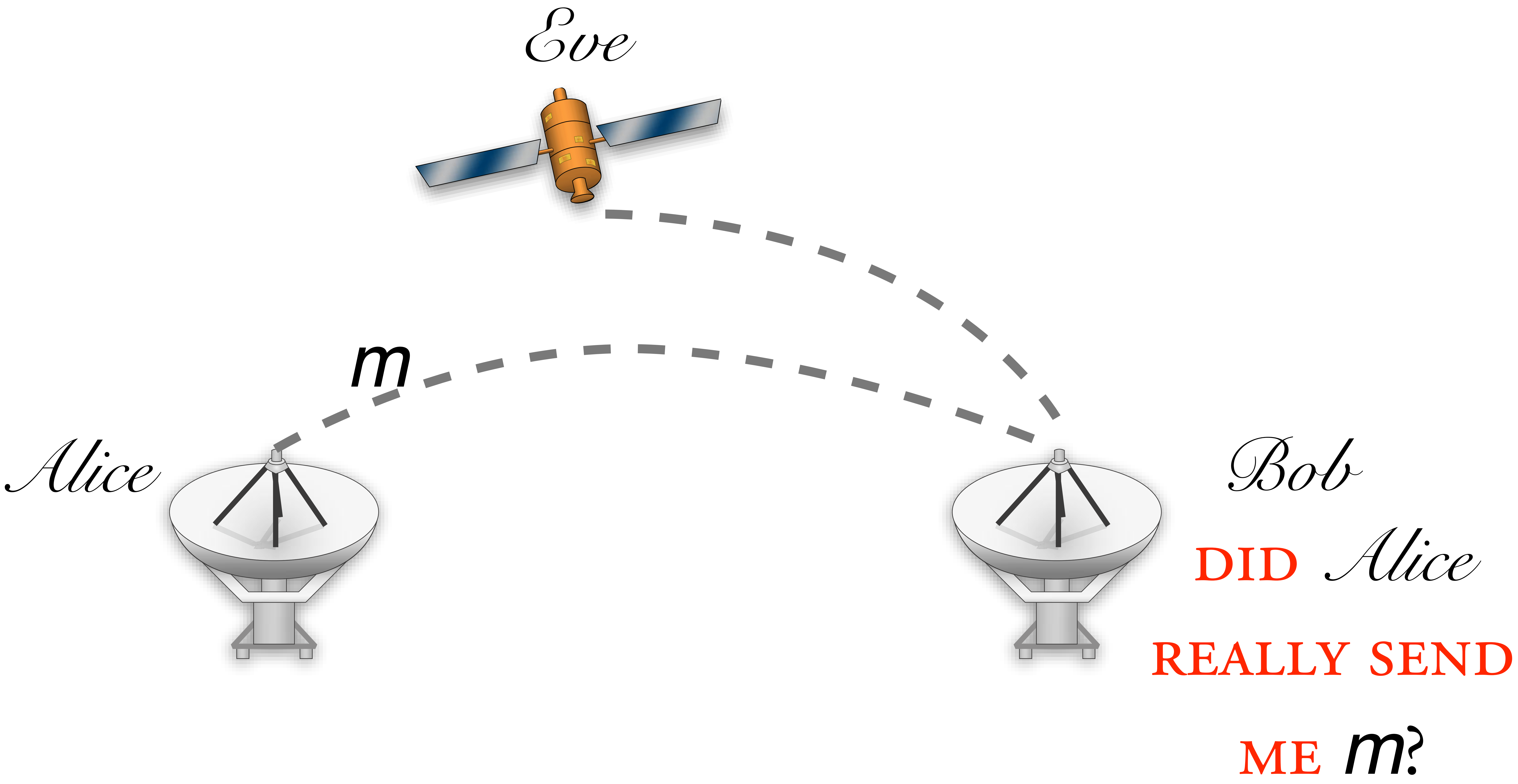
New Problem



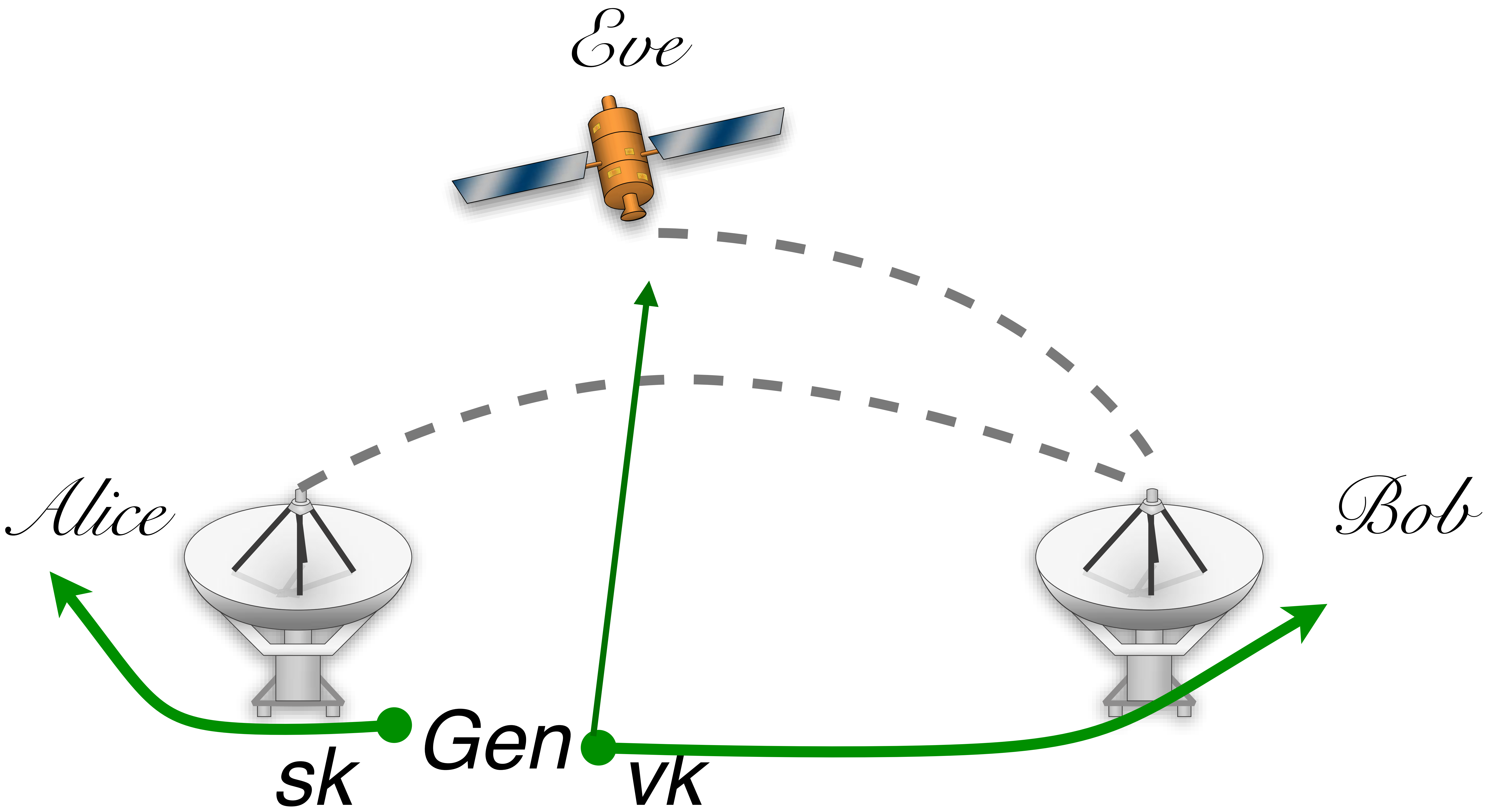
New Problem



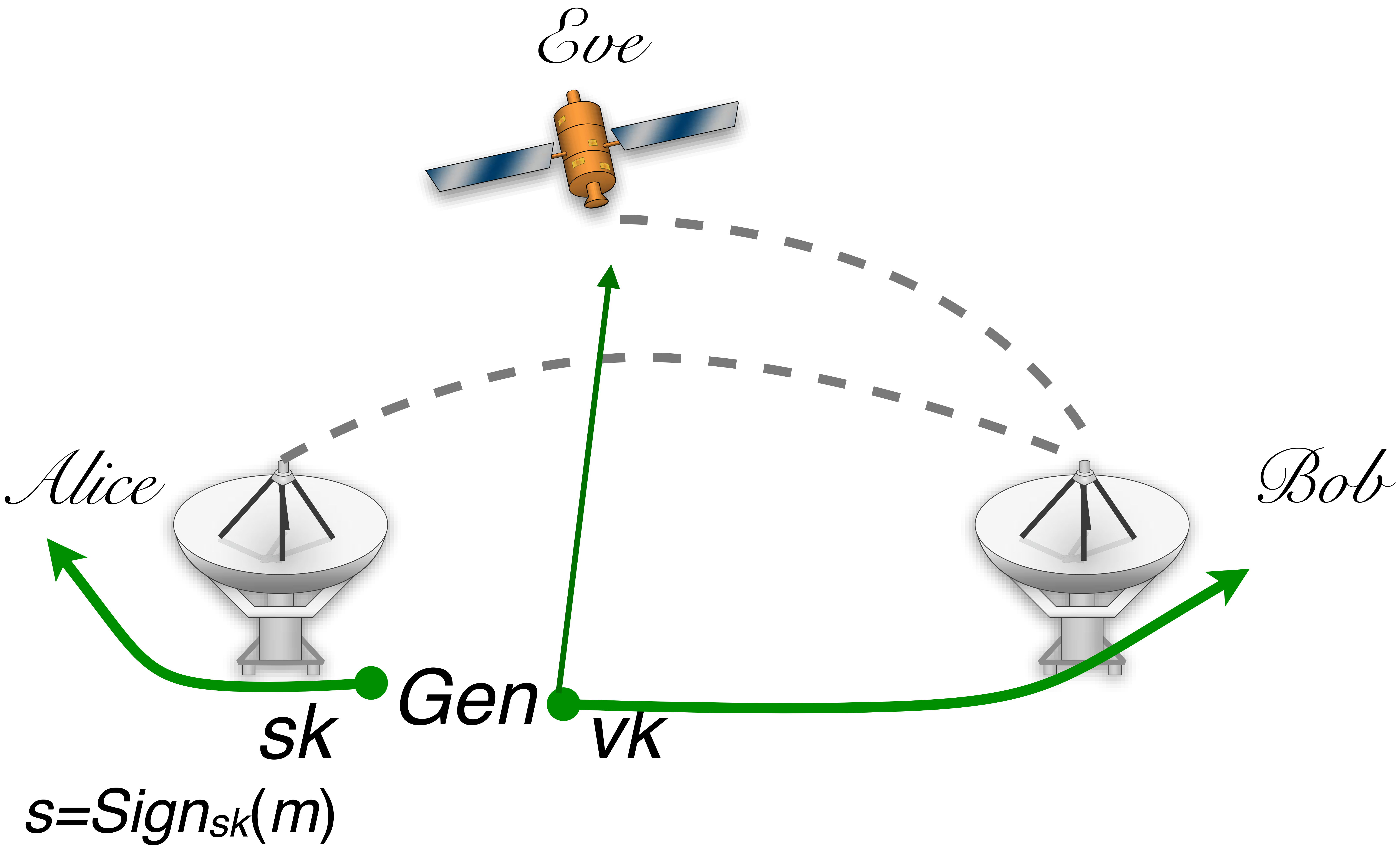
New Problem



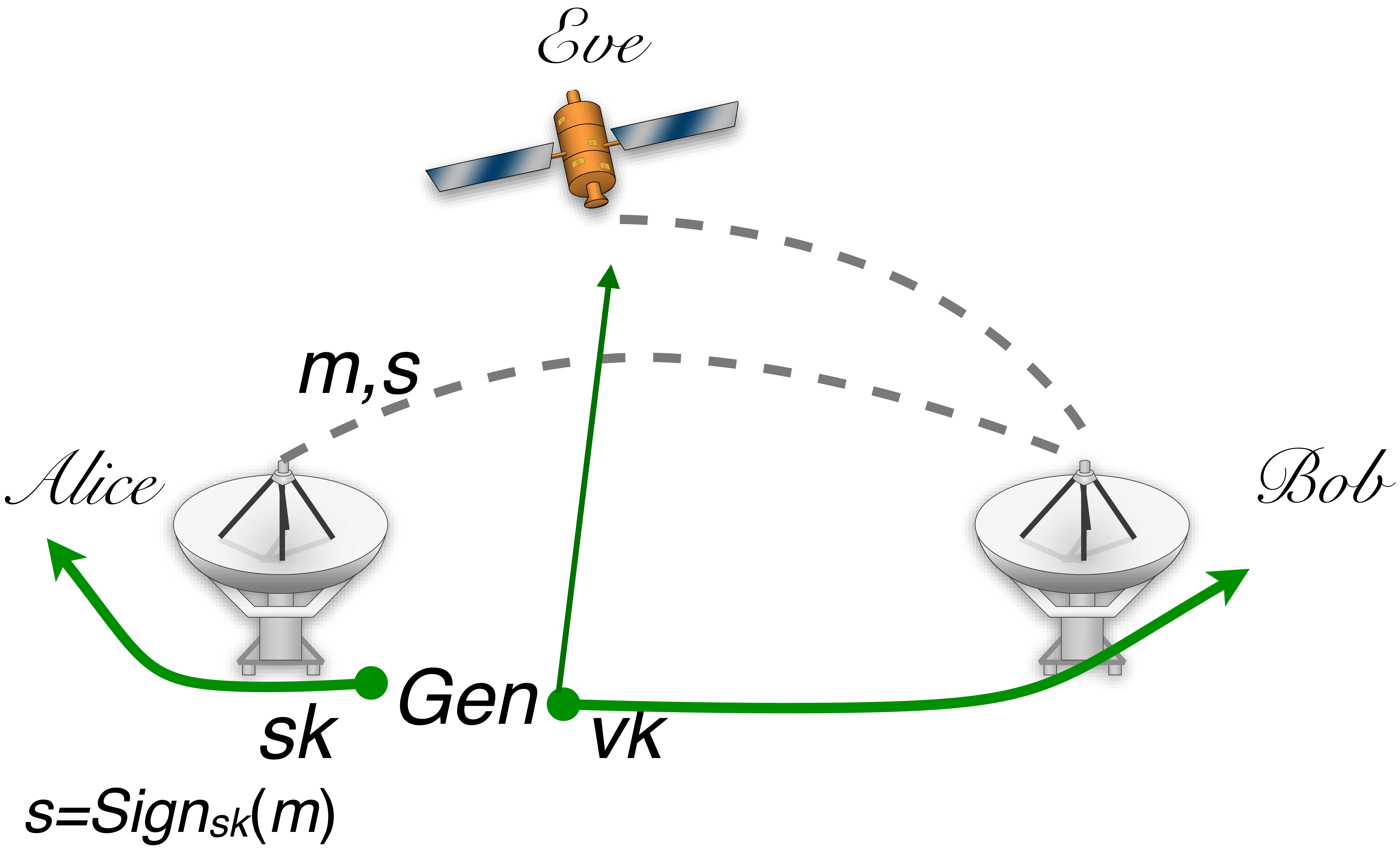
Public key digital signature



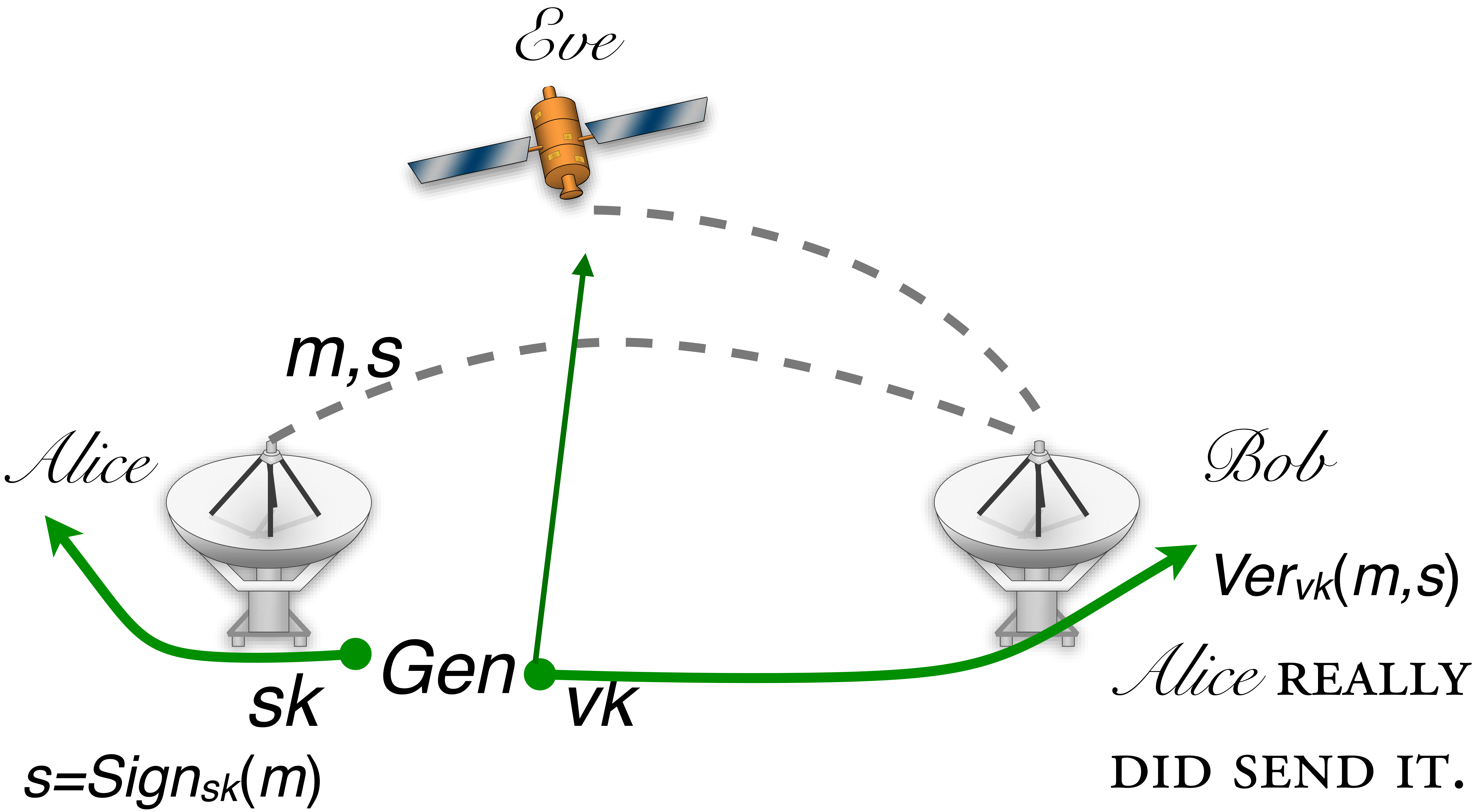
Public key digital signature



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

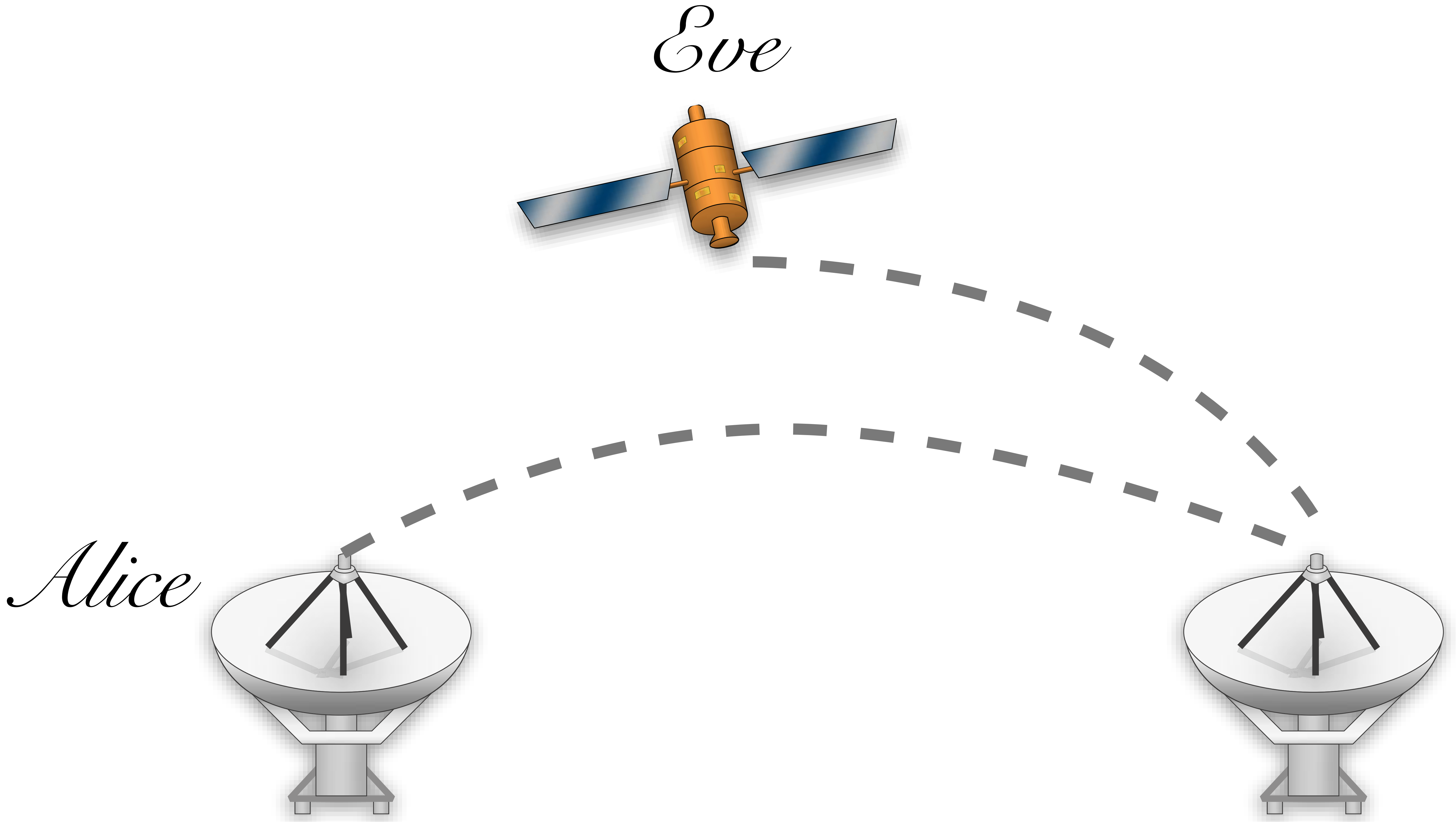
$$\Pr[k \leftarrow Gen(1^n) : Ver_{vk}(m, Sign_{sk}(m)) = 1] = 1$$

existential unforgability

"EVEN WHEN GIVEN A SIGNING ORACLE,

AN ADVERSARY CANNOT FORGE A SIGNATURE FOR

ANY MESSAGE OF ITS CHOOSING"

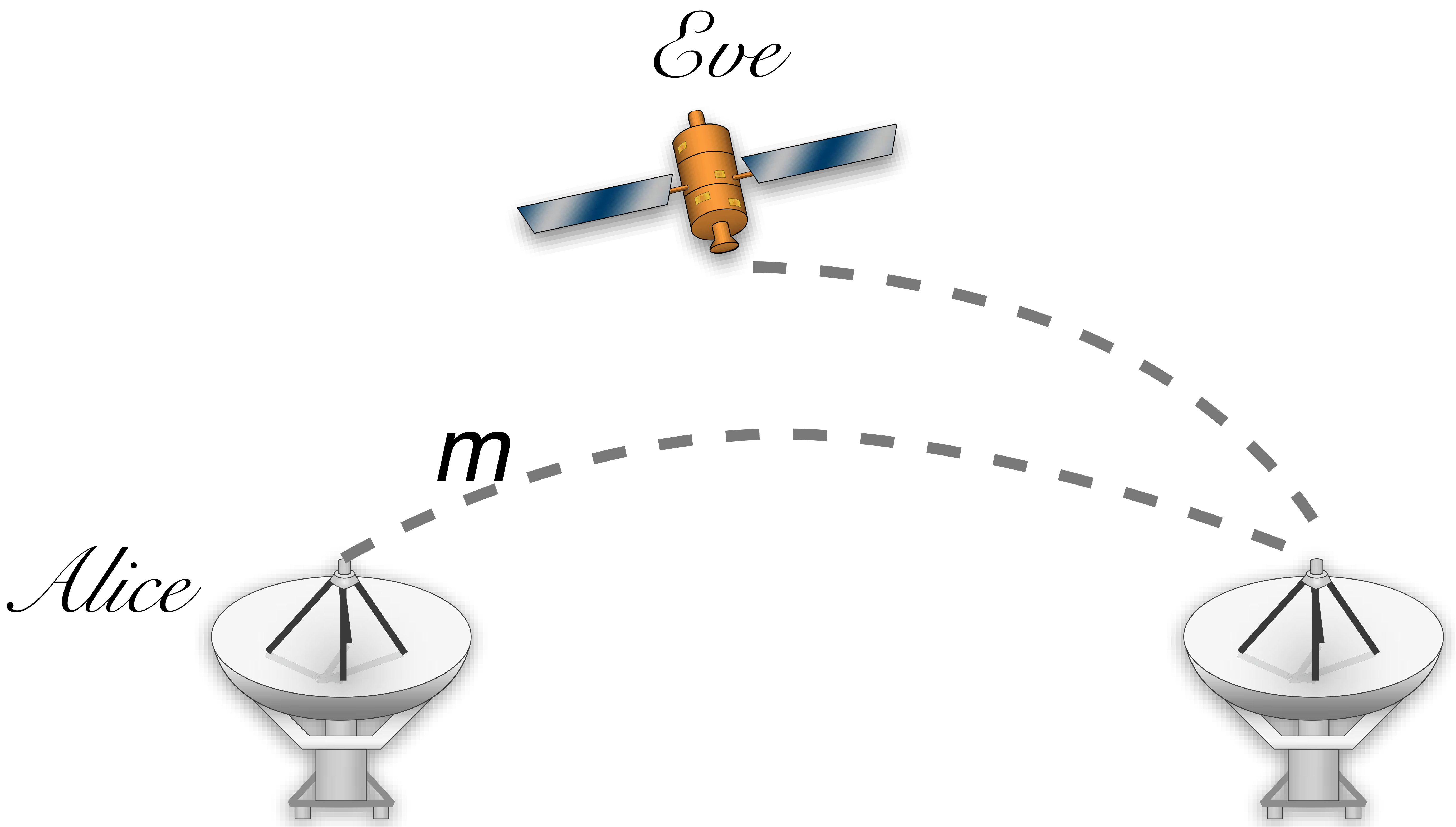


existential unforgability

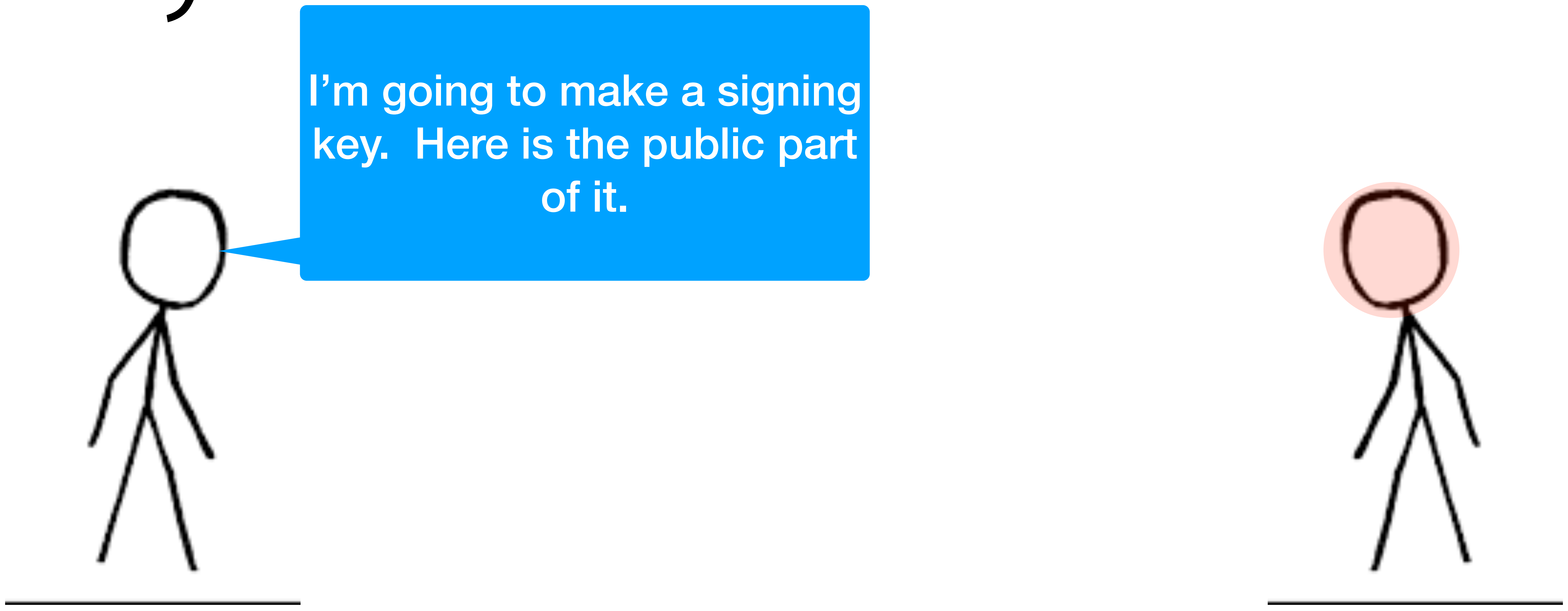
"EVEN WHEN GIVEN A SIGNING ORACLE,

AN ADVERSARY CANNOT FORGE A SIGNATURE FOR

ANY MESSAGE OF ITS CHOOSING"



Signature security



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

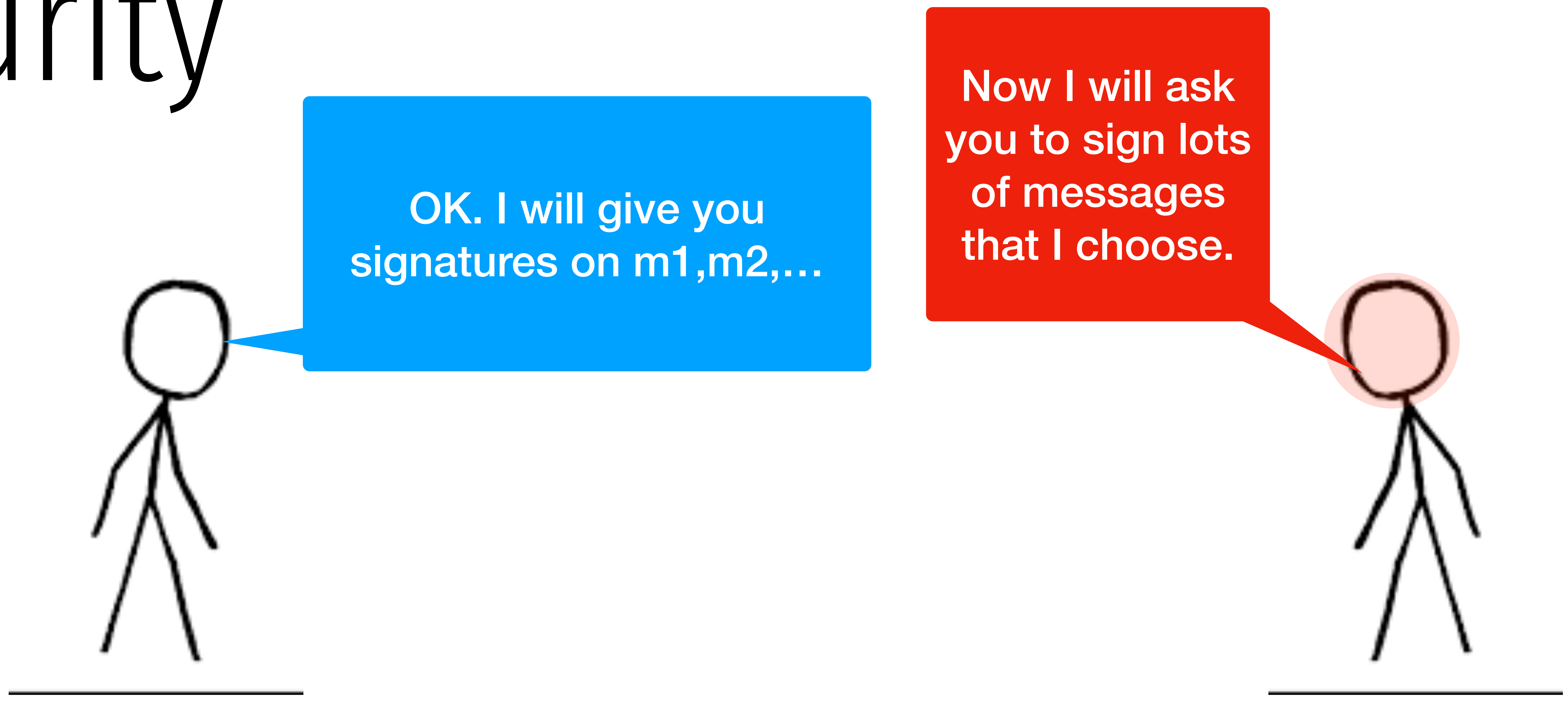
Signature security

$m_0, m_1, \ldots$

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

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

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

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

vk

$s_1, s_2, \ldots$

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