

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!

George

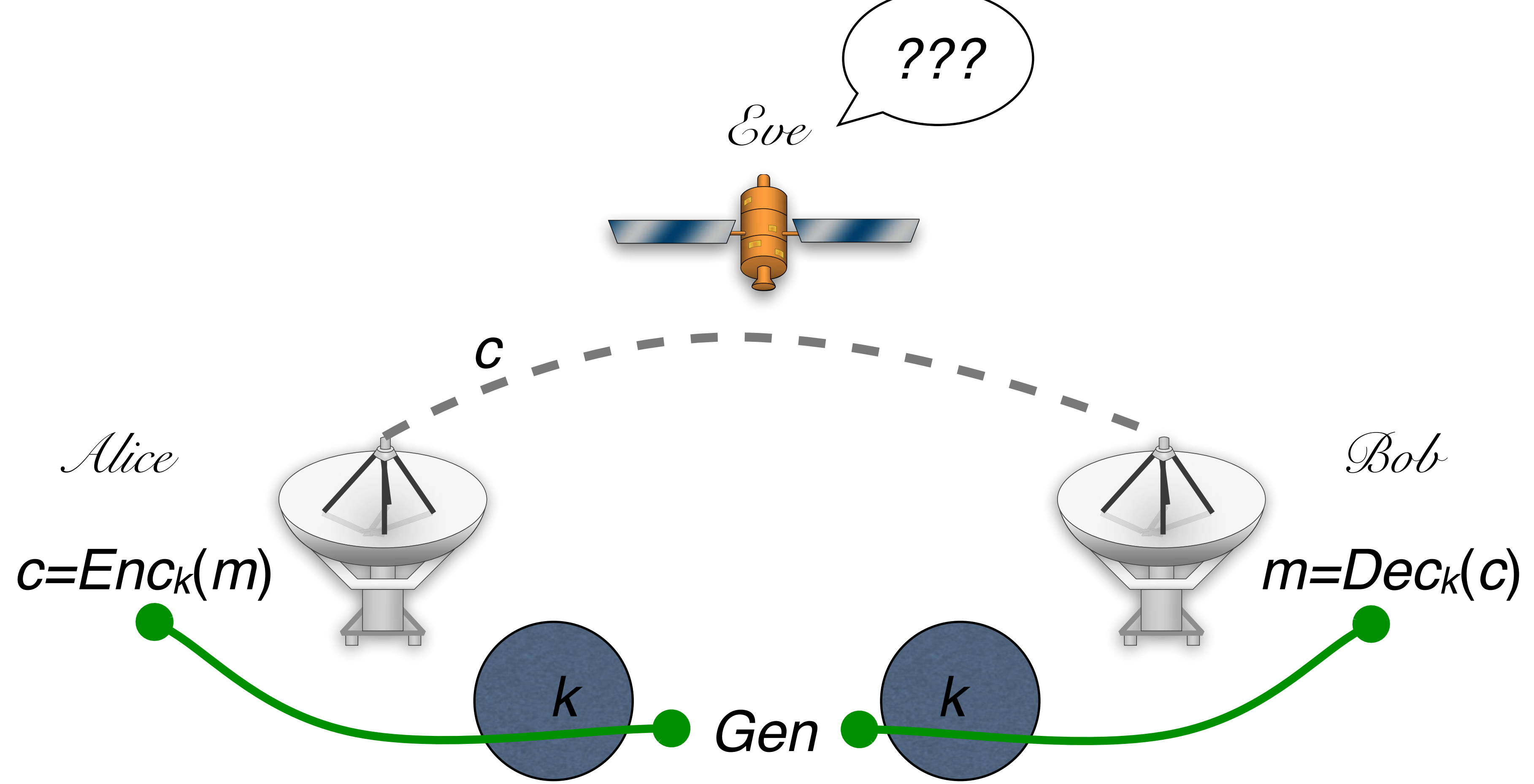
$k_{ga}, k_{gb}, k_{gc}, k_{gd}, k_{ge}, k_{gf}$

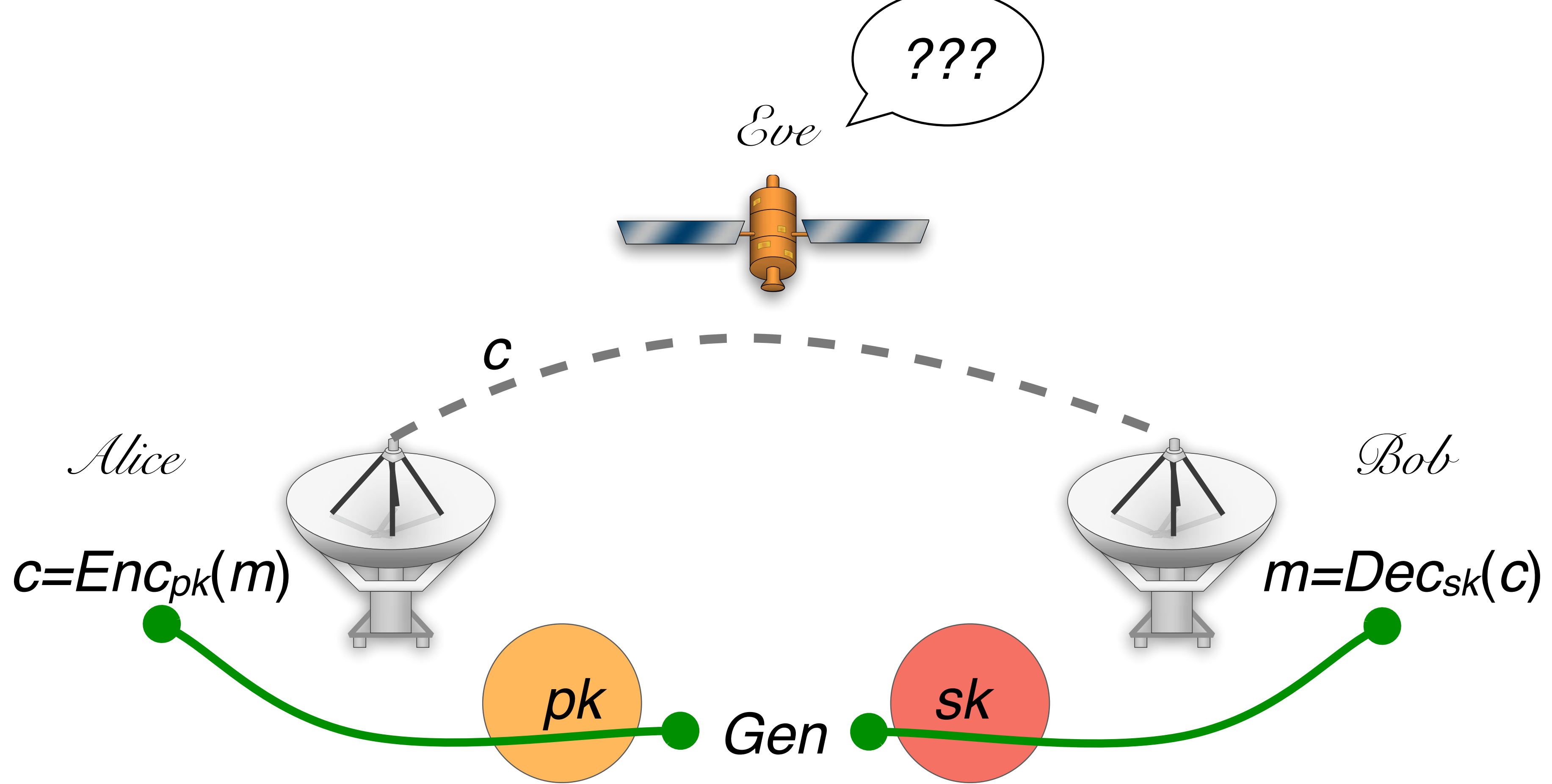
Evan

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

Francis

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





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

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

Are publicly posted

sk_a

George

sk_g

Evan
 sk_e

Francis

sk_f

Public key encryption

Gen Enc Dec

3 algorithms

Gen (key generation)

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

Enc (encryption)

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

Dec (decryption)

Public key encryption

Gen Enc Dec

3 algorithms

Gen (key generation)

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

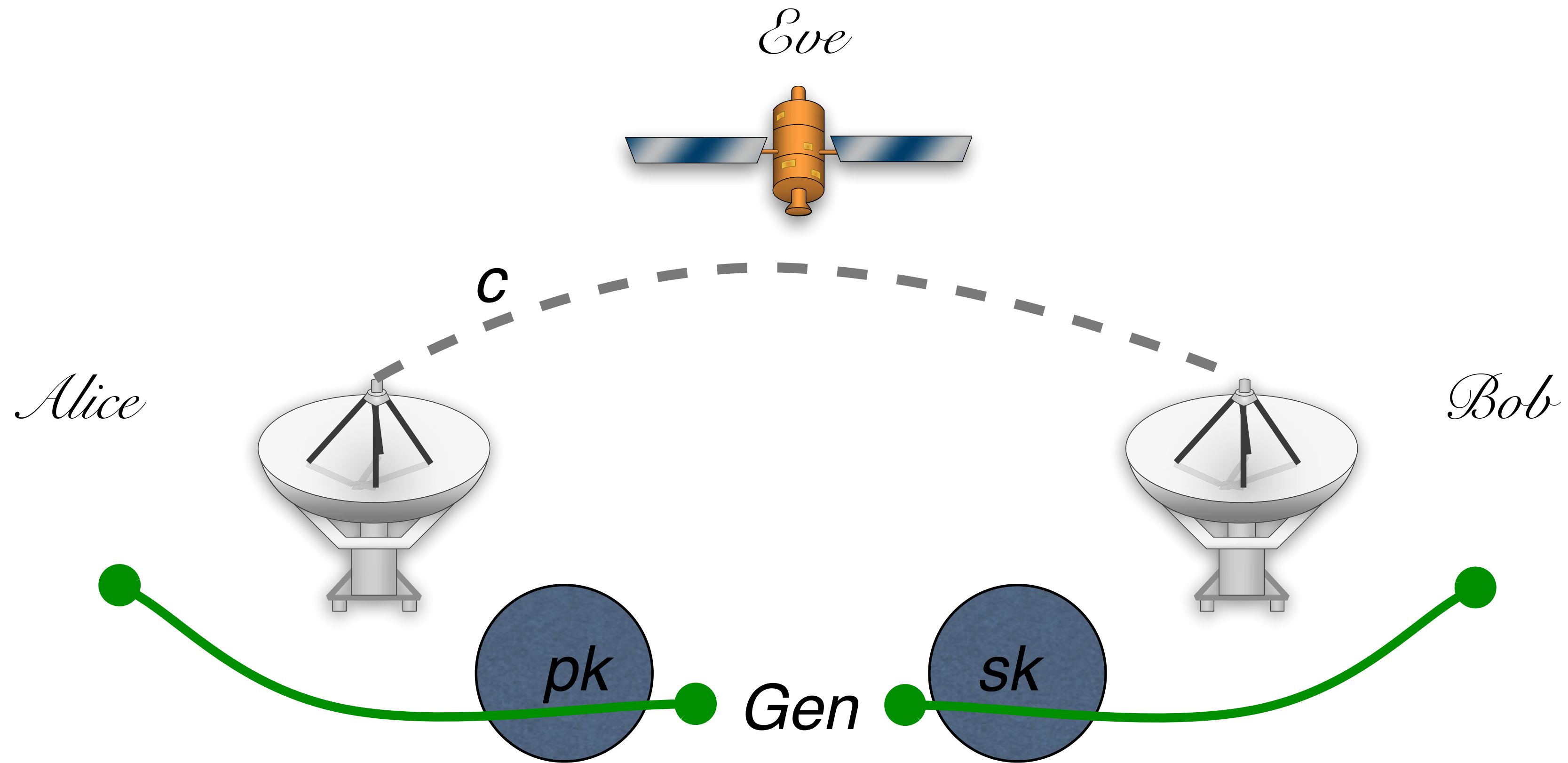
Enc (encryption)

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

Dec (decryption)

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

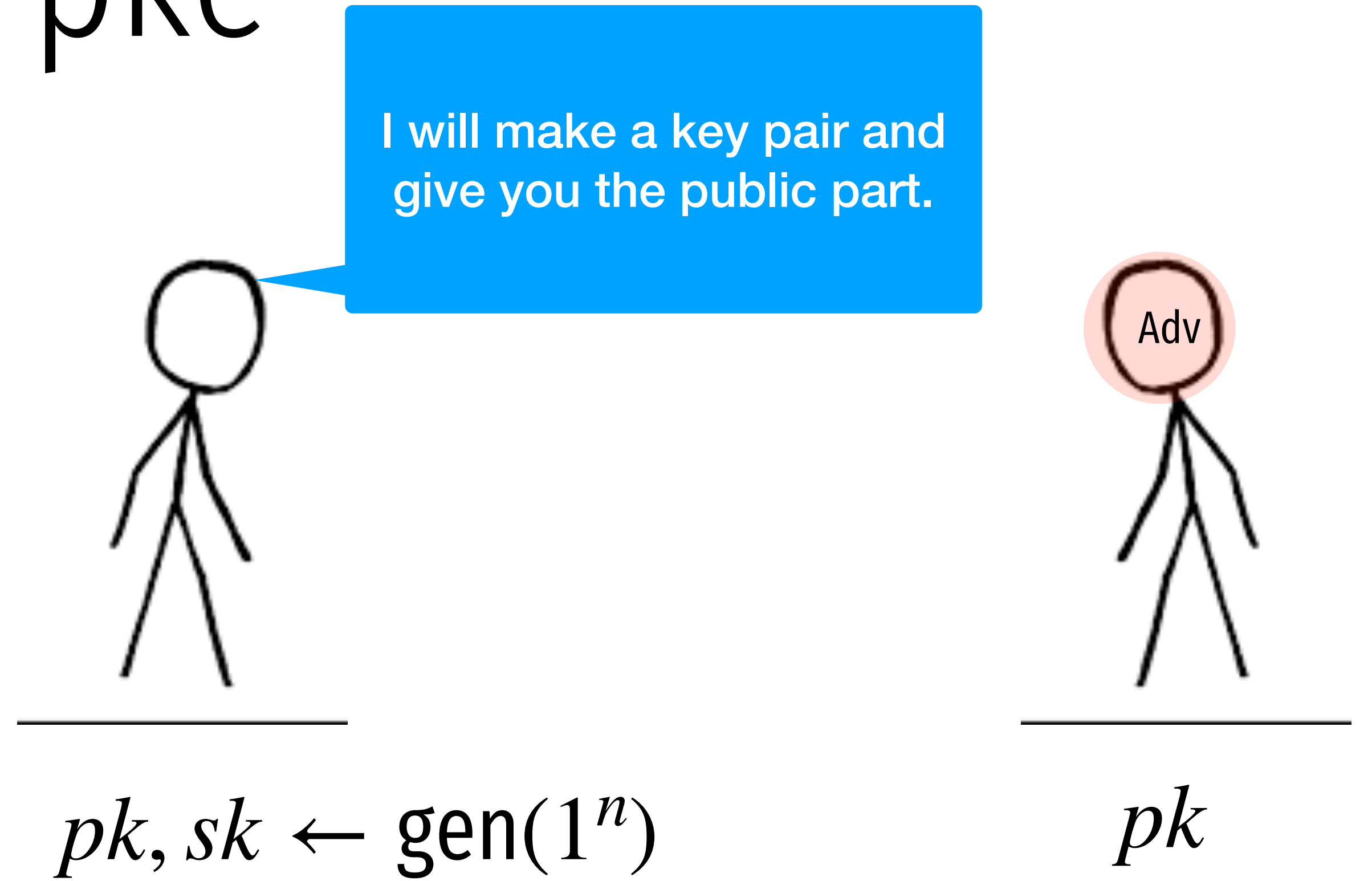
$$\Pr[\text{Dec}_{sk}(\text{Enc}_{pk}(m)) = m] = 1$$



“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)



IND-CPA security for pke

(weakest notion of security)



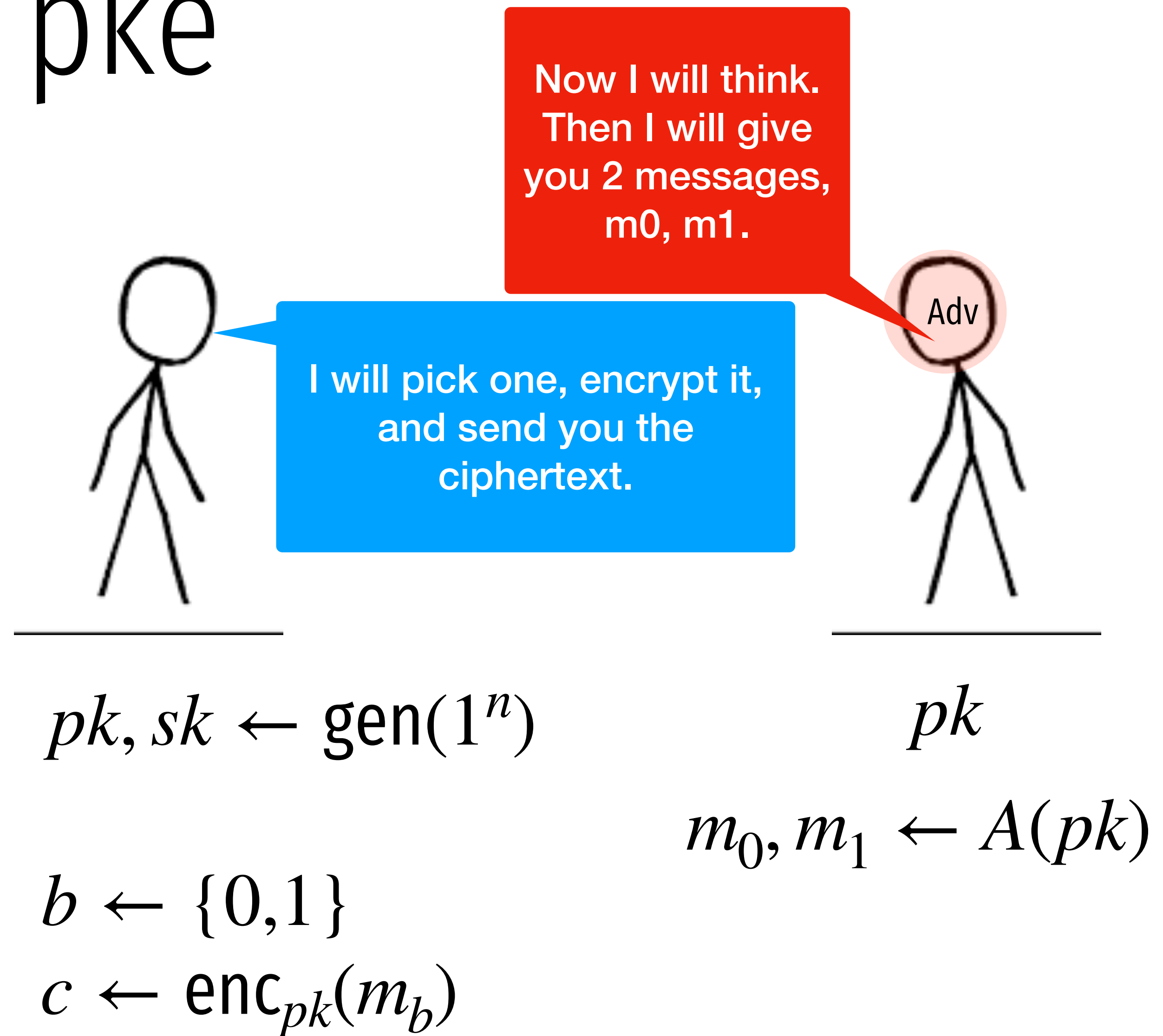
$$pk, sk \leftarrow \text{gen}(1^n)$$

$$pk$$

$$m_0, m_1 \leftarrow A(pk)$$

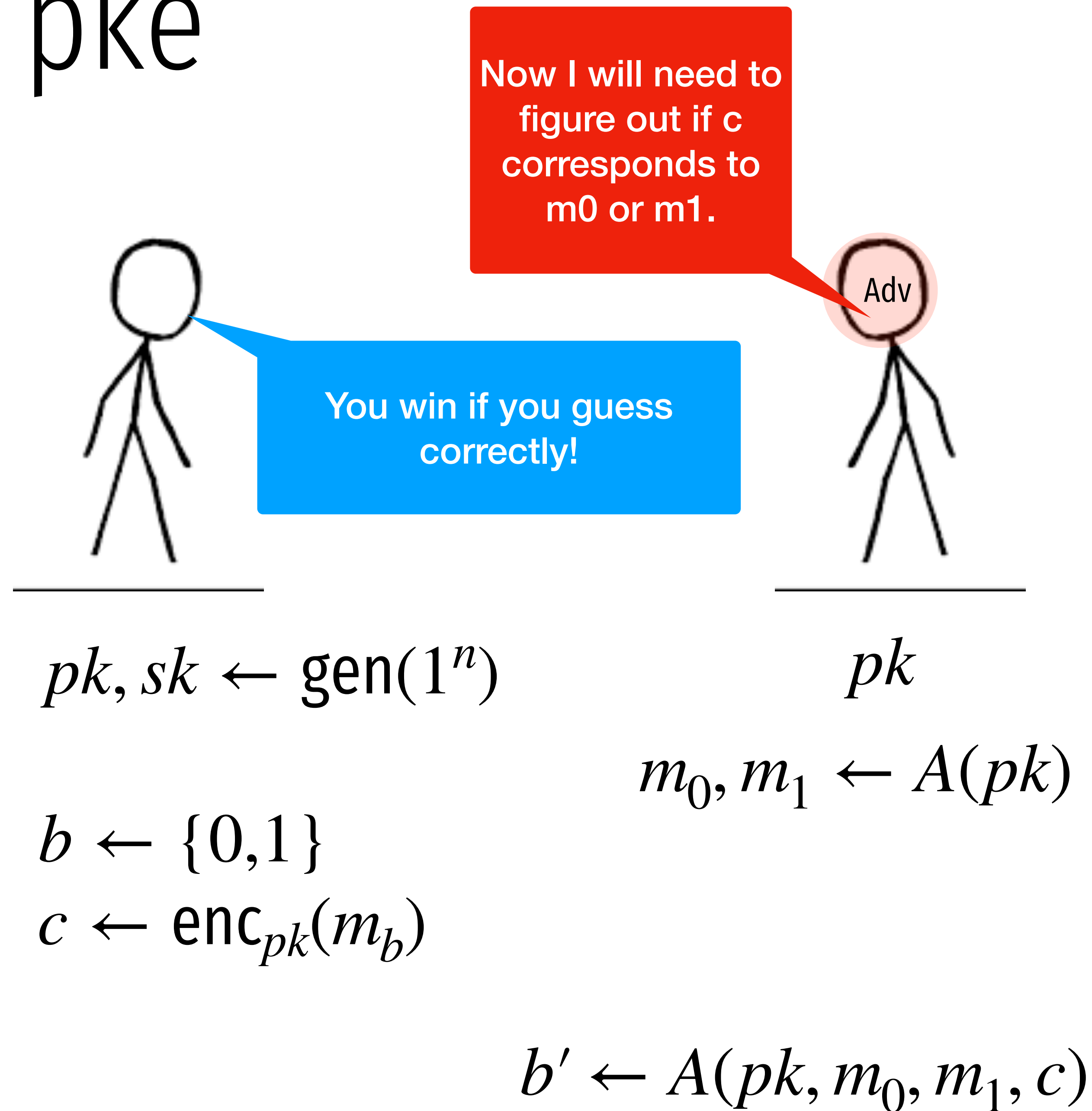
IND-CPA security for pke

(weakest notion of security)



IND-CPA security for pke

(weakest notion of security)



IND-CPA security for pke

(weakest notion of security)

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

$$m_0, m_1 \leftarrow A(pk)$$

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

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

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

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

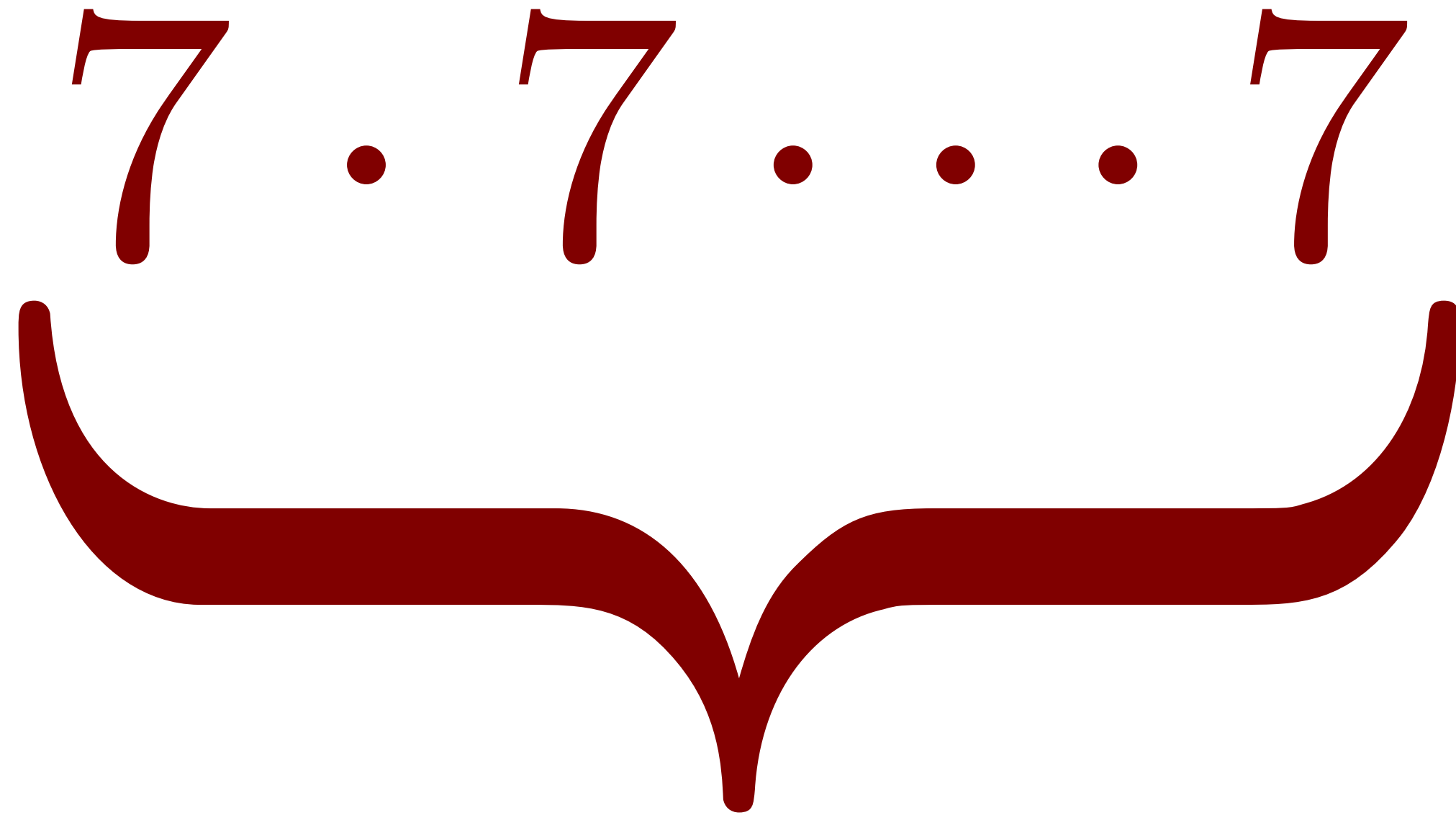
How to build public key encryption?

Basic Number theory

Modular Exponentiation

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

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



19 times

Modular Exponentiation

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

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

Modular Exponentiation

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

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

Modular Exponentiation

$$(a, x, n) \rightarrow a^x \pmod n$$

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

$$7^1$$

$$7^2$$

$$7^4$$

$$7^8$$

$$7^{16}$$

(mod 31)

Modular Exponentiation

$$(a, x, n) \rightarrow a^x \pmod{n}$$

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

$$7^1$$

$$7^2$$

$$7^4$$

$$7^8$$

$$7^{16}$$

(mod 31)

7

18

14

10

7

Modular Exponentiation

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

Algorithm 2: ModularExponentiation(a, x, n)

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

```
1  $r \leftarrow 1$ 
2 while  $x > 0$  do
3   if  $x$  is odd then
4      $r \leftarrow r \cdot a \bmod n$ 
5    $x \leftarrow \lfloor x/2 \rfloor$ 
6    $a \leftarrow a^2 \bmod n$ 
7 Return  $r$ 
```

Modular Exponentiation

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

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

Algorithm 2: ModularExponentiation(a, x, n)

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

```
1  $r \leftarrow 1$ 
2 while  $x > 0$  do
3   if  $x$  is odd then
4      $r \leftarrow r \cdot a \bmod n$ 
5    $x \leftarrow \lfloor x/2 \rfloor$ 
6    $a \leftarrow a^2 \bmod n$ 
7 Return  $r$ 
```

Greatest Common Divisor

$$\text{GCD}(A, B) = \text{GCD}(\quad \quad \quad)$$

Greatest Common Divisor

$$\text{GCD}(A, B) = \text{GCD}(B, A \bmod B)$$

Greatest Common Divisor

GCD (6809 , 1641)

Greatest Common Divisor

$$\text{GCD}(6809, 1641)$$

$$\text{GCD}(1641, 245)$$

$$\text{GCD}(245, 171)$$

$$\text{GCD}(171, 74)$$

$$\text{GCD}(74, 23)$$

$$\text{GCD}(23, 5)$$

$$\text{GCD}(5, 3)$$

$$\text{GCD}(3, 2)$$

$$\text{GCD}(2, 1)$$

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

$$1641 = 6 \cdot 245 + 171$$

$$245 = 1 \cdot 171 + 74$$

$$171 = 2 \cdot 74 + 23$$

$$74 = 3 \cdot 23 + 5$$

$$23 = 4 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

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. $ax + by = \gcd(a, b)$

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

2 | Return $(0, 1)$

3 **else**

4 | $(x, y) \leftarrow \text{ExtendedEuclid}(b, a \bmod b)$

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

Greatest Common Divisor

$$\text{GCD}(6809, 1641)$$

$$\text{GCD}(1641, 245)$$

$$\text{GCD}(245, 171)$$

$$\text{GCD}(171, 74)$$

$$\text{GCD}(74, 23)$$

$$\text{GCD}(23, 5)$$

$$\text{GCD}(5, 3)$$

$$\text{GCD}(3, 2) \quad (1, 0 - 1*1)$$

$$\text{GCD}(2, 1) \quad (0, 1)$$

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

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

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

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

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

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

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

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

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

Greatest Common Divisor

$$\text{GCD}(6809, 1641)$$

$$\text{GCD}(1641, 245)$$

$$\text{GCD}(245, 171)$$

$$\text{GCD}(171, 74)$$

$$\text{GCD}(74, 23)$$

$$\text{GCD}(23, 5)$$

$$\text{GCD}(5, 3)$$

$$\text{GCD}(3, 2)$$

$$\text{GCD}(2, 1)$$

$$(0, 1)$$

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

$$1641 = 6 \cdot 245 + 171$$

$$245 = 1 \cdot 171 + 74$$

$$171 = 2 \cdot 74 + 23$$

$$74 = 3 \cdot 23 + 5$$

$$23 = 4 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Greatest Common Divisor

$$\text{GCD}(6809, 1641)$$

$$\text{GCD}(1641, 245)$$

$$\text{GCD}(245, 171)$$

$$\text{GCD}(171, 74)$$

$$\text{GCD}(74, 23)$$

$$\text{GCD}(23, 5)$$

$$\text{GCD}(5, 3)$$

$$\text{GCD}(3, 2) \quad (1, 0 - 1*1)$$

$$\text{GCD}(2, 1) \quad (0, 1)$$

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

$$1641 = 6 \cdot 245 + 171$$

$$245 = 1 \cdot 171 + 74$$

$$171 = 2 \cdot 74 + 23$$

$$74 = 3 \cdot 23 + 5$$

$$23 = 4 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Greatest Common Divisor

$$\text{GCD}(6809, 1641)$$

$$\text{GCD}(1641, 245)$$

$$\text{GCD}(245, 171)$$

$$\text{GCD}(171, 74)$$

$$\text{GCD}(74, 23)$$

$$\text{GCD}(23, 5)$$

$$\text{GCD}(5, 3)$$

$$\text{GCD}(3, 2)$$

$$\text{GCD}(2, 1)$$

$$(1, -1)$$

$$(0, 1)$$

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

$$1641 = 6 \cdot 245 + 171$$

$$245 = 1 \cdot 171 + 74$$

$$171 = 2 \cdot 74 + 23$$

$$74 = 3 \cdot 23 + 5$$

$$23 = 4 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Greatest Common Divisor

$$\text{GCD}(6809, 1641)$$

$$\text{GCD}(1641, 245)$$

$$\text{GCD}(245, 171)$$

$$\text{GCD}(171, 74)$$

$$\text{GCD}(74, 23)$$

$$\text{GCD}(23, 5)$$

$$\text{GCD}(5, 3)$$

$$\text{GCD}(3, 2)$$

$$\text{GCD}(2, 1)$$

$$(-1, 2)$$

$$(1, -1)$$

$$(0, 1)$$

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

$$1641 = 6 \cdot 245 + 171$$

$$245 = 1 \cdot 171 + 74$$

$$171 = 2 \cdot 74 + 23$$

$$74 = 3 \cdot 23 + 5$$

$$23 = 4 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Greatest Common Divisor

$$\text{GCD}(6809, 1641)$$

$$\text{GCD}(1641, 245)$$

$$\text{GCD}(245, 171)$$

$$\text{GCD}(171, 74)$$

$$\text{GCD}(74, 23)$$

$$\text{GCD}(23, 5)$$

$$\text{GCD}(5, 3)$$

$$\text{GCD}(3, 2)$$

$$\text{GCD}(2, 1)$$

$$(2, -9)$$

$$(-1, 2)$$

$$(1, -1)$$

$$(0, 1)$$

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

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

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

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

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

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

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

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

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

Greatest Common Divisor

GCD (6809 , 1641)

GCD allows us to
compute modular
inverses.

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

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

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

$$\mathbb{Z}_{15}^\star = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

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

Euler theorem

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

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 $N = p \cdot q$ where p, q are primes.

“Textbook” RSA (insecure)

Pick $N = p \cdot q$ where p, q are primes.

Pick e, d such that $e \cdot d = 1 \pmod{\phi(N)}$

“Textbook” RSA (insecure)

Pick $N = p \cdot q$ where p, q are primes.

Pick e, d such that $e \cdot d = 1 \pmod{\phi(N)}$

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

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

“Textbook” RSA (insecure)

Pick $N = p \cdot q$ where p, q are primes.

Pick e, d such that $e \cdot d = 1 \pmod{\phi(N)}$

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

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

$$(m^e)^d \pmod{N} =$$

Example of Textbook RSA

$m=5$

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

“Textbook” RSA (insecure)

Pick $N = p \cdot q$ where p, q are primes.

Pick e, d such that $e \cdot d = 1 \pmod{\phi(N)}$

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

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

Why is it insecure
against IND-CPA attack?

pkcs1.5

$\text{ENC}_{pk}(m)$

PICK r AS A RANDOM STRING WITH NO 0 s

(TYPICALLY 8 BYTES)

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

“PADDING ORACLE” ATTACK AGAINST THIS SCHEME

RSA-OAEP+

GEN(1^n)

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

ENC_{pk}(m)

$r \leftarrow U_n$

$s \leftarrow R_1(r) \oplus m \parallel R_2(r||m)$

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

$c \leftarrow f(s||t)$

$R_1 : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^n$

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

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

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

www.apple.com Apple Public EV Server RSA CA 2 - G1 DigiCert High Assurance EV Root CA

Subject Name

Business Category	Private Organization
Inc. Country	US
Inc. State/Province	California
Serial Number	C0806592
Country	US
State/Province	California
Locality	Cupertino
Organization	Apple Inc.
Common Name	www.apple.com

Issuer Name

Country	US
Organization	Apple Inc.
Common Name	Apple Public EV Server RSA CA 2 - G1

Validity


Not Before	Fri, 23 Aug 2024 17:30:11 GMT
Not After	Thu, 21 Nov 2024 17:40:11 GMT

Subject Alt Names

DNS Name	www.apple.com
DNS Name	images.apple.com
DNS Name	www.apple.com.cn


Public Key Info


Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	C8:A2:02:8A:C1:1C:A7:9A:EE:58:49:9B:10:3C:41:8D:BF:EF:6F:23:7E:64:05...


 **Safari is using an encrypted connection to www.apple.com.**

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.apple.com.

DigiCert, Inc. has identified www.apple.com as being owned by Apple Inc. in Cupertino, California, US.

 DigiCert High Assurance EV Root CA

 DigiCert SHA2 Extended Validation Server CA-3

 www.apple.com

Serial Number 03 8E 3F 9E 09 D7 ED C7 B1 80 3F 74 A7 4C 35 AB

Version 3

Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.1)

Parameters None

Not Valid Before Tuesday, October 6, 2020 at 8:00:00 PM Eastern Daylight Time

Not Valid After Friday, October 8, 2021 at 8:00:00 AM Eastern Daylight Time

Public Key Info


Algorithm RSA Encryption (1.2.840.113549.1.1.1)

Parameters None

Public Key 256 bytes : CA 1B 1C 21 78 15 3D 40 CF A3 79 3F 9D CF B2 53 AB A9 41 FF 3E 06 A1 29 69 8A 04 46 9E FB C4 0D 56 7A CA E6 80 E7 AF C6 C0 BF 8B 60 71 CA 9A E8 76 0C 06 C8 9B 77 B8 F3 1B EA 7E E7 3A 84 CB A3 88 A5 93 04 3F 69 66 77 CF AE 06 D1 D9 E1 10 08 7A E0 24 98 E7 56 97 0F 73 68 7B 4D 69 46 28 26 FF 05 81 0C C0 DA FC 21 71 81 65 9A 39 C9 E9 68 36 36 02 5F 81 80 B7 7E 8A 5B FE 34 D0 CE 76 2D D9 8B 3E D4 13 C0 EC EB 0F 2C 77 AD 1E 7B 20 F6 DA 92 98 FD 89 F3 A7 CB 53 16 2E B0 B9 62 BE C8 C3 28 40 CF 8C 5C 61 77 8F 92 3D 2F 23 F2 0A AB 65 82 22 B8 98 CE BA C8 00 95 E4 67 34 6E 76 E5 D1 D3 2D 51 91 BC EF C0 C8 DE F8 7B CC 46 45 00 76 D9 CB 30 31 E9 56 FD 0E 68 F4 36 F9 1B 5F 88 61 62 8F 60 A8 DE 43 7B 5C C1 15 73 D4 06 12 6E 85 9B 50 9C 24 BF 5F FC F4 68 95 67 D5 BF 44 71

Exponent 65537

Key Size 2,048 bits

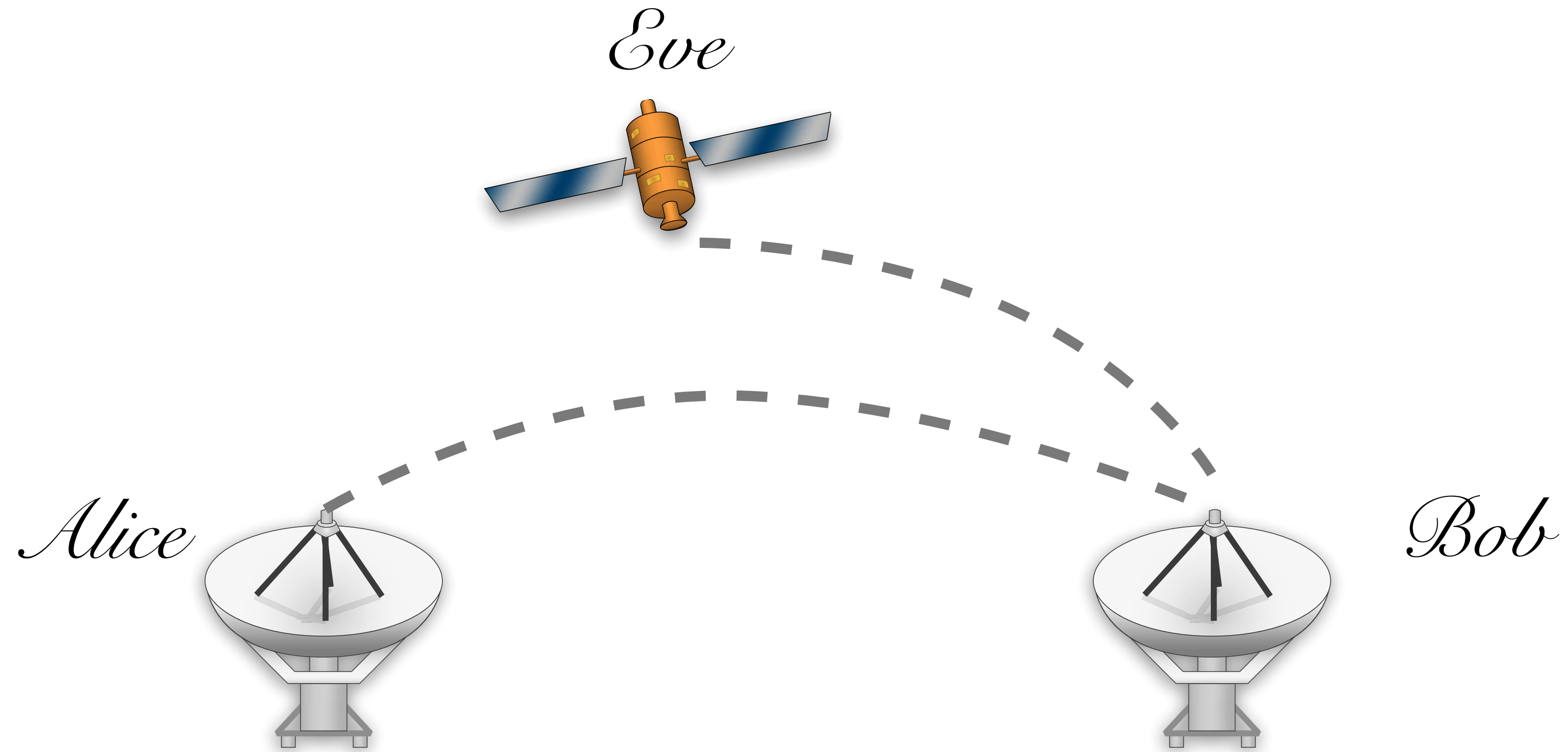


Very old problem

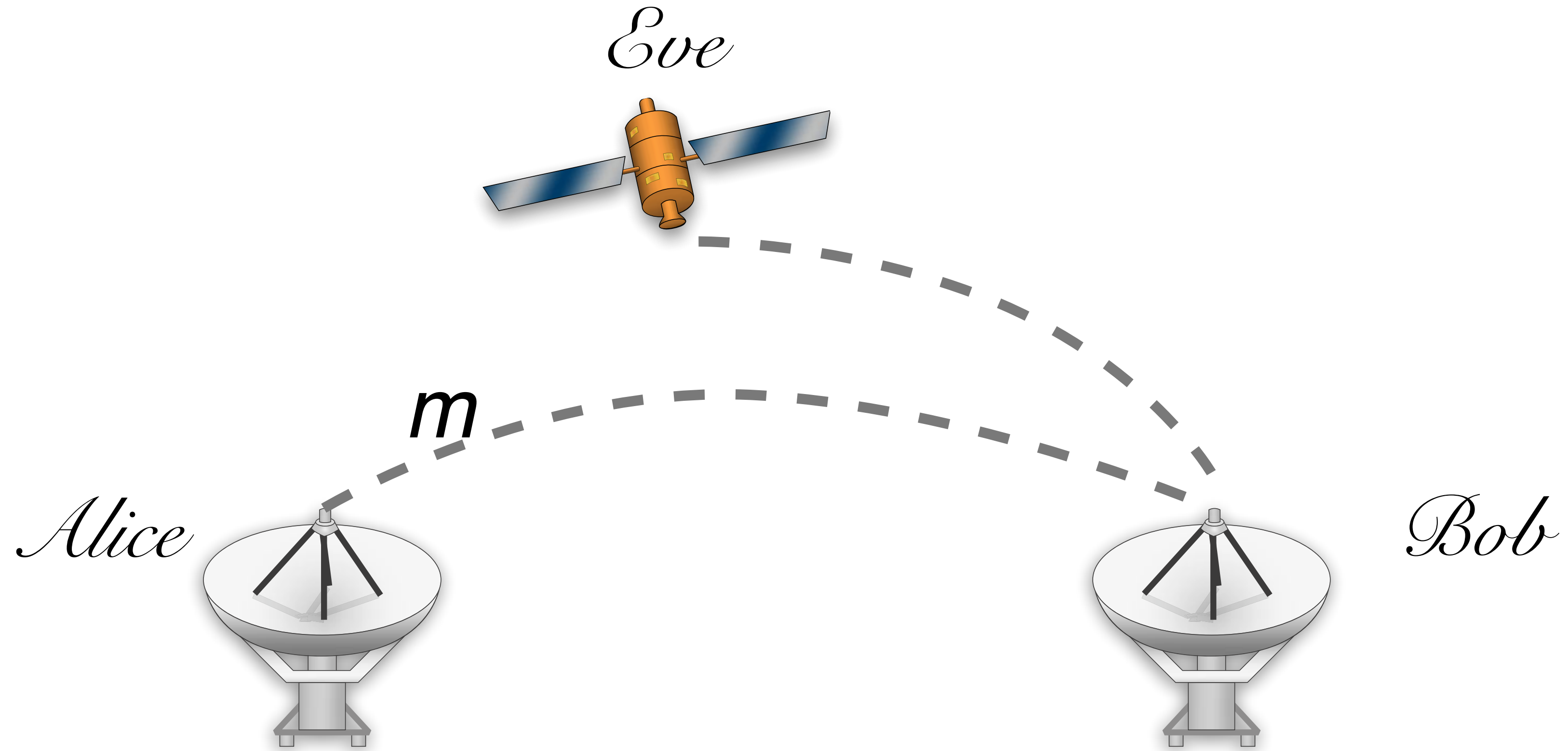
John Hancock



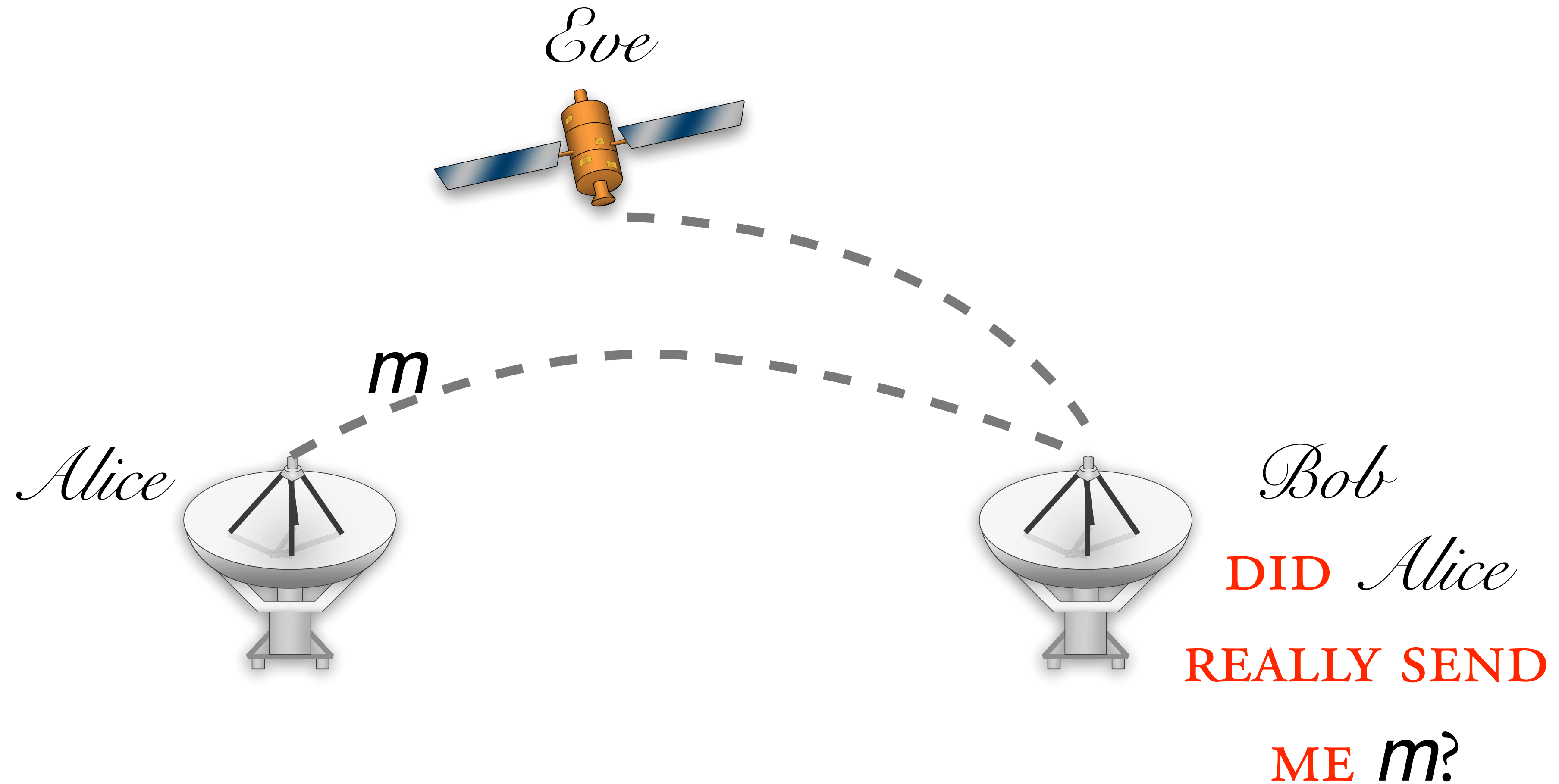
New Problem



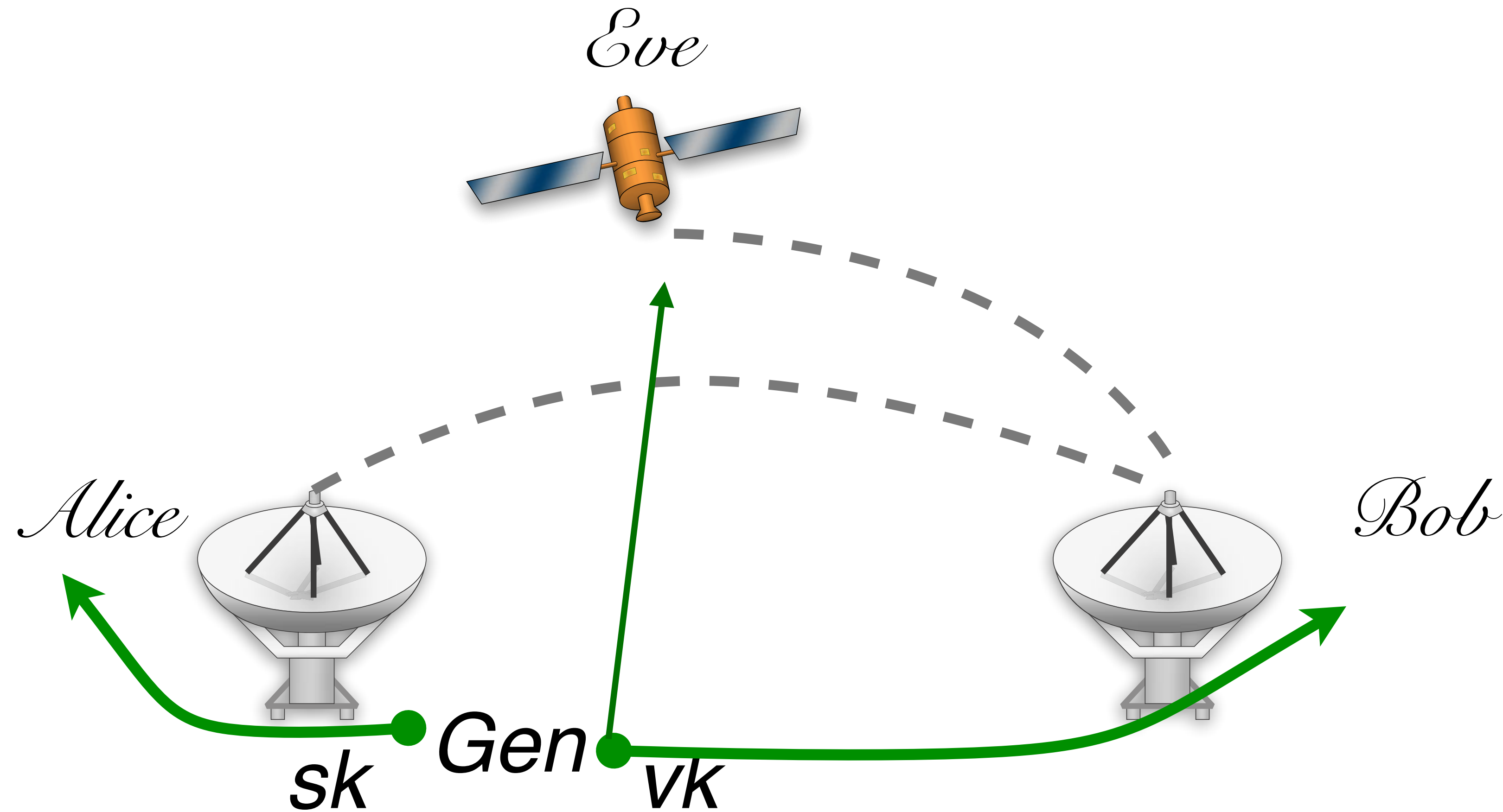
New Problem



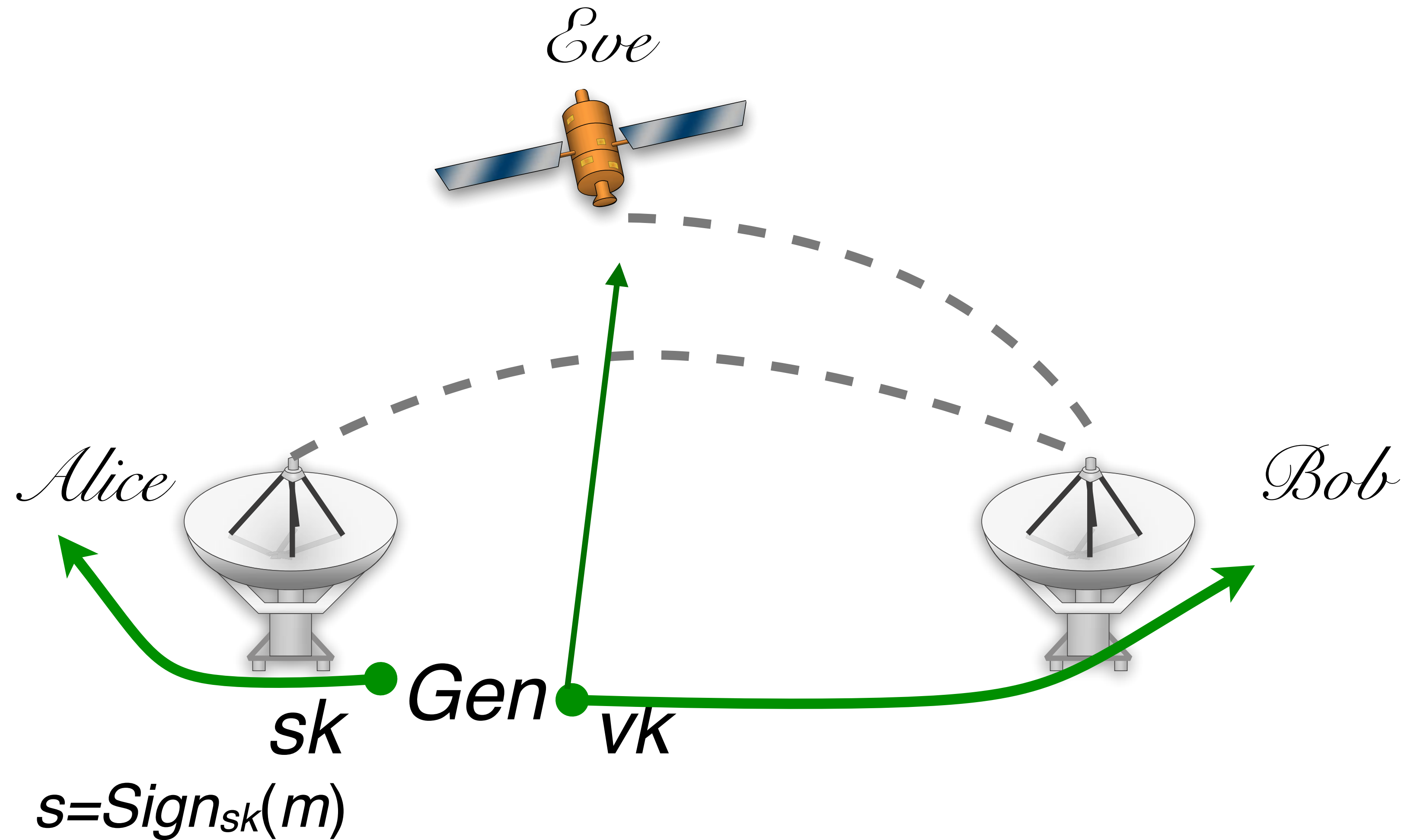
New Problem



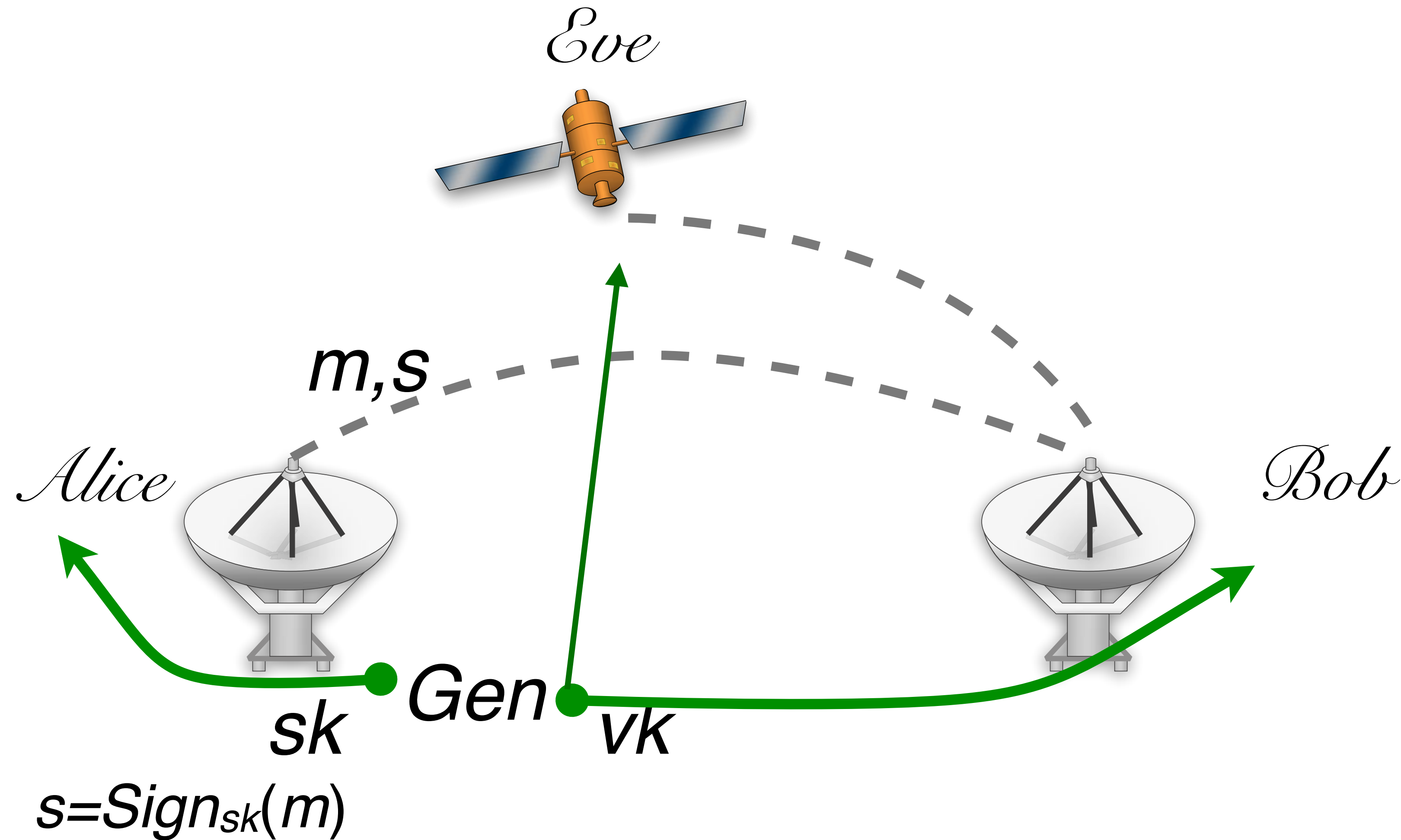
Public key digital signature



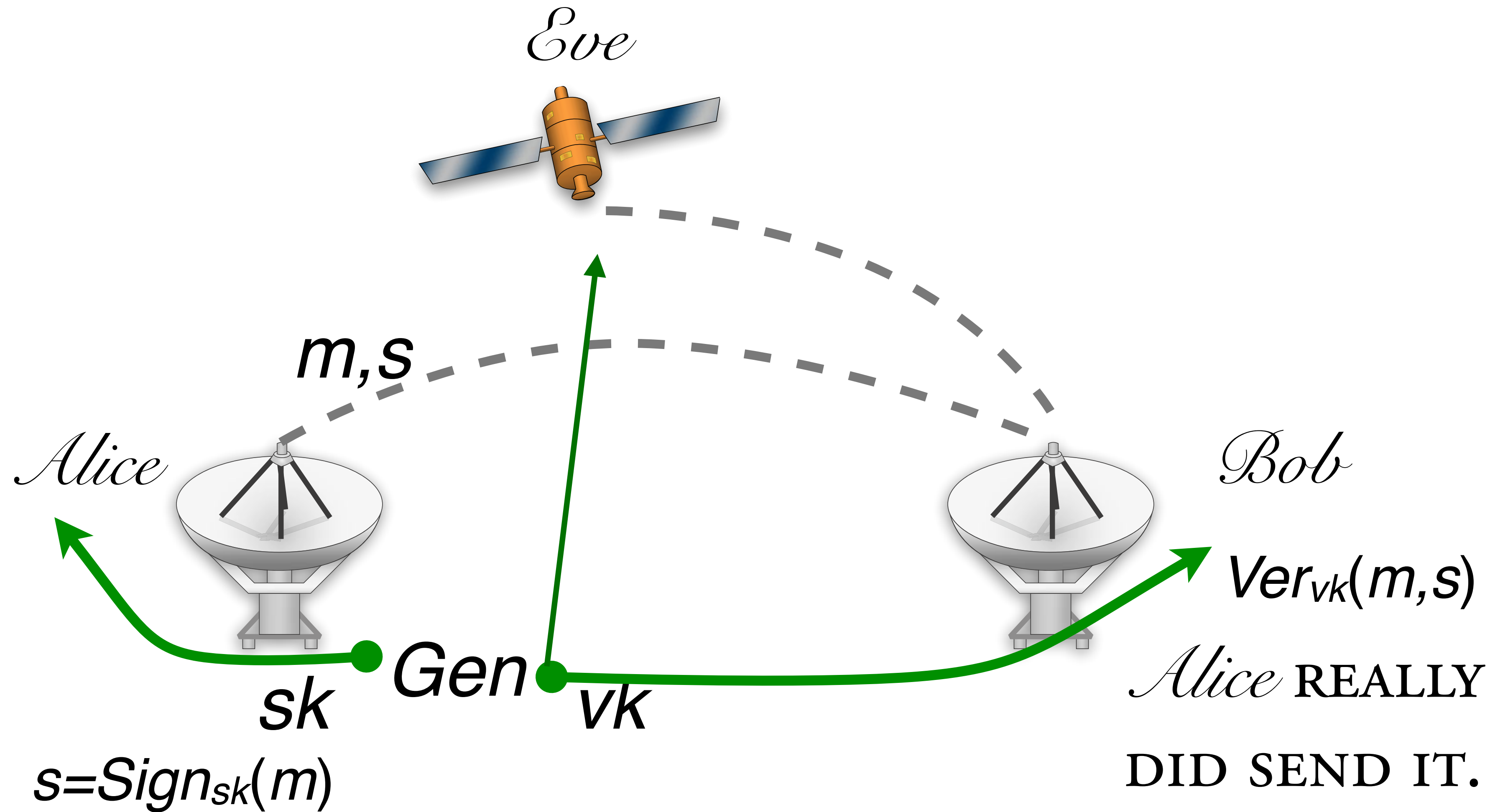
Public key digital signature



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

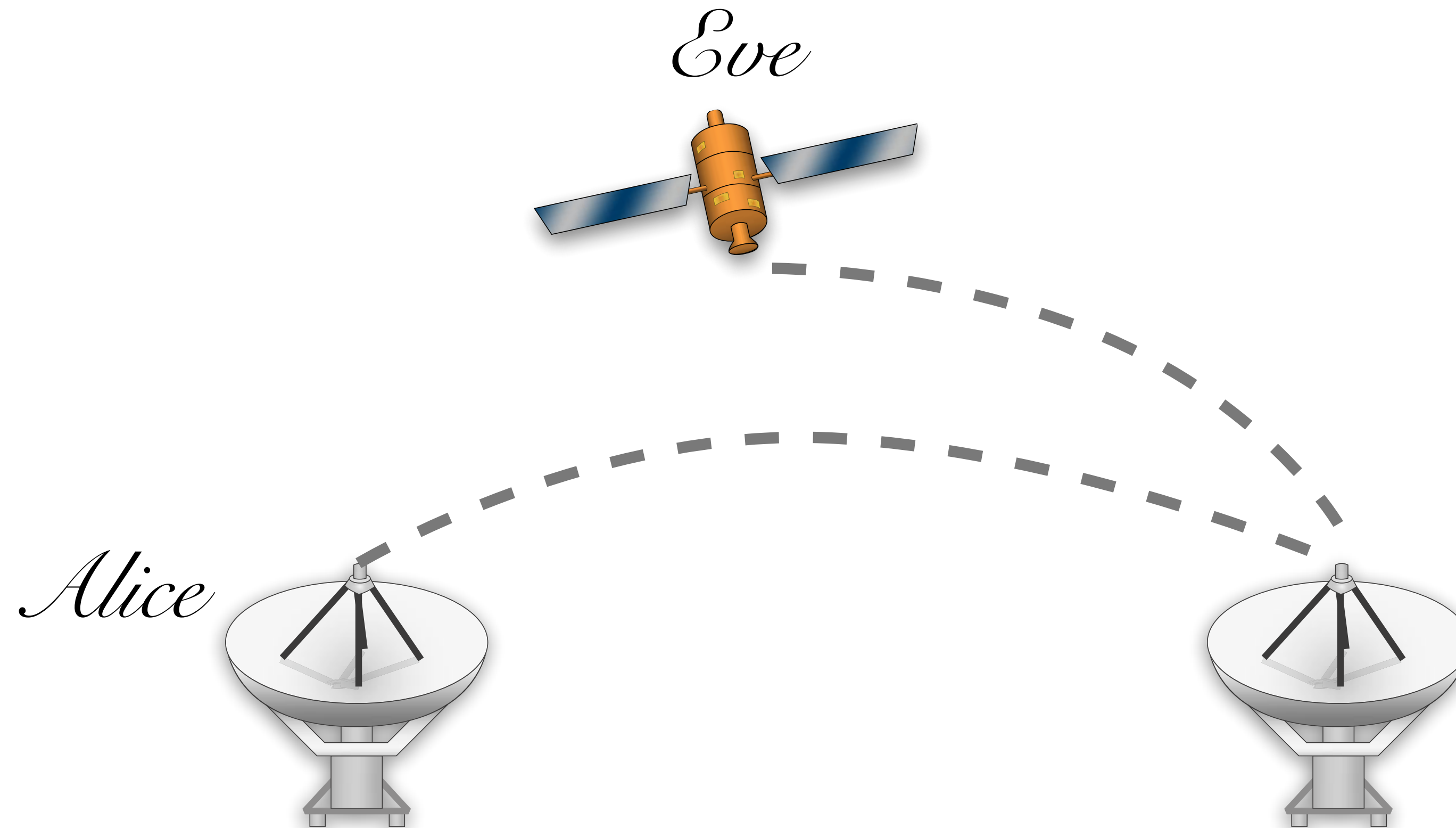
Sign _{sk} (m) GENERATES A **SIGNATURE** **S** FOR
 $m \in \mathcal{M}_n$

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

$$\Pr[k \leftarrow \text{Gen}(1^n) : \text{Ver}_{vk}(m, \text{Sign}_{sk}(m)) = 1] = 1$$

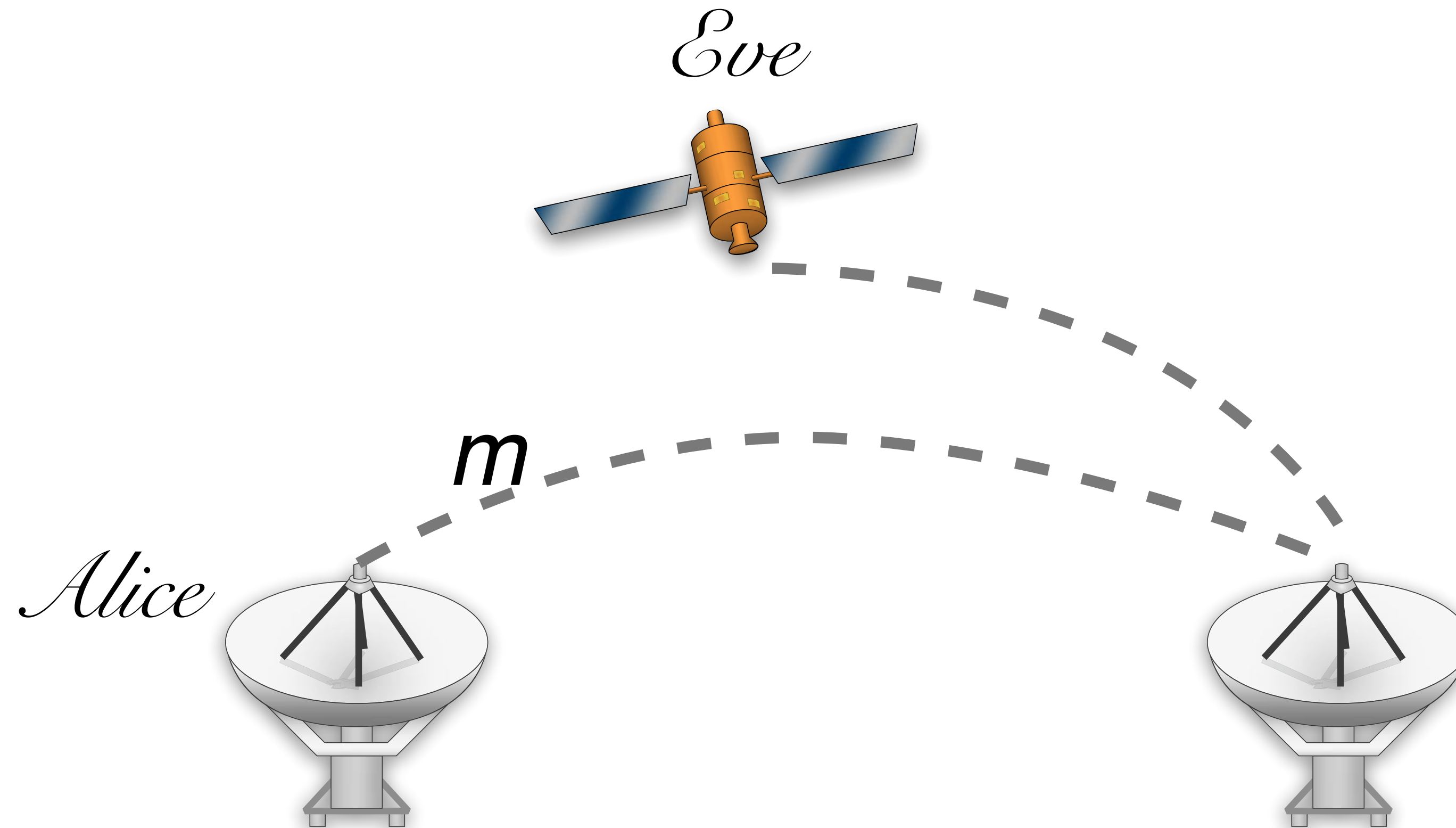
existential unforgeability

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

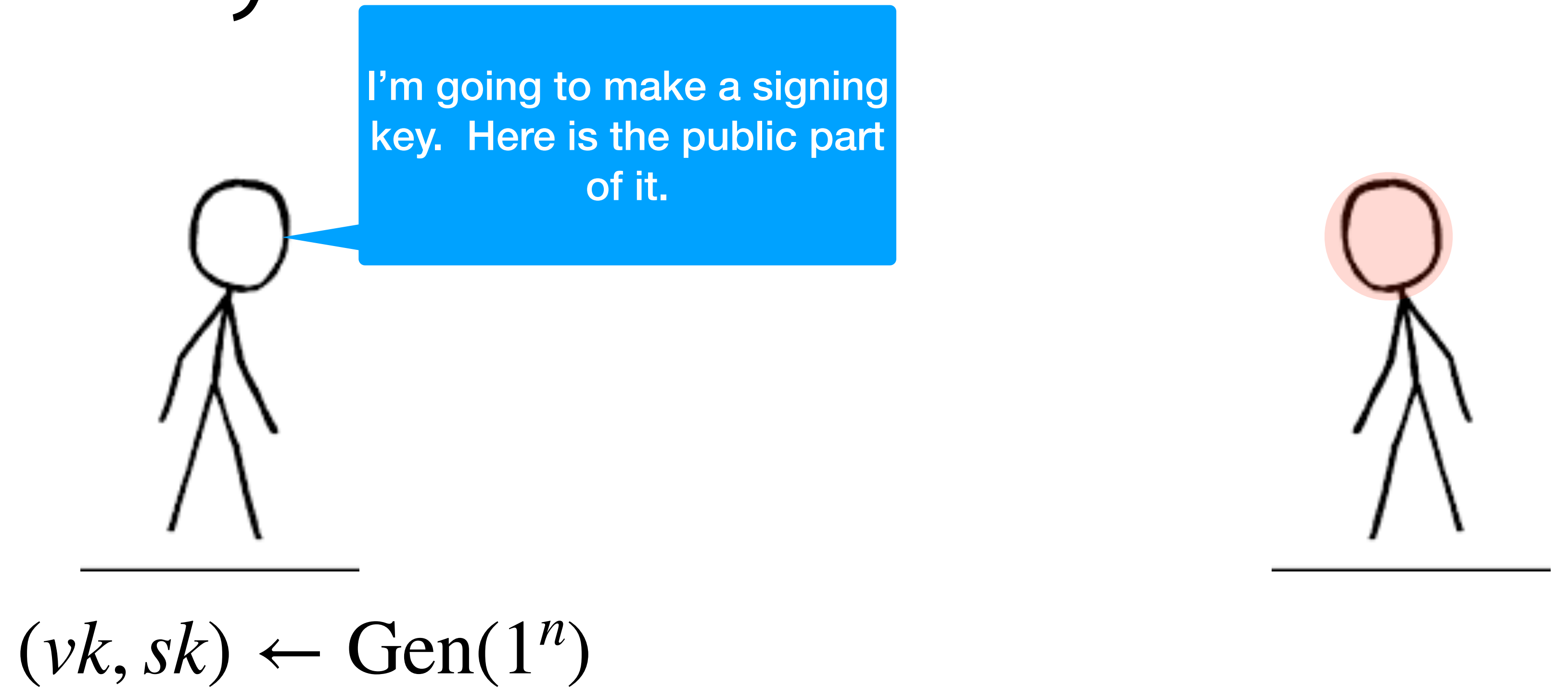


existential unforgeability

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



Signature security



Signature security



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

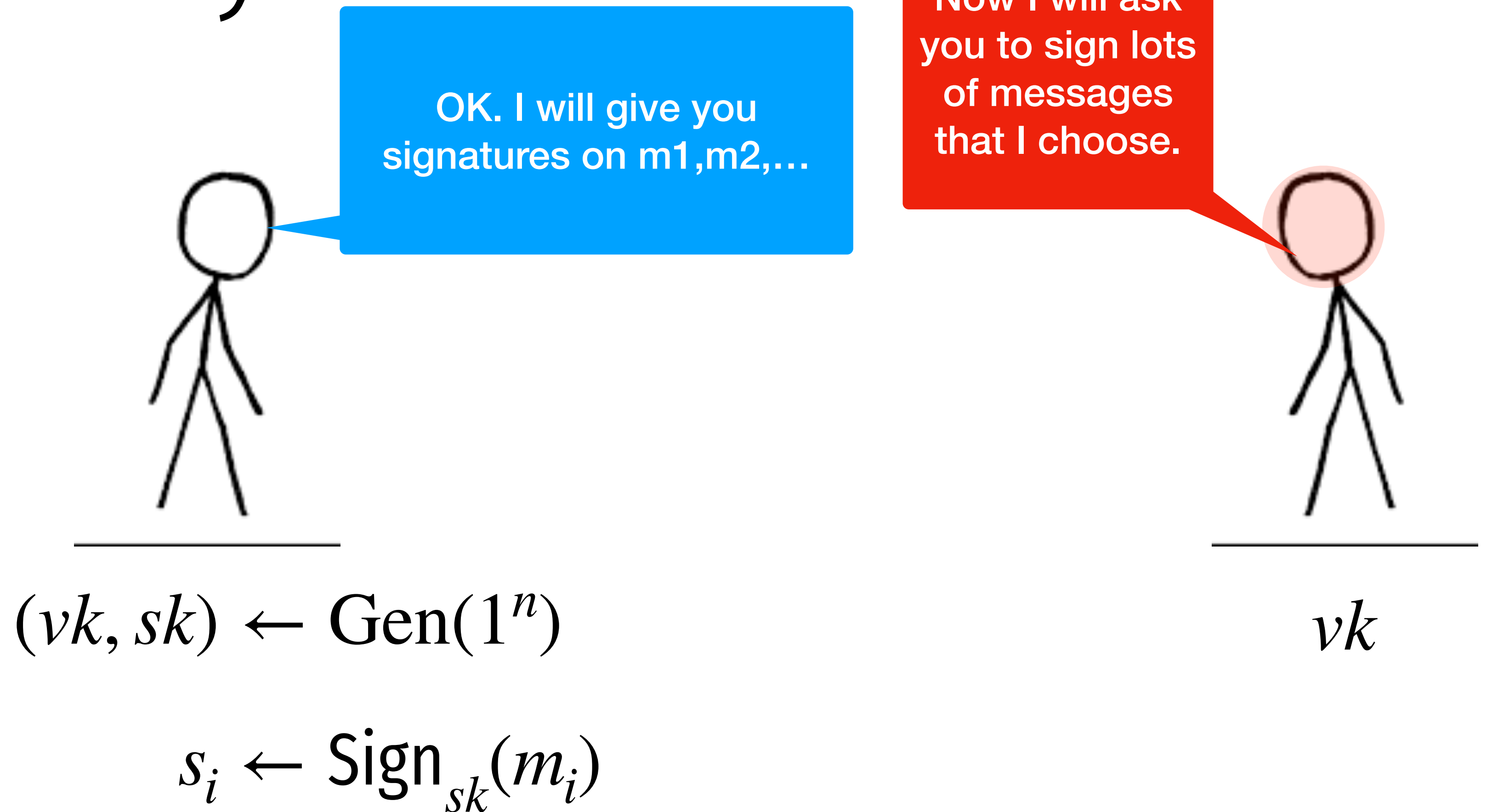
Now I will ask you to sign lots of messages that I choose.

m_0, m_1, \dots



vk

Signature security



Signature security



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

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

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



vk

s_1, s_2, \dots

Signature security

If you do, you
have won the
game!

Now I will try to create a
new (msg^*, sig^*) pair...one
that I didn't receive from
you.



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



Textbook RSA Signatures (insecure)

Pick $N = p \cdot q$ where p, q are primes.

Pick e, d such that $e \cdot d = 1 \pmod{\phi(N)}$

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

Compute the signature: $\sigma \leftarrow m^d \pmod{N}$

Verify($(pk=e, N)$, σ , m):

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

RSA Signatures in GPG

Sign((sk, N) m):

Compute the padding: $z \leftarrow 00 \cdot 01 \cdot FF \dots FF \cdot 00 \cdot ID_H \cdot H(m)$

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