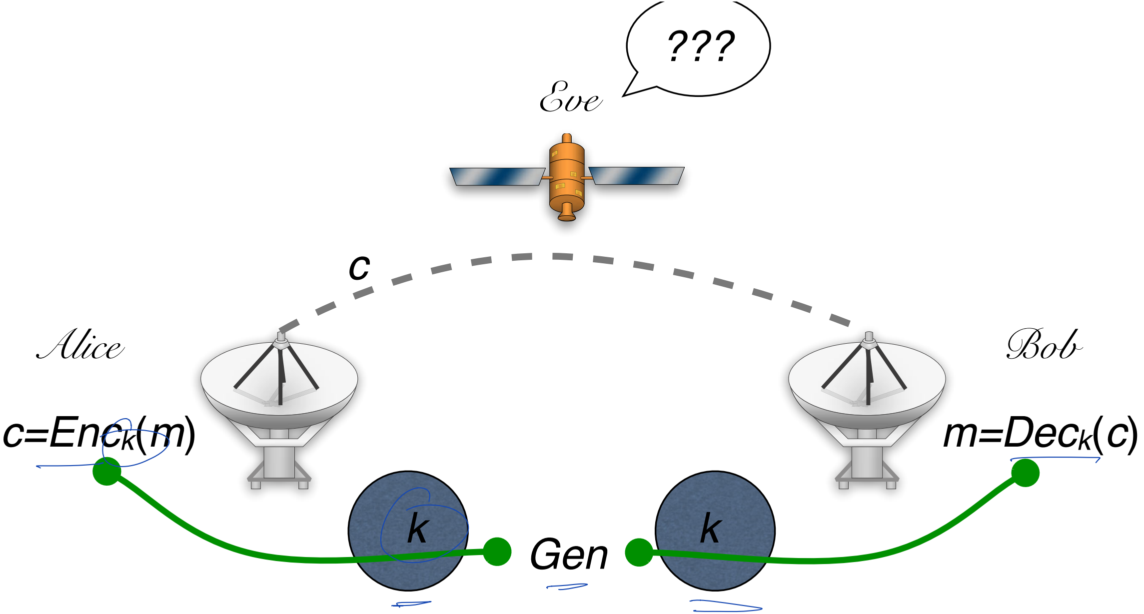
2550 Intro to cybersecurity

L12: Crypto: PKC

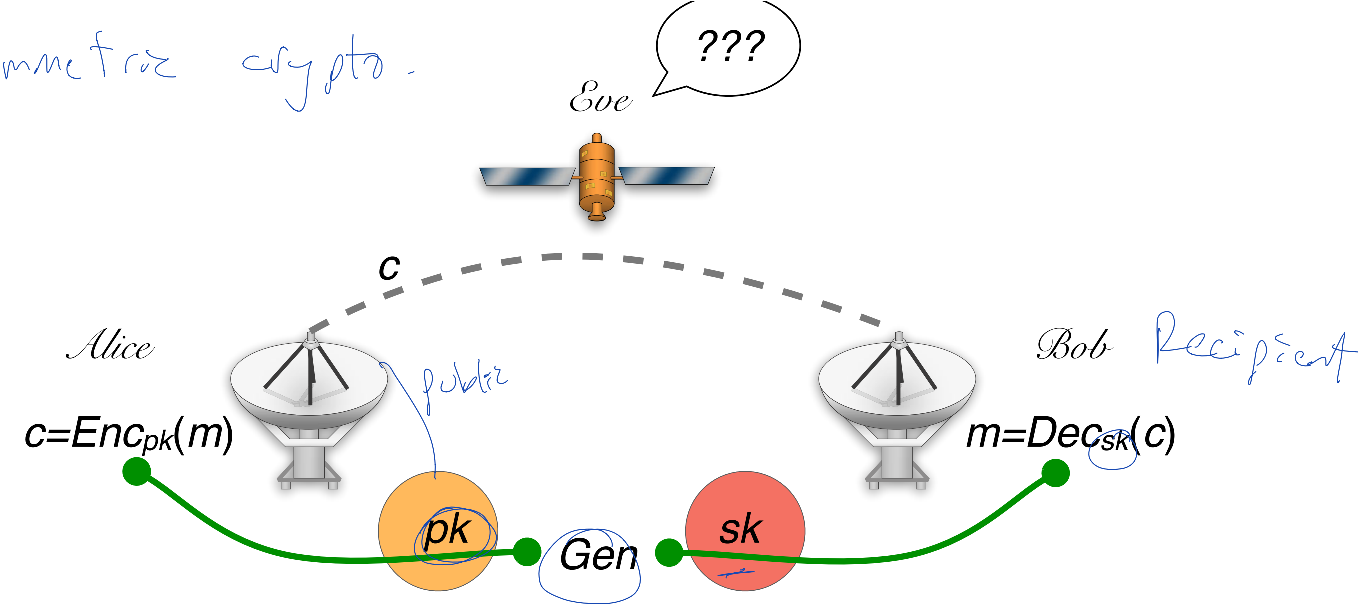
Ran Cohen/abhi shelat

Revisit our model for Encryption



Symmetric key model

Asymmetric crypto.



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)

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

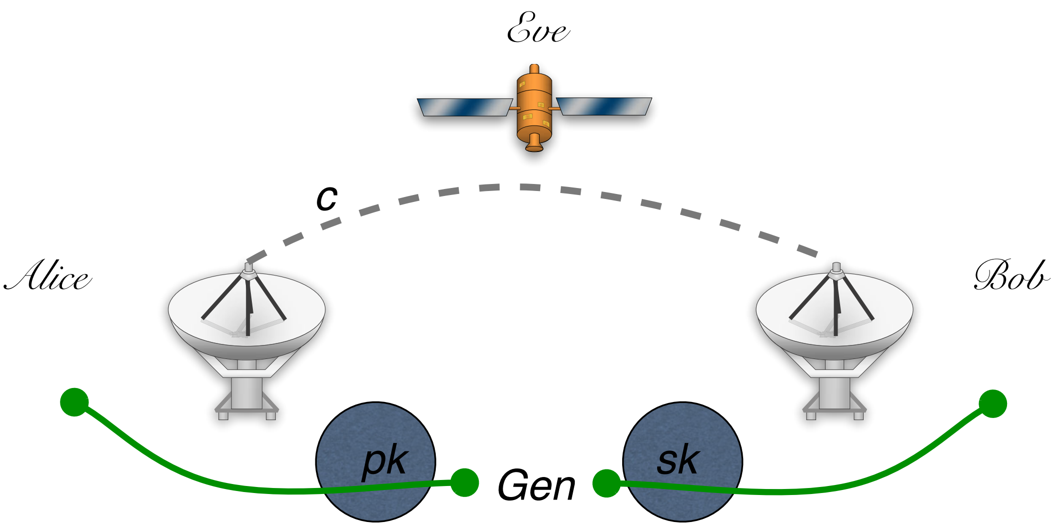
Enc (encryption)

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

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

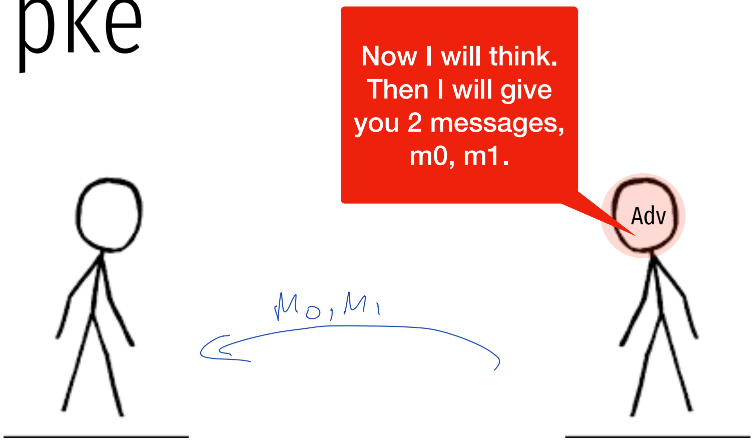
(weakest notion of security)

* how is this different from symmetric key IND-CPA game??

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

IND-CPA security for pke

(weakest notion of security)



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

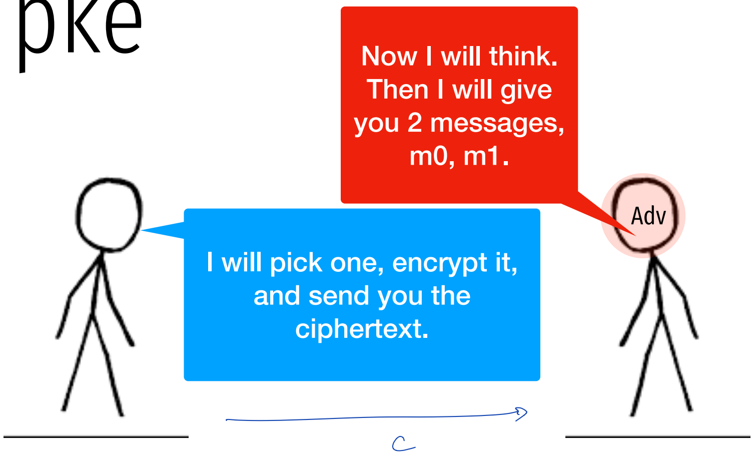
pk

$m_0, m_1 \leftarrow A(pk)$

$|m_0| = |m_1|$

IND-CPA security for pke

(weakest notion of security)



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

pk

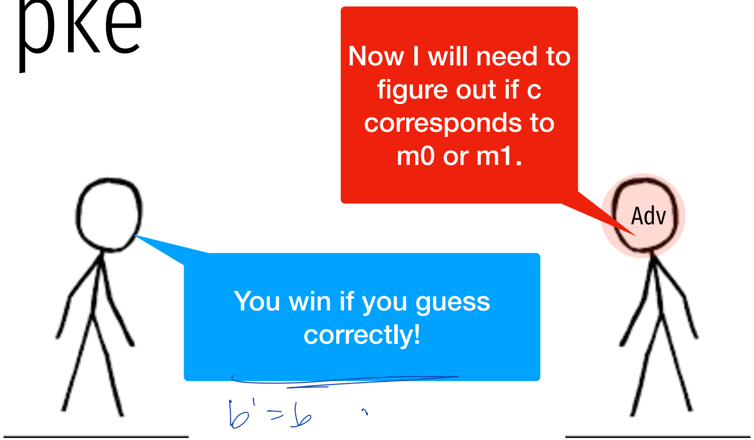
$m_0, m_1 \leftarrow A(pk)$

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

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

IND-CPA security for pke

(weakest notion of security)



$b' = b$

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

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)

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

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

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

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

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

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

How to build public key encryption?

Basic Number theory

$$\underbrace{a \bmod p}_{\text{"the remainder after dividing } a \text{ by } p\text{"}}$$

$17 \bmod 11 = \boxed{6}$

$$\begin{array}{r} 1 \\ 11 \overline{)\,17} \\ \underline{11} \\ 6 \end{array}$$

$135433238 \bmod 11$

$$11 \overline{)\,135433238}$$

$\boxed{6}$

$a \bmod p$

$17 \bmod 11$ $=6$

$135433238 \bmod 11$ $=6$

$$
\begin{array}{r}
12312112 \quad R\,6 \\
11\,\overline{)\,135433238} \\
11 \\
\hline
25 \\
22 \\
\hline
34 \\
33 \\
\hline
13 \\
11 \\
\hline
23 \\
22 \\
\hline
12 \\
11 \\
\hline
13 \\
11 \\
\hline
28
\end{array}
$$

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

$3 + 10 \bmod 17 = \boxed{13}$

$2 \cdot 11 \bmod 17 = 5$

$\underbrace{15 + 15}_{30} \bmod 17 = \boxed{13}$

$22 \bmod 17 = \underline{5}$

Modular Exponentiation

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

$7^{19} \bmod 31$

$7^{19} = 7^{16} \cdot 7^{2} \cdot 7^{1} \bmod 31$

$= 7 \cdot 18 \cdot 7 \bmod 31 = \boxed{14}$

"repeated squaring"

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

$49 - 31 = 18$

$18 \cdot 18 = 324$, $324 - 310 = 14$

$14 \cdot 14 = 196$, $196 - 186 = 10$

$100 - 93 = 7$

Modular Exponentiation

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

this is fast

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

$r \leftarrow 1$

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

Greatest Common Divisor

EUCLID

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

Greatest Common Divisor

$\mathrm{GCD}(6809, 1639) =$

$\mathrm{GCD}(1639, 253) =$ $\qquad 6809 = 4 \cdot 1639 + 253$

$\mathrm{GCD}(253, 121) =$ $\qquad 1639 = 6 \cdot 253 + 121$

$\mathrm{GCD}(121, 11) = \boxed{11}$ $\qquad 253 = 2 \cdot 121 + 11$

$\mathrm{GCD}(11, 0) = 11$

Greatest Common Divisor

GCD(6809, 1641) = 1

$6809 \cdot (-643) + (1641)(2668) = 1$

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

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

groups

(group theory)

set $\quad$ operation

$$(G, \oplus)$$

closure : if $a, b \in G$, $a \oplus b \in G$.

associativity : $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

identity : $\exists\, i \in G$ such that $a \oplus i = a \quad \forall a \in G$.

inverse

$\forall a \in G, \ \exists\, a' \in G$ s.t. $a \oplus a' = i$

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

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

$n = 17$

$Z_{17} = \{0, 1, 2, \ldots 16\}$

$16 + 1 \mod 17 = 0$

$a, b \in Z_{17}$, $a + b \in Z_{17}$. closure ✓

identity : 0

inverse : $13 + 4 = 0 \mod 17$.

Example of groups

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

multiplicative group, mod n

$$\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$5 \cdot 7 = 35 \bmod 13 = 9 \qquad 5 \cdot 8 = 1 \bmod 13$$

- every element here has an inverse.

$\Rightarrow$ Euclid GCD algorithm: Because $\gcd(a,n) = 1$

$\Rightarrow \exists\, x, y$ s.t. $a \cdot x + n \cdot y = 1 \Rightarrow a \cdot x = 1 \bmod n$.

verify

$gcd(2,4) = 2$

$Z_4^* = \{1, 3\}$

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

is a group

$1 \cdot 1 = 1$

$1 \cdot 3 = 3$

$3 \cdot 3 = 1$

closure ✓

associativity ✓

identity → 1

inverse? → follows from the GCD algorithm

Euler totient

$\phi(N)$ = # of positive intergers up to N that are relatively prime to N.

$$\phi(13) = |Z_{13}^*| = |\{1,2,3 \ldots 12\}| = 12$$

$\phi(p) = p-1$ if p is prime.

Euler totient

$p \quad q$

$15 = 3 \cdot 5$

$\phi(n) = (p-1)(q-1)$ if n is $n = p \cdot q$ for primes p, q.

$\phi(15) = 8$

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

5 multiples of 3.

3 multiples of 5

we are counting 15 twice.

$\phi(15) = 15 - 5 - 3 + 1 = (5-1)(3-1)$

Euler totient

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

prime

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

product
of 2 primes

$$\Phi(n) = (p-1)(q-1)$$

Euler theorem

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

Examples

$p = 31$. $\phi(31) = 30$

$7^{30} \bmod 31 = 7^{16} \cdot 7^{8} \cdot 7^{4} \cdot 7^{2}$

7^1	7^2	7^4	7^8	7^{16}
7	18	14	10	7

$18 \cdot 14 =_{31} 252$

248

(1) $\boxed{4}$

$4 \cdot 10 =_{31} 40$

(2) $\boxed{9} \cdot 7 = \boxed{63}$.

mod 31

1

Examples

$\phi(15) = (5-1)(3-1) = (4\cdot 2) = 8$

$2^8 \bmod 15 = \quad 256 \bmod 15 = \boxed{1}$

$$
\begin{array}{r}
17 \\
15\,\overline{)\,256} \\
\underline{15} \\
106 \\
\underline{105} \\
1
\end{array}
$$

Euler's theorem

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

$\mathbb{Z}_{31}^*$

$p = 31$

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

a $2a$ ... $15a$ $30a$

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

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

Euler's theorem

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

- these 2 lists are the same numbers in different order.

multiply all together

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

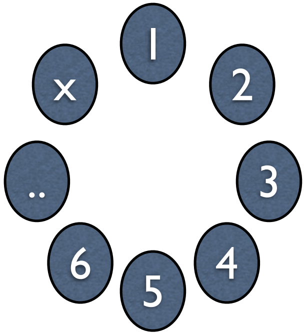
a = 3.

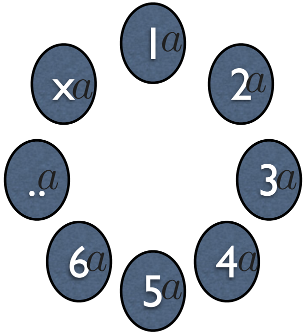
3 6 9 12 15 18 21 24 27 30 2 5 8 11 14 17 20 23 26 29 1 4 7 10 13 16 19 22 25

$$\boxed{\cancel{\prod_{x \in \mathbb{Z}_n^*}} x} = \prod_{x \in \mathbb{Z}_n^*} ax = \boxed{a^{\phi(n)} \cdot \cancel{\prod_{x \in \mathbb{Z}_n^*}} x} \Rightarrow 1 = a^{\phi(n)} \bmod N$$

Euler theorem

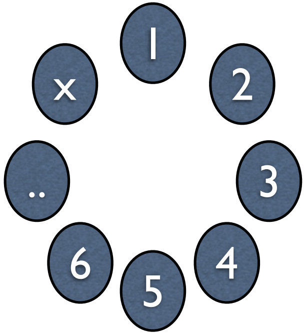
$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$

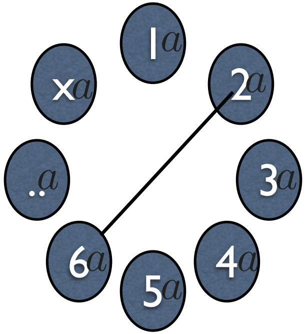




Euler theorem

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





argue: all are distinct

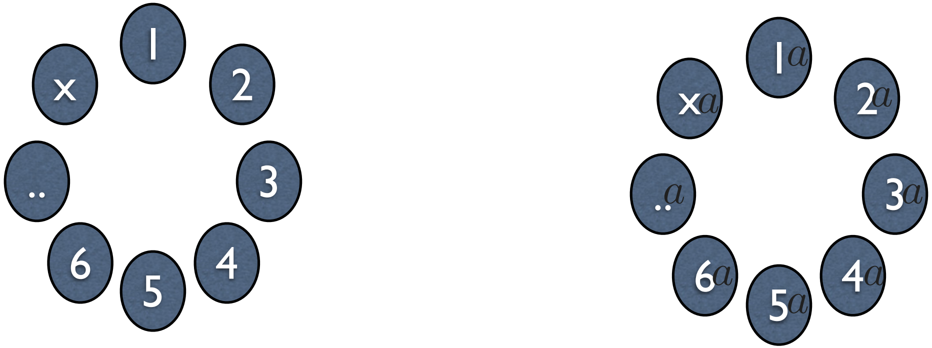
spse two are equal.

multiply by a^{-1}

this implies 2=6!

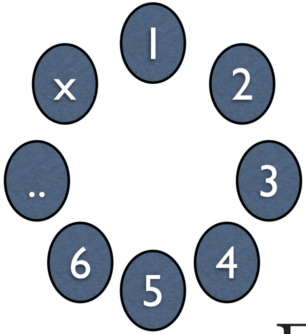
Euler theorem

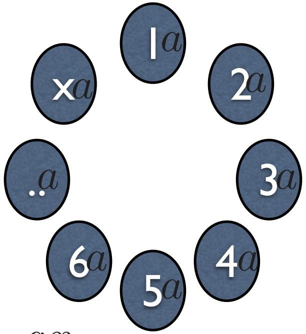
$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$



Euler theorem

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

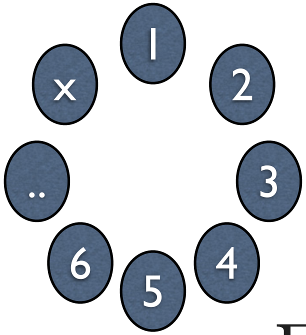


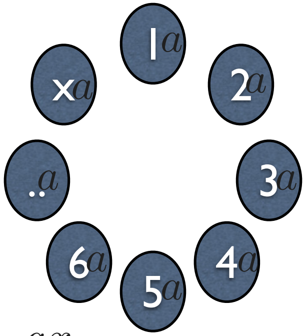


$$\prod_{x \in Z_N^\star} x \qquad \prod_{x \in Z_N^\star} ax$$

Euler theorem

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

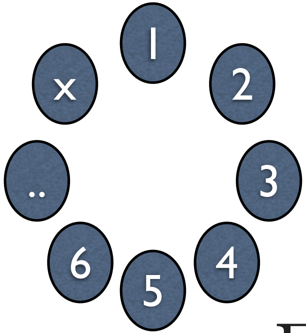


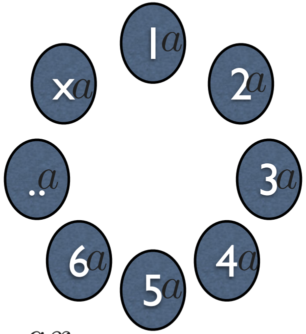


$$\prod_{x \in Z_N^\star} x = \prod_{x \in Z_N^\star} ax$$

Euler theorem

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



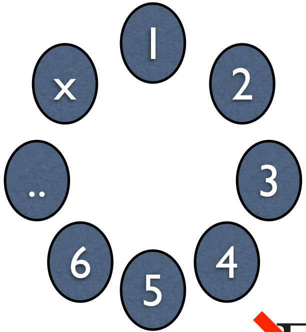


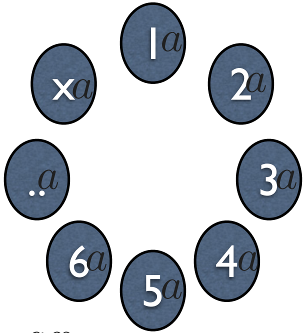
$$\prod_{x \in Z_N^\star} x = \prod_{x \in Z_N^\star} ax$$

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

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

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

$$= (1)^{10} \bmod N = \underline{1}$$

$a^{x} \bmod N$

$= a^{x \bmod \phi(n)} \bmod n.$

x

$$a^{\boxed{k\phi(N)+1}} \bmod N = \underbrace{\left(a^{k \cdot \phi(n)}\right)} \cdot a^{1} \bmod N$$

$$= 1 \cdot a^{1} \bmod N$$

$$= \underline{a^{1}}$$

compute

$$\underbrace{11^{\underbrace{30^{2021}}}}\ \text{mod}\ 23$$

(show your work)

$$11^{30^{2021}}\ \text{mod}\ 23 = \left.\underbrace{11^{\underline{(30^{2021}\ \text{mod}\ \phi(23))}}\ \text{mod}\ 23,}\right\}\ \text{by Euler}$$

simplify the exponent mod $\phi(n)$.

$$30^{2021}\ \text{mod}\ \phi(23) = \underbrace{30^{(2021\ \text{mod}(\phi(\phi(23))))}}\ \text{mod}\ \phi(23)$$

↳ by Euler

"Textbook" RSA (insecure)

NOT IND-CPA Secure.

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

$p=11$ $q=13$ $N=143$

“Textbook” RSA (insecure)

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

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

$N = 143 = 13 \cdot 11$

using Euclid

$e = 7$ $d = 103$

$7 \cdot 103 = 721 = 1 \bmod (13-1)(11-1)$

$= 1 \bmod (120)$

"Textbook" RSA (insecure)

$k^2 \mod N$

$\stackrel{?}{=}$

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

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

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

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

simplifying the exponent mod $\phi(n)$.

$$\mathrm{Dec}_{N,d}(\mathrm{Enc}_{N,e}(m)) \stackrel{1}{=} (m^e)^d \mod N$$

$$\stackrel{2}{=} m^{e \cdot d} \mod N \stackrel{3}{=} m^{1+k\cdot\phi(n)} \stackrel{4}{=} \underline{m \mod N}.$$

“Textbook” RSA (insecure)

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

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

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

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

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

Not randomized!!

Enc("MIDWAY")

always the same!!!

Example of Textbook RSA

m=5

$N = 143, \boxed{e = 7}$ pk

$\boxed{d = 103}$ sk

$m^e = 5^7 \bmod 143 \rightarrow c$

$c^{103} \bmod 143 =$

$\boxed{N, e} \rightarrow$ public key

$\boxed{N, d} \rightarrow$ private key

(Please do this @ home)

"Textbook" RSA (insecure)

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

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

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

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

Why is it insecure against IND-CPA attack?

Not randomized

pkcs1.5

|| mean
"concat"

can be more than 1 zero.

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

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)

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

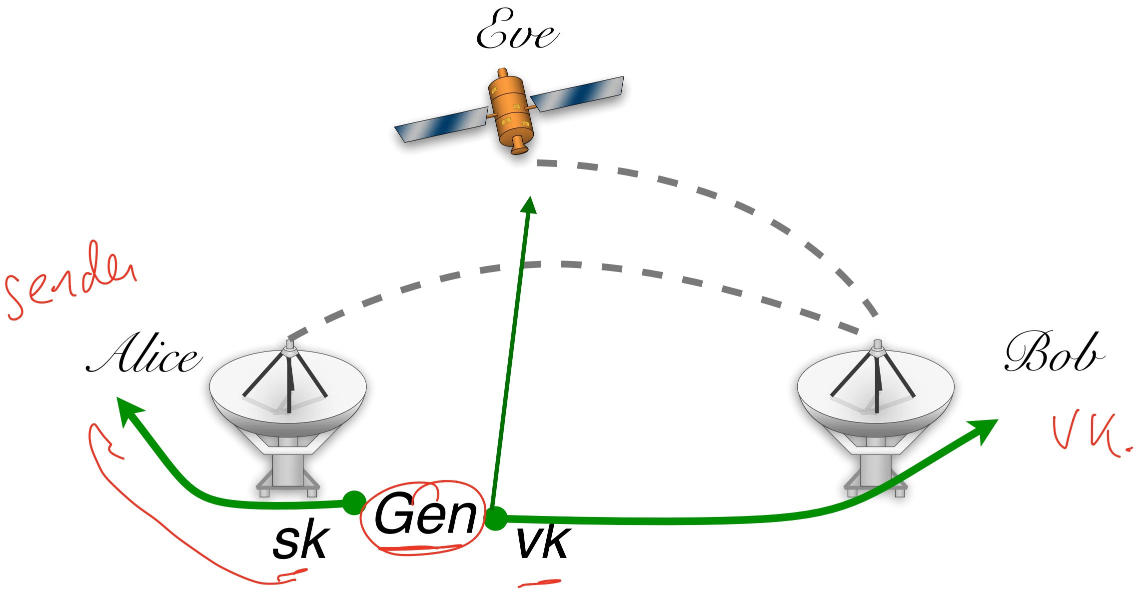
$(s = (s_1, s_2), t) \leftarrow f^{-1}(c)$

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

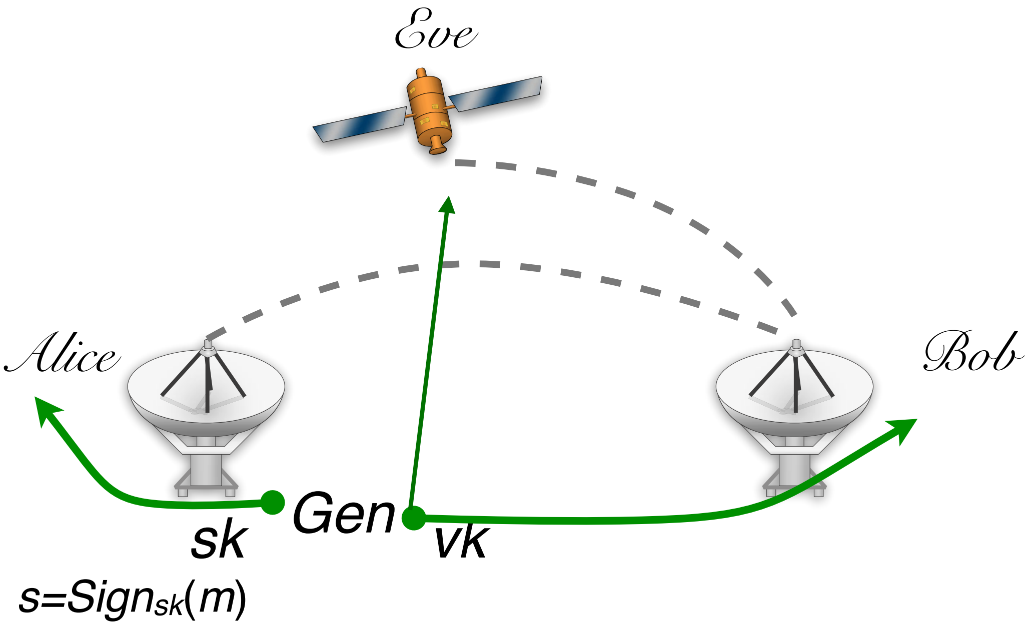
$m \leftarrow R_1(r) \oplus s_1$

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

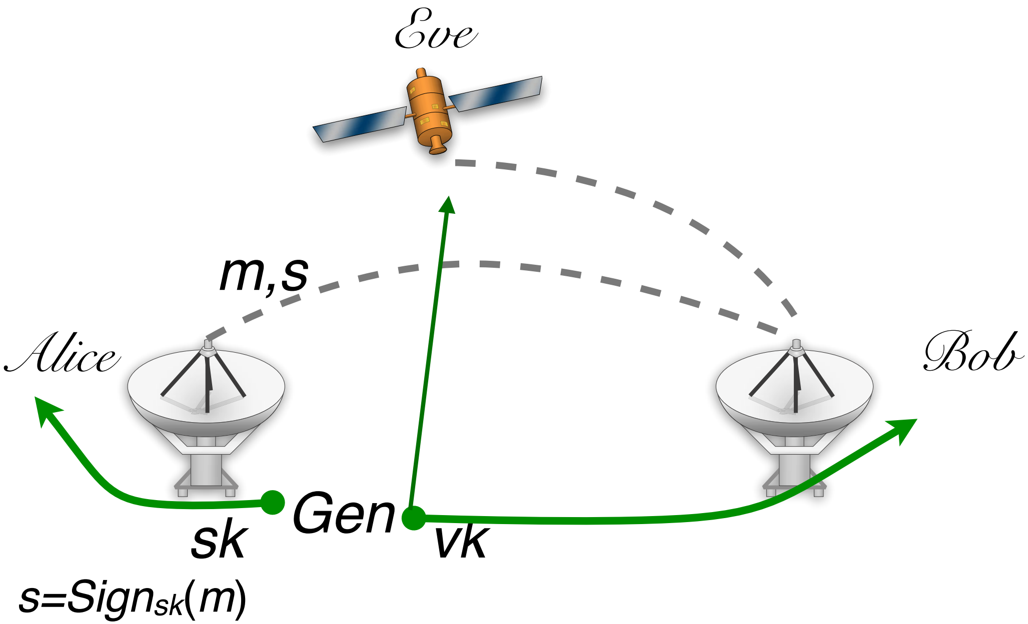
Public key digital signature



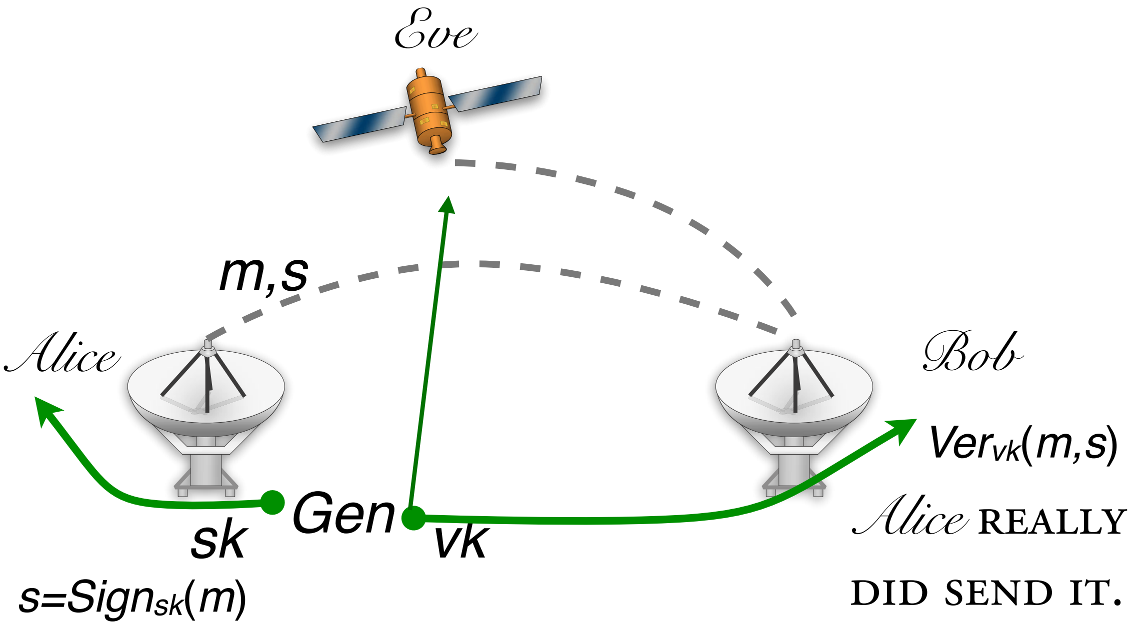
Public key digital signature



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 $m \in \mathcal{M}_n$

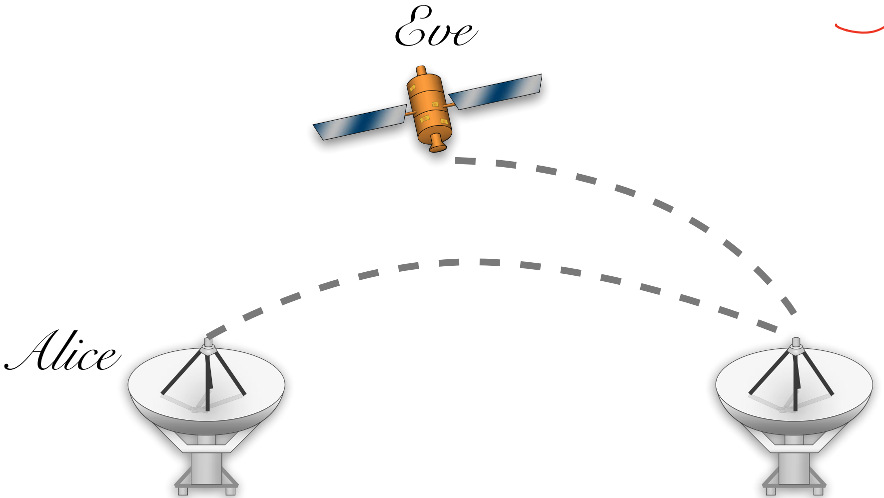
Ver$_{vk}$(*m,s*) ACCEPTS OR REJECTS A MSG,SIG PAIR

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

existential unforgability

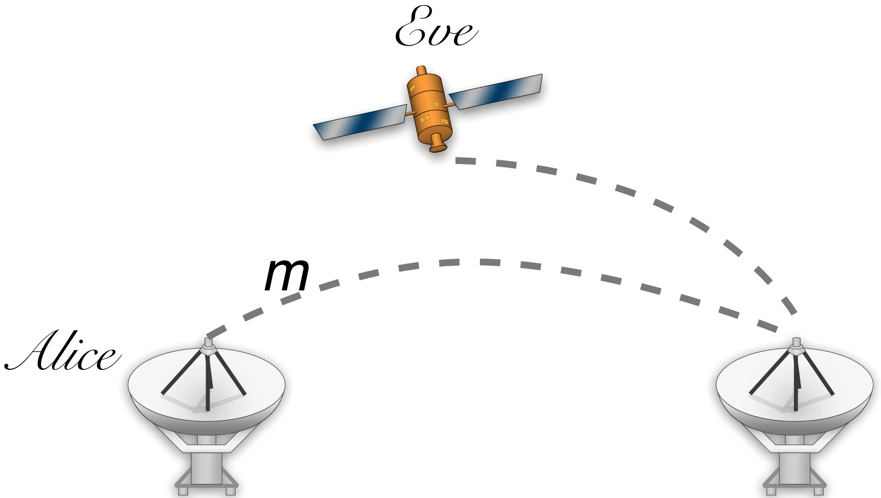
MAC:

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

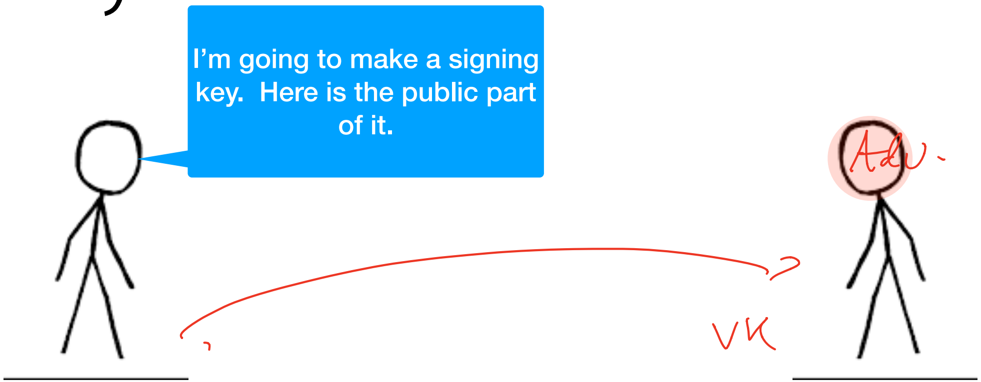


existential unforgability

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

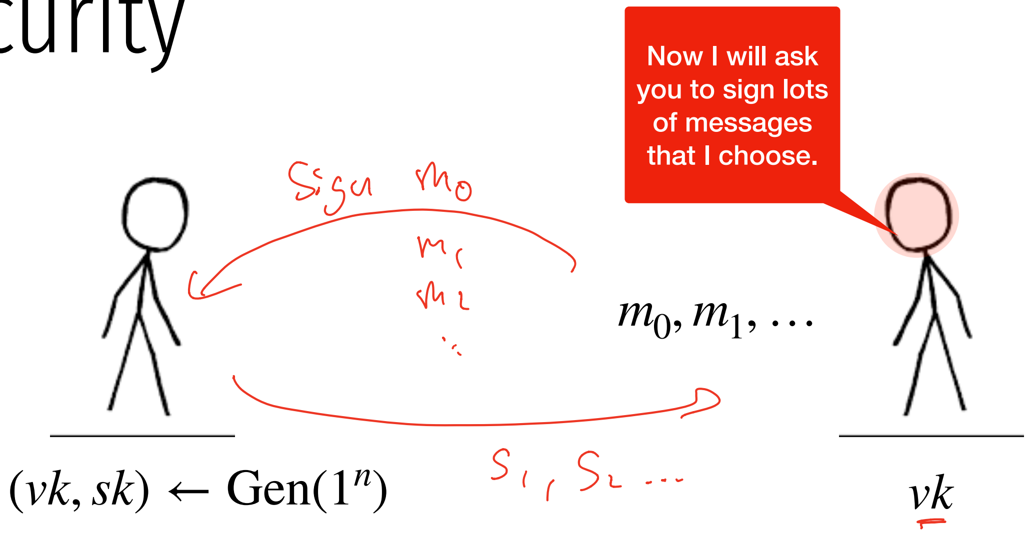


Signature security

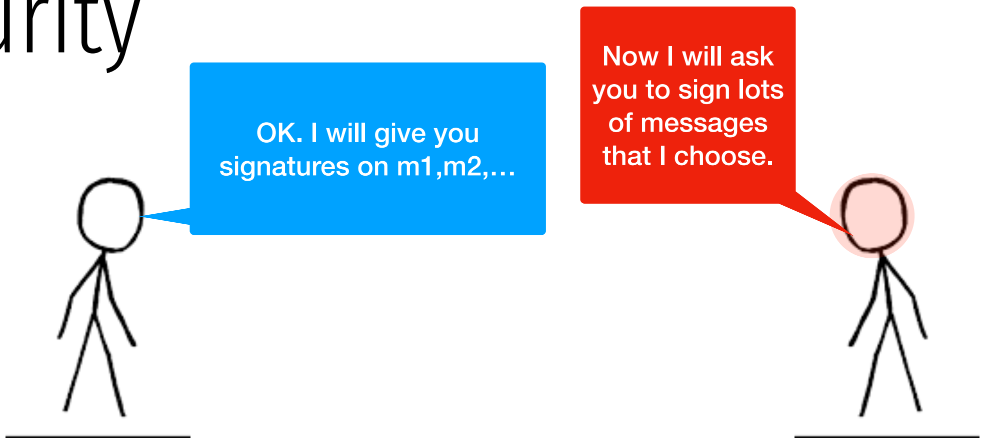


$$(vk, sk) \leftarrow \text{Gen}(1^n)$$

Signature security



Signature security



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

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

vk

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

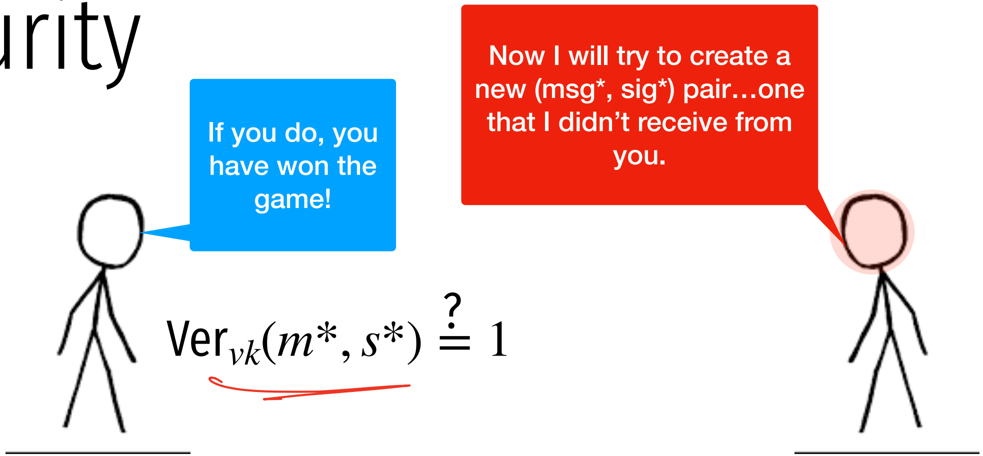
$(vk, sk) \leftarrow \mathrm{Gen}(1^n)$

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

vk

$s_1, s_2, \ldots$

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: $\sigma \leftarrow m^{d} \bmod N$ sk.

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

Why are these schemes secure??

→ Both rely on the "hardness" of the "RSA problem"

≈ similar to "factoring a large N"