

CSCI 1515 Applied Cryptography

This Lecture:

- RSA Assumption/Encryption (continued)
- Diffie-Hellman Assumptions
- ElGamal Encryption
- Diffie-Hellman Key Exchange
- Message Integrity
- RSA Signature

Basic Number Theory

$\gcd(a, N) = 1$: a & N are coprime

$\Rightarrow \exists b$ st. $a \cdot b \equiv 1 \pmod{N}$: a is invertible modulo N ,
 b is its inverse, denoted as a^{-1} .

$$\mathbb{Z}_N^* := \{a \mid a \in [1, N-1], \gcd(a, N) = 1\}$$

Euler's phi (totient) function $\phi(N) := |\mathbb{Z}_N^*|$

Ex: $N = p \cdot q$ (p, q are primes) $\phi(N) = (p-1) \cdot (q-1)$.

Euler's Theorem $\forall a, N$ where $\gcd(a, N) = 1$, $a^{\phi(N)} \equiv 1 \pmod{N}$.

Corollary If $d \equiv e^{-1} \pmod{\phi(N)}$, then $\forall a \in \mathbb{Z}_N^*$, $(a^d)^e \equiv a \pmod{N}$.

RSA Assumption

- Factoring Assumption:

Generate two n -bit primes p, q ($p \neq q$)

Compute $N = p \cdot q$

Given N , it's computationally hard to find p & q (classically)

- RSA Assumption:

Generate two n -bit primes p, q ($p \neq q$)

Compute $N = p \cdot q$, $\phi(N) = (p-1)(q-1)$

Choose e s.t. $\gcd(e, \phi(N)) = 1$

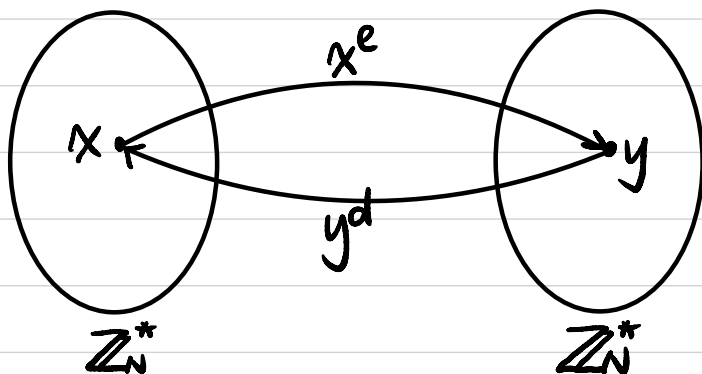
Compute $d = e^{-1} \bmod \phi(N)$

Given (N, e) & a random $y \leftarrow \mathbb{Z}_N^*$, it's computationally hard to find x s.t.
 $x^e \equiv y \pmod{N}$

If breaking Factoring



then break RSA



"Plain" RSA Encryption

$\lambda = 128$: best attack takes time 2^{128}

• Gen(1^λ):

$n = O(\lambda)$

$n = 1024$, key length 2048

Generate two n -bit p, q ($p \neq q$)

Compute $N = p \cdot q$, $\phi(N) = (p-1)(q-1)$

Choose e s.t. $\gcd(e, \phi(N)) = 1$

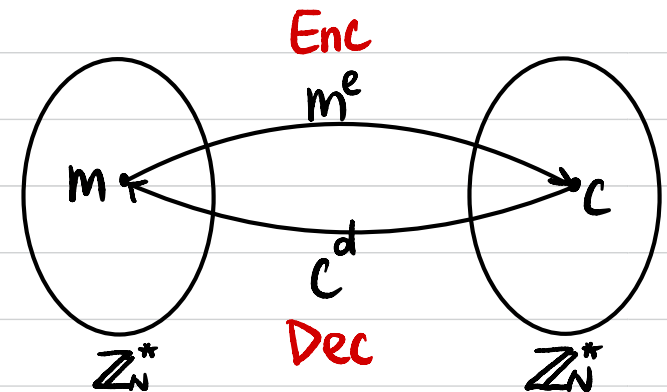
Compute $d = e^{-1} \bmod \phi(N)$.

$pk = (N, e)$

$sk = d$.

• $Enc_{pk}(m)$: $c = m^e \bmod N$

• $Dec_{sk}(c)$: $m = c^d \bmod N$



Any security issues? CPA secure?

Computational Security

Chosen-Plaintext Attack (CPA) Security

$k \leftarrow \text{Gen}(1^\lambda)$

Alice



$$c_0 \leftarrow \text{Enc}_k(m_0)$$

$$c_1 \leftarrow \text{Enc}_k(m_1)$$

$$c_2 \leftarrow \text{Enc}_k(m_2)$$

$\vdots$

$$m_0, m_1 \in \{0, 1\}^n$$

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

$$c \leftarrow \text{Enc}_k(m_b)$$

③ choose



(PPT) $\xrightarrow{\text{⑤ Output}} b'$

Chosen-Plaintext Attack (CPA) Security

Bob



$$m_0 := \text{Dec}_k(c_0)$$

$$m_1 := \text{Dec}_k(c_1)$$

$$m_2 := \text{Dec}_k(c_2)$$

$\vdots$

$c_0, c_1, c_2, \dots$

c

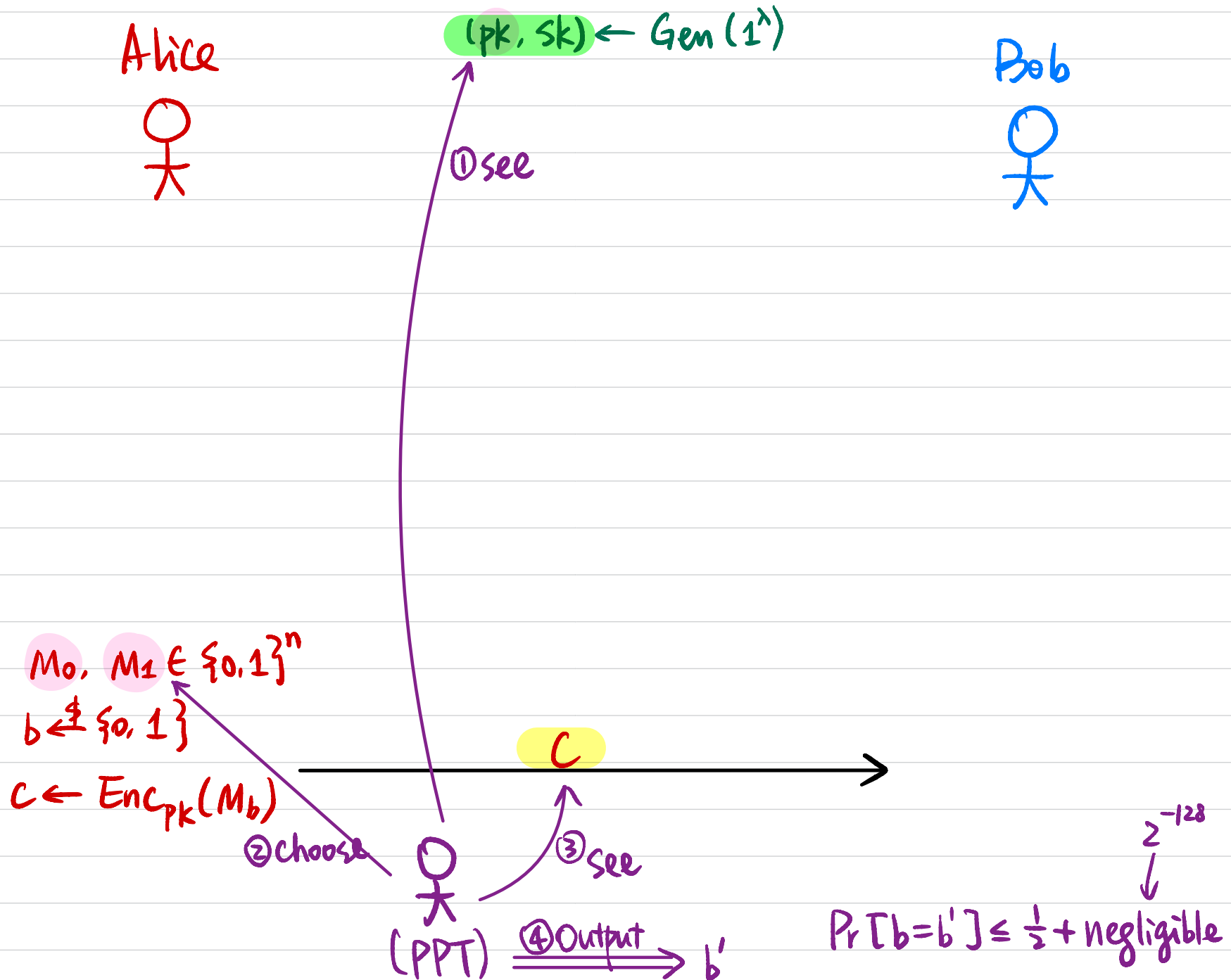
④ see

$$\Pr[b = b'] \leq \frac{1}{2} + \text{negligible}$$

2^{-128}

Computational Security

Chosen-Plaintext Attack (CPA) Security



Basic Group Theory

Def A group is a set G along with a binary operation $\circ$ with properties:

① Closure: $\forall g, h \in G, g \circ h \in G$

② Existence of an identity: $\exists e \in G$ st. $\forall g \in G, e \circ g = g \circ e = g$.

③ Existence of inverse: $\forall g \in G, \exists h \in G$ st. $g \circ h = h \circ g = e$

Inverse of g denoted as g^{-1} .

④ Associativity: $\forall g_1, g_2, g_3 \in G, (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

We say a group is **abelian** if it satisfies:

⑤ Commutativity: $\forall g, h \in G, g \circ h = h \circ g$

Exercises: Is this a group?

• $(\mathbb{Z}, +)$

• $(\mathbb{Z}, \cdot)$

• $(G = \{0, 1, \dots, N-1\}, + \text{ mod } N)$

• $(\mathbb{Z}_N^*, \cdot \text{ mod } N)$

Basic Group Theory

Group Exponentiation

For a group $(G, \cdot)$, $g^m := \overbrace{g \cdot g \cdots g}^m$ $g^0 := e$ $g^{-m} := (g^{-1})^m$

$g^{m_1} \cdot g^{m_2} = g^{m_1+m_2}$ $(g^{m_1})^{m_2} = g^{m_1 \cdot m_2}$ $g^m \cdot h^m = (g \cdot h)^m$ $g^{-m} = (g^m)^{-1}$

Def For a **finite group**, we use $|G|$ to denote its **order** (# of elements)

Let G be a finite group of order m .

$\forall g \in G, \langle g \rangle := \{g^0, g^1, \dots, g^{m-1}\} \quad (g^m = e)$ $\underbrace{e, g, g^2, \dots}_{|\langle g \rangle|}, \underbrace{e, g, g^2, \dots}, \dots, g^m = e$

G is a **cyclic group** if $\exists g \in G$ s.t. $\langle g \rangle = G$. g is a **generator** of G .

Thm $\mathbb{Z}_p^*$ for a prime p is a cyclic group of order $p-1$.

$p=7, \quad \langle 3 \rangle = \{1, 3, 2, 6, 4, 5\} \quad \langle 2 \rangle = \{1, 2, 4\}$

Thm If G has prime order, then G is cyclic and every element except the identity is a generator.

Prime-Order Subgroups of $\mathbb{Z}_p^*$

Def For a group $(G, \cdot)$, $H \subseteq G$ is a **subgroup** of G if $(H, \cdot)$ forms a group.

A prime p is a **safe prime** if $p = 2q + 1$ and q is a prime.

$\mathbb{Z}_p^*$ is a cyclic group of order $p-1 = 2q$.

Define $H := \{x^2 \bmod p \mid x \in \mathbb{Z}_p^*\}$

Thm H is a subgroup of $\mathbb{Z}_p^*$ of order q .

$$p=7, \quad H = \{1, 2, 4\} = \langle 2 \rangle = \langle 4 \rangle$$

Diffie-Hellman Assumptions

Integer group key 2048-bit
Elliptic Curve group key 256-bit

$$(G, q, g) \leftarrow G(1^\lambda)$$

$O(\lambda)$ -bit integer
↙

Cyclic group G of order q with generator g

- **Discrete Logarithm (DLOG) Assumption:**

$$x \leftarrow \mathbb{Z}_q, \text{ compute } h = g^x \quad g^x \stackrel{?}{\Rightarrow} x$$

Given (G, q, g, h) , it's computationally hard to find x (classically).

If breaking DLOG

- **Computational Diffie-Hellman (CDH) Assumption:**

$$x, y \leftarrow \mathbb{Z}_q, \text{ compute } h_1 = g^x, h_2 = g^y \quad (g^x, g^y) \stackrel{?}{\Rightarrow} g^{xy}$$

Given (G, q, g, h_1, h_2) , it's computationally hard to find g^{xy} .

Break CDH

- **Decisional Diffie-Hellman (DDH) Assumption:**

$$x, y, z \leftarrow \mathbb{Z}_q, \text{ compute } h_1 = g^x, h_2 = g^y$$

Given (G, q, g, h_1, h_2) , it's computationally hard to distinguish

$$(g^x, g^y, g^{xy}) \stackrel{c}{=} (g^x, g^y, g^z)$$

between g^{xy} and g^z .

Break DDH

ElGamal Encryption

- $\text{Gen}(1^\lambda)$:
 $(G, q, g) \leftarrow G(1^\lambda)$ $\leftarrow$ can be re-used
 $x \xleftarrow{\$} \mathbb{Z}_q$, compute $h = g^x$
 $\text{pk} = (G, q, g, h)$ $\text{sk} = x$
- $\text{Enc}_{\text{pk}}(m)$: $m \in G$
 $y \xleftarrow{\$} \mathbb{Z}_q$
 $C = \langle g^y, h^y \cdot m \rangle$
- $\text{Dec}_{\text{sk}}(C)$:
 $C = \langle C_1, C_2 \rangle$
 $m = C_2 \cdot (C_1^*)^{-1}$

Correctness?

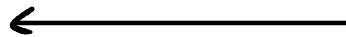
CPA Security?

Secure Key Exchange

Alice



k



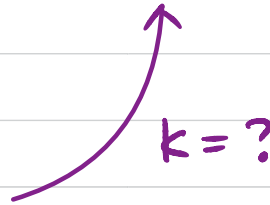
Bob



k



(Eavesdropper)



$k = ?$

Thm (Informal): It's impossible to construct secure key exchange from SK_E in a black-box way.

Diffie-Hellman Key Exchange

Alice



$$(G, q, g) \leftarrow G(1^\lambda)$$

$$x \xleftarrow{\$} \mathbb{Z}_q, \text{ compute } h_A = g^x$$

$$(G, q, g, h_A)$$



Bob



$$y \xleftarrow{\$} \mathbb{Z}_q, \text{ compute } h_B = g^y$$

h_B



$$\Downarrow \\ k = h_B^x$$



(Eavesdropper)

$$k = ?$$

$$\Downarrow \\ k = h_A^y$$

Correctness?

Security?

What happens in practice

Alice



k

Diffie-Hellman Key Exchange

Bob



k

Symmetric-Key Encryption

Message Integrity

Alice



"Let's meet @ 9am" →

Bob



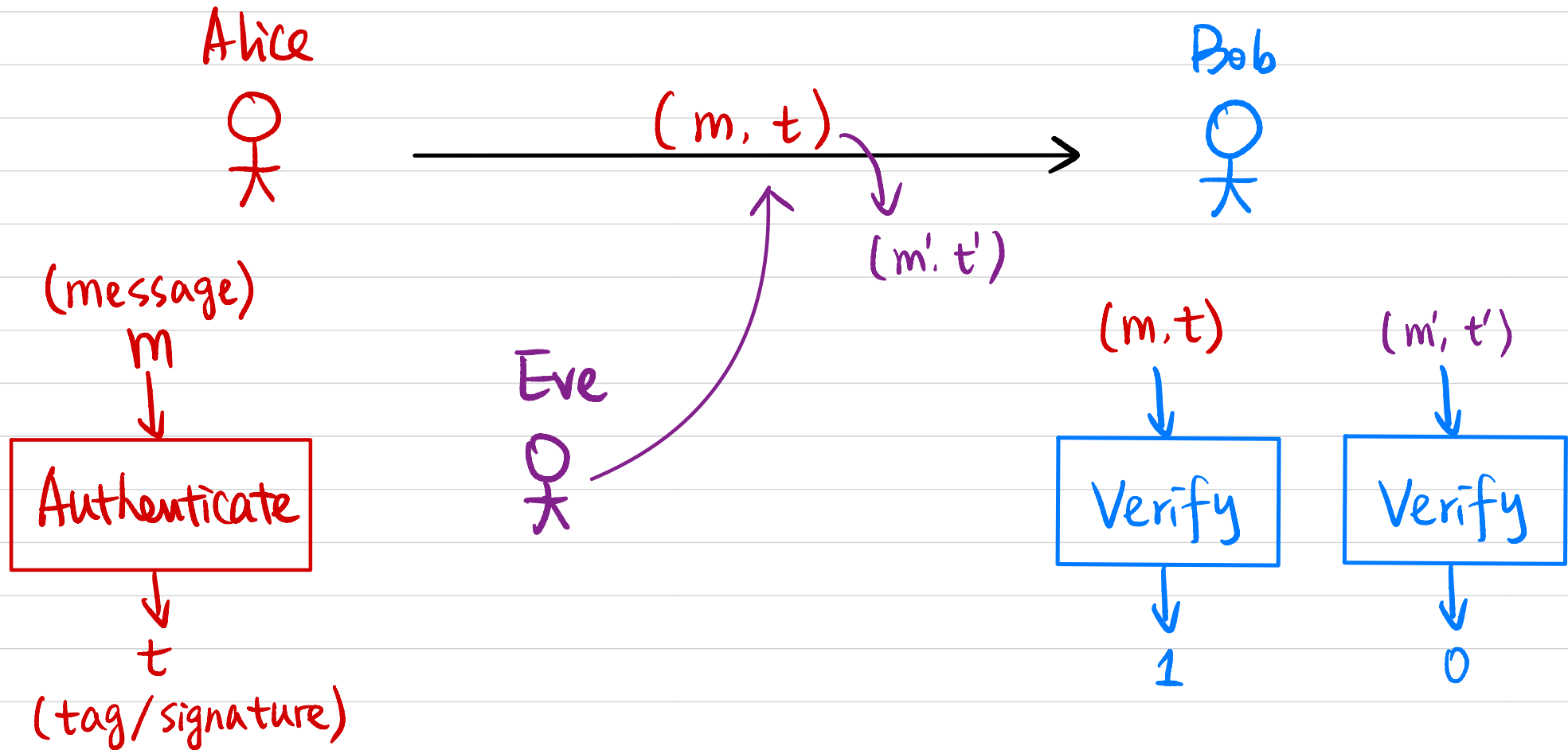
tamper with

Eve



Is it from Alice?

Message Integrity



Message Authentication Code (MAC)

Alice



(message)

m

k

Authenticate



t

(tag)



(m, t)



(m', t')

Eve



Bob



(m, t)

k

Verify



0/1



Digital Signature

Alice



(message)

m

sk

Authenticate



σ

(signature)



(secret)

(m, σ)

(m', σ')

Eve



Bob



(m, σ)

pk

Verify



0/1



(public)

Syntax

Message Authentication Code (MAC) Scheme $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$

$$k \leftarrow \text{Gen}(1^\lambda)$$

$$t \leftarrow \text{Mac}_k(m)$$

$$0/1 := \text{Vrfy}_k(m, t)$$

Digital Signature Scheme $\Pi = (\text{Gen}, \text{Sign}, \text{Vrfy})$

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

$$\sigma \leftarrow \text{Sign}_{sk}(m)$$

$$0/1 := \text{Vrfy}_{pk}(m, \sigma)$$

RSA Signature

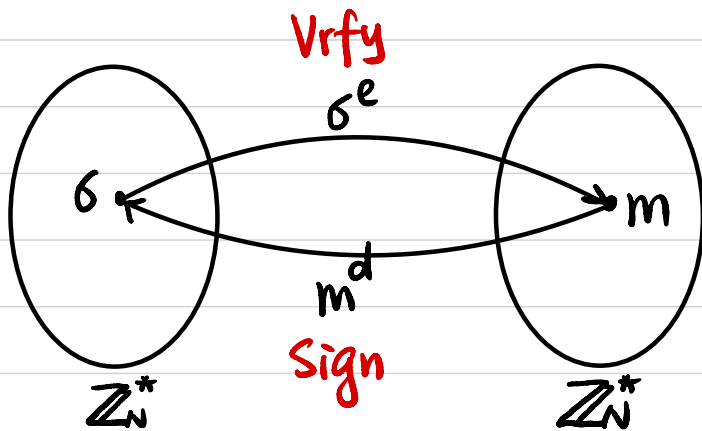
Generate two n -bit primes p, q ($p \neq q$)

Compute $N = p \cdot q$, $\phi(N) = (p-1)(q-1)$

Choose e s.t. $\gcd(e, \phi(N)) = 1$

Compute $d = e^{-1} \bmod \phi(N)$.

Given (N, e) & a random $y \leftarrow \mathbb{Z}_N^*$, it's computationally hard to find x s.t.
 $x^e \equiv y \pmod{N}$



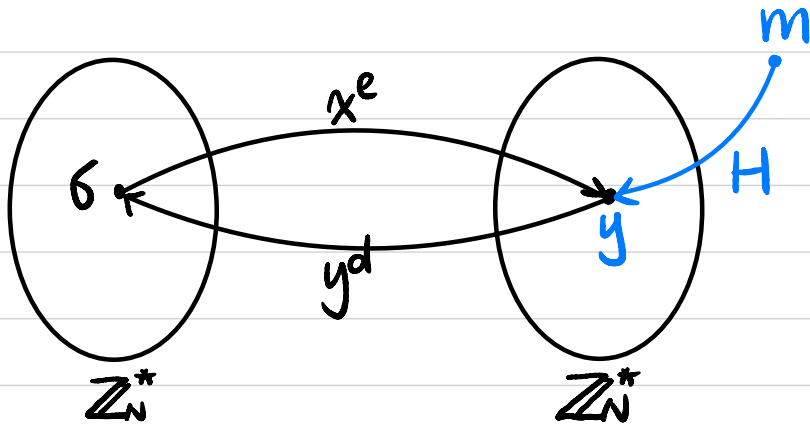
$$sk = d \quad pk = (N, e)$$

$$Sign_{sk}(m) = m^d \bmod N$$

$$Vrfy_{pk}(m, \sigma): \sigma^e \stackrel{?}{\equiv} m \pmod{N}$$

RSA Signature

Given (N, e) & a random $y \leftarrow \mathbb{Z}_N^*$, it's computationally hard to find x s.t.
 $x^e \equiv y \pmod{N}$



$$sk = d \quad pk = (N, e)$$

$$Sign_{sk}(m) = H(m)^d \pmod{N}$$

$$Vrfy_{pk}(m, \sigma): \sigma^e \stackrel{?}{\equiv} H(m) \pmod{N}$$

$$H: \{0, 1\}^* \rightarrow \mathbb{Z}_N^*$$

↑
public, deterministic function
that gives a (pseudo)random output

Security?