Lecture 3: Public Key Cryptography

-COMP 6712 Advanced Security and Privacy

Haiyang Xue

haiyang.xue@polyu.edu.hk

2022/1/30

Public Key Cryptography

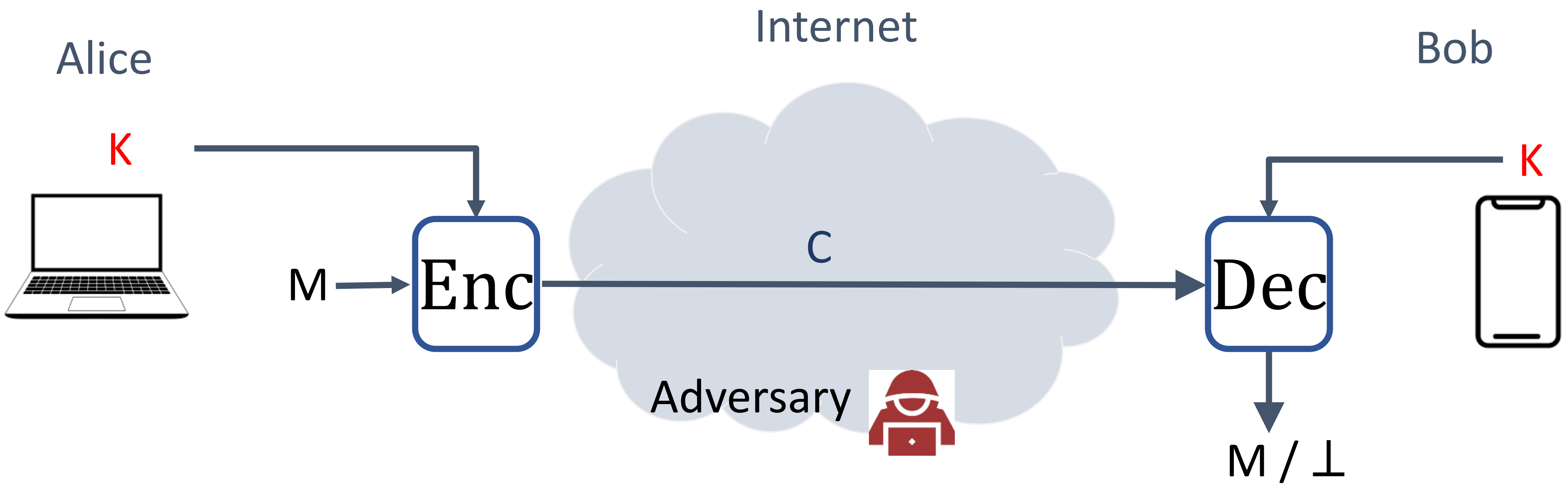
- Recall symmetric key cryptography (big picture)

- Diffie-Hellman Key Exchange

- Public key encryption: ElGamal, RSA

- Digital signature

Symmetric-key encryption



Enc : encryption algorithm (public)

K : shared key between Alice and Bob

Dec : decryption algorithm (public)

1.Kerckhoffs’ Principle (1883)

- Bob must have some information that Adversary doesn’t have

- How about keeping the decryption algorithm secret?
  - NO. algorithms for every user; share; need new design once broken

Design your system to be secure even if the attacker has complete knowledge of all its algorithms

- The only secret Bob has and Adversary doesn’t have is the SECRET KEY

2. Security definitions

- As said in lecture 2, we consider computational security (i.e., the adversary is computationally bounded)

Definition: A scheme Π is said to be **computationally secure** if any PPT adversary succeeds in breaking the scheme with negligible probability.

- But what is exactly mean by breaking?
- This is measured by the Aim and Capability of the adversary.

2. Security definitions

- Breaking/security is measured by the Aim and Capability of the adversary.

Aim

Try to learn something meaningful from the target ciphertext C^*

Capability

The ciphertext C^* + Learn more from system

2. Security definitions

- Breaking/security is measured by the Aim and Capability of the adversary.

Aim

Try to learn something meaningful from the target ciphertext C^*

Given $C^* = \mathrm{Enc}(m),\ f(m) \leftarrow A(C^*, .)$

⇕

A chooses any m_0, m_1
Given $C^* = \mathrm{Enc}(m_b)$, Guess $b,\ b' \leftarrow A(C^*, .)$

Capability

The ciphertext C^* + Learn more from system

2. Security definitions

- Breaking/security is measured by the Aim and Capability of the adversary.

Aim

Try to learn something meaningful from the target ciphertext C^*

Given $C^* = \mathrm{Enc}(m),\ f(m) \leftarrow A(C^*,.)$

$\Updownarrow$

A chooses any m_0, m_1
Given $C^* = \mathrm{Enc}(m_b)$, Guess b, $b' \leftarrow A(C^*,.)$

Capability

The ciphertext C^* + Learn more from system

Only C^* XXX=eav

C^* and the adversary can choose plaintext
XXX=CPA; denoted by $A^{\mathrm{Enc}(\,)}$

C^* and adversary can further choose ciphertext
XXX=CCA; denoted by $A^{\mathrm{Enc}(\,),\mathrm{Dec}(\,)}$

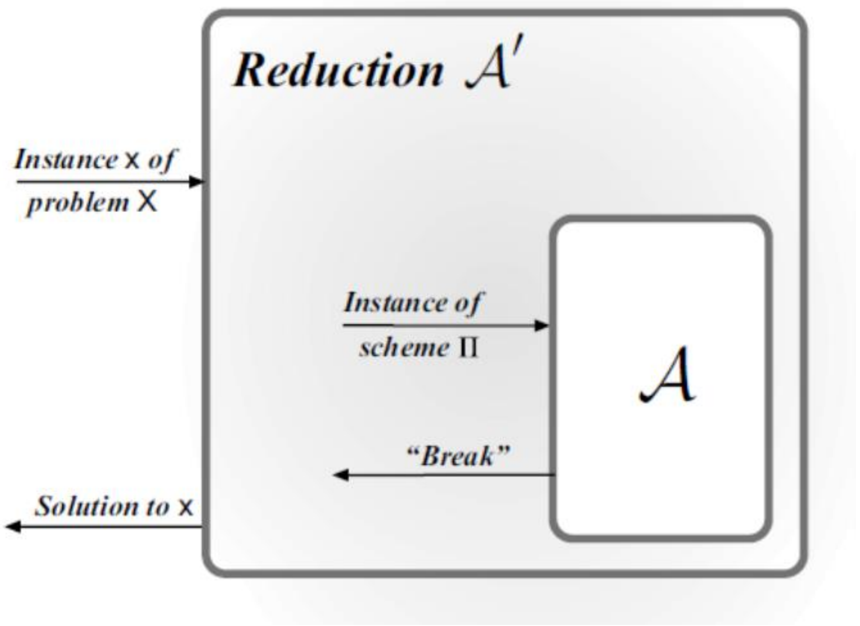
IND-XXX Security

3. Security Proof: reduction

Let us first talk about
how to show Problem A is harder than B?

Proving Π is secure is showing
Breaking Π is harder than Problem X

If Problem X is hard → Breaking Π is hard,
which means Π is secure

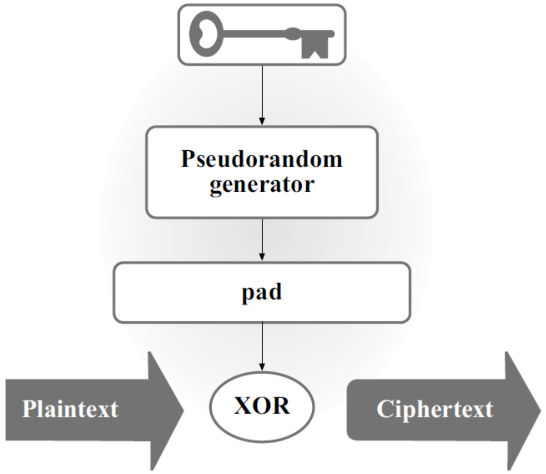


3. Security Proof: reduction: IND-eav as an example

$\Pi 1.\mathrm{Gen}: K \leftarrow \{0,1\}^k$

$\Pi 1.\mathrm{Enc}(\mathrm{K},\mathrm{M}): C = G(K) \oplus M$

$\Pi 1.\mathrm{Enc}(\mathrm{K},\mathrm{C}): M = G(K) \oplus C$



Test me on M_0, M_1 →

← $C^* = G(K) \oplus M_b$

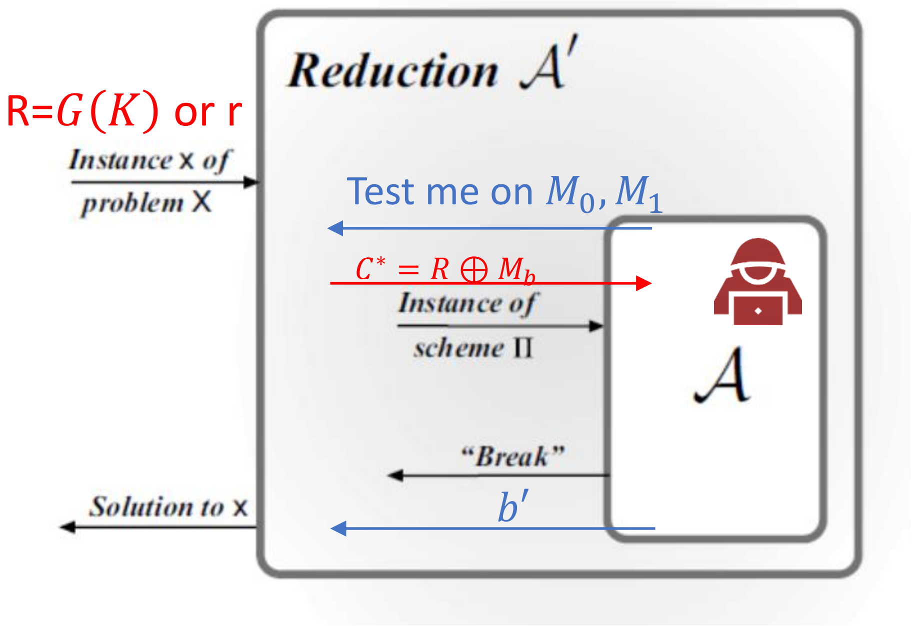
b' →

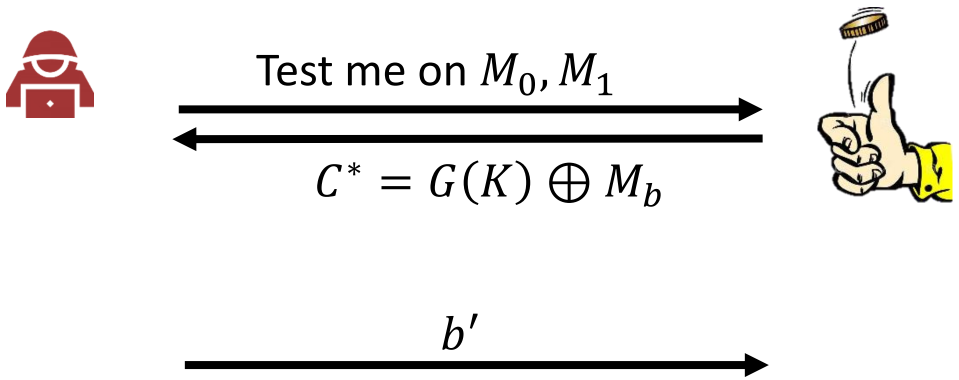
3. Security Proof: reduction: IND-eav as an example

$\Pi 1.\mathrm{Gen}: K \leftarrow \{0,1\}^k$

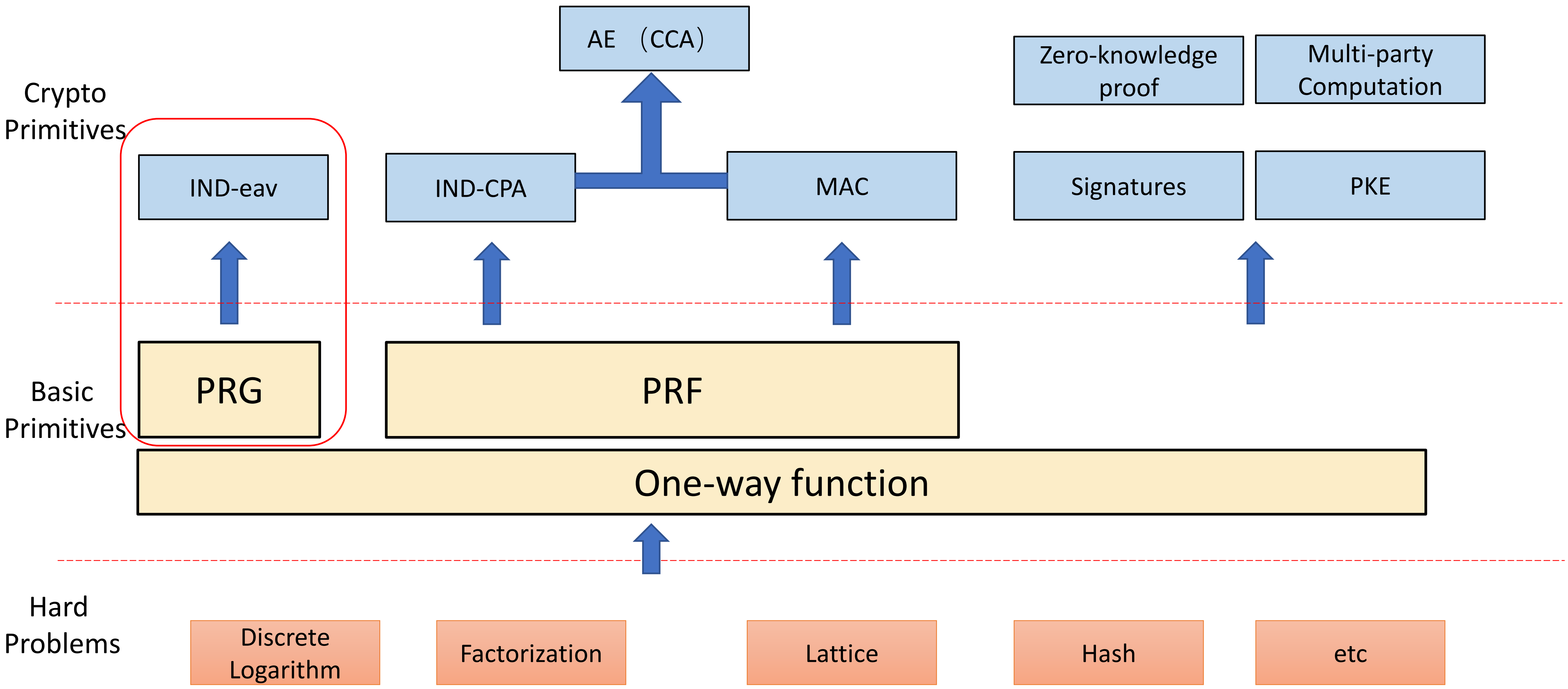
$\Pi 1.\mathrm{Enc}(\mathrm{K},\mathrm{M}): C = G(K) \oplus M$

$\Pi 1.\mathrm{Enc}(\mathrm{K},\mathrm{C}): M = G(K) \oplus C$

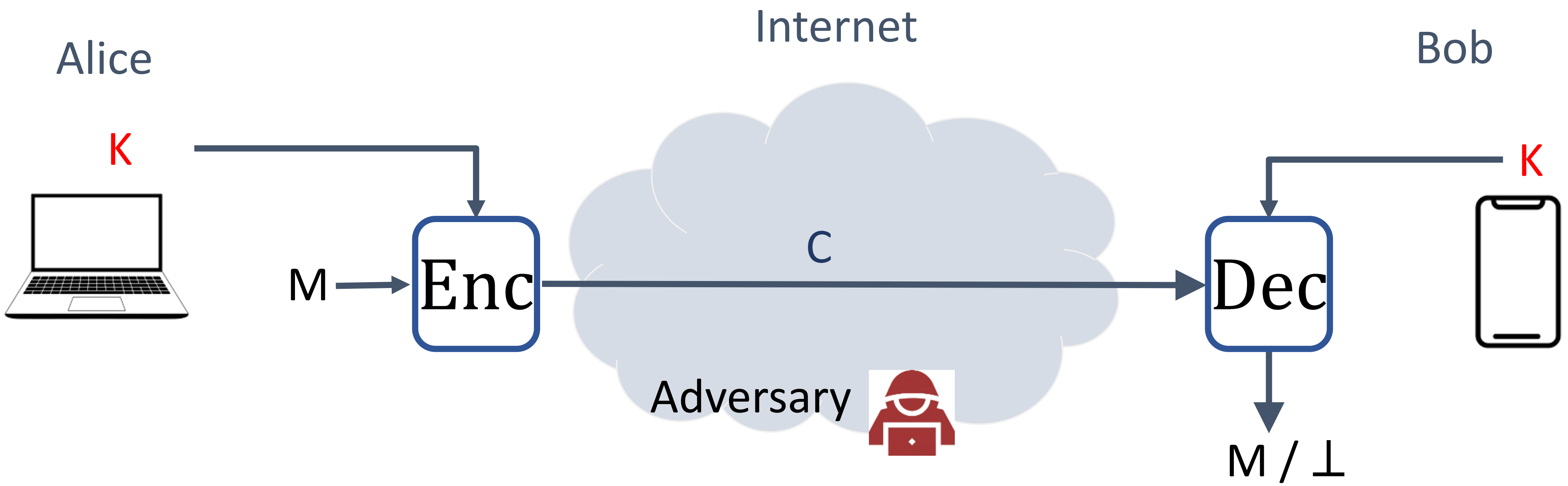




Big picture of Cryptography



Symmetric-key cryptography



Enc : encryption algorithm (public)

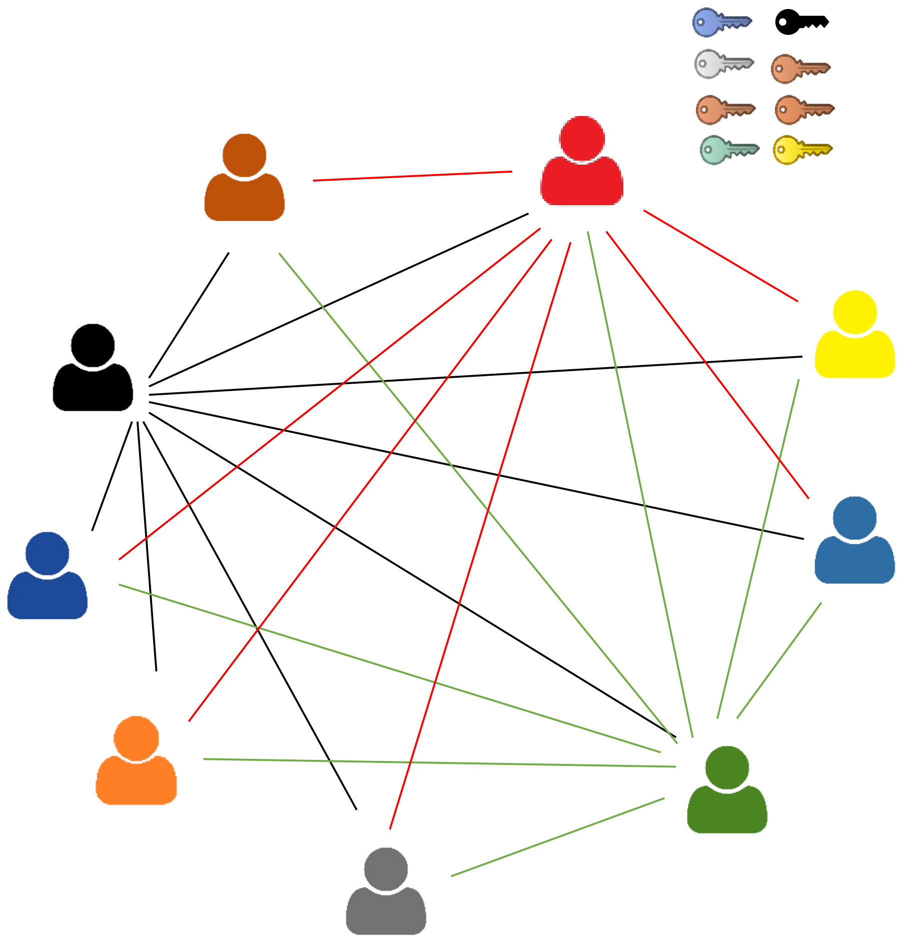
Dec : decryption algorithm (public)

K : shared key between Alice and Bob

Ignore for now: How to achieve this??

Drawback of symmetric key

- One user needs to store N symmetric keys when communicating with N other users
- $\frac{N(N-1)}{2} = \mathcal{O}(N^2)$ keys in total
- Difficult to store and manage so many keys securely



$G = \langle g \rangle$

$$A = g^{a} \longrightarrow$$

$$B = g^{b} \longleftarrow$$

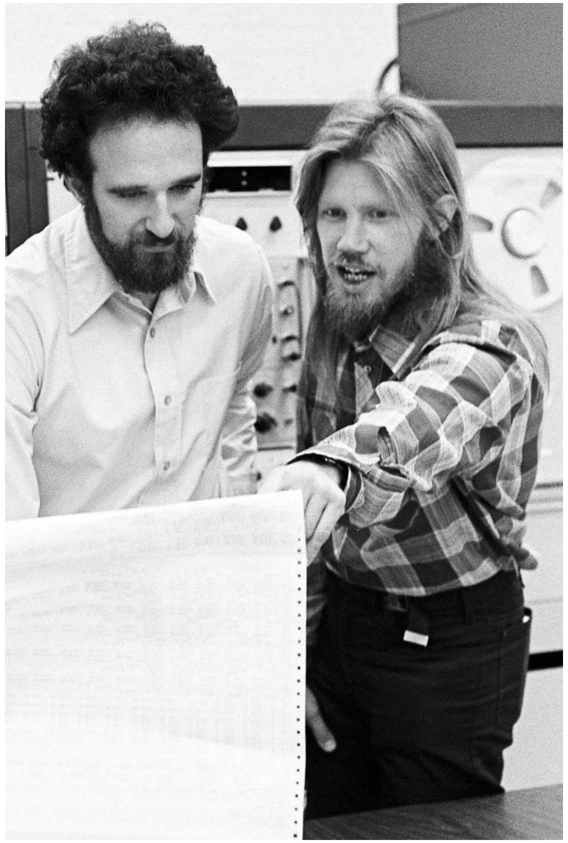
$K \leftarrow B^{a} = g^{ab}$

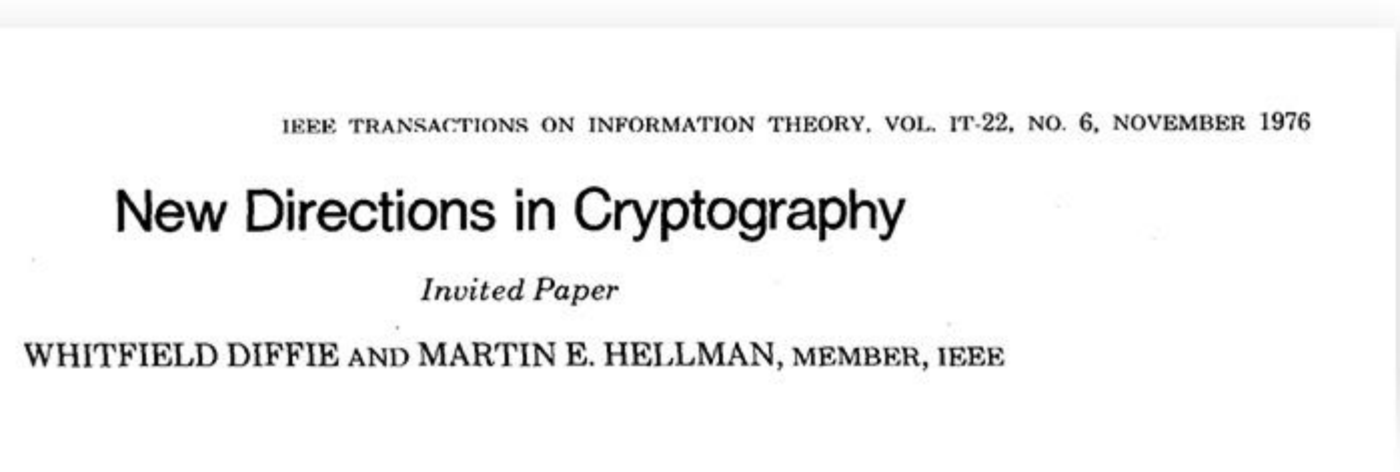
$K \leftarrow A^{b} = g^{ab}$

Diffie-Hellman Key Exchange

PKC

- Diffie-Hellman 1976 [New Directions in Cryptography]





IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

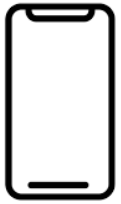
New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Diffie-Hellman Key Exchange

$G = \langle g \rangle$ ← public



$A = g^{a}$

$B = g^{b}$

$a \stackrel{\$}{\leftarrow} \{1, \ldots, |G|\}$

$b \stackrel{\$}{\leftarrow} \{1, \ldots, |G|\}$

$\mathrm{K} \leftarrow B^{a} = g^{ab}$

$\mathrm{K} \leftarrow A^{b} = g^{ab}$

Examples:

$G = (\boldsymbol{Z}_p^*, \cdot)$

$G = (E(\boldsymbol{Z}_p), +)$

G=($\boldsymbol{Z}_p^*$,·) preliminary

(integers) $\boldsymbol{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$

(integers "residue mod n") $\boldsymbol{Z}_n = \{0, 1, 2, \dots, n-1\}$

(integers "residue mod p") $\boldsymbol{Z}_p = \{0, 1, 2, \dots, p-1\}$ $\boldsymbol{Z}_p^* = \boldsymbol{Z}_p \setminus \{0\}$ p is a prime

Examples:

$$\boldsymbol{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

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

Define Group

Definition: A **group** $(G,\circ)$ is a set G together with a binary operation $\circ$ satisfying the following axioms.

$\mathbf{1}$: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c, \in G$ (associativity)

$\mathbf{2}$: $\exists e \in G$ such that $e \circ a = a \circ e = a$ for all $a \in G$ (identity)

$\mathbf{3}$: $\forall a \in G$ there exists $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$ (inverse)

A group is **commutative** if: $a \circ b = b \circ a$ for all $a, b \in G$

The **order** of a group is the number of elements in G, denoted $|G|$

Examples

Definition: A **group** $(G,\circ)$ …

1: $(a \circ b) \circ c = a \circ (b \circ c)$ (associativity)
2: $\exists e \in G: e \circ a = a \circ e = a$ (identity)
3: $\exists a^{-1} \in G:\ a \circ a^{-1} = a^{-1} \circ a = e$ (inverse)

Groups

$(\boldsymbol{Z}, +)$ $\quad e = 0 \quad "3^{-1}" = -3$

$(\boldsymbol{Z}_n, +_n)$ $\quad e = 0 \quad "3^{-1}" = x:\ \ 3 + x \equiv 0 \bmod n$

$(\boldsymbol{Z}_p^*, \ \cdot_p)$ $\quad e = 1$

$"3^{-1}" = x:\ \ 3 \cdot x \equiv 1 \bmod p$

Not groups

$(\boldsymbol{Z}, \cdot)$ $\quad 2^{-1} = ?$

$(\boldsymbol{Z}, -)$ $\quad (1-2) - 3 \neq 1 - (2-3)$

$(\boldsymbol{Z}_n, \cdot_n)$ $\quad 2x = 1 \pmod 4$?

Group arithmetic

$$g^0 \overset{\text{def}}{=} e$$

$$g^n \overset{\text{def}}{=} \overbrace{g \circ g \circ \cdots \circ g}^{n}$$

$$g^{-n} \overset{\text{def}}{=} (g^{-1})^n$$

Fact: $$g^n g^m = \underbrace{\overbrace{g \circ \cdots \circ g}^{n} \circ \overbrace{g \circ \cdots \circ g}^{m}}_{n+m} = g^{n+m}$$

Fact: $$(g^n)^m = g^{nm} = (g^m)^n$$

$(\boldsymbol{Z}_7^*, \cdot)$

$3^5\ mod\ 7 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 81 \cdot 3\ mod\ 7 = 5$

Cyclic groups

Definition: A **group** $(G,\circ)$ is **cyclic** if there exists $g \in G$ such that

$$G = \{\, g^i \mid i \in \boldsymbol{Z} \,\} = \{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, g^3, \dots\}$$

Element g is called a **generator** for G and we write $(G,\circ) = \langle g \rangle$

Examples:

$$(\boldsymbol{Z}, +) = \langle 1 \rangle$$

$$(\boldsymbol{Z}_n, +_n) = \langle 1 \rangle$$

$$(\boldsymbol{Z}_p^*, \cdot) = \langle a \rangle$$

$$\begin{aligned}(\boldsymbol{Z}_7^*, \cdot) &= \langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} \\ &= \langle 5 \rangle = \{5^0, 5^1, 5^2, 5^3, 5^4, 5^5\} = \{1, 5, 4, 6, 2, 3\} \\ &\neq \langle 2 \rangle = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4, 1, 2, 4\} = \{1, 2, 4\}\end{aligned}$$

Cyclic groups

Theorem: if $(G, \circ)$ is a finite group, then for all $g \in G$:

$$g^{|G|} = e$$

Proof (finite cyclic groups):

$|G| = |\langle g \rangle| = n$

$$\overbrace{e \quad g^1 \quad g^2 \quad g^3 \quad \cdots \quad g^{n-1}}^{G} \quad g^n \quad g^{n+1} \quad g^{n+2} \quad \cdots$$

$g^n = g^3 \quad \Longrightarrow \quad g^{n-3} = e \quad \Longrightarrow \quad g^j = e \quad j < n$ contradiction!

Corollary I: $g^i = g^{i \bmod n} = g^{i \bmod |G|}$

$$(\boldsymbol{Z}_7^*, \cdot) = \langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\}$$
$$= \langle 5 \rangle = \{5^0, 5^1, 5^2, 5^3, 5^4, 5^5\} = \{1, 5, 4, 6, 2, 3\}$$
$$\neq \langle 2 \rangle = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4, 1, 2, 4\} = \{1, 2, 4\}$$

$\langle 2 \rangle$ is a sub-group of $(\boldsymbol{Z}_7^*, \cdot)$ with order 3

Suppose $p = 2q + 1$, with q being prime. $(\boldsymbol{Z}_p^*, \cdot)$ has a sub-group $\langle g \rangle$ of order q

Denoted by $\langle g \rangle < \boldsymbol{Z}_p^*$

Example: $\boldsymbol{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

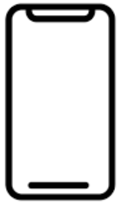
$11 = 2 \cdot 5 + 1$

For $g = 3,4,5,9$, $\langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 9 \rangle = \{1, 3, 4, 5, 9\} < \boldsymbol{Z}_{11}^*$

https://sagecell.sagemath.org/

Diffie-Hellman Key Exchange

$G = \langle g \rangle$ public



$$A = g^{a}$$

$$B = g^{b}$$

$a \xleftarrow{\$} \{1, \ldots, |G|\}$

$b \xleftarrow{\$} \{1, \ldots, |G|\}$

$\mathrm{K} \leftarrow B^{a} = g^{ab}$

$\mathrm{K} \leftarrow A^{b} = g^{ab}$

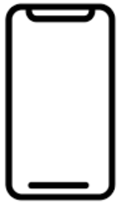
Examples:

$G = (\boldsymbol{Z}_p^*, \cdot)$

Diffie-Hellman Key Exchange

public

$G = \langle g = 3 \rangle$



$\xrightarrow{A = 9 = 3^2 \bmod 11}$

$\xleftarrow{B = 5 = 3^3 \bmod 11}$

$2 \overset{\$}{\leftarrow} \{1, \dots, 5\}$

$3 \overset{\$}{\leftarrow} \{1, \dots, 5\}$

$\mathrm{K} = 4 \leftarrow B^a = g^{ab}$

$\mathrm{K} = 4 \leftarrow A^b = g^{ab}$

Exp. $G = (\boldsymbol{Z}_p^*, \cdot), p = 11, g = 3$

To be secure: length p must be large

https://www.rfc-editor.org/rfc/rfc2409#section-6.2; rfc3526#page-3

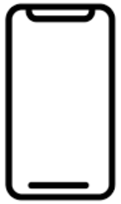
Diffie-Hellman Key Exchange

$G = \langle g \rangle$ public

Capability:
Passive adversary

$A = g^a$

$B = g^b$



$\mathrm{K} \leftarrow B^a = g^{ab}$

$\mathrm{K} \leftarrow A^b = g^{ab}$

Aim: $\mathrm{K} \approx_c$ random key???

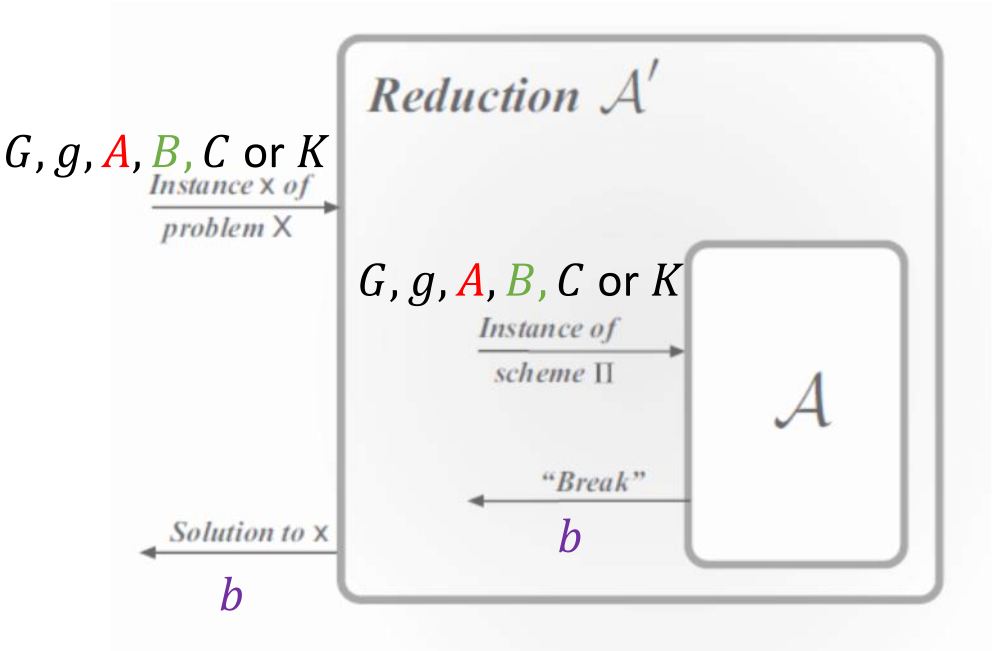
Security (given G, g, A, B):

- Must be hard to distinguish $\mathrm{K} \leftarrow g^{ab}$ from random key

Proof security under DH assumption

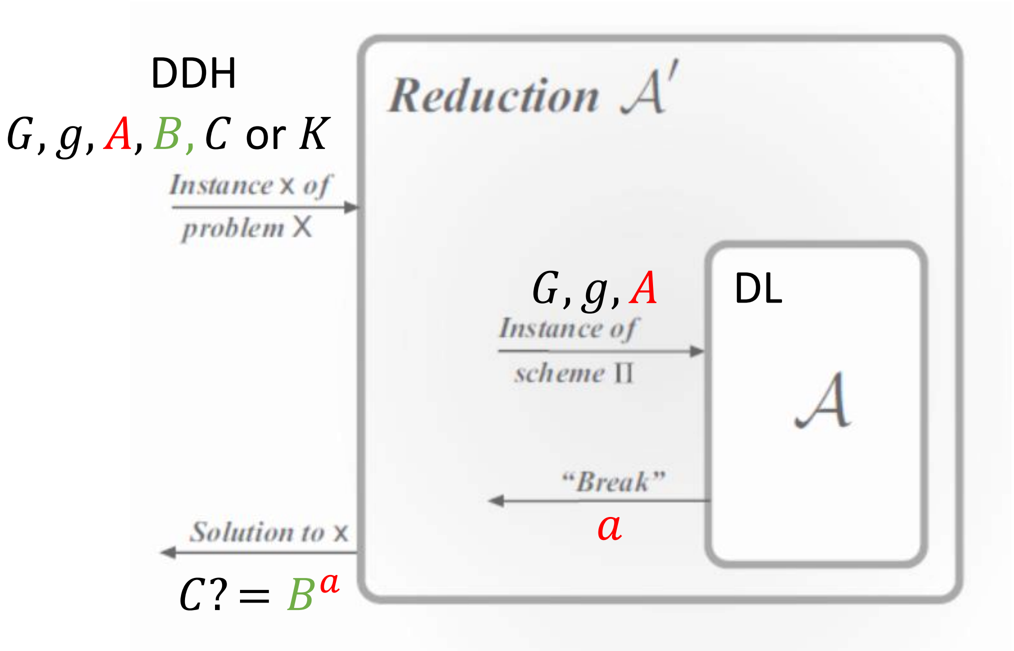
DDH assumption: **given** G, g, A, B**:**

- Must be hard to distinguish $\mathrm{K} \leftarrow g^{ab}$ from random key C



Discrete logarithm (DL) assumption

Discrete logarithm assumption: **given** G, g, A**:**
- it is hard to find a such that $A = g^a$



DDH assumption: **given** G, g, A, B**:**
- Must be hard to distinguish $\mathrm{K} \leftarrow g^{ab}$ from random key C

DL ≥ DDH

To let DDH assumption holds, $|< g >|$ should be large

Diffie-Hellman $-(\boldsymbol{Z}_p^*,\cdot)$ -group 14 of RFC 3526

$p =$ 32317006071311007300338913926423828248817941241140239112842009751400741706634354222619689417363569347117901737909704191754605873209195028853758986185622153212175412514901774520270235796078236248884246189477587641
105928646099411723245426622522193230540919037680524235519125679715870117001058055877651038861847280257976054903569732561526167081339361799541336476559160368317896729073178384589680639671900097720219416864722587103
141133642931953619347163653320971707744822798858856536920864529663607725026895550592836275112117409697299806841055435958486658329164213621823107899099944865246826241697203591185250704536109055 9

$= 2 \cdot q + 1$

$\langle g \rangle = \langle 2 \rangle < (\boldsymbol{Z}_p^*,\cdot)$

$A = 2$ 41334972764978697476888131477953691590598302888048789 1
41980374225868022299895295637179960494385138311397470 8
27349590849981792329486604009042615297868979897330484 9
21927831225177595784265889055839696808031719452907682 5
13329106414714573595610370323158171874543264533536374 2
42406009085230708167811180522224268061203552983076449 5
48543977119571456641273876821013022850701466853350734 6
34588800753314418345842915139086907784354458905455294 4
06190328202385893725332194725264134364059863364082229 1
60749341432910198888044659747023558016168252167306980 6
05647973065295774322785381793841598013402958235279155 8
061335118703485395914 9 $\bmod p$

$\xrightarrow{\hspace{3em}}$

41334972764978697476888131477953691590598302888048789 1
41980374225868022299895295637179960494385138311397470 8
27349590849981792329486604009042615297868979897330484 9
21927831225177595784265889055839696808031719452907682 5
13329106414714573595610370323158171874543264533536374 2
42406009085230708167811180522224268061203552983076449 5
48543977119571456641273876821013022850701466853350734 6
34588800753314418345842915139086907784354458905455294 4
06190328202385893725332194725264134364059863364082229 1
60749341432910198888044659747023558016168252167306980 6
05647973065295774322785381793841598013402958235279155 8
061335118703485395914 9 $\overset{\$}{\leftarrow} \{1 \dots q\}$

$B = 2$ 47237897596539658251883225633564531876117073609653596 8
57880669992230757150404954632247448495838204004394852 8
92967126950710924526617462128447779993791896462878963 1
23481522726270693237920555856790321199248897271347298 27
72848744522640803022909928099136539284836286481767224 1
30593205980001749703989217159254733610890590640543624 6
69876206617841554271770719791386563503187312354629674 8
60703821404739110104286042063247209755506195200644989 0
56168347836274008201576298205028867732402557380478014 9
80309799207390616115837997519340000775681197631190406 7
31683727944709941956370245115081620783256133515159656 0
05724264334220129144 0 $\bmod p$

$\xleftarrow{\hspace{3em}}$

47237897596539658251883225633564531876117073609653596 8
57880669992230757150404954632247448495838204004394852 8
92967126950710924526617462128447779993791896462878963 1
23481522726270693237920555856790321199248897271347298 27
72848744522640803022909928099136539284836286481767224 1
30593205980001749703989217159254733610890590640543624 6
69876206617841554271770719791386563503187312354629674 8
60703821404739110104286042063247209755506195200644989 0
56168347836274008201576298205028867732402557380478014 9
80309799207390616115837997519340000775681197631190406 7
31683727944709941956370245115081620783256133515159656 0
05724264334220129144 0 $\overset{\$}{\leftarrow} \{1 \dots q\}$

Corollary I: $g^i = g^{i \bmod |H|}$

$Z \leftarrow 2$ 41334972764978697476888131477953691590598302888048789 1
41980374225868022299895295637179960494385138311397470 8
27349590849981792329486604009042615297868979897330484 9
21927831225177595784265889055839696808031719452907682 5
13329106414714573595610370323158171874543264533536374 2
42406009085230708167811180522224268061203552983076449 5
48543977119571456641273876821013022850701466853350734 6
34588800753314418345842915139086907784354458905455294 4
06190328202385893725332194725264134364059863364082229 1
60749341432910198888044659747023558016168252167306980 6
05647973065295774322785381793841598013402958235279155 8
061335118703485395914 9 $\times$ 47237897596539658251883225633564531876117073609653596 8
57880669992230757150404954632247448495838204004394852 8
92967126950710924526617462128447779993791896462878963 1
23481522726270693237920555856790321199248897271347298 27
72848744522640803022909928099136539284836286481767224 1
30593205980001749703989217159254733610890590640543624 6
69876206617841554271770719791386563503187312354629674 8
60703821404739110104286042063247209755506195200644989 0
56168347836274008201576298205028867732402557380478014 9
80309799207390616115837997519340000775681197631190406 7
31683727944709941956370245115081620783256133515159656 0
05724264334220129144 0 $\bmod p$

Demo

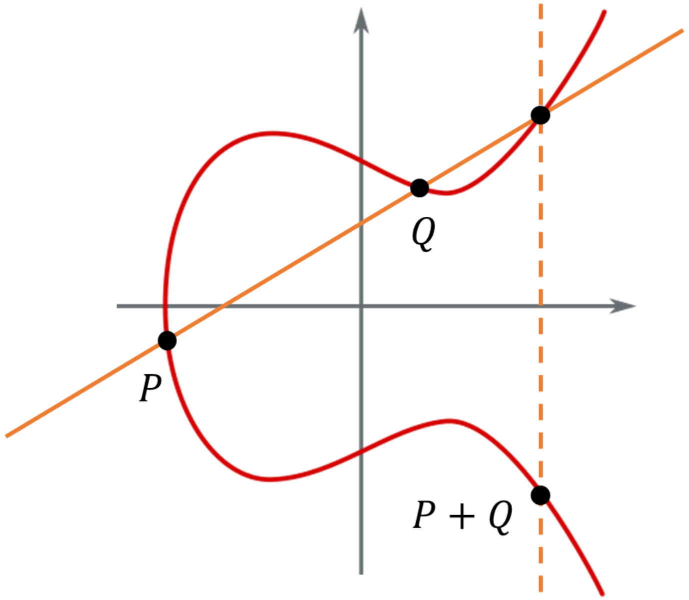
- RFC 3526
- Demonstration using SageMath
- https://sagecell.sagemath.org/

Better alternatives to $\boldsymbol{Z}_p^*$?

Elliptic curves

$$y^2 = x^3 + ax + b$$

$$a, b, x, y \in \boldsymbol{R}$$



- There is elliptic curves defined over $\boldsymbol{Z}_p$
- Such that the points on an elliptic curve (+ a infinite point) form a group of order $\sim p^2$
- Denoted by $(E(\boldsymbol{Z}_p), +)$

Cryptographic groups in practice

- $(\boldsymbol{Z}_p^*, \cdot)$ groups:
  - **TLS 1.3:** five specific groups allowed
    - size $\approx 2^{2048}, 2^{3072}, 2^{4096}, 2^{6144}, 2^{8192}$ (RFC 7919)
  - **IKEv2** (IPsec key exchange protocol): MODP groups
    - size $\approx 2^{768}, 2^{1024}, 2^{1536}, 2^{2048}, 2^{3072}, 2^{4096}, 2^{6144}, 2^{8192}$ (RFC 7296 and RFC 3526)
  - all p's are **safe primes** (i.e., of the form $p = 2q + 1$ where q is prime)

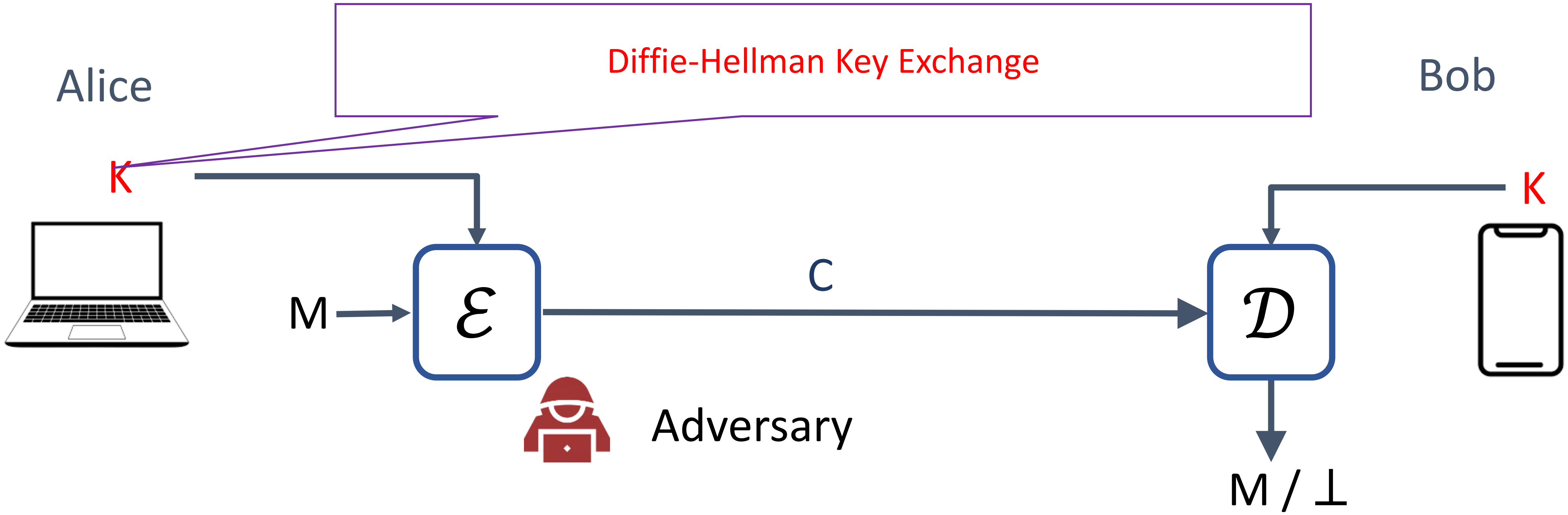
- $(E(\boldsymbol{Z}_p), +)$ groups
  - NIST groups: P-224, P-256, P-384, P-521
  - Curve25519 ($E : y^2 = x^3 + 486662x^2 + x$ and $p = 2^{255} - 19$) (Daniel J. Bernstein)
  - Curve448 ($E : y^2 + x^2 = 1 - 39081x^2y^2$ and $p = 2^{448} - 2^{224} - 1$) (Mike Hamburg)

A short summary

- Diffie-Hellman Key Exchange could help to share a secret
- Using group $(\boldsymbol{Z}_p^*, \cdot)$ or $(E(\boldsymbol{Z}_p), +)$
- DH problem is the underlying hard problem

Public key encryption

Diffie-Hellman then Symmetric-key cryptography

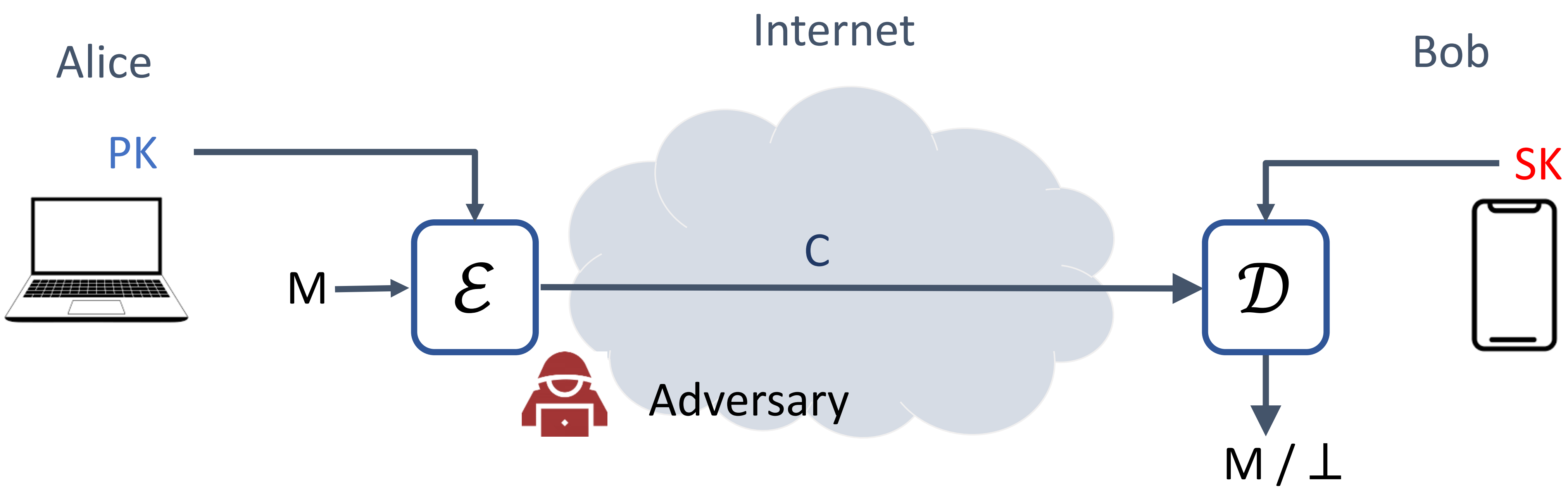


Enc: encryption algorithm (public)

Dec: decryption algorithm (public)

K : shared key between Alice and Bob

Public-key Encryption directly???



Enc: encryption algorithm (public)

PK : public key of Bob (public)

Dec : decryption algorithm (public)

SK : secret key (secret)

Public-key encryption – syntax

A **public-key encryption scheme** is a tuple $\Sigma = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ of algorithms

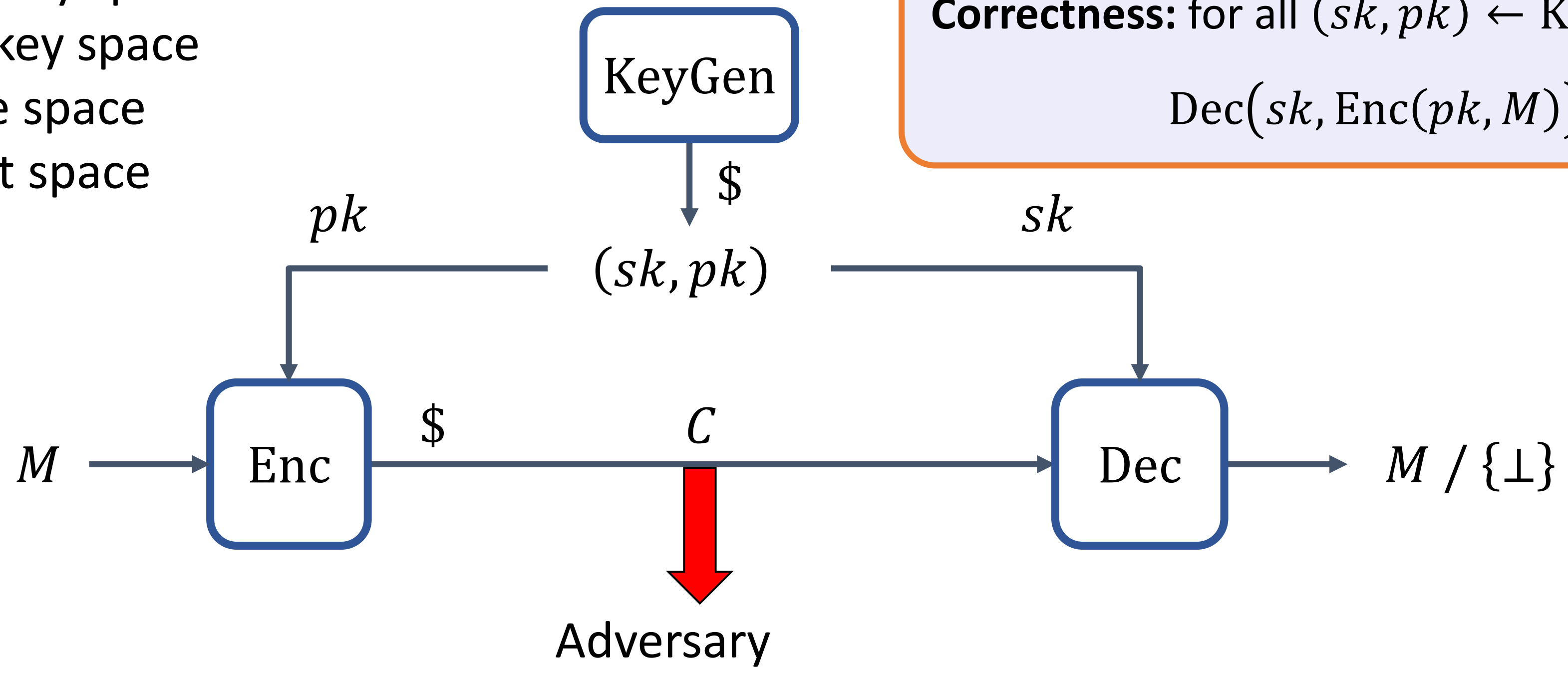
$$\mathrm{Enc} : \mathcal{PK} \times \mathcal{M} \to \mathcal{C} \qquad \mathrm{Dec} : \mathcal{SK} \times \mathcal{C} \to \mathcal{M} \cup \{\perp\}$$

$$(sk, pk) \xleftarrow{\$} \mathrm{KeyGen} \qquad \mathrm{Enc}(pk, M) = \mathrm{Enc}_{pk}(M) = C \qquad \mathrm{Dec}(sk, C) = \mathrm{Dec}_{SK}(C) = M/\perp$$

- $\mathcal{SK}$ – private key space
- $\mathcal{PK}$ – public key space
- $\mathcal{M}$ – message space
- $\mathcal{C}$ – ciphertext space

Correctness: for all $(sk, pk) \leftarrow \mathrm{KeyGen}$:

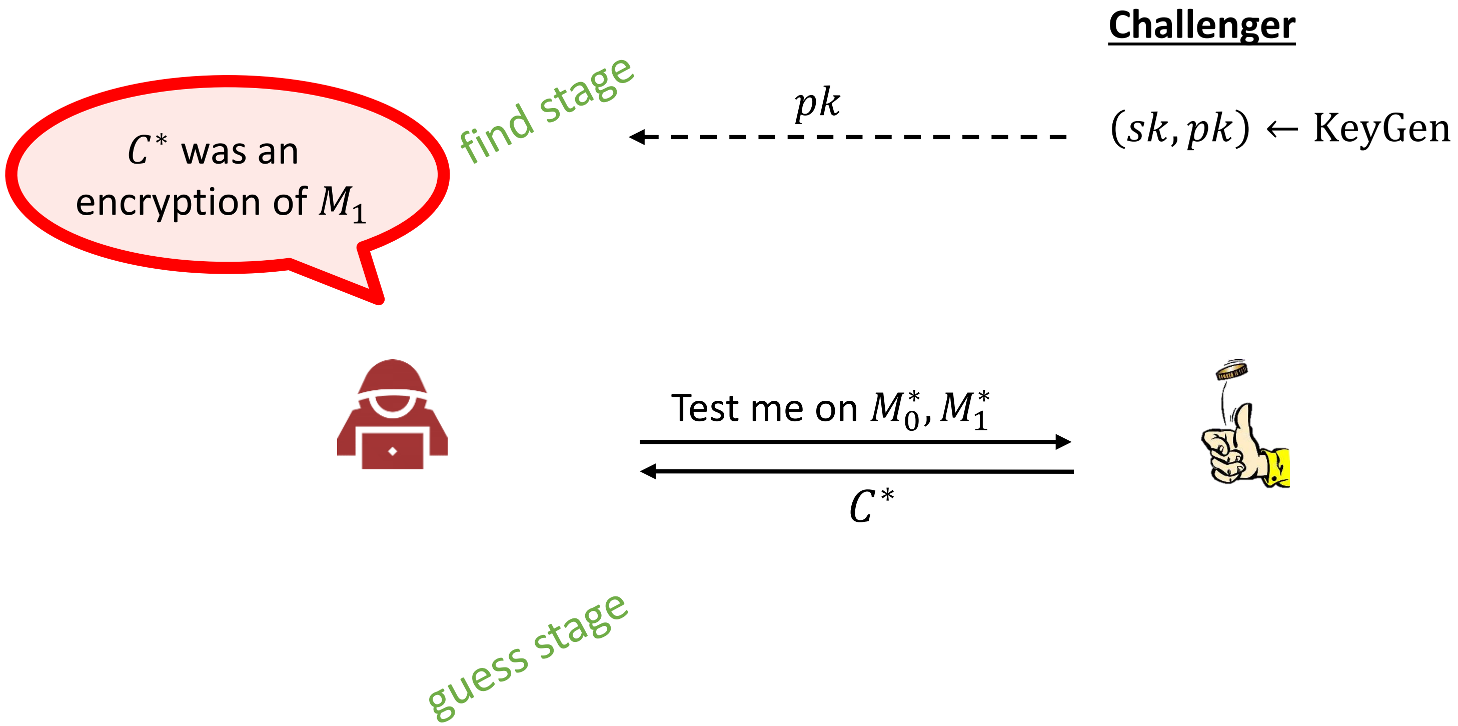
$$\mathrm{Dec}\big(sk, \mathrm{Enc}(pk, M)\big) = M$$



Public-key encryption – security: IND-CPA

$\mathbf{Exp}_{\Sigma}^{\text{ind-cpa}}(A)$

$b \xleftarrow{\$} \{0,1\}$
$(sk, pk) \xleftarrow{\$} \Sigma.\mathrm{KeyGen}$
$M_0^*, M_1^* \leftarrow A(pk)$ // find stage
if $|M_0^*| \neq |M_1^*|$ **then**
  return $\perp$
$C^* \leftarrow \Sigma.\mathrm{Enc}(pk, M_b^*)$
$b' \leftarrow A(pk, C^*)$ // guess stage
return $b' \stackrel{?}{=} b$



Definition: The **IND-CPA-advantage** of an adversary A is

$$\mathbf{Adv}_{\Sigma}^{\text{ind-cpa}}(A) = \left|2 \cdot \Pr\left[\mathbf{Exp}_{\Sigma}^{\text{ind-cpa}}(A) \Rightarrow \mathrm{true}\right] - 1\right|$$

Public-key encryption – security: IND-CCA

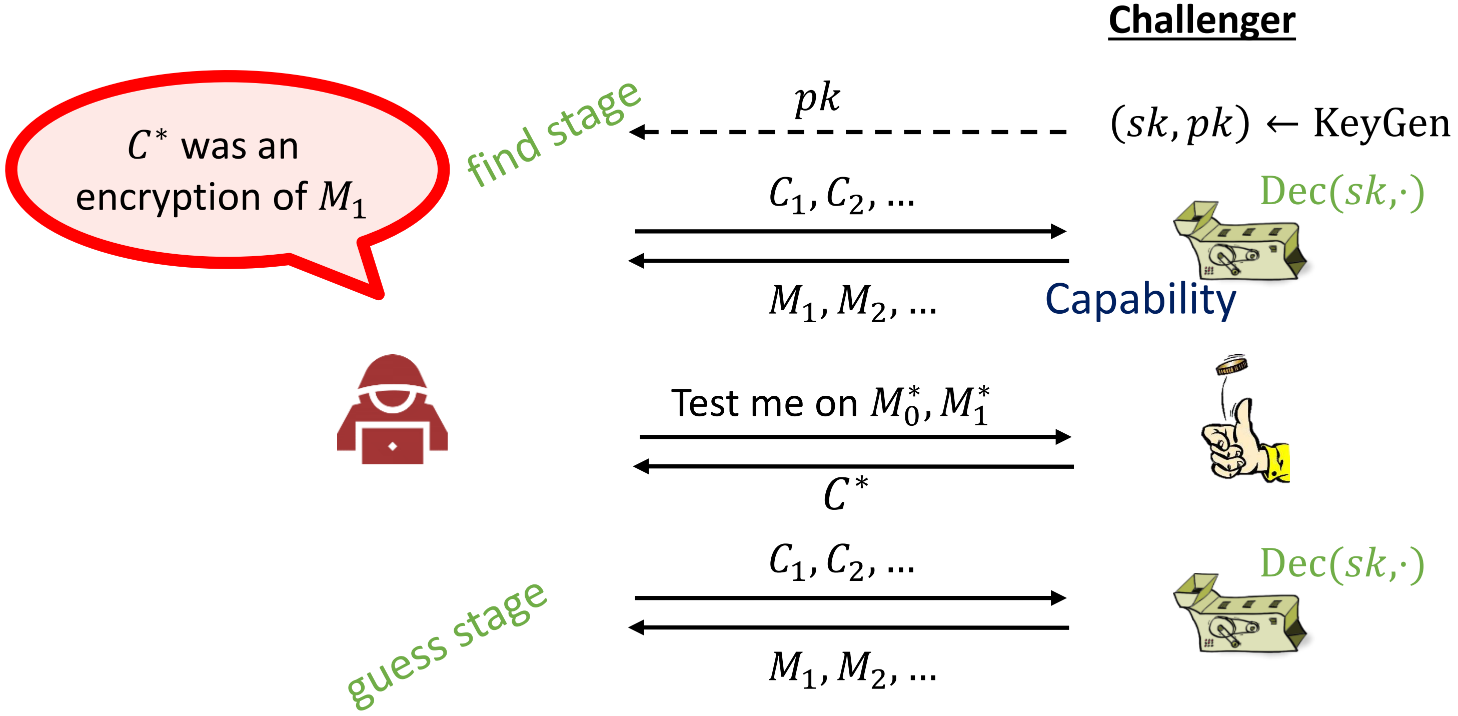
$\mathbf{Exp}_{\Sigma}^{\text{ind-cca}}(A)$

$b \xleftarrow{\$} \{0,1\}$
$(sk, pk) \xleftarrow{\$} \Sigma.\mathrm{KeyGen}$
$M_0^*, M_1^* \leftarrow A^{\mathcal{D}_{sk}(\cdot)}(pk)$ // find stage
if $|M_0^*| \neq |M_1^*|$ **then**
  return $\perp$
$C^* \leftarrow \Sigma.\mathrm{Enc}(pk, M_b^*)$
$b' \leftarrow A^{\mathcal{D}_{sk}(\cdot)}(pk, C^*)$ // guess stage
return $b' \stackrel{?}{=} b$

$\mathcal{D}_{sk}(C)$

---

if $C = C^*$ **the** // cheating!
  return $\perp$
return $\Sigma.\mathrm{Dec}(sk, C)$



Definition: The **IND-CCA-advantage** of an adversary A is

$$\mathbf{Adv}_{\Sigma}^{\text{ind-cca}}(A) = \left|2 \cdot \Pr\left[\mathbf{Exp}_{\Sigma}^{\text{ind-cca}}(A) \Rightarrow \text{true}\right] - 1\right|$$

Scheme ElGamal

$$G = \langle g \rangle$$

$$\xrightarrow{\quad A \quad}$$

$$\xleftarrow{\quad B \quad}$$

$$b \stackrel{\$}{\leftarrow} \{1, \dots, |G|\}$$

$$B \leftarrow g^{b}$$

$$a \stackrel{\$}{\leftarrow} \{1, \dots, |G|\}$$

$$A \leftarrow g^{a}$$

$$K \leftarrow B^{a} = g^{ab}$$

$$K \leftarrow A^{b} = g^{ab}$$

ElGamal

$$G = \langle g \rangle$$

$$b \xleftarrow{\$} \{1, \dots, |G|\}$$

$$B \leftarrow g^{b}$$

$$\xleftarrow{\quad B \quad}$$

$$\xrightarrow{\quad A \quad}$$

$$a \xleftarrow{\$} \{1, \dots, |G|\}$$

$$A \leftarrow g^{a}$$

$$K \leftarrow B^{a} = g^{ab}$$

$$K \leftarrow A^{b} = g^{ab}$$

ElGamal

$$G = \langle g \rangle$$

$b \xleftarrow{\$} \{1, \dots, |G|\}$

$B \leftarrow g^b$

$\xleftarrow{\quad B \quad}$

$\xrightarrow{\quad A, C \quad}$

$a \xleftarrow{\$} \{1, \dots, |G|\}$

$A \leftarrow g^a$

$K \leftarrow B^a = g^{ab}$

$C \leftarrow K \cdot M$

$K \leftarrow A^b = g^{ab}$

$M \leftarrow C/K$

ElGamal

$$G = \langle g \rangle$$

KeyGen

1. $sk = b \xleftarrow{\$} \{1, \dots, |G|\}$
2. $pk = B \leftarrow g^b$
3. **return** (sk, pk)

$\xleftarrow{\quad B \quad}$

$\xrightarrow{\quad A, C \quad}$

$a \xleftarrow{\$} \{1, \dots, |G|\}$

$A \leftarrow g^a$

$K \leftarrow B^a = g^{ab}$

$C \leftarrow K \cdot M$

$K \leftarrow A^b = g^{ab}$

$M \leftarrow C/K$

ElGamal

$$G = \langle g \rangle$$

B

A, C

KeyGen

1. $sk = b \xleftarrow{\$} \{1, \dots, |G|\}$
2. $pk = B \leftarrow g^b$
3. **return** (sk, pk)

Enc(pk, M)

1. $a \xleftarrow{\$} \{1, \dots, |G|\}$
2. $A \leftarrow g^a$
3. $K \leftarrow B^a = g^{ab}$
4. $C \leftarrow K \cdot M$
5. **return** (A, C)

$$Z \leftarrow A^b = g^{ab}$$

$$M \leftarrow C/K$$

ElGamal

$\mathrm{ElGamal.Enc}: G \times G \to \quad G \times \mathcal{C}$

$\mathrm{ElGamal.Dec}: \boldsymbol{Z}_p \times G \times G \to G$

$$G = \langle g \rangle$$

$\xleftarrow{\quad B \quad}$

$\xrightarrow{\quad A, C \quad}$

KeyGen

1. $sk = \ b \xleftarrow{\$} \{1, \dots, |G|\}$
2. $pk = \ B \leftarrow g^b$
3. **return** (sk, pk)

Enc$(\boldsymbol{pk}, \boldsymbol{M})$

1. $a \xleftarrow{\$} \{1, \dots, |G|\}$
2. $A \leftarrow g^a$
3. $K \leftarrow B^a = g^{ab}$
4. $C \leftarrow K \cdot M$
5. **return** (A, C)

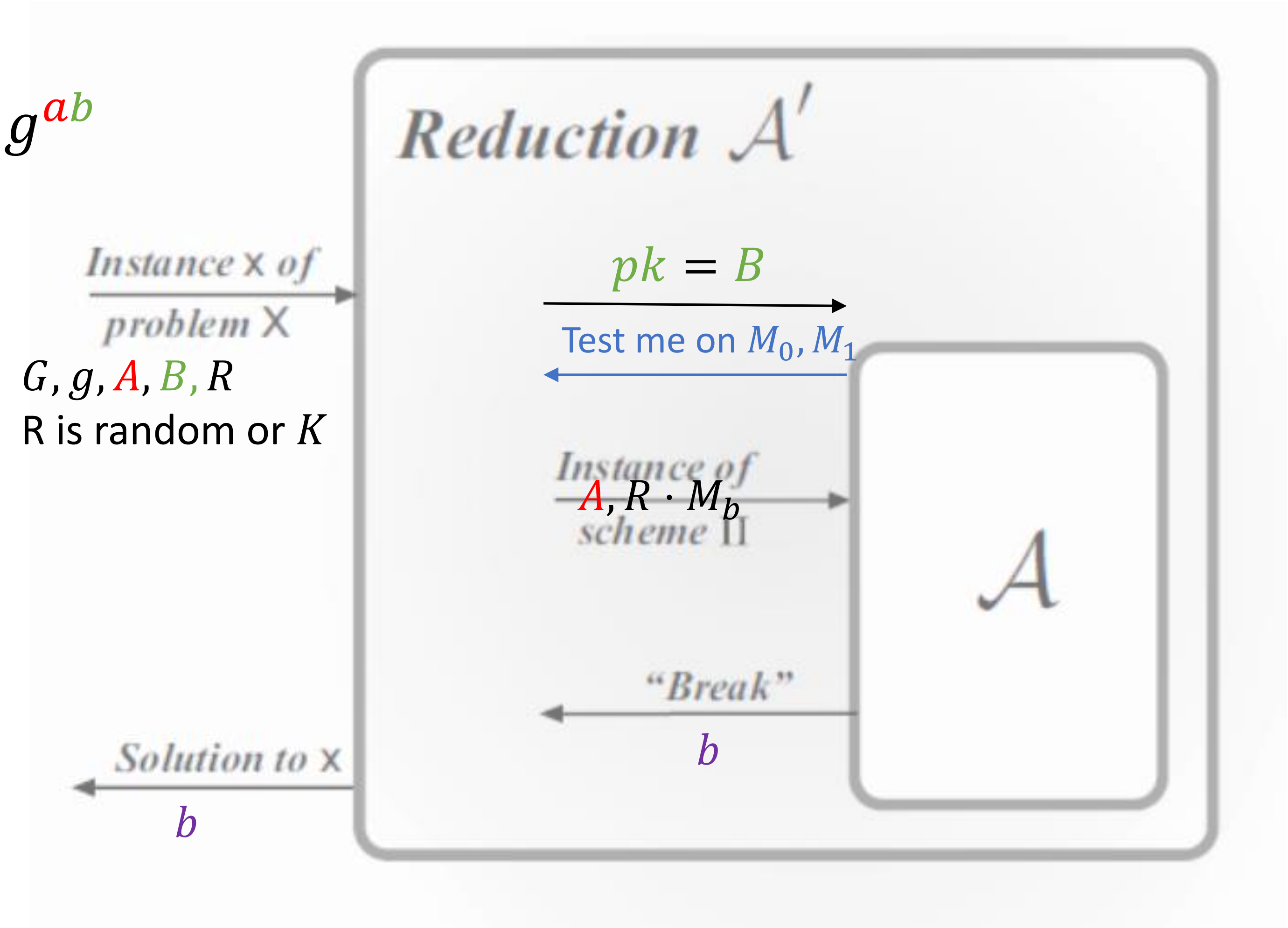
Dec$(\boldsymbol{sk}, \boldsymbol{C})$

1. $Z \leftarrow A^b = g^{ab}$
2. $M \leftarrow C/K$
3. **return** M

ElGamal is IND-CPA under DDH assumption

DDH assumption: **given** G, g, A, B**:**

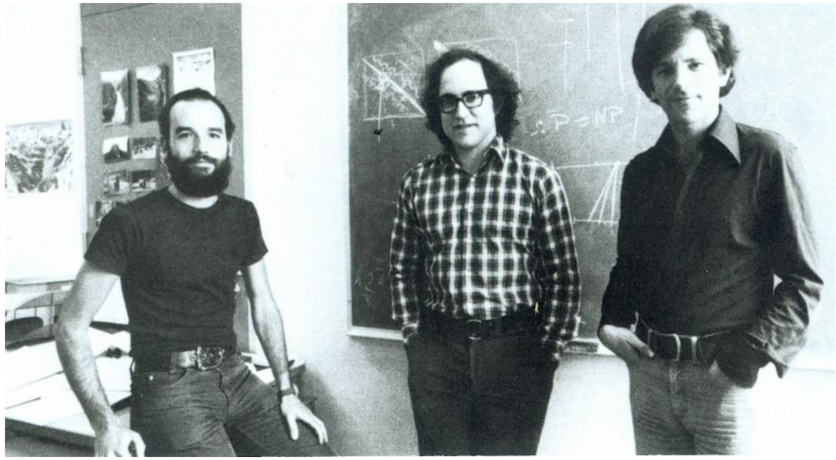
- Must be hard to distinguish $\mathrm{K} \leftarrow g^{ab}$ from random key R



RSA in 1977

- The RSA encryption scheme

$$c = E\,(m) = m^e \pmod N$$



Adi Shamir Ron Rivest Leonard Adleman

The group $(\boldsymbol{Z}_n^*, \cdot)$

$\boldsymbol{Z}_p = \{0, 1, \dots, p-1\}$ $\quad$ $(\boldsymbol{Z}_p, \cdot)$ is *not* a group!

$\boldsymbol{Z}_p^* = \{1, \dots, p-1\}$ $\quad$ $(\boldsymbol{Z}_p^*, \cdot)$ *is* a group!

$\boldsymbol{Z}_n = \{0, 1, \dots, n-1\}$ $\quad$ $(\boldsymbol{Z}_n, \cdot)$ is *not* a group!

$\boldsymbol{Z}_n^* \neq \underbrace{\{1, \dots, n-1\}}_{\boldsymbol{Z}_n^+}$ $\quad$ $(\boldsymbol{Z}_n^+, \cdot)$ is *also not* a group!

$$\boldsymbol{Z}_n^* = \underbrace{\text{invertible elements in } \boldsymbol{Z}_n}_{(\boldsymbol{Z}_n^*, \cdot) \textit{ is} \text{ a group!}} = \{\, a \in \boldsymbol{Z}_n \mid \gcd(a, n) = 1 \,\}$$

Not invertible	Invertible
$2, 4, 5, 6, 8$	$1, 3, 7, 9$

$\boldsymbol{Z}_{10}^+ = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$2 \cdot 1 = 2 \mod 10$

$2 \cdot 2 = 4 \mod 10$

$2 \cdot 3 = 6 \mod 10$

$2 \cdot 4 = 8 \mod 10$

$2 \cdot 5 = 0 \mod 10$

$2 \cdot 6 = 2 \mod 10$

$2 \cdot 7 = 4 \mod 10$

$2 \cdot 8 = 6 \mod 10$

$2 \cdot 9 = 8 \mod 10$

$1 \cdot 1 = 1 \mod 10$

$3 \cdot 7 = 21 = 1 \mod 10$

$9 \cdot 9 = 81 = 1 \mod 10$

$10 = 2 \cdot 5$

$2 = 2$

$4 = 2 \cdot 2$

$5 = 5$

$6 = 2 \cdot 3$

$8 = 2 \cdot 2 \cdot 2$

$\boldsymbol{Z}_{10}^* = \{1,3,7,9\}$

Euler's $\phi(n)$ function

- $\phi(n) \overset{\text{def}}{=} |\boldsymbol{Z}_n^*| = |\{\, a \in \boldsymbol{Z}_n \mid \gcd(a, n) = 1 \,\}|$
- $\phi(p) = p - 1$
- $\phi(p \cdot q) = (p - 1) \cdot (q - 1)$
- **Note:** $\phi(n) \approx n - 2\sqrt{n} \approx n$
  - i.e.: *almost all* integers are invertible for large p, q

$$\overbrace{1 \cdot p,\ 2 \cdot p,\ 3 \cdot p,\ \cdots\ (q-1) \cdot p}^{q-1}$$

$$\underbrace{1 \cdot q,\ 2 \cdot q,\ 3 \cdot q,\ \cdots\ (p-1) \cdot q}_{p-1}$$

$$\phi(pq) = \#\text{numbers less than } pq - \#\text{numbers less than } pq \text{ with } \gcd(x, pq) \neq 1$$

$$= (pq - 1) - (q - 1 + p - 1)$$

$$= pq - q - p + 1$$

$$= (p - 1) \cdot (q - 1)$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$	**1**	**1**	**2**	**2**	**4**	**2**	**6**	**4**	**6**	**4**	**10**	**4**	**12**	**6**	**8**

Euler's Theorem

Theorem: if $(G,\circ)$ is a finite group, then for all $g \in G$:

$$g^{|G|} = e$$

- $(\boldsymbol{Z}_p^*,\cdot)$: $|\boldsymbol{Z}_p^*| = p - 1 \quad e = 1$

Fermat's theorem: if p is prime, then for all $a \neq 0 \pmod p$:

$$a^{p-1} \equiv 1 \pmod p$$

- $(\boldsymbol{Z}_n^*,\cdot)$: $|\boldsymbol{Z}_n^*| = \phi(n) \quad e = 1$

Euler's theorem: for all positive integers n, if $\gcd(a, n) = 1$ then

$$a^{\phi(n)} \equiv 1 \pmod n$$

Textbook RSA

$$\mathrm{RSA.Enc}: \underbrace{\mathbf{Z}^{+} \times \mathbf{Z}^{*}_{\phi(n)}}^{\mathcal{PK}} \times \overset{\mathcal{M}}{\mathbf{Z}^{*}_{n}} \to \overset{\mathcal{C}}{\mathbf{Z}^{*}_{n}}$$

$$\mathrm{RSA.Dec}: \underset{\mathcal{SK}}{\mathbf{Z}^{*}_{\phi(n)}} \times \underset{\mathcal{C}}{\mathbf{Z}^{*}_{n}} \to \underset{\mathcal{M}}{\mathbf{Z}^{*}_{n}}$$

Enc$(pk = (n, e), M \in \mathbf{Z}^{*}_{n})$

1. $C \leftarrow M^{e} \mod n$
2. **return** C

pk

C

KeyGen

1. $p, q \xleftarrow{\$}$ two random prime numbers
2. $n \leftarrow p \cdot q$
3. $\phi(n) = (p-1)(q-1)$
4. **choose** e such that $\gcd(e, \phi(n)) = 1$
5. $d \leftarrow e^{-1} \mod \phi(n)$
6. $sk \leftarrow d \quad pk \leftarrow (n, e)$
7. **return** (sk, pk)

Dec$(sk = d, C \in \mathbf{Z}^{*}_{n})$

1. $M \leftarrow C^{d} \mod n$
2. **return** M

Common choices of e: 3, 17, 65 537

$11_2 \quad 10001_2 \quad 1\,0000\,0000\,0000\,0001_2$

Textbook RSA – correctness

Theorem: if $(G,\circ)$ is a finite group, then for all $g \in G$:

$$g^{|G|} = e$$

Euler's theorem: for all $a \in \boldsymbol{Z}_n^*$

$$a^{\phi(n)} \equiv 1 \ (\mathrm{mod}\, n)$$

Corollary I: $a^i = a^{i \bmod |G|} = a^{i \bmod \phi(n)}$

$$\mathrm{Dec}\big(sk, \mathrm{Enc}(pk, M)\big) = M$$

$$d = e^{-1} \bmod \phi(n) \iff ed = 1 \bmod \phi(n)$$

$$C^d = M^{ed} = M^{ed \bmod \phi(n)} = M^1 = M \bmod n$$

Fact: RSA also works for $M \in \boldsymbol{Z}_n$

KeyGen

1. $p, q \xleftarrow{\$}$ two random prime numbers
2. $n \leftarrow p \cdot q$
3. $\phi(n) = (p-1)(q-1)$
4. **choose** e such that $\gcd\big(e, \phi(n)\big) = 1$
5. $d \leftarrow e^{-1} \bmod \phi(n)$
6. $sk \leftarrow d \quad pk \leftarrow (n, e)$
7. **return** (sk, pk)

Enc$(pk = (n, e), M \in \boldsymbol{Z}_n^*)$

1. $C \leftarrow M^e \bmod n$
2. **return** C

Dec$(sk = d, C \in \boldsymbol{Z}_n^*)$

1. $M \leftarrow C^d \bmod n$
2. **return** M

Textbook RSA – security

- Textbook RSA is *not* IND-CPA secure!
  - Deterministic
  - Malleable

- Many other attacks as well*

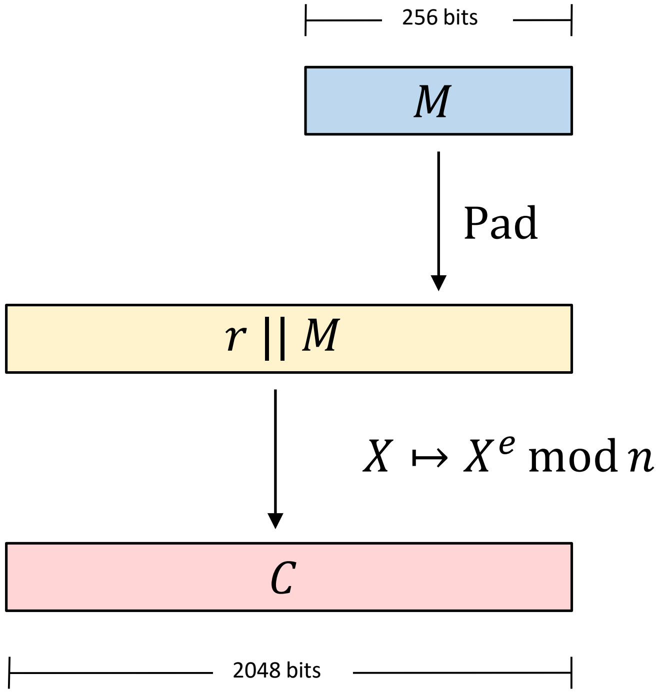
- Textbook RSA is *not* an encryption scheme!

- So what is it? Answer: a *one-way (trapdoor) permutation*

•* https://crypto.stackexchange.com/questions/20085/which-attacks-are-possible-against-raw-textbook-rsa

RSA in practice

- Textbook RSA is deterministic $\Longrightarrow$ cannot be IND-CPA secure
- How to achieve IND-CPA, IND-CCA?
  - *pad* message with random data before applying RSA function
  - PKCS#1v1.5 (RFC 2313)
  - RSA-OAEP (RFC 8017)
- RSA encryption not used much in practice anymore
- RSA digital signatures still very common



Hard problems

- RSA problem (RSA): given $pk = (e, n)$ and $C = M^e \bmod n$
  find M

- Factoring problem (FACT): given $n = pq$ find p and q

- FACT $\geq$ RSA

Demo RSA encryption

- Demonstration using SageMath

- https://sagecell.sagemath.org/

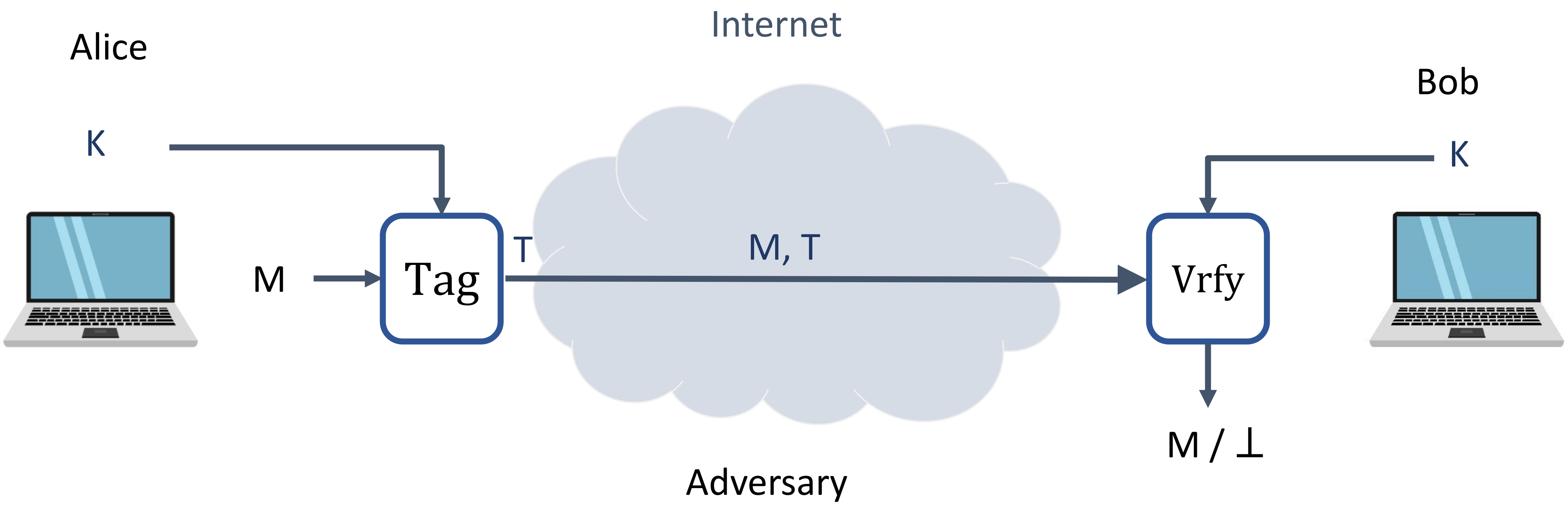
A short summary

- We can build IND-CPA secure ElGamal scheme based on DDH assumption

- Padding with randomness, we can transfer Textbook RSA to IND-CPA scheme

Digital Signature

Achieving integrity: MACs

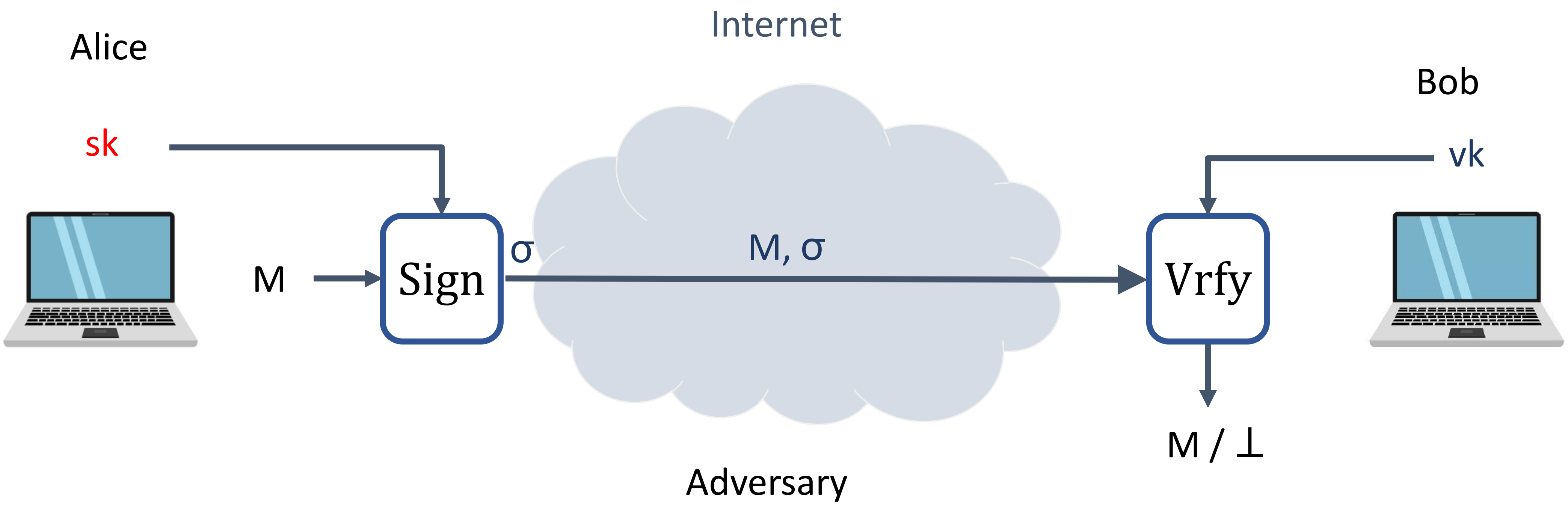


Tag : tagging algorithm (public)

K : tagging / verification key (secret)

Vrfy: verification algorithm (public)

Achieving integrity: digital signatures



Sign : tagging algorithm (public)

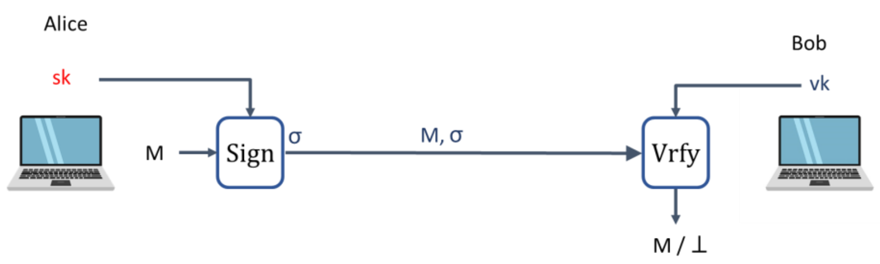
sk : signing key (secret)

Vrfy : verification algorithm (public)

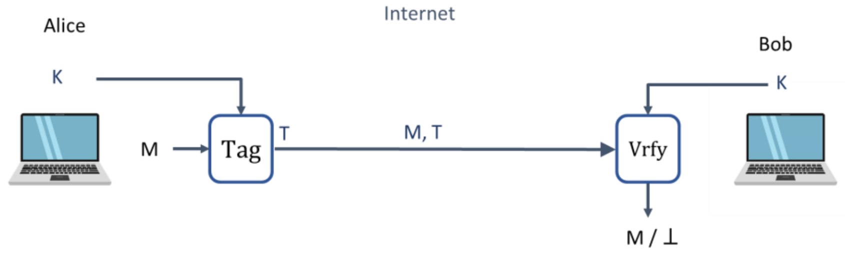
vk : verification key (public)

Digital signatures vs. MACs

- Digital signatures can be verified by *anyone*



- MACs can only be verified by party sharing the same key



- **Non-repudiation:** Alice cannot deny having created σ
  - But she can deny having created T (since Bob could have done it)

Digital signatures – syntax

A **digital signature** scheme is a tuple of algorithms $\Sigma = (\mathrm{KeyGen}, \mathrm{Sign}, \mathrm{Vrfy})$

$\mathrm{KeyGen} : (\,) \to \mathcal{SK} \times \mathcal{VK}$

$\mathrm{Sign} : \mathcal{SK} \times \mathcal{M} \to \mathcal{S}$

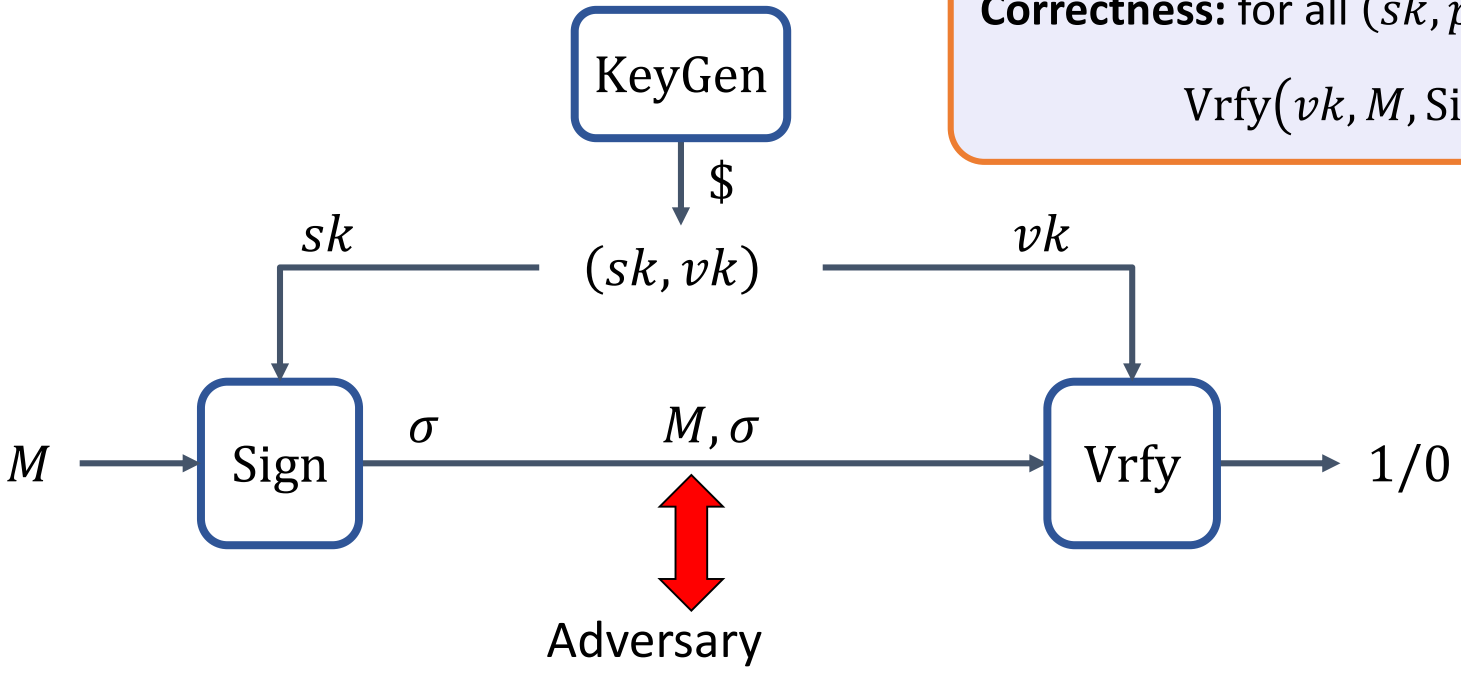
$\mathrm{Sign}(sk, M) = \mathrm{Sign}_{sk}(M) = \sigma$

$\mathrm{Vrfy} : \mathcal{VK} \times \mathcal{M} \times \mathcal{S} \to \{0,1\}$

$\mathrm{Vrfy}(vk, M, \sigma) = \mathrm{Vrfy}_{vk}(M, \sigma) = 1/0$

Correctness: for all $(sk, pk) \leftarrow \mathrm{KeyGen}$:

$$\mathrm{Vrfy}\big(vk, M, \mathrm{Sign}(sk, M)\big) = 1$$



64

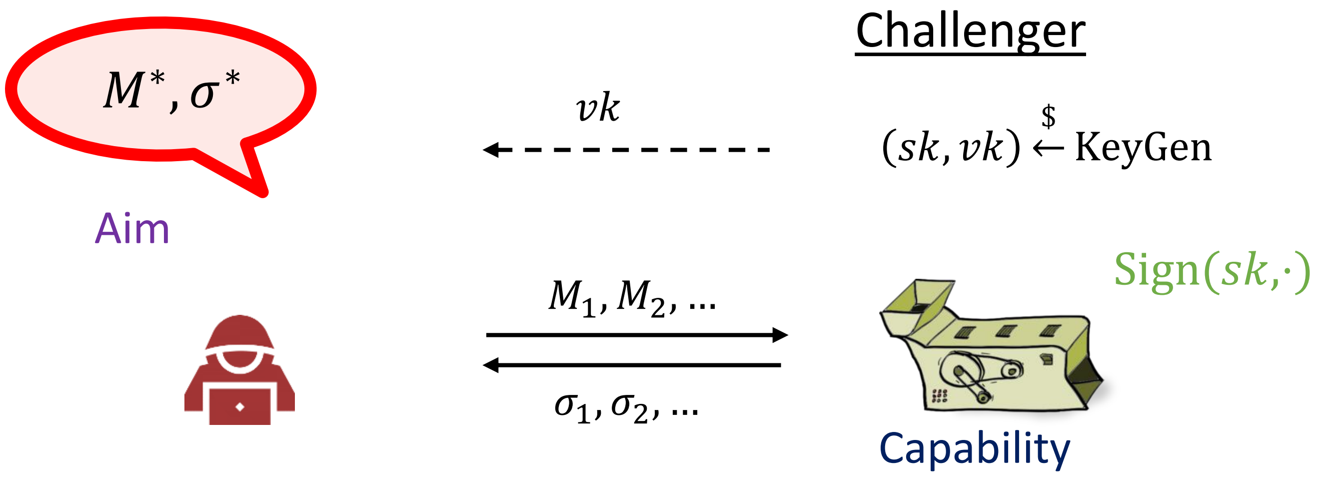
Digital signatures – security: UF-CMA

$\mathbf{Exp}_{\Sigma}^{\text{uf-cma}}(A)$

$(sk, vk) \xleftarrow{\$} \Sigma.\mathrm{KeyGen}$
$S \leftarrow [\,]$
$(M^*, \sigma^*) \leftarrow A^{\mathrm{SIGN}_{sk}(\cdot)}(vk)$
if $\Sigma.\mathrm{Vrfy}(vk, M^*, \sigma^*) = 1$ and $M \notin S$ **then**
  return 1
 else
  return 0

$\mathrm{SIGN}_{sk}(M)$

$\sigma \leftarrow \Sigma.\mathrm{Sign}(sk, M)$
$S.\mathrm{add}(M)$
return σ



If σ^* is a valid signature for M^* (not asked before) then the adversary has **forged** a signature

Definition: The **UF-CMA-advantage** of an adversary A is

$$\mathbf{Adv}_{\Sigma}^{\text{uf-cma}}(A) = \Pr\left[\mathbf{Exp}_{\Sigma}^{\text{uf-cma}}(A) \Rightarrow 1\right]$$

Textbook RSA signatures

$$\text{RSA.Sign: } \overbrace{\boldsymbol{Z}^{+} \times \boldsymbol{Z}_{\phi(n)}^{*}}^{\mathcal{SK}} \times \overbrace{\boldsymbol{Z}_{n}^{*}}^{\mathcal{M}} \rightarrow \overbrace{\boldsymbol{Z}_{n}^{*}}^{\mathcal{S}}$$

$$\text{RSA.Vrfy: } \underbrace{\boldsymbol{Z}^{+} \times \boldsymbol{Z}_{\phi(n)}^{*}}_{\mathcal{PK}} \times \underbrace{\boldsymbol{Z}_{n}^{*}}_{\mathcal{M}} \times \underbrace{\boldsymbol{Z}_{n}^{*}}_{\mathcal{S}} \rightarrow \{1,0\}$$

Vrfy$(vk = (n, e), M \in \boldsymbol{Z}_n^*, \sigma)$

```
if σ^e = M mod n then
    return 1
else
    return 0
```

vk

M, σ

KeyGen

1. $p, q \xleftarrow{\$}$ two random prime numbers
2. $n \leftarrow p \cdot q$
3. $\phi(n) = (p-1)(q-1)$
4. **choose** e such that $\gcd(e, \phi(n)) = 1$
5. $d \leftarrow e^{-1} \bmod \phi(n)$
6. $sk \leftarrow (n, d) \quad vk \leftarrow (n, e)$
7. **return** (sk, vk)

Sign$(sk = (n, d), M \in \boldsymbol{Z}_n^*)$

1. $\sigma \leftarrow M^d \bmod n$
2. **return** σ

$$d = e^{-1} \bmod \phi(n) \iff ed = 1 \bmod \phi(n)$$

$$\sigma^e = M^{de} = M^{ed \bmod \phi(n)} = M^1 = M \bmod n$$

Insecurity of Textbook RSA signature

Given $\sigma_1 = M_1^d, \sigma_2 = M_2^d$

$\sigma_1\sigma_2 = (M_1M_2)^d mod\ n$ is a signature of $M_1M_2\ mod\ n$

Many other attacks exist

Hash-then sign paradigm

$$\text{RSA.Sign: } \overbrace{\boldsymbol{Z}^+ \times \boldsymbol{Z}^*_{\phi(n)}}^{\mathcal{SK}} \times \overset{\mathcal{M}}{\{0,1\}^*} \to \overset{\mathcal{S}}{\boldsymbol{Z}^*_n}$$

$$\text{RSA.Vrfy: } \underbrace{\boldsymbol{Z}^+ \times \boldsymbol{Z}^*_{\phi(n)}}_{\mathcal{PK}} \times \underset{\mathcal{M}}{\{0,1\}^*} \times \underset{\mathcal{S}}{\boldsymbol{Z}^*_n} \to \{1,0\}$$

KeyGen

$p, q \xleftarrow{\$}$ two random prime numbers
$n \leftarrow p \cdot q$
$\phi(n) = (p-1)(q-1)$
choose e such that $\gcd(e, \phi(n)) = 1$
$d \leftarrow e^{-1} \bmod \phi(n)$
$sk \leftarrow (n, d) \quad vk \leftarrow (n, e)$
return (sk, vk)

Vrfy$(vk = (n, e), M \in \boldsymbol{Z}^*_n, \sigma)$

if $\sigma^e = H(M) \bmod n$ **then**
    return 1
else
    return 0

vk

M, σ

$$H : \{0,1\}^* \to \boldsymbol{Z}^*_n$$

Sign$(sk = (n, d), M \in \boldsymbol{Z}^*_n)$

$\sigma \leftarrow H(M)^d \bmod n$
return σ

Theorem: For *any* UF-CMA adversy A against hashed RSA making q $\mathrm{SIGN}_{sk}(\cdot)$ queries, there is an algorithm B solving the RSA-problem:

$$\mathbf{Adv}_{\mathrm{RSA},\,H}^{\mathrm{uf\text{-}cma}}(A) \leq q \cdot \mathbf{Adv}_{n,e}^{\mathrm{RSA}}(B)$$

where H is assumed perfect*

* H is assumed to be random oracle, which is out of the scope of this course. Refer to [KL] Section 5

Discrete-log-based signatures: (EC)DSA

- Schnorr
  - Elegant design
  - Has formal security proof (based on DLOG problem and H assumed perfect)
  - Patented (expired in February 2008)

- (EC)DSA
  - Non-patented alternative
  - Derived from ElGamal-based signature scheme
  - More complicated design than Schnorr
  - No security proof
  - Standardized by NIST
  - Very widely used

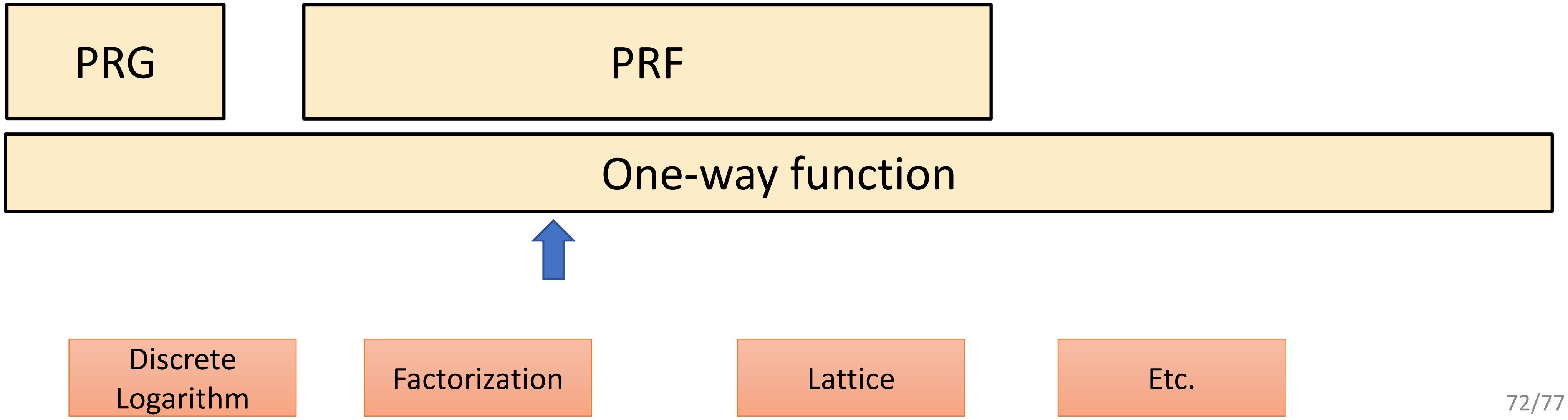
A short summary

- Hash-then sign paradigm of RSA gives a secure signature

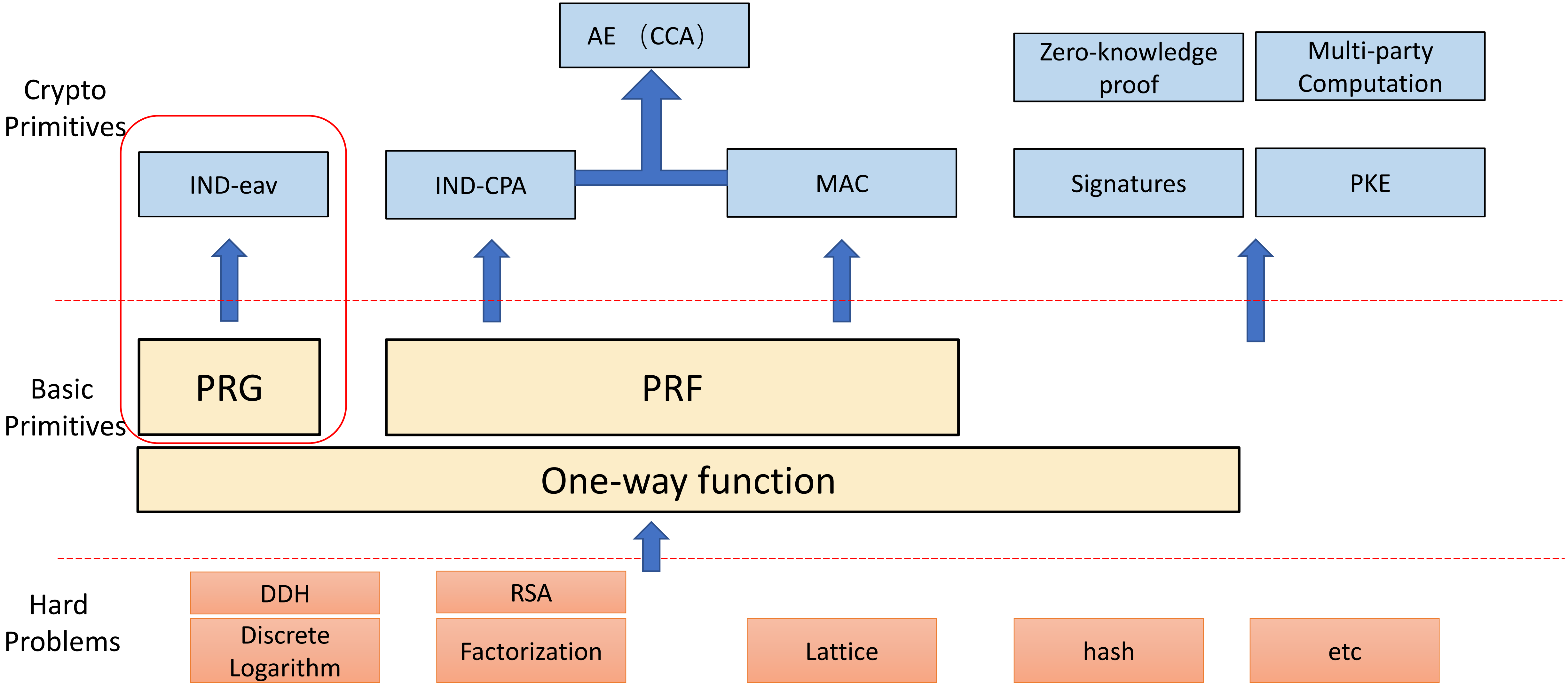
- There are Discrete-log-based signatures, ECDSA, and Schnorr

One more thing

- We leave the construction of Pseudorandom generator (PRG) and Pseudorandom function (PRF) in lecture 2
- One-way function f: given $\mathrm{y} = f(x)$ for random x, it is hard to find x' such that $\mathrm{y} = f(x')$



Big picture of Cryptography



Primitive	Functionality + syntax	Hardness assumption	Security	Examples
Diffie-Hellman	Derive shared value (key) in a cyclic group $A^b = g^{ab} = B^a$	Discrete logarithm (DLOG) Decisional Diffie-Hellman (DDH)		$(\boldsymbol{Z}_p^*, \cdot)$ −DH $(E(\boldsymbol{F}_p), +)$ −DH
RSA function	One-way trapdoor function/permutation	Factoring problem RSA-problem		Textbook RSA
Public-key encryption	Encrypt variable-length input $\text{Enc} : \mathcal{PK} \times \mathcal{M} \to \mathcal{C}$	Decisional Diffie-Hellman (DDH) Factoring problem RSA-problem	IND-CPA IND-CCA	ElGamal Padded RSA
Digital signatures	$\text{Sign} : \mathcal{SK} \times \mathcal{M} \to \mathcal{S}$ $\text{Vrfy} : \mathcal{VK} \times \mathcal{M} \times \mathcal{S} \to \{1,0\}$	RSA-problem Discrete logarithm (DLOG)	UF-CMA	Hashed-RSA ECDSA Schnorr

Assignment 1 (4 weeks)

- Write the ElGamal Enc algorithm in Sage
  - Provide “known answer-test” (KAT) values （i.e., example of pk, sk, m and c）
- Write the Textbook RSA signature in Sage
  - And show the attack that if $\sigma_1 = M_1^d, \sigma_2 = M_2^d$ $\sigma_1\sigma_2$ is the signature of M_1M_2
  - Provide “known answer-test” (KAT) values
- Instructors will be given later..

Thank you