Cryptography

Lecture 8

Arpita Patra

Quick Recall and Today's Roadmap

>> Hash Functions- stands in between public and private key world

>> Key Agreement

>> Assumptions in Finite Cyclic groups - DL, CDH, DDH

- Groups
- Finite groups
- Finite cyclic groups
- Finite Cyclic groups of prime orders (special advantages)

Division for Modular Arithmetic

- If b is invertible modulo N (i.e. b^{-1} exists) then division by b modulo N is defined as:

$$[a/b \bmod N] \overset{def}{=} [ab^{-1} \bmod N]$$

  - If ab = cb mod N and if b is invertible then a = c mod N
    - "Dividing" each side by b (which actually means multiplying both sides by b^{-1})

- Which integers b are invertible modulo a given modulus N ?

Proposition: Given integers b and N, with $b \geq 1$ and $N > 1$, then b is invertible modulo N if and only if gcd(b, N) = 1 (i.e. b & N are relatively prime).

Proof (<=): Inverse finding algorithm (if the number is invertible) --- Extended Euclid (GCD) algorithm

- Given any b, N, the Extended Euclid algorithm outputs X and Y such that

$$bX + NY = \gcd(b, N)$$

- If gcd(b, N) = 1 then above equation implies that bX + NY = 1
- Taking mod N both sides gives $bX = 1 \bmod N \rightarrow b^{-1} = [X \bmod N]$

Algorithms for Modular Arithmetic

- $\mathbb{Z}_N$ --- set of integers modulo N: {0, 1, …, N - 1}
- Let |N| = n --- number of bits to represent N : $n = \Theta(\log N)$
- Let a, b $\in \mathbb{Z}_N$ --- each represented by at most n bits

Theorem: Given integers N > 1, a and b, it is possible to perform the following operations in poly time in |a|, |b| and n:

>> a mod N

>> a+b mod N, a-b mod N, ab mod N

>> Determining if a^{-1} mod N exists (if it exists)

>> a^{-1} mod N (if it exists)

>> a^b mod N

>> Choosing a random element of $\mathbb{Z}_N$

Group

Definition(Group): A group is a set G along with a binary operation o satisfying the following axioms :

- Closure : for every $g, h \in G$, the value $g \circ h \in G$
- Associativity: for every $g_1, g_2, g_3 \in G$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$
- Existence of Identity Element: there exists an identity element $e \in G$, such that for all $g \in G$
  - $(e \circ g) = g = (g \circ e)$
- Existence of Inverse: for every $g \in G$, there exists an element $h \in G$, such that
  - $(g \circ h) = e = (h \circ g)$

Definition (Order of a Group:) If G has finite number of elements, then $|G|$ denotes the number of elements in G and is called the order of G

Definition(Abelian Group:) If G satisfies the following additional property then it is called a commutative (Abelien) group: For every $g, h \in G$, $(g \circ h) = (h \circ g)$

Proposition: There exists only one identity element in a group. Every element in a group has a unique inverse

Group Theory

- The set of integers $\mathbb{Z}$ is an abelian group with respect to the addition operation (+)
  - Closure and associativity holds
  - The integer 0 is the identity element --- for every integer x, 0 + x = x = x + 0
  - For every integer x, there exists an integer –x, such that x + (-x) = 0 = (-x) + x
  - For any two integers x, y, we have x + y = y + x --- commutativity

We are interested only in Finite groups

Finite Groups

- Finite groups using modular arithmetic.
- Define $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ and the operation + in $\mathbb{Z}_N$ as $a + b \overset{def}{=} (a + b) \bmod N$, for every $a, b \in {}_N$
  - Closure, commutative and associativity holds --- trivial to verify
  - $0 \in \mathbb{Z}_N$ is the identity element --- for every $a \in \mathbb{Z}_N$, $(a + 0) \bmod N = (0 + a) \bmod N = a$
  - Element $(N - a)$ is additive inverse of a modulo N
    - Inverse of a will be $(N - a) \in {}_N$ --- $(a + N - a) \bmod N = (N - a + a) \bmod N = 0$
- The set $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ is a group with respect to addition modulo N
- Define operation * in Z_N as $a * b \overset{def}{=} (ab) \bmod N$, for every $a, b \in \mathbb{Z}_N$
  - The identity element is 1 as for every $a \in \mathbb{Z}_N$, we have $(a \,.\, 1) = (1 \,.\, a) = (a \bmod N) = a$
  - Will every element have an inverse ?
    - Element 0 will have no inverse --- $a \in Z_N$ such that $(a0 \bmod N) = 1$
    - Element a will have an inverse if and only if $\gcd(a, N) = 1$
  - So $\mathbb{Z}_N$ is not a group with respect to multiplication modulo N
  - Can we construct a set from $\mathbb{Z}_N$ which will be a group with respect to multiplication modulo N ?

Finite Groups

- Let $\mathbb{Z}_N^*$ = {b: {1, …, N-1} | gcd(b, N) = 1). Then $\mathbb{Z}_N^*$ is a group with respect to multiplication modulo N
  - The set $\mathbb{Z}_N^*$ is the set of integers relatively prime to N
  - Element 1 is the identity element. Every element is invertible. Associativity holds.
  - Is $\mathbb{Z}_N^*$ closed with respect to multiplication mod N ? --- given a, b $\in \mathbb{Z}_N^*$, will [ab mod N] $\in \mathbb{Z}_N^*$
  - Claim: gcd(N, [ab mod N]) = 1 --- element [ab mod N] has multiplicative inverse [$b^{-1}a^{-1}$ mod N]

Group Exponentiation in Groups

- Exponentiation: applying same operation on the same element a number of times in a group (G, o)

Using Multiplication Notation:

- $g^m \overset{def}{=} g \circ g \circ \ldots \circ g$ (m times)
- $g^{-m} \overset{def}{=} (g^{-1} \circ g^{-1} \circ \ldots \circ g^{-1})$ (m times)
- $g^0 \overset{def}{=}$ e, the group identity element

Using Addition Notation:

- $mg \overset{def}{=} g \circ g \circ \ldots \circ g$ (m times)
- $-mg \overset{def}{=} (-g + -g + \ldots + -g)$ (m times)
- $0g \overset{def}{=}$ e, the group identity element

Group Order and Identity Element

Theorem: Let (G, o) be a group of order m, with identity element e. Then for every element $g \in G$:

$$\underbrace{g \circ g \circ \ldots \circ g}_{m \text{ times}} = e$$

I.e. Any group element composed with itself m times results in the identity element

Proof: Let $G = \{g_1, \ldots, g_m\}$ --- for simplicity assume G to be an Abelian group

Let g be an arbitrary element of G

- Claim: elements $(g \circ g_1), (g \circ g_2), \ldots, (g \circ g_m)$ are all distinct
  - On contrary if for distinct g_i, g_j, we have $(g \circ g_i) = (g \circ g_j) \rightarrow (g^{-1} \circ g \circ g_i) = (g^{-1} \circ g \circ g_j) \rightarrow g_i = g_j$
- Thus $\{(g \circ g_1), (g \circ g_2), \ldots, (g \circ g_m)\} = G$
- So $g_1 \circ g_2 \circ \ldots \circ g_m = (g \circ g_1) \circ (g \circ g_2) \circ \ldots \circ (g \circ g_m)$ -- (both side we have all the elements of G)

$= (g \circ g \circ \ldots \circ g) \circ (g_1 \circ g_2 \circ \ldots \circ g_m)$ -- (by associative and commutative property)

$e = (g \circ g \circ \ldots \circ g) \circ e$ -- (multiply by $(g_1 \circ g_2 \circ \ldots \circ g_m)^{-1}$ both sides)

$e = (g \circ g \circ \ldots \circ g)$ -- $(a \circ e = a)$

Order of Important Finite Groups

$\mathbb{Z}_N^*$ = {b: {1, …, N-1} | gcd(b, N) = 1). It is a group with respect to multiplication modulo N

$\varphi(N)$ = order of the above group

- N is a prime number, say p
  - $\mathbb{Z}_p^*$ = {1, 2, …, p-1} --- every number from 1 to p-1 is relatively prime to p

- N = p.q, where p and q are primes
  - $|\mathbb{Z}_N^*|$ = (p-1)(q-1) --- follows from the principle of mutual inclusion-exclusion
  - Which numbers in {1, 2, …, N-1} are not relatively prime to N ?
    - Numbers which are divisible by p --- q-1 such numbers
    - Numbers which are divisible by q --- p-1 such numbers
    - Numbers which are divisible by both p and q --- 0 such number
  - How many numbers in {1, 2, …, N-1} are not relatively prime to N ? --- p + q - 2
  - How many numbers in {1, 2, …, N-1} are relatively prime to N ? --- N -1 - p – q + 2 = (p-1)(q-1)

Group Order and Identity Element

Theorem: Let (G, o) be a group of order m, with identity element e. Then for every element $g \in G$:

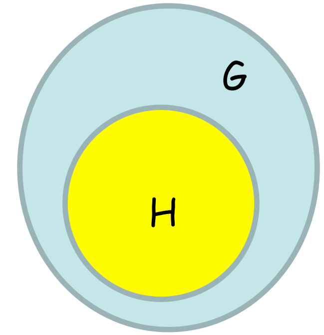
$$\underbrace{g \circ g \circ \ldots \circ g}_{m \text{ times}} = e$$

I.e. Any group element composed with itself m times results in the identity element

- Implications of the above theorem in the multiplicative group $\mathbb{Z}_N^*$
  - Take any arbitrary N > 1 and any $a \in \mathbb{Z}_N^*$. Then:
    - $[[[[a \,.\, a \bmod N] \,.\, a \bmod N] \,.\, a \bmod N] \,.\, a \bmod N] \,.\, \ldots \,.\, a \bmod N] = [a^{\varphi(N)} \bmod N] = 1$

      ← φ(N) times →
  - If N is a prime number, say p, then for any $a \in \{1, 2, \ldots, p-1\}$, we have :
    - $[a^{p-1} \bmod p] = 1$
  - If N is a composite number, p.q, then for any a we have :
    - $[a^{(p-1)(q-1)} \bmod N] = 1$

Subgroup of a Group & Cyclic Group



- Let (G, o) be a group
- Let $H \subseteq G$

Definition (Subgroup): If (H, o) is also a group, then H is called a subgroup of G w.r.t operation o

- Every group (G, o) has two trivial subgroups:
  - The group (G, o) itself and the group (e, o)
  - A group may/may not have subgroups other than trivial subgroups

- Given a finite group (G, o) of order m and an arbitrary element $g \in G$, define
  $\langle g \rangle = \{g^0, g^1, \ldots, \}$ --- elements generated by different non-negative powers of g
  - The sequence is finite as $g^m = 1$ and g^0 is also 1
  - Let $i \leq m$ be the smallest positive integer such that $g^i = 1$. Then:
    $\langle g \rangle = \{g^0, g^1, \ldots, g^{i-1}\}$ --- as $g^i = 1$, after which the sequence starts repeating

Proposition: $(\langle g \rangle, o)$ is a subgroup of (G, o) of order i

Definition (Order of an element): Smallest positive integer i such that $g^i = 1$

Definition (Generator): If g has order m, then $\langle g \rangle = G$ --- then g is called a generator of G and G is called a cyclic group generated by g

Examples

- Consider ($\mathbb{Z}_7^*$, * mod 7) --- it is a group with respect to multiplication modulo 7
  - Does 2 belong to the group ? --- Yes, as gcd(2, 7) = 1; 2 is relatively prime to 7
  - What is <2> ? --- <2> = {2^0 mod 7, 2^1 mod 7, 2^2 mod 7} = {1, 2, 4}
  - Is (<2>, * mod 7) a subgroup of ($\mathbb{Z}_7^*$, * mod 7) ?

	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

- ✓ Closure
- ✓ Associativity
- ✓ Identity --- 1
- ✓ Inverse
  - $1^{-1} = 1$, $2^{-1} = 4$, $4^{-1} = 2$

  - Does 3 belong to the group ? --- Yes, as gcd(3, 7) = 1; 3 is relatively prime to 7
  - What is <3> ? --- <3> = {3^0 mod 7, 3^1 mod 7, 3^2 mod 7, 3^3 mod 7, 3^4 mod 7, 3^5 mod 7, 3^6 mod 7 } = {1, 3, 2, 6, 4, 5} = the original group
  - 2 does not "generate" the entire group $\mathbb{Z}_7^*$
  - 3 "generates" the entire group $\mathbb{Z}_7^*$ --- 3 is a generator

Important Finite Cyclic Groups

Theorem: The group ($\mathbb{Z}_p^*$, * mod p) is a cyclic group of order p – 1.

- Every element need not be a generator
- Ex: ($\mathbb{Z}_7^*$, * mod 7) is a cyclic group with generator 3
  - Element 2 is not a generator for this group --- <2> = {1, 2, 4}

Useful Propositions on Order of a Group Element

- Let (G, o) be a group of order m and let $g \in G$ such that g has order i $(1 \le i \le m)$ --- $g^i = e$

Proposition: For any integer x, we have $g^x = g^{[x \bmod i]}$

x times

$$g^x = \underbrace{(g \circ g \dots \circ g)}_{i \text{ times}} \circ \underbrace{(g \circ g \circ \dots \circ g)}_{i \text{ times}} \circ \dots \circ \underbrace{(g \circ g \circ \dots \circ g)}_{x \bmod i \text{ times}}$$

$$e \circ e \circ \dots \circ g^{[x \bmod i]} = g^{[x \bmod i]}$$

Proposition: For any integer x, y, we have $g^x = g^y$ if and only if $x = y \bmod i$; i.e. $[x \bmod i] = [y \bmod i]$

Proof: If $[x \bmod i] = [y \bmod i]$, then from the previous claim $g^x = g^y$

If $g^x = g^y \rightarrow g^{x-y} = g^{x-y \bmod i} = 1 \rightarrow x - y \bmod i = 0$

Proposition: The order of g divides the order of G --- i divides m

Proof: Element g has order $i \rightarrow g^i = e$

- For any g, we have $g^m = e$
- So $g^m = g^i \rightarrow [m \bmod i] = [i \bmod i] \rightarrow [m \bmod i] = 0$

The last claim has several interesting implications

Finite Cyclic Groups of Prime Order

Corollary: If (G, o) is a group of prime order p then G is cyclic and all elements of G, except the identity element will be generators of G

- Any arbitrary element $g \in G$ apart from the identity element will have order p --- the only positive numbers which divides a prime p are 1 and p
- Ex: consider the group ($\mathbb{Z}_7$, + mod 7) --- cyclic group, with identity element 1 and generators 1, 2, 3, 4, 5 and 6

Instances of Cyclic groups of prime order??

Theorem: The group ($\mathbb{Z}_p^*$, * mod p) is a cyclic group of order p – 1.

We can construct cyclic groups of prime order from the above group when p has a specific format

Prime-order Cyclic Subgroup of $\mathbb{Z}_p^*$

Definition (Safe Primes): Prime numbers in the format p = 2q+1 where q is also a prime.

- Example (5, 11), (11, 23), … several such pairs

Definition (Quadratic Residue Modulo p): Call $y \in \mathbb{Z}_p^*$ a quadratic residue modulo p if there exists an $x \in \mathbb{Z}_p^*$, with $y = x^2 \bmod p$. x is called square-root of y modulo p

Theorem: The set of quadratic residues modulo p is a cyclic subgroup of $\mathbb{Z}_p^*$ of order q. I.e.

$Q = \{x^2 \bmod p \mid x \in \mathbb{Z}_p^*\}$, then (Q, * mod p) is a cyclic subgroup of ($\mathbb{Z}_p^*$, * mod p) of order q

Proof:

Step I: To show that (Q, * mod p) is a subgroup of ($\mathbb{Z}_p^*$, * mod p)

Step II: Show that (Q, * mod p) is of order q

Prime-order Cyclic Subgroup of $\mathbb{Z}_p^*$

Theorem: The set of quadratic residues modulo p is a cyclic subgroup of $\mathbb{Z}_p^*$ of order q. I.e.
$Q = \{x^2 \bmod p \mid x \in \mathbb{Z}_p^*\}$, then (Q, * mod p) is a cyclic subgroup of ($\mathbb{Z}_p^*$, * mod p) of order q

Proof:

Step I: To show that (Q, * mod p) is a subgroup of ($\mathbb{Z}_p^*$, * mod p)

- Closure: (Q, * mod p) satisfies the closure property
  - Given arbitrary $y_1, y_2 \in Q$, show that $(y_1 * y_2) \bmod p \in Q$
    - $y_1 \in Q \rightarrow y_1 = x_1^2 \bmod p$, for some $x_1 \in \mathbb{Z}_p^*$
    - $y_2 \in Q \rightarrow y_2 = x_2^2 \bmod p$, for some $x_2 \in \mathbb{Z}_p^*$
    - $(y_1 * y_2) \bmod p = (x_1 * x_2)^2 \bmod p = (x_3)^2 \bmod p$, where $x_3 = (x_1 * x_2) \in \mathbb{Z}_p^*$
    - So $(y_1 * y_2) \bmod p \in Q$

Prime-order Cyclic Subgroup of $\mathbb{Z}_p^*$

Theorem: The set of quadratic residues modulo p is a cyclic subgroup of $\mathbb{Z}_p^*$ of order q. I.e. $Q = \{x^2 \bmod p \mid x \in \mathbb{Z}_p^*\}$, then (Q, * mod p) is a cyclic subgroup of ($\mathbb{Z}_p^*$, * mod p) of order q

Proof:

Step I: To show that (Q, * mod p) is a subgroup of ($\mathbb{Z}_p^*$, * mod p)

- Closure: (Q, * mod p) satisfies the closure property
- Associativity: trivial to verify that given arbitrary $y_1, y_2, y_3 \in Q$, we have

  $(y_1 * y_2) * y_3 \bmod p = y_1 * (y_2 * y_3) \bmod p$

- Identity: The element 1 will be present in Q, which will be the identity element for Q

  $1 = 1^2 \bmod p$

- Inverse: Show that every element $y \in Q$ has a multiplicative inverse $y^{-1} \in Q$, with $(y * y^{-1} \bmod p) = 1$

  $y \in Q \rightarrow y = (x^2 \bmod p)$, for some $x \in \mathbb{Z}_p^*$

  What can you say about $z = (x^{-1})^2 \bmod p$?

  - $x \in \mathbb{Z}_p^* \rightarrow x^{-1} \in \mathbb{Z}_p^*$, which implies that $z \in Q$
  - From the above we get that $(y * z \bmod p) = 1$

Prime-order Cyclic Subgroup of $\mathbb{Z}_p^*$

Theorem: The set of quadratic residues modulo p is a cyclic subgroup of $\mathbb{Z}_p^*$ of order q. I.e.

$Q = \{x^2 \bmod p \mid x \in \mathbb{Z}_p^*\}$, then (Q, * mod p) is a cyclic subgroup of ($\mathbb{Z}_p^*$, * mod p) of order q

Proof: Step I: To show that (Q, * mod p) is a subgroup of ($\mathbb{Z}_p^*$, * mod p)

Step II: Show that (Q, * mod p) is of order q

- We will show that f: $\mathbb{Z}_p^* \rightarrow Q$ is a 2-to-1 function --- exactly 2 elements have the same image

  $|\mathbb{Z}_p^*| = (p - 1)$, the above will imply that $|Q| = (p - 1)/2 = q$

- Let g be a generator of $\mathbb{Z}_p^*$ --- $\mathbb{Z}_p^* = \{g^0, g^1, \ldots, g^{p-2}\}$

- Consider an arbitrary element g^i in $\mathbb{Z}_p^*$ and its corresponding image $(g^i)^2 \bmod p$ in Q

- Claim: there exists only one more element g^j in $\mathbb{Z}_p^*$, with $(g^i)^2 \bmod p = (g^j)^2 \bmod p$

  - If $(g^i)^2 \bmod p = (g^j)^2 \bmod p \rightarrow [2i \bmod p-1] = [2j \bmod p-1] \rightarrow (p - 1)$ divides $(2i - 2j) \rightarrow q \mid (i - j)$

  - The above implies that for a fixed $i \in \{0, \ldots, p-2\}$, there is only 1 possible j, namely $(i + q) \bmod p-1$

    - $(i + 2q) \bmod (p - 1) = i$

Generalization

For Prime numbers in the format $p = rq+1$ where q is also a prime.

Theorem: The set of rth residues modulo p is a cyclic subgroup of $\mathbb{Z}_p^*$ of order q. I.e.

$Q = \{x^r \bmod p \mid x \in \mathbb{Z}_p^*\}$, then (Q, * mod p) is a cyclic subgroup of ($\mathbb{Z}_p^*$, * mod p) of order q

Easy Problems in Finite Cyclic Groups (of Prime Order)

1. Generating Cyclic Groups / Cyclic Groups of Prime Order
   - » How to sample a prime number of n bits /
     how to sample primes of specific format (safe primes)
     (Miller-Rabin, Agrawal-Kayal-Saxena)
   - » Finding a generator
   - » Given generator, how to generate an element of the group (requires exponentiation)
2. Sampling an uniform random group element

Cyclic Group $\mathbb{Z}_p^*$	Prime Order Cyclic Group $Q = \{x^r \bmod p \mid x \in \mathbb{Z}_p^*\}$
There exists a generator	Every element except the identity element is a generator
Group order (p-1) is not a prime. Every exponent may not have multiplicative inverse modulo (p-1)	Group order q. Every exponent have multiplicative inverse modulo q and easy to compute
If group order (p-1) has small prime factors, there exists no-trivial algo to break the hard problems that we discuss next	The attacks does not work here

Discrete Logarithm

- Let (G, o) be a cyclic group of order q (with $|q| = n$ bits) and with generator g
  - $\{g^0, g^1, g^2, \ldots, g^{q-1}\} = G$ --- g has order q as it is the generator
  - Given any element $h \in G$, it can be expressed as some power of g
    - $\exists$ a unique $x \in \mathbb{Z}_q = \{0, 1, \ldots, q-1\}$, such that $h = g^x$
    - x is called the discrete log of h with respect to g --- expressed as $\log_g h$

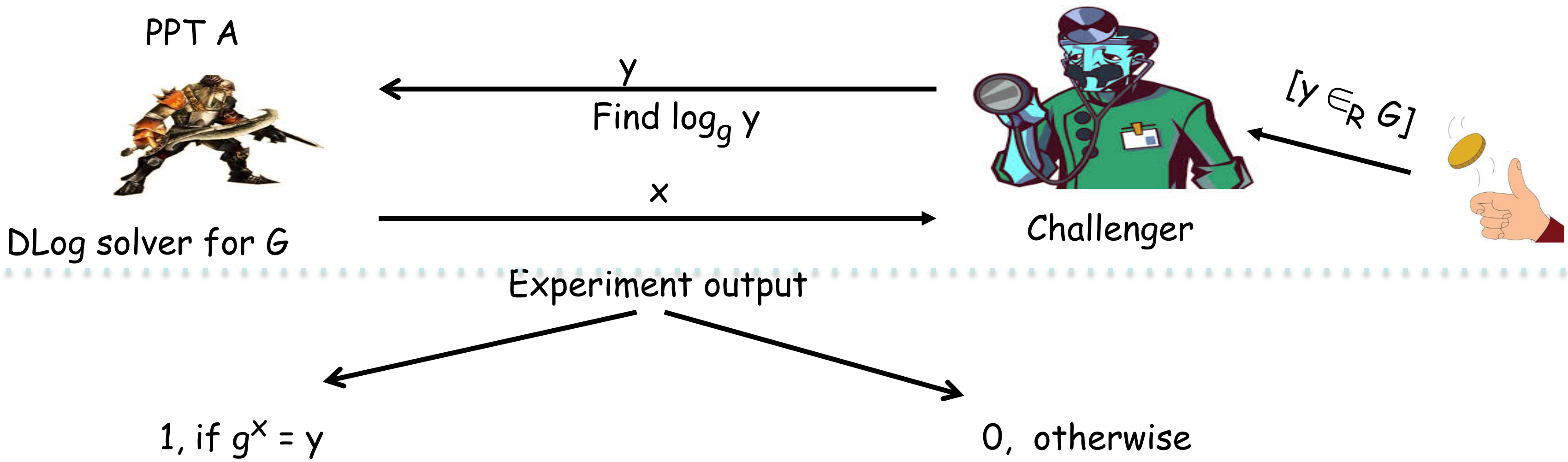
- Discrete log follows certain rules of standard logarithms
  - $\log_g e = 0$
  - $\log_g h^r = [r \log_g h \bmod q]$
  - $\log_g [h_1 \circ h_2] = [(\log_g h_1 + \log_g h_2) \bmod q]$

Discrete Logarithm Problem

- How difficult is it to compute the DLog of a random group element ?

  For certain groups, there exists no better algorithm than the inefficient brute-force

Modeled as a challenge-response experiment: $DLog_{A,\,G}(n)$ (G, o, g, q) output by an group gen algo



- DLog problem is hard relative to the group G, if for every PPT algorithm A, there exists a negligible function negl(), such that:

$$\Pr[DLog_{A,\,G}(n) = 1] \leq negl()$$

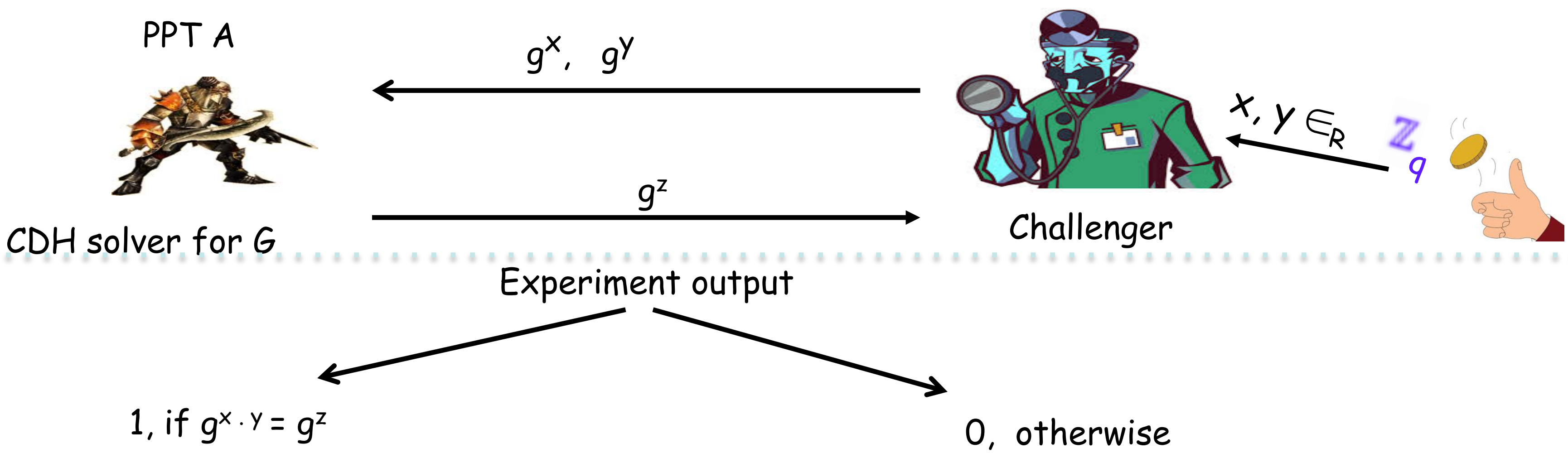
- DLog Assumption: there exists some group G, relative to which DLog problem is hard

  - We have seen will see such candidates earlier

Computational Diffie-Hellman (CDH) Problem

- Given a cyclic group $(G, \circ)$ of order q and a generator g for G.
- The CDH problem for the group $(G, \circ)$ is to compute $g^{x \cdot y}$ for random group elements g^x, g^y

Modeled as a challenge-response experiment: $CDH_{A,G}(n)$ $(G, \circ, g, q)$



CDH problem is hard relative to the group G, if for every PPT algorithm A:

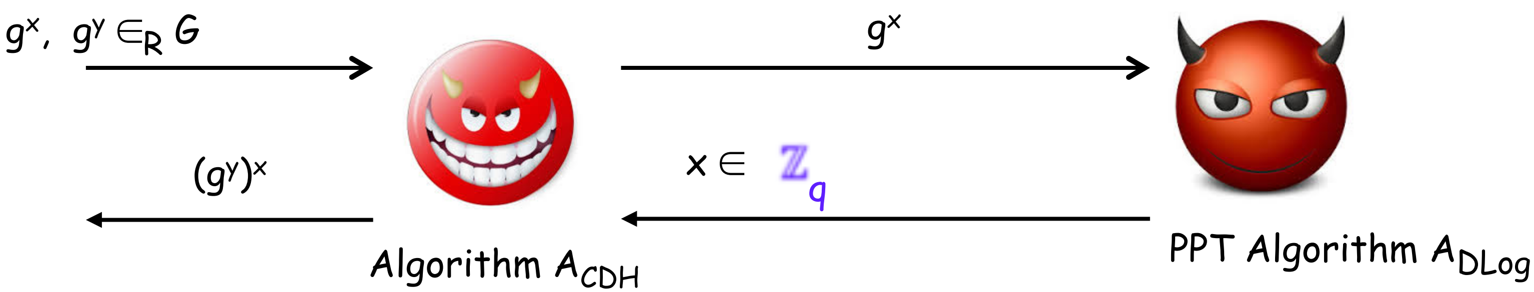
$$\Pr[CDH_{A,G}(n) = 1] \leq negl()$$

Relation between CDH and DLog Problems

- Given a cyclic group (G, o) of order q and a generator g for G:

Hardness of CDH $\overset{?}{\longleftrightarrow}$ Hardness of DLog

- If CDH is hard in (G, o) then DLog is hard in (G, o).



- Advantage of  same as 

- If DLog is hard in (G, o) then CDH is hard in (G, o) ? --- nothing is known
- CDH (hardness) is a stronger assumption than DLog (hardness) assumption
  - CDH might be solved even without being able to solve the DLog problem

Decisional Diffie-Hellman (DDH) Problem

- The DDH problem for the group (G, o) is to distinguish $g^{x \cdot y}$ from a random group element g^z, if g^x, g^y are random

DDH problem is hard relative to (G, o) if for every PPT algorithm A:

$$\left| \Pr[A(G, o, q, g, g^x, g^y, g^{xy}) = 1] - \Pr[A(G, o, q, g, g^x, g^y, g^z) = 1] \right| \leq \text{negl}()$$

Probability over uniform choice of x and y (first term) — Probability over uniform choice of x, y and z (second term)

- Claim: If DDH is hard relative to (G, o) then CDH is also hard relative to (G, o)
  - If CDH can be solved, then given g^x and g^y, compute g^{xy} and compare it with the third element

- Nothing is known regarding the converse --- DDH is a stronger assumption than CDH
  - DDH might be solved even without being able to solve CDH

Cryptographic Assumptions in Cyclic Groups

DDH ⟶ CDH ⟶ DL

Cyclic Groups of Prime Order is best choice.

>> DL is harder in this group compared to cyclic group $\mathbb{Z}_p^*$ (Pohlig-Hellman Algo)

>> DDH can be broken in cyclic group $\mathbb{Z}_p^*$ but believed to hold good it its prime order subgroup

6th Chalk and Talk topic

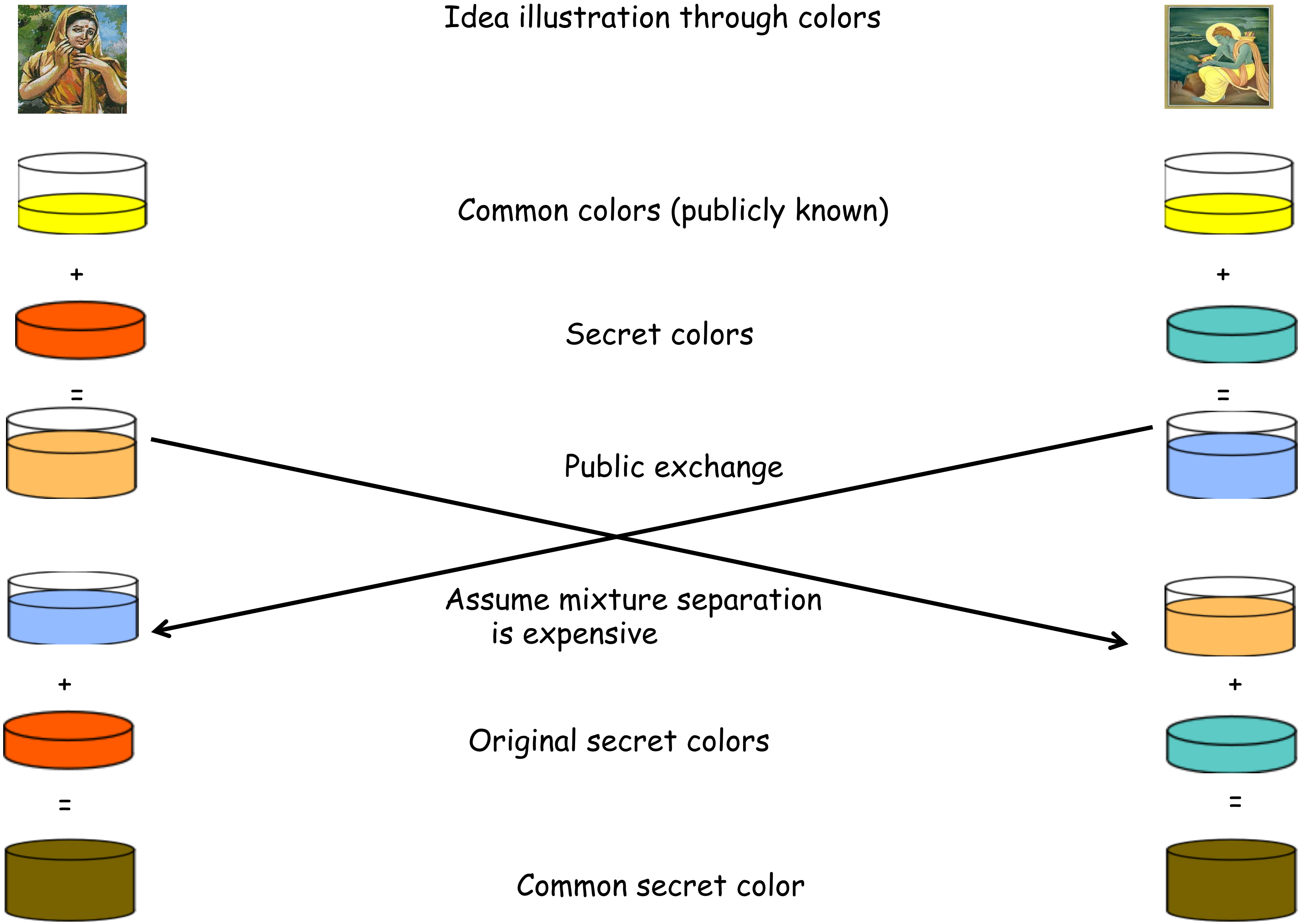
Attacks on Discrete Log Assumptions-

(i) Pohlig-Hellman Algorithm

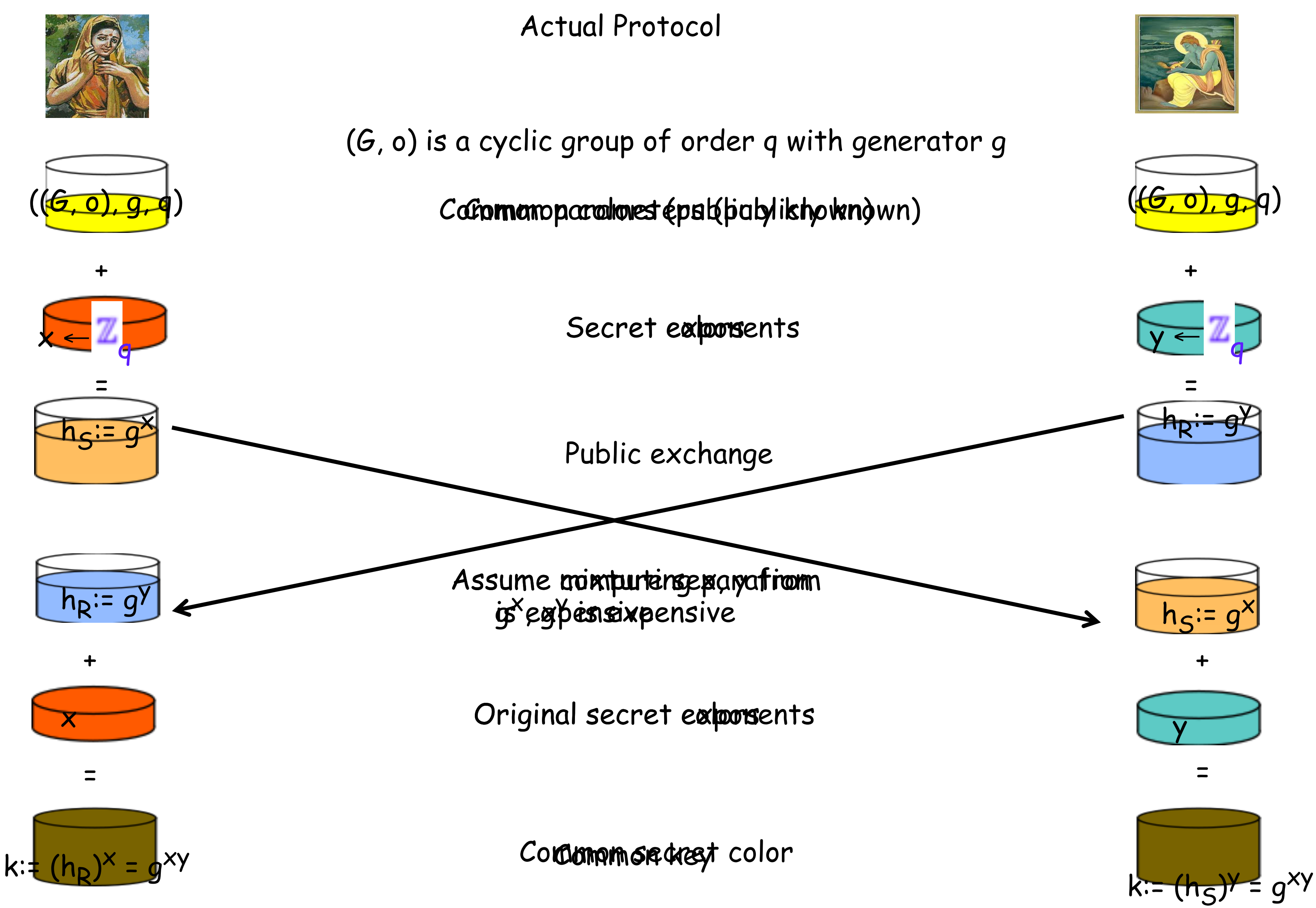
(ii) Shanks Baby-step/Giant-step algorithm

(iii) Discrete Logs from Collisions

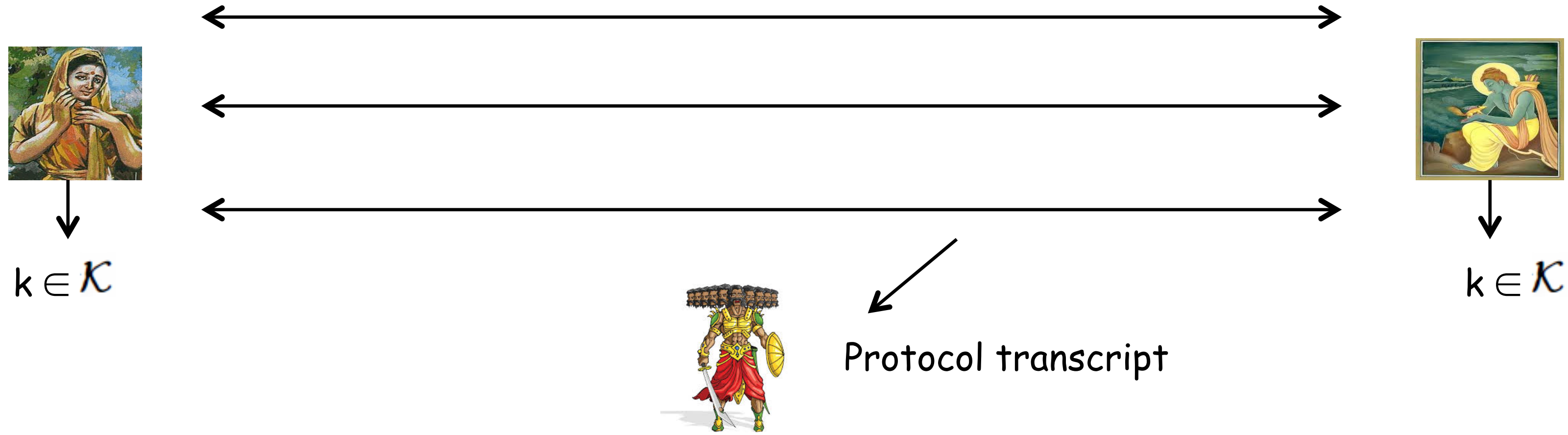
Diffie-Hellman Key-Exchange Protocol



Diffie-Hellman Key-Exchange Protocol

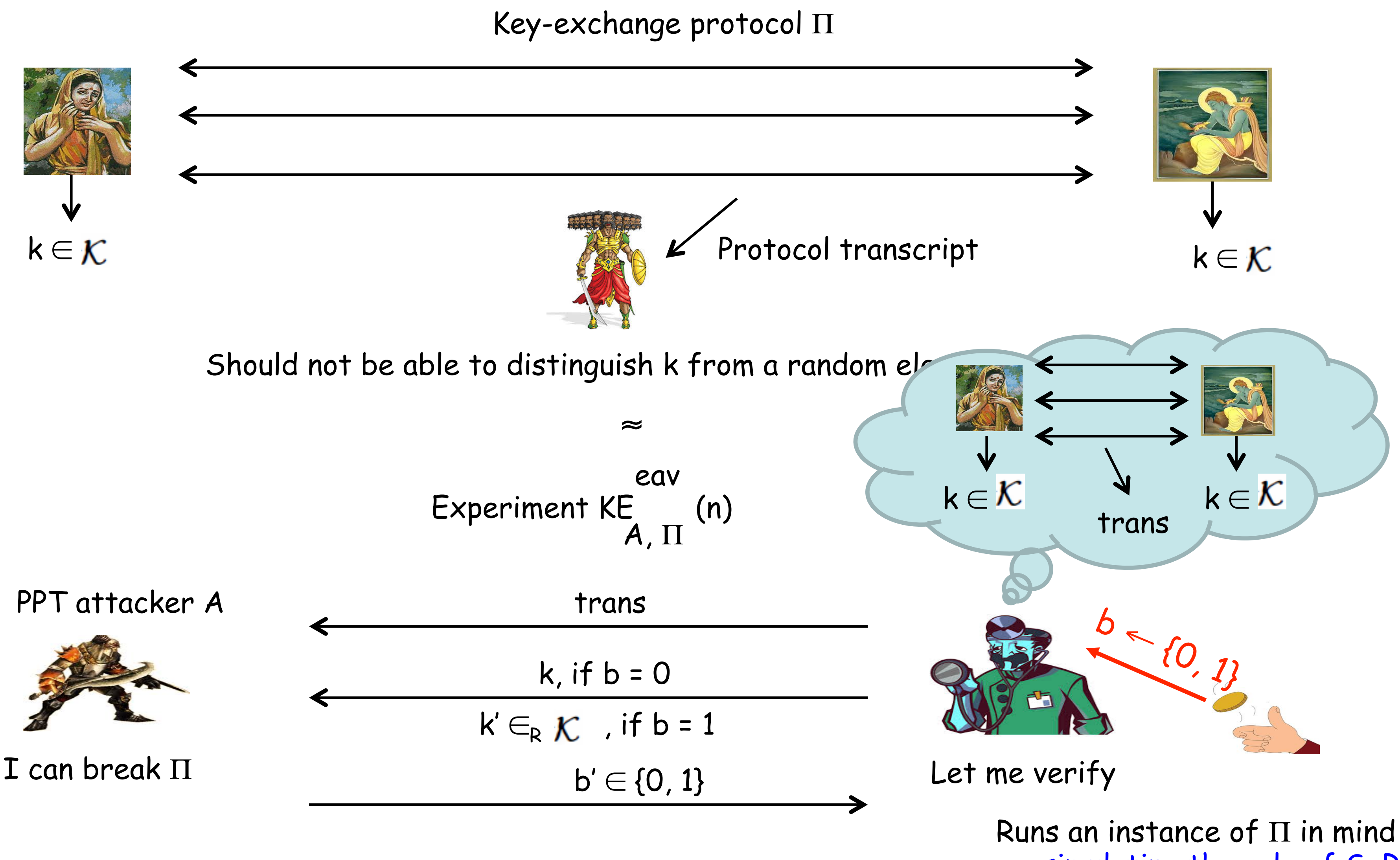


Key-Exchange Protocol: Security



- ❑ Given an arbitrary key-exchange protocol, whose execution is monitored by a PPT eavesdropper
  - ➢ What security property we demand from such a protocol ?
    - ❖ Option I: the output key k should remain hidden from the eavesdropper
    - ❖ Option II: the output key k should remain indistinguishable for the eavesdropper from a uniformly random key from the key-space $\mathcal{K}$
  - ➢ We actually want to have option II
    - ❖ If we want the key to be used as the secret-key for some higher level primitive

Key-Exchange Protocol: Security Experiment



- Experiment output is 1 if and only if b' = b
- Π is a secure KE protocol if:

$$\Pr\left[KE^{eav}_{A,\Pi}(n) = 1 \right] \leq \frac{1}{2} + \text{negl}(n)$$

Diffie-Hellman Key-Exchange Protocol: Security

$h_S = g^x$, where $x \leftarrow \mathbb{Z}_q$

$h_R = g^y$, where $y \leftarrow \mathbb{Z}_q$

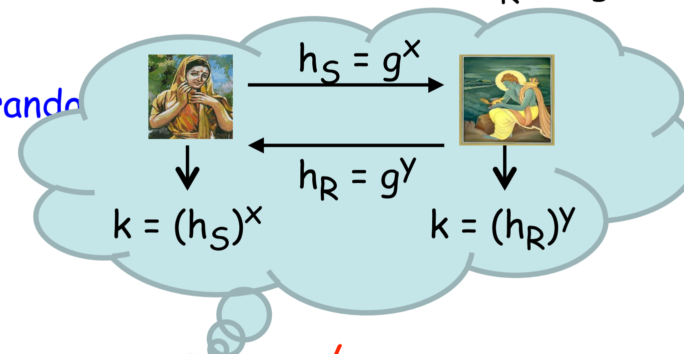
$k = (h_S)^x = g^{xy}$

Protocol transcript

$k = (h_R)^y = g^{xy}$

Should not be able to distinguish $k = g^{xy}$ from a rando

- Same as the DDH problem



Experiment $KE^{eav}_{A, DH}(n)$

PPT attacker A

I can break Π

$h_S = g^x, \ h_R = g^y$

g^{xy}, if $b = 0$

$g^z \in_R G$, if $b = 1$

$b' \in \{0, 1\}$

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

Let me verify

Runs an instance of DH in mind
simulating the role of S, R

- What is the probability that the output of the experiment is 1 ?
  - Same with which A can distinguish g^{xy} from a random group element g^z

Uniform Group Elements vs Uniform Random Strings

- DH key-exchange protocol enables the parties to agree on a (pseudo)random group element g^{xy}

- In reality, the parties would like to agree on (pseudo)random bit string which can be used as a secret-key for higher level primitive, such as PRF, MAC, etc

- Required: a method of deriving (pseudo)random bit strings from (pseudo)random group elements

  - Potential solution (used in practice)

    - Use the binary representation of the group element g^{xy} as the required key

    - Claim: the resultant bit-string will be (pseudo)random if the group element is (pseudo)random

  - The above claim need not be true --

  - Ex: consider the pr ... rime

  - Subgroup (Q

    - In practic

    - The agreed key g ... generator of Q, x, y $\in \mathbb{Z}_q$

    - Number of bits to represen ... ments of Q = Number of bits to represent elements of $\mathbb{Z}_p^*$

      - But Q does not contain all possible bit-strings of length log p --- $|Q| = q \approx 2^{\log_2 p} / 2$

      - So binary representation of the agreed key does not correspond to a random $\log_2$ p-bit string

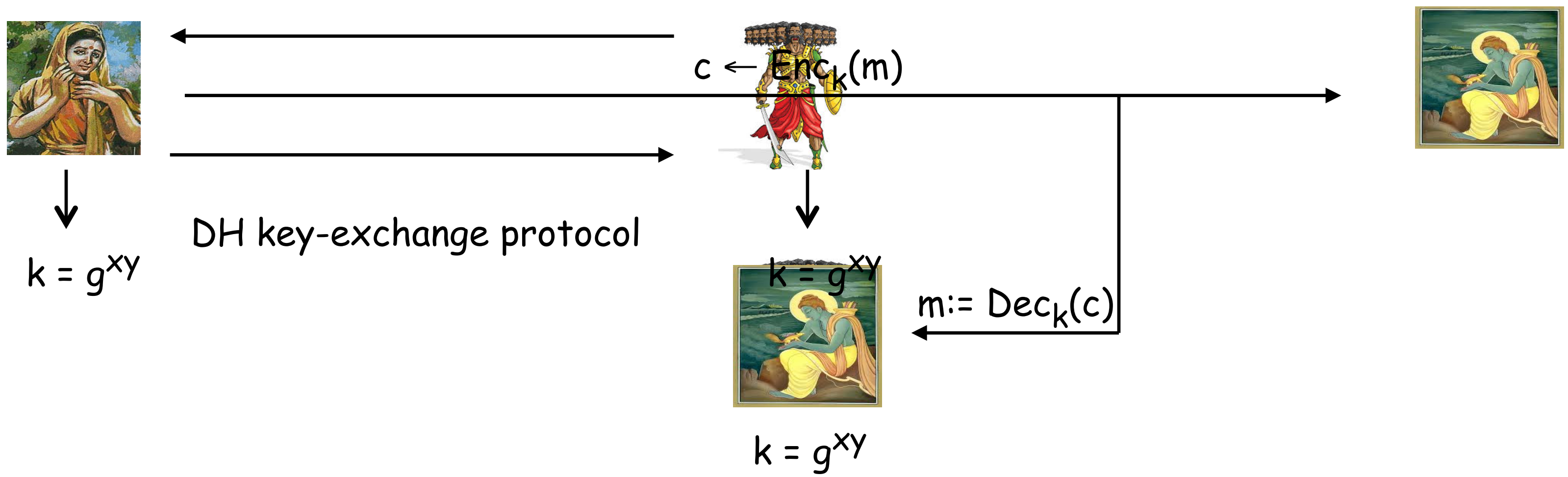
- A suitable key-derivation function (KDF) is applied to g^{xy} to derive pseudorandom key

  - Typically KDFs are based on hash functions

  - Details out of scope of this course

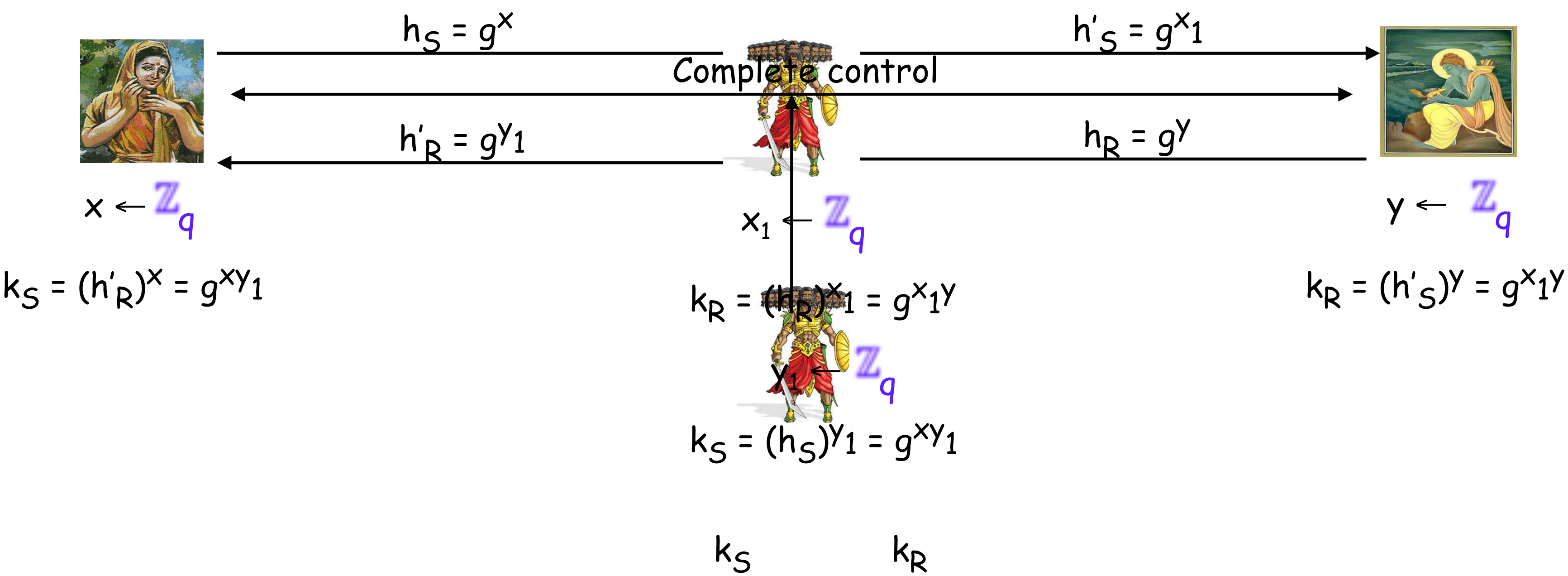
Active Attacks Against DH Key-Exchange Protocol

- DH key-exchange protocol assumes a passive attacker --- only listens the conversation
- In reality, the attacker may be malicious/active --- can change information, inject its own messages, etc
- Two types of active attacks against DH key-exchange protocol
  - Impersonation attack :



Active Attacks Against DH Key-Exchange Protocol

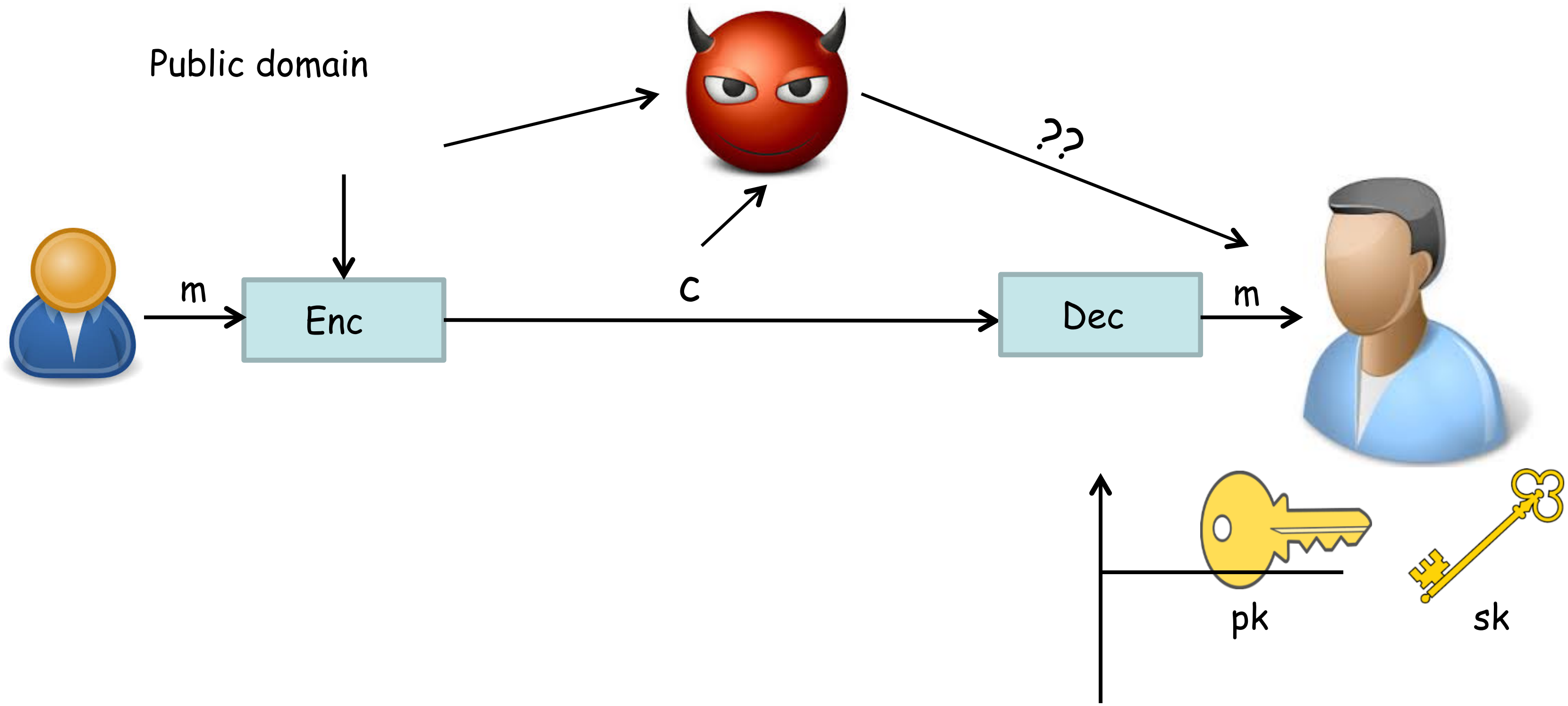
- DH key-exchange protocol assumes a passive attacker --- only listens the conversation
- In reality, the attacker may be malicious/active --- can change information, inject its own messages, etc
- Two types of active attacks against DH key-exchange protocol
  - Impersonation attack :
  - Man-in-the-middle attack :



- In practice, robust mechanisms are used in the DH key-exchange protocol to deal with the man-in-the-middle attack --- ex: TLS protocol

The Public-key Revolution

- In their seminal paper on the key-exchange, Diffie-Hellman also proposed the notion of public-key cryptography (asymmetric-key cryptography)



Public-key Crypto vs Private-key Crypto

Private-Key Crypto	Public-Key Crypto
- Key distribution has to be done apriori.	+ Key distribution can be done over public channel !!
- In multi-sender scenario, a receiver need to hold one secret key per sender	+ One receiver can setup a single public-key/ secret key and all the senders can use the same public key
- Well-suited for closed organization (university, private company, military). Does not work for open environment (Internet Merchant)	+ Better suited for open environment (Internet) where two parties have not met personally but still want to communicate securely (Internet merchant & Customer)
+ Very fast computation. Efficient Communication. Only way to do crypto in resource-constrained devices such as mobile, RFID, ATM cards etc	- Orders of magnitude slower than Private-key. Heavy even for desktop computers while handling many operations at the same time
+ only those who shares a key can send a message	- Anyone can send message including unintended persons
	- Relies on the fact that there is a way to correctly send the public key to the senders (can be ensured if the parties share some prior info or there is a trusted party)

- Diffie and Hellman could not come up with a concrete construction; though a public-key encryption scheme was "hidden" in their key-exchange protocol
- Cryptography spread to masses just due to advent of public-key cryptography

Thank You!