CS557: Cryptography

Public-key Cryptography-IV

S. Tripathy
IIT Patna

Present Class

- Public Key Cryptography
  - Public Key Encryption
    - RSA
      - Factorization problem
    - Diffie-Hellman Key exchange
    - Elgammal Encryption
      - Discrete Logarithm Problem

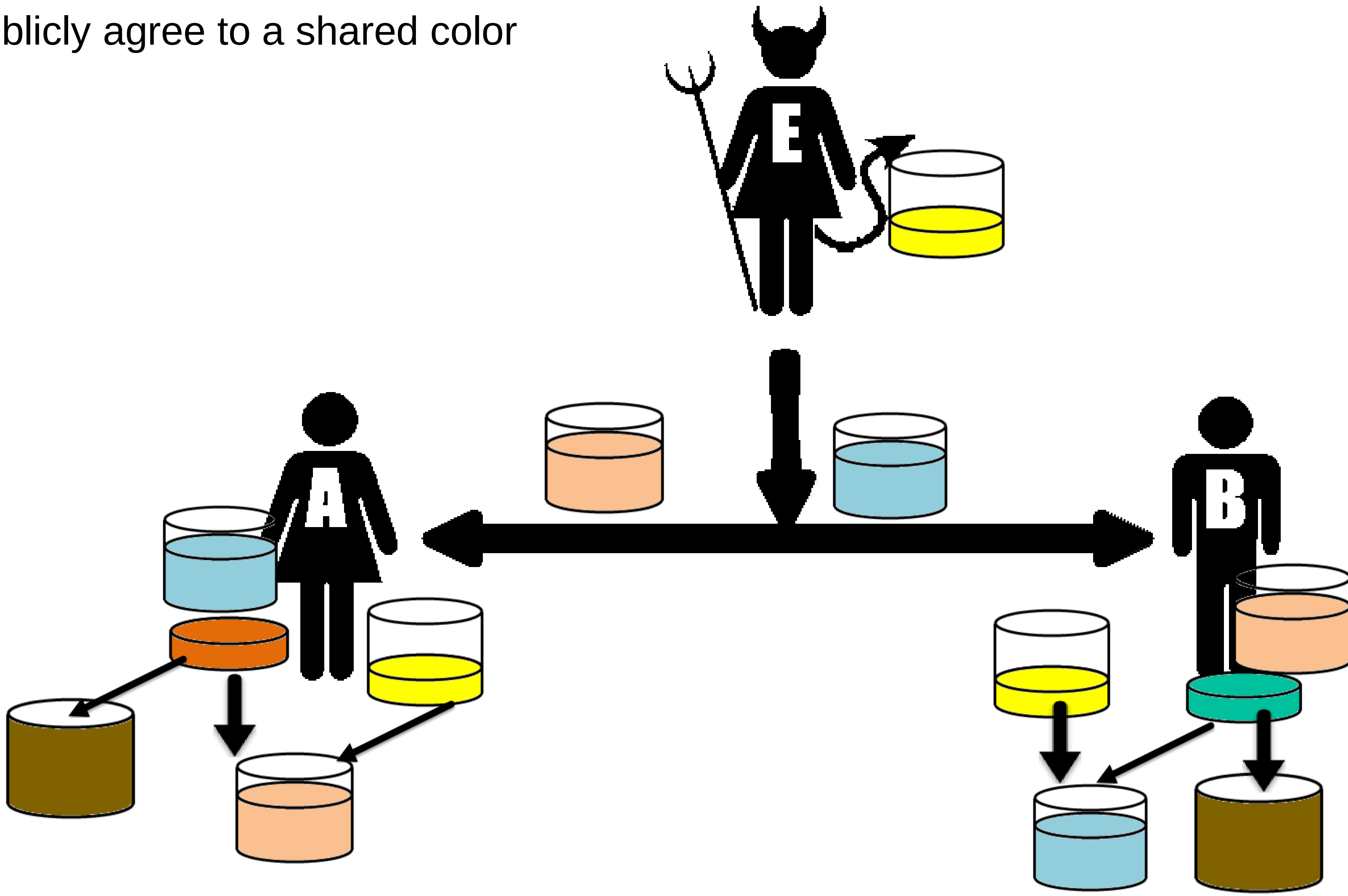
ELGAMAL PUBLIC KEY CRYPTOGRAPHY
BASED ON
DIFFIE HELLMAN KEY EXCHANGE

Diffie-Hellman key exchange (D-H) is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Color Exchange (DH Ex.)

Both publicly agree to a shared color



Diffie-Hellman Key Exchange

- Public: prime (1024 bit), generator *g* of group Z_p^*

Alice		Bob
Pick random $1 \le r_A \le p-1$	$\xrightarrow{g^{r_A}}$	Pick random $1 \le r_B \le p-1$
Output: $g^{r_A r_B}$	$\xleftarrow{g^{r_B}}$	Output: $g^{r_A r_B}$
Erase r_A		Erase r_B

Diffie-Hellman problem: Obtain g^{ab} with given (g^a, g^b)

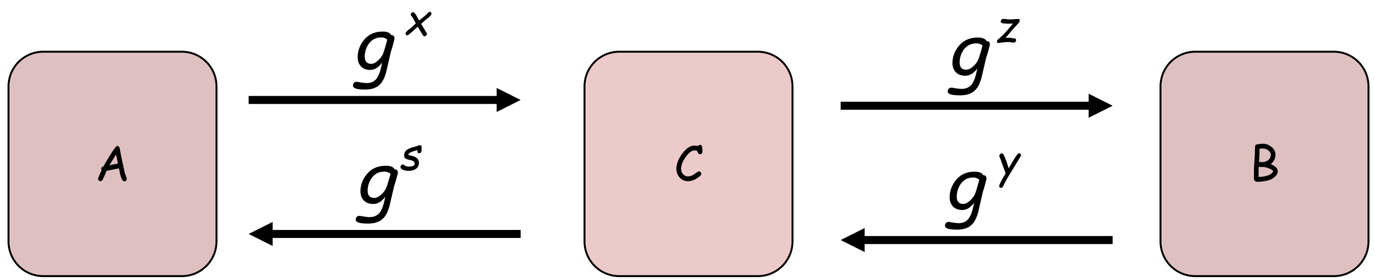
Easy if we can compute x from g^x

No better way known

implicit key authentication (only if attacker is passive)

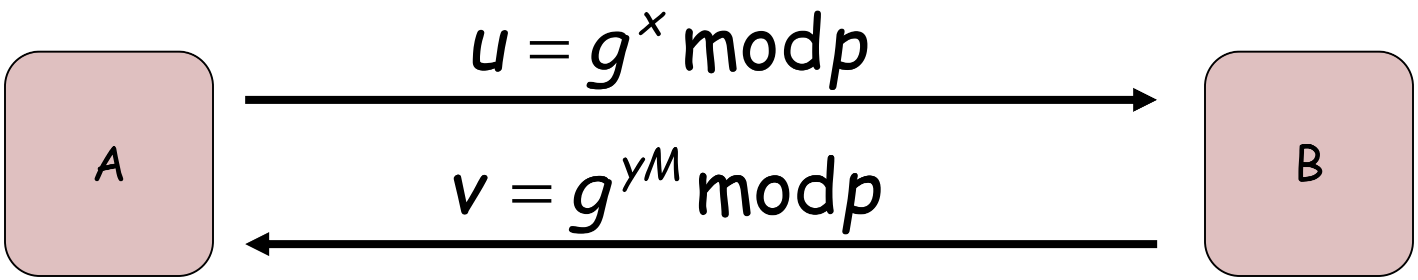
D-H is susceptible to man-in-the-middle attack

- D-H is susceptible to man-in-the-middle attack.



$$K_1 = g^{xs} \qquad\qquad K_2 = g^{zy}$$

Adding authentication

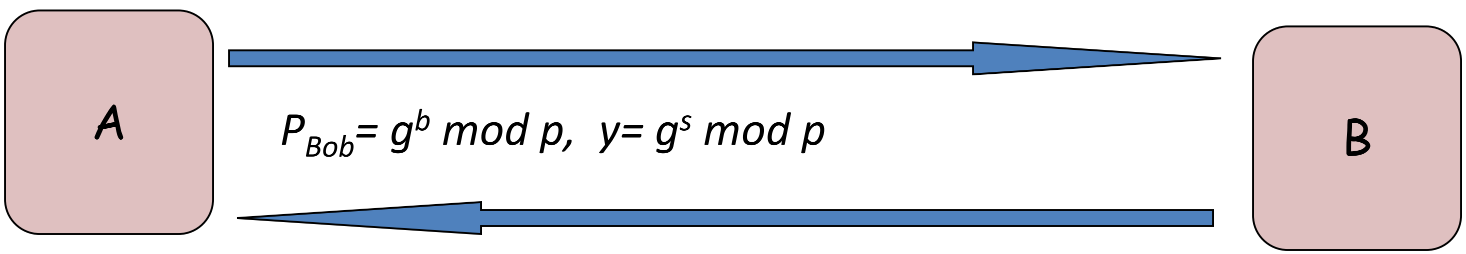


Here, $g^{M} = P_{Alice}$, the public key of Alice.

$$K = v^{xM^{-1}} = g^{xy} \qquad\qquad K = u^{y} = g^{xy}$$

Mutual-Authenticated DH

$P_{Alice}= g^a \bmod p,\ h= g^r \bmod p$



$P_{Bob}= g^b \bmod p,\ \ y= g^s \bmod p$

$K = (P_{Bob})^r\, y^a \bmod p$

$K = (P_{Alice})^s\, h^b \bmod p$

$K = g^{sa + rb} \bmod p$

CDH and DDH

- Discrete Log problem
  - Given y and g in Zp where p is prime, find the unique x in Zp , such that $y = g^x \bmod p$.
  - No efficient algorithm
- Computational Diffie-Hellman (CDH)
  - Given a multiplicative group (G, *), an element $g \in G$ having order q, given g^x and g^y, find g^xy
- Decision Diffie-Hellman (DDH)
  - Given a multiplicative group (G, *), an element $g \in G$ having order q, given g^x, g^y, and g^z, determine

    if g^xy $\equiv$ g^z mod n

- Discrete Log is at least as hard as CDH, which at least as hard as DDH

Solving Discrete Logarithm

- Exhaustive Search

- Shank's Algorithm
  - Baby step approach

- Pollard-Rho Method

Baby step Giant step approach

- Let G be a cyclic multiplicative group of size n. Let g be a generator of G. $g^x = y \in G$. Let $m = \sqrt{n}$.
  - Baby steps: For $i \in \{0, 1, 2, . . . , m - 1\}$, compute gi , and store (i, gi) sorted with respect to the second element.
  - Giant steps: For $j = 0, 1, 2, . . . , m - 1$, compute $y.g^{(-jm)}$, and try to locate $y.g^{-jm}$ in the table of baby steps.
  - If a search is successful, we have $y.g^{-jm} = g^i$ for some i, j,
    => $y = g\ jm+i$
    => $\text{ind}\ g(y) = jm + i$

Pollard rho discrete logarithm Technique

- partition the group G into three roughly equal-sized set S1 , S2 and S3 .

$$x_{i+1} = \begin{cases} y\,x_i & for\; x_i \in S_1 \\ x_i^{\,2} & for\; x_i \in S_2 \\ g.x_i & for\; x_i \in S_3 \end{cases}$$

$$a_{i+1} = \begin{cases} a_i \pmod{n} & for\; x_i \in S_1 \\ 2a_i \pmod{n} & for\; x_i \in S_2 \\ a_i + 1 & for\; x_i \in S_3 \end{cases}$$

$$b_{i+1} = \begin{cases} b_i + 1 & for\; x_i \in S_1 \\ 2b_i \pmod{n} & for\; x_i \in S_2 \\ b_i \pmod{n} & for\; x_i \in S_3 \end{cases}$$

Let $x_i = g^{a_i} y^{b_i}$

- This sequence of group elements defines two sequences of integers
- a_o, a_1,..... and b_0,b_1...... satisfying
- At x_i=x_{2i}

$$x = g^{ai} y^{bi}$$

- g^(a_i).y^(b_i) = g^(a_{2i})y^(b_{2i})
-
- $\log_g^y = x = (a_{2i} - a_i)/(b_i - b_{2i})$

El-Gamal encryption

Public parameters: p is a prime

g generator of G_p

Secret key of a user: d (where $0 < d < p-1$)

Public key of this user: $e = g^d \bmod p$

Message (or "plaintext") : m

Encryption technique (to encrypt m using e)

1. Pick a number k randomly from [0…p-1]
2. Compute $C1 = e^k . m \bmod p$
   $C2 = g^k \bmod p$
3. Output (C1,C2)

Decryption technique (to decrypt (C1,C2) using d)

Compute m: $C1 / C2^d = \dfrac{e^k . m}{(g^k)^d} = \dfrac{g^{dk} . m}{g^{kd}}$

El Gamal encryption: Ex:

Public parameters: p is a prime $p = 19$

g generator $g = 10$

Secret key of a user: (where $d < p-1$) $d = 5$

Public key of this user: $e = g^d \bmod p$

$e = 10^5 = 3 \bmod 19$

Message (or "plaintext") : m $m = 17$

Encryption technique to encrypt m using e)

1. Pick a number k randomly from [0…p-1]
2. Compute $c1 = e^k . m \bmod p$
3. $c2 = g^k \bmod p$
4. Output (c1,c2)

k = 6

$c1 = 3^6.17 = 12393 \bmod 19 = 5$

$c2 = 10^6 \bmod 19 = 11$

Output (5,11)

Decryption technique (to decrypt (c1,c2) using d)

Compute m: $c1 / c2^d$

5/ 11^5 mod 19= 5/7 mod 19 =

= 5 *11 mod 19 = 17

Security Analysis

- If the Computational Diffie-Hellman (CDH) holds in the underlying cyclic group , then the encryption function is one-way.
- If the decisional Diffie–Hellman assumption (DDH) holds in , then ElGamal achieves semantic security
- Its not secure under chosen ciphertext attack. Like discussed in RSA

- Thanks