CS171: Cryptography

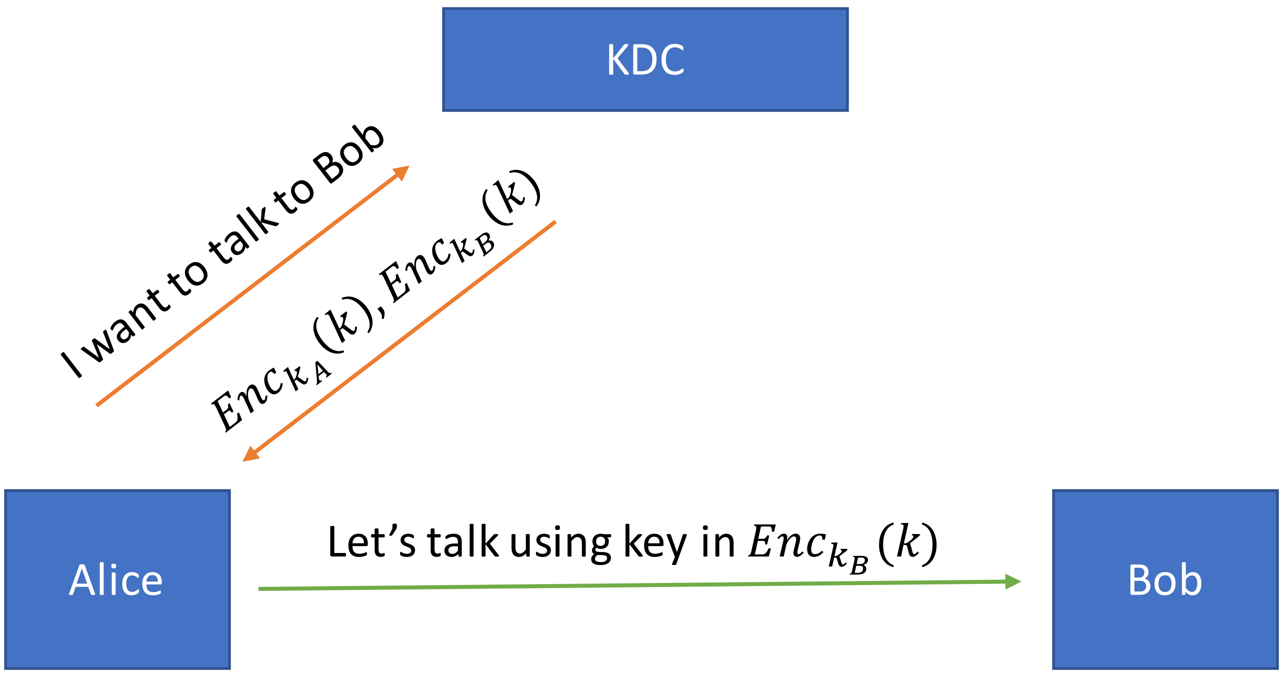
Lecture 13

Sanjam Garg

Drawbacks of Private-Key Cryptography

- Key-Distribution is a problem
- Storing a large number of keys is problematic
- Inapplicability to open systems (cannot meet)

A Partial Solution: Key-Distribution Center



Public-Key Cryptography

Number Theoretic Background

- A group G, is a set with a binary operation $\cdot$
    1. Closure: $\forall g, h \in G$ we have that $\mathrm{g} \cdot h \in G$
    2. Existence of an identity: $\exists e \in G$ such that for $\forall g \in G$, such that $\mathrm{g} \cdot e = g = e \cdot g$. (Denote e by 1 sometime)
    3. Existence of an inverse: $\forall g \in G, \exists h \in G$ such that $\mathrm{g} \cdot h = e = h \cdot g$.
    4. Associativity: For all $g_1, g_2, g_3 \in G$ we have that $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$

Example of a Group

- Is $(Z, +)$ a group?
    1. Closure: $\forall g, h \in Z$ we have that $\mathrm{g} + h \in Z$?
    2. Existence of an identity: $\exists e \in Z$ such that for $\forall g \in Z$, such that $\mathrm{g} + e = g = e + g$?
    3. Existence of an inverse: $\forall g \in Z, \exists h \in Z$ such that $\mathrm{g} + h = e = h + g$?
    4. Associativity: For all $g_1, g_2, g_3 \in Z$ we have that $(g_1+g_2) + g_3 = g_1 + (g_2 + g_3)$

Example of a Group

- Is $(Z,\cdot)$ a group?
  1. Closure: $\forall g, h \in Z$ we have that $g \cdot h \in Z$?
  2. Existence of an identity: $\exists e \in Z$ such that for $\forall g \in Z$, such that $g \cdot e = g = e \cdot g$?
  3. Existence of an inverse: $\forall g \in Z, \exists h \in Z$ such that $g \cdot h = e = h \cdot g$?
  4. Associativity: For all $g_1, g_2, g_3 \in Z$ we have that $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$?

Example of a Group

- Let $N > 1$ be an integer. Let G be the set $\{0,1,\ldots N-1\}$ with respect to addition modulo N (i.e., $a + b = a + b \; mod \; N$)
- Is $(G,+)$ a group?
  1. Closure: $\forall g, h \in G$ we have that $g + h \in G$?
  2. Existence of an identity: $\exists e \in G$ such that for $\forall g \in G$, such that $g + e = g = e + g$?
  3. Existence of an inverse: $\forall g \in G, \exists h \in G$ such that $g + h = e = h + g$?
  4. Associativity: For all $g_1, g_2, g_3 \in G$ we have that $(g_1+g_2) + g_3 = g_1 + (g_2 + g_3)$

More definitions for a group

- When G has a finite number of elements, then we say that G is finite and let $|G|$ denote the order of the group.
- We say that a group G is abelian if:
  - (Commutativity): For all $g, h \in G, g \cdot h = h \cdot g$.
- Subgroup: $(H, \cdot)$ is a subgroup of $(G, \cdot)$ if
  - $(H, \cdot)$ is a group
  - $H \subseteq G$

Which one is finite and abelian?

- $(Z, +)$
- $(G, +)$, $\mathrm{G} = \{0,1, \dots N - 1\}$ with respect to addition modulo N

Group Exponentiation

- For a group, $(G, \cdot)$:

$g^n = g \cdot g \cdots g$ (n times)

Properties

- Theorem: Let G be a group and $a, b, c \in G$. If $ac = bc$, then $a = b$. In particular, if $ac = c$ then a is the identity in G.
- Proof: Given $ac = bc$, multiple both sides with c^{-1} and we have that $a = b$. By the same argument, if $ac = c$ then a is the identity in G.

Properties

- Theorem: Let G be a finite group with order m. Then for any element $g \in G$, we have $g^m = 1$.
- Proof: (We will prove only for the abelian case)

$$
\begin{aligned}
g_1 \cdot g_2 \dots g_m &= (g \cdot g_1) \dots (g \cdot g_m) \\
&= g^m \cdot (g_1 \dots g_m)
\end{aligned}
$$

Thus, $g^m = 1$.

- Observe that $\forall\, i, j, g \cdot g_i \neq g \cdot g_j$

Group Exponentiation

- For a group, $(G,\cdot)$, finite group with order m:

$g^n = g \cdot g \cdots g$ (n times)

- $\forall\ g, \in G$ and integer x, $g^x = g^{x \bmod m}$

More Groups Definitions

- Let G be a finite group of order m.
- Then for any $g \in G$, we can define $\langle g \rangle = \{g^1 \dots g^m\}$.
- We know than g^m = 1. Let $i \leq m$ be the smallest value such than $g^i = 1$.
- As before, $g^x = g^{x \, mod \, i}$
- Lemma: i divides m, (We say i is the order of g)
- Proof: Assume $m = a\, i + b$, with $b < i$ then
- $1 = g^m = g^{ai} \cdot g^b = g^b$. Which is a contradiction.

Cyclic Group

- A group G is a cyclic group $\exists g \in G$ such that $\langle g \rangle = G$.
- Also we say that g is a generator of G.
- Lemma: If G is a group of prime order p, then G is cyclic. Moreover, every element except the identity is a generator of G.
- Another example (no proof): If p is a prime then Z_p^* is a cyclic group of order $p - 1$. $Z_p^* = \{1, \dots p - 1\}, a \cdot b = a \times b \ mod \ p$
- Example of cyclic group of prime order: If p and q are primes such that $2q \ = \ p - 1$, and let g $\in Z_p^*$ be an elements of order q. Then, $H \ = \langle g \rangle$ is of prime order.

The Discrete-Log Problem

- Let $\mathcal{G}(1^n)$ be a PPT algorithm that generates description of a cyclic group, i.e., order q (where $|q| = n$) and a generator g.
- Unique bit representation for each element and group operation can be performed in time polynomial in n.
- Sampling a uniform group element: Sample $x \leftarrow Z_q$ and compute g^x.

DLOG Problem

$\mathrm{DLog}_{A,\mathcal{G}}$(n)

1. Run $\mathcal{G}(1^n)$ to obtain (G, g, q).
2. Pick uniform $h \in G$.
3. A is given (G, g, q, h) and it outputs x.
4. Output 1 if $g^x = h$ and 0 otherwise

Discrete-Log Problem is hard relative to $\mathcal{G}$ if

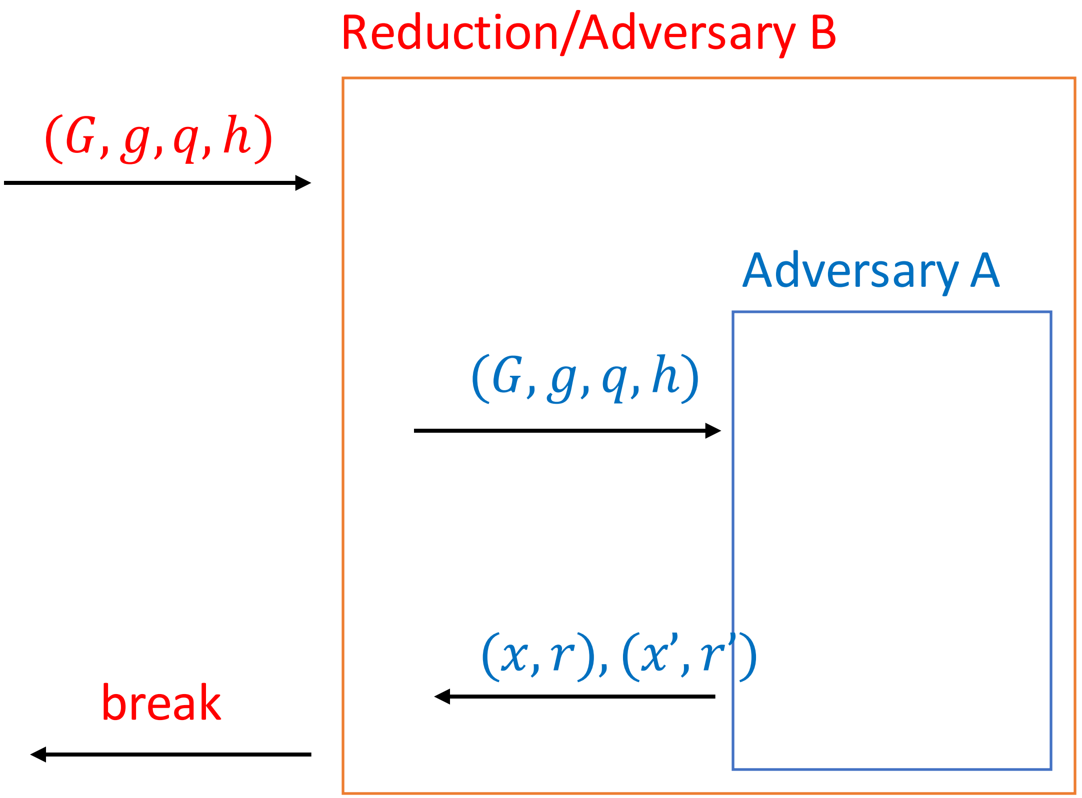
$\forall$ $PPT\ A$ $\exists$ $negl$ such that:

$\left|\Pr\left[\mathrm{DLog}_{A,\mathcal{G}}(\mathrm{n}) = 1\right]\right| \leq$ negl(n).

Collision Resistant Hash Functions

- (Gen, H)
- $Gen(1^n)$:
  1. $(G, g, q) \leftarrow \mathcal{G}(1^n)$
  2. Sample uniform group element h
  3. Output $s = (G, g, q, h)$
- $H^s(x||r) = g^x h^r$

Proof by Reduction (If $DLOG$ then CRHF)



- Given: $H(x||r) = H(x'||r')$
- Or, $g^x h^r = g^{x'} h^{r'}$
- Or, $h = g^{\frac{x-x'}{r'-r}}$
- B outputs $\frac{x-x'}{r'-r}$

The Diffie-Hellman Problems

- The computational variant: given g^x and g^y compute g^{xy}
- The decisional variant: given g^x and g^y distinguish between g^{xy} and a random group element.

Computational Diffie-Hellman Problem

$\mathrm{CDH}_{A,\mathcal{G}}$(n)

1. Run $\mathcal{G}(1^n)$ to obtain (G, g, q).
2. $a, b \leftarrow Z_q^*$.
3. A is given (G, g, q, g^a, g^b) and it outputs h.
4. Output 1 if $g^{ab} = h$ and 0 otherwise

CDH is hard relative to $\mathcal{G}$ if

$\forall$ $PPT\ A$ $\exists$ $negl$ such that:

$\left|\Pr\left[\mathrm{CDH}_{A,\mathcal{G}}(n) = 1\right]\right| \leq$ negl(n).

Decisional Diffie-Hellman Problem

$\mathrm{DDH}_{A,\mathcal{G}}(n)$

1. Run $\mathcal{G}(1^n)$ to obtain (G, g, q).
2. $a, b, r \leftarrow Z_q^*$. Sample a uniform bit c.
3. A is given $(G, g, q, g^a, g^b, g^{ab+cr})$ and it outputs c'.
4. Output 1 if $c = c'$ and 0 otherwise

DDH is hard relative to $\mathcal{G}$ if

$\forall\ PPT\ A\ \exists\ negl$ such that:

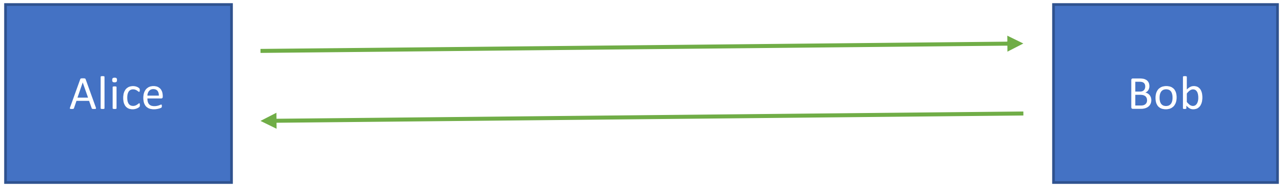
$\left|\Pr\left[\mathrm{DDH}_{A,\mathcal{G}}(n) = 1\right]\right| \leq$ ½ + negl(n).

Diffie-Hellman Problems

$$\begin{tikzcd} & \text{DLOG} \arrow[d, Rightarrow] & \text{CDH} \arrow[l, Rightarrow] & \text{DDH} \arrow[l, Rightarrow] \\ \text{OWF} & \text{CRHF} \arrow[l, Rightarrow] & & \end{tikzcd}$$

- If p and q are primes such that $rq = p - 1$ and let g $\in Z_p^*$ be an elements of order q. Let $H = \langle g \rangle$ be the group of order q.
- Elliptic Curve Groups

Key Exchange



k_{A} k_B

- Correctness: $k = k_{\mathrm{A}} = k_B$
- Security (Informally): Eve listening on the channel should not be able to guess k.

Key Exchange: Security

$\mathrm{KE}_{A,\Pi}^{eav}$ (n)

1. Two parties holding 1^n execute Π. This results in a transcript Ω of the communication and a key k output for each party.
2. Sample a uniform bit b. If $b = 0$, then set $\hat{k} = k$, else set $\hat{k}$ uniformly.
3. A is given $(\Omega, \hat{k})$ and it outputs b'.
4. Output 1 if $b' = b$ and 0 otherwise

A key-exchange protocol Π is secure if

$\forall$ PPT A $\exists$ $negl$ such that:

$\left|\Pr\left[\mathrm{KE}_{A,\Pi}^{eav}(n) = 1\right]\right| \leq$ ½ + negl(n).

The Diffie-Hellman Key Exchange Protocol

G, g, q can be fixed once and for all.

$x \leftarrow Z_q$ $h_A := g^x$	Alice	$\xrightarrow{G, g, q, h_A}$ $\xleftarrow{h_B}$	Bob	$y \leftarrow Z_q$ $h_B := g^y$

$k_A := h_B^x$

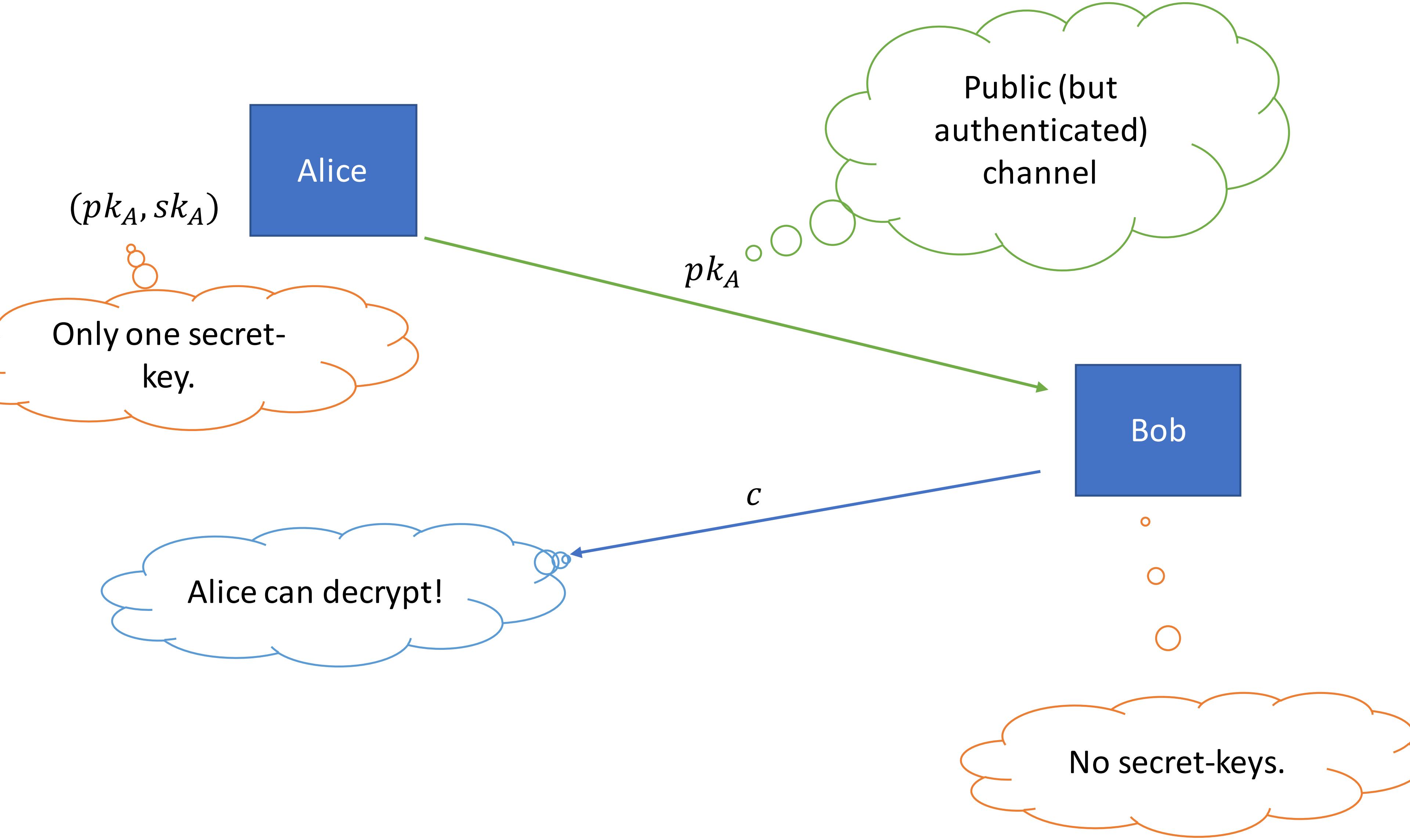
$k_B := h_A^y$

- Correctness: $k = k_A = k_B$
- Security (Informally): Follows from the DDH assumption.
- Subtle point: The key is indistinguishable from a random group element not a random string.

Public-Key Cryptography

- Public-Key Encryption
- Digital Signatures

Public-Key Encryption



Thank You!