Key Exchange

CS 601.642/442 Modern Cryptography

Fall 2019
A group $G$ is defined by a set of elements and an operation which maps two elements in the set to a third element.

$(G, \bullet)$ is a group if it satisfies the following conditions:

- **Closure**: For all $a, b \in G$, we have $a \bullet b \in G$.
- **Associativity**: For all $a, b, c \in G$, we have $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.
- **Identity**: There exists an element $e$ such that for all $a \in G$, we have $e \bullet a = a$.
- **Inverse**: For every $a \in G$, there exists $b \in G$ such that $a \bullet b = e$.

Think: Is $a \bullet b$ always equal to $b \bullet a$?

Read: Abelian Groups

Example: $(\mathbb{Z}, +)$
A group \((G, \cdot)\) is a cyclic group if it is generated by a single element. That is: \(G = \{1 = e = g^0, g^1, \ldots, g^{n-1}\}\), where \(|G| = n\).

Written as: \(G = \langle g \rangle\)

Order of \(G\): \(n\)
Discrete Logarithm Problem

- Let \((G, \cdot)\) be a cyclic group of order \(p\) with generator \(g\), where \(p\) is an \(n\)-bit “safe prime” number (i.e., \(p = 2q + 1\) for some large prime \(q\)).
- Given \((g, b = g^a)\), where \(a \leftarrow \{0, \ldots, p - 1\}\), it is hard to predict \(a\).
Discrete Logarithm Problem: Definition

Definition (Discrete Logarithm Problem)

Let \((G, \cdot)\) be a cyclic group of order \(p\) (where \(p\) is a safe prime) with generator \(g\), then for every non-uniform PPT adversary \(A\), there exists a negligible function \(\varepsilon\) such that

\[
\Pr[a \leftarrow \{0, \ldots, p - 1\}, a' \leftarrow A(G, p, g, g^a) : a = a'] \leq \varepsilon
\]
Let $G$ be a cyclic group $(G, \cdot)$ of order $p$ with generator $g$, where $p$ is an n-bit safe prime number.

Give $(g, g^a, g^b)$ to the adversary

Hard to find $g^{ab}$
Definition (Computational Diffie-Hellman Assumption)

Let $(G, \cdot)$ be a cyclic group of order $p$ (where $p$ is a safe prime) with generator $g$, then for every non-uniform PPT adversary $A$, there exists a negligible function $\varepsilon$ such that

$$\Pr[a, b \leftarrow \{0, \ldots, p-1\}, y \leftarrow A(G, p, g, g^a, g^b) : g^{ab} = y] \leq \varepsilon$$
Decisional Diffie-Hellman Assumption

- Let \((G, \cdot)\) be a cyclic group of order \(p\) with generator \(g\), where \(p\) is an \(n\)-bit safe prime number.
- Pick \(b \leftarrow \{0, 1\}\)
- If \(b = 0\), send \((g, g^a, g^b, g^{ab})\), where \(a, b \leftarrow \{0, \ldots, p - 1\}\)
- If \(b = 1\), send \((g, g^a, g^b, g^r)\), where \(a, b, r \leftarrow \{0, \ldots, p - 1\}\)
- Adversary has to guess \(b\)
- Effectively: \((g, g^a, g^b, g^{ab}) \approx (g, g^a, g^b, g^r)\), for \(a, b, r \leftarrow \{0, \ldots, p - 1\}\) and any \(g\)
Decisional Diffie-Hellman Assumption: Definition

Definition (Decisional Diffie-Hellman Assumption)

Let \((G, \cdot)\) be a cyclic group of order \(p\) (where \(p\) is a safe prime) with generator \(g\), then the following two distributions are computationally indistinguishable:

- \(\{a, b \leftarrow \{0, \ldots, p - 1\} : (G, p, g, g^a, g^b, g^{ab})\}\)
- \(\{a, b, r \leftarrow \{0, \ldots, p - 1\} : (G, p, g, g^a, g^b, g^r)\}\)
Relationship

DDH $\implies$ CDH $\implies$ DL
Alice and Bob want to share a key.

They want to establish a shared by by sending each other messages over a channel.

However, there is an adversary (Eavesdropper) that is eavesdropping on this channel and sees the messages that are sent over it.

How to securely establish a shared key while keeping it hidden from the eavesdropper?
Key Agreement: Definition

- Alice picks a local randomness $r_A$
- Bob picks a local randomness $r_B$
- Alice and Bob engage in a protocol and generate the transcript $\tau$
- Alice’s view $V_A = (r_A, \tau)$ and Bob’s view $V_B = (r_B, \tau)$
- Eavesdropper’s view $V_E = \tau$
- Alice outputs $k_A$ as a function of $V_A$ and Bob outputs $k_B$ as a function of $V_B$
- Correctness: $\Pr_{r_A, r_B}[k_A = k_B] \approx 1$
- Security: $(k_A, V_E) \equiv (k_B, V_E) \approx (r, \tau)$
Key Agreement: Construction (Diffie-Hellman)

- Let $(G, \cdot)$ be a cyclic group of order $p$ (where $p$ is a safe prime) with generator $g$.
- Alice picks $a \leftarrow \{0, \ldots, p - 1\}$ and sends $g^a$ to Bob.
- Bob picks $b \leftarrow \{0, \ldots, p - 1\}$ and sends $g^b$ to Alice.
- Alice outputs $(g^b)^a$ and Bob outputs $(g^a)^b$.
- Adversary sees: $(g^a, g^b)$
- Correctness?
- Security? Use DDH to say that $g^{ab}$ is hidden from adversary’s view.
- Think: Is this scheme still secure if the adversary is allowed to modify the messages?