QF Group Theory CC2022
By
Zaiku Group

Lecture 09

Delivered by Bambordé Baldé

Friday, 24/6/2022

Session Agenda

1. Learning Journey Timeline
2. Course Approach Overview

Pre-session Comments

+

1. Discrete Logs over Cyclic Groups
2. Discrete Log Problem
3. Diffie-Hellman Problem
4. Symmetric Cipher
5. Diffie-Hellman Key Exchange

Main Session

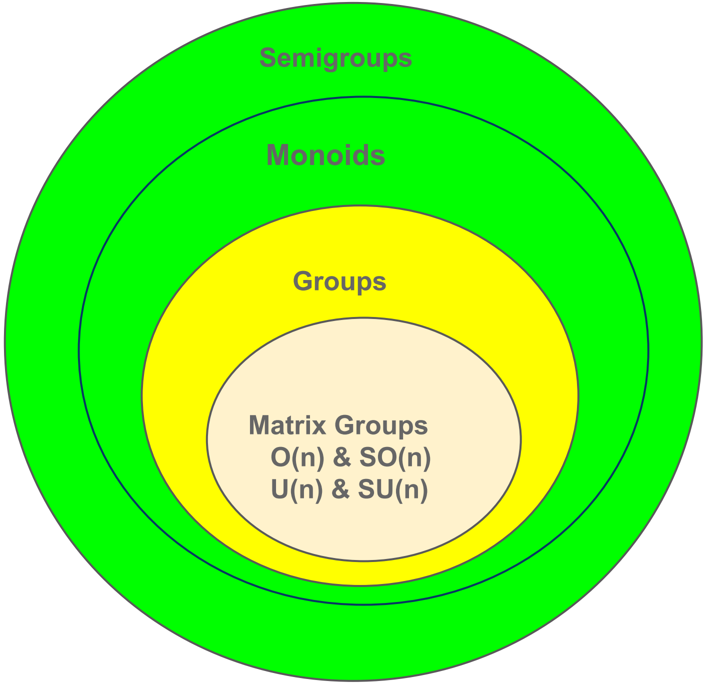
Learning Journey Timeline

Topology & Differential Geometry
9

Group Theory
9/20?

Lie Groups & Rep.
10 - 16?

Completed | Ongoing | TBC (summer) | n is the number of live lectures |



Course Approach Overview

Completed!

We’re here!

Discrete Logarithms over Cyclic Groups

Definition 1.0 (Theorem)

Let $G = \langle g \rangle$ be a cyclic group of order n. Then for each $x \in G$ there exists a unique integer $0 \leq k \leq n - 1$ such that $g^k = x$.

- The integer k is called the discrete logarithm of x in respect to the generator (or base) g.
- We write $log_g^x = k$ to denote the fact that k is the discrete logarithm of x in respect to base g.

Concrete toy examples:

1. Consider the cyclic group $\mathbb{F}_5^* = \{1, 2, 3, 4\}$ under mod 5 multiplication. We have seen before that 2 is a generator for $\mathbb{F}_5^*$ i.e. $\mathbb{F}_5^* = \langle 2 \rangle$. Then $log_2^1 = 4$ because $2^4 = 1$. Also, $log_2^2 = 1$ because $2^1 = 2$ right?
2. Consider again the cyclic group $\mathbb{F}_5^* = \{1, 2, 3, 4\}$ under mod 5 multiplication. We have seen before that 3 is also a generator for $\mathbb{F}_5^*$ i.e. $\mathbb{F}_5^* = \langle 3 \rangle$ right? Then $log_3^2 = 3$ because $3^3 = 2$ right?

The Discrete Logarithm Problem (DLP)

Definition 1.1

Given a cyclic group $G = \langle g \rangle$ of order n and $x \in G$, compute log_g^x i.e. find the integer $0 \leq k \leq n-1$ such that $g^k = x$.

- For the additive cyclic group $\mathbb{Z}_n$, computing log_g^x is equivalent to solving $kg \equiv x \mod n$.
- For the multiplicative group $\mathbb{F}_p^*$, computing log_g^x is equivalent to solving $g^k \equiv x \mod p$.

Simple toy challenge:

- Consider $\mathbb{F}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Incidentally 2 is also a generator for $\mathbb{F}_{11}^*$ i.e. $\mathbb{F}_{11}^* = \langle 2 \rangle$. What is log_2^9 in $\mathbb{F}_{11}^*$?
    1. 3 because $2^3 = 9$ i.e. 3 is the solution to the equation $2^k \equiv 9 \mod 11$?
    2. 4 because $2^4 = 9$ i.e. 4 is the solution to the equation $2^k \equiv 9 \mod 11$?
    3. 6 because $2^6 = 9$ i.e. 6 is the solution to the equation $2^k \equiv 9 \mod 11$?
    4. 8 because $2^8 = 9$ i.e. 8 is the solution to the equation $2^k \equiv 9 \mod 11$?

Some Comments on DLP

1. There is no known efficient classical algorithm that solves DLP for cyclic groups of large orders n. This makes DLP a good security assurance to build upon classical cryptographic systems. This gave birth to the so-called discrete log cryptography i.e. cryptography systems based on DLP. This includes the following well cryptographic systems:
    - Diffie-Hellman Key Exchange
    - ElGamal Encryption
    - Digital Signature Algorithm (DSA)
    - Elliptic Curves Cryptography (ECC)
    - Hyper Elliptic Curves Cryptography (HCC)
2. There is a quantum algorithm (Shor) that solves DLP efficiently!
    - Hence, quantum computers are a threat to all the cryptographic systems above that depend on DLP!
    - On a side note, the quantum algorithm for DLP is related to another problem known as 'Hidden Subgroup Problem (HSP)'.

Diffie-Hellman Problem (DHP)

Definition 1.2

Let $G = \langle g \rangle$ be a cyclic group of order n. Given g^{k_1} and g^{k_2} for two integers (secret) $0 \leq k_1, k_2 \leq n - 1$, determine $g^{k_1 k_2}$.

- Note that $g^{k_1 k_2} = (g^{k_1})^{k_2}$ (recall the group exponentiation).

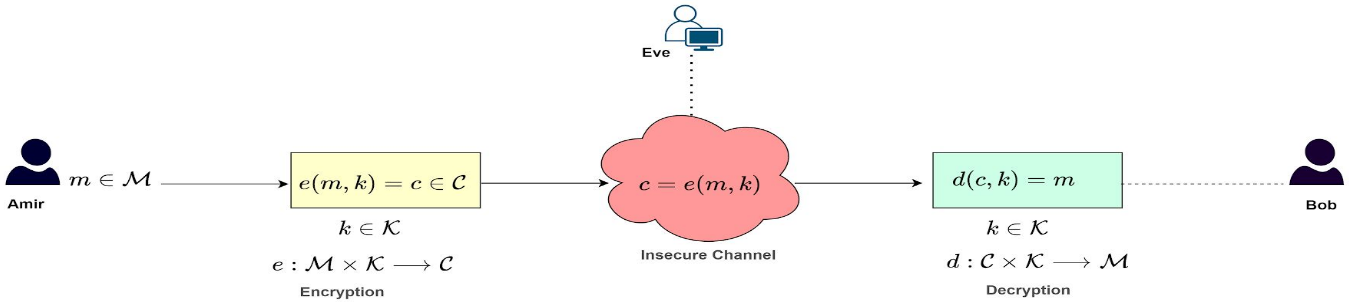
Natural Questions:

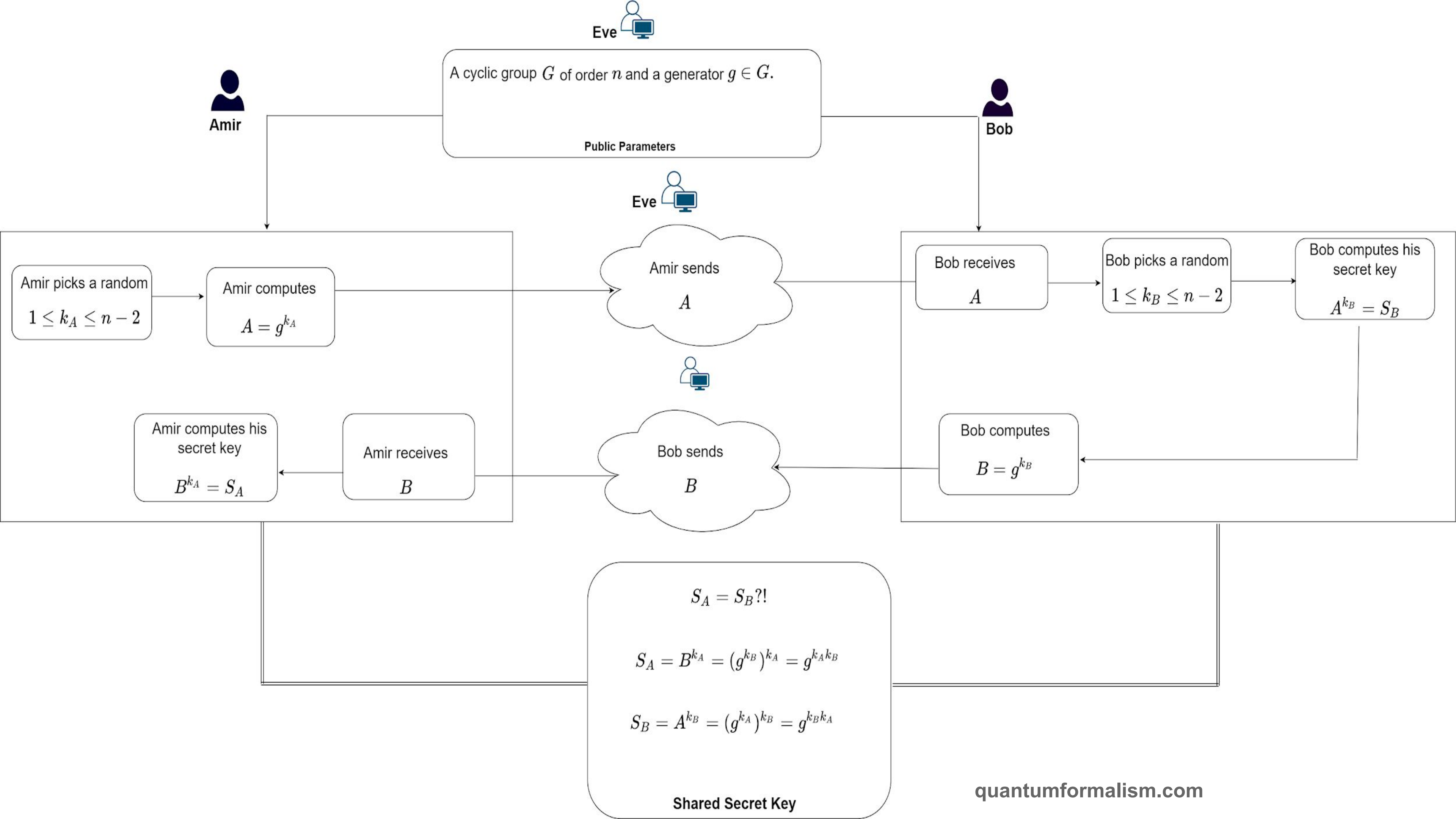
1. Does solving DLP means solving DHP? What about the other way round i.e. does solving DHP imply solving DLP?
2. Is DLP the only way to crack DHP?

DHKE Practical Implementation

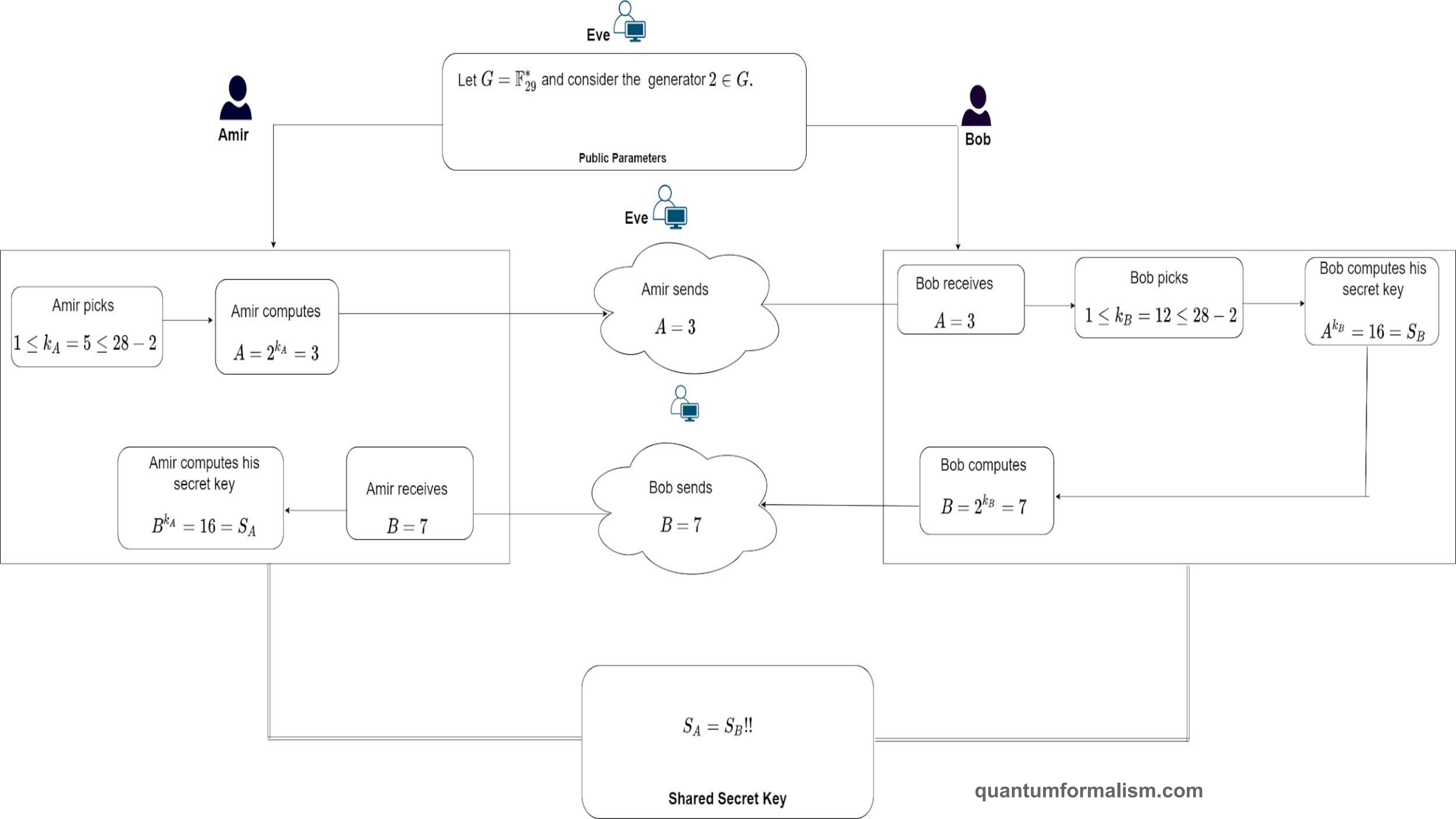
- For most practical applications of DHKE, the following multiplicative cyclic groups are used:
  1. $\mathbb{F}_p^*$ where p is a very large prime number similar to the size of RSA primes and p is a safe prime number.
  2. $GF(2^m)^*$ i.e. the multiplicative group of the Galois field extension $GF(2^m)$.
- DHKE is ubiquitous and used in many important and popular cryptographic protocols including:
  1. The Secure Shell Protocol (SSH)
  2. Transport Layer Security (TLS)
  3. Internet Protocol Security (IPSec)

Symmetric Ciphers 101


Eve
Amir
$m \in \mathcal{M}$
$e(m, k) = c \in \mathcal{C}$
$k \in \mathcal{K}$
$e : \mathcal{M} \times \mathcal{K} \longrightarrow \mathcal{C}$
Encryption
$c = e(m, k)$
Insecure Channel
$d(c, k) = m$
$k \in \mathcal{K}$
$d : \mathcal{C} \times \mathcal{K} \longrightarrow \mathcal{M}$
Decryption
Bob



Eve
A cyclic group G of order n and a generator $g \in G$.
Public Parameters
Amir
Bob
Eve
Amir picks a random $1 \leq k_A \leq n-2$
Amir computes $A = g^{k_A}$
Amir sends A
Bob receives A
Bob picks a random $1 \leq k_B \leq n-2$
Bob computes his secret key $A^{k_B} = S_B$
Bob computes $B = g^{k_B}$
Bob sends B
Amir receives B
Amir computes his secret key $B^{k_A} = S_A$
$S_A = S_B$?!
$S_A = B^{k_A} = (g^{k_B})^{k_A} = g^{k_A k_B}$
$S_B = A^{k_B} = (g^{k_A})^{k_B} = g^{k_B k_A}$
Shared Secret Key
quantumformalism.com


Eve
Let $G = \mathbb{F}_{29}^*$ and consider the generator $2 \in G$.
Public Parameters
Amir
Bob
Eve
Amir picks
$1 \leq k_A = 5 \leq 28 - 2$
Amir computes
$A = 2^{k_A} = 3$
Amir sends
$A = 3$
Bob receives
$A = 3$
Bob picks
$1 \leq k_B = 12 \leq 28 - 2$
Bob computes his secret key
$A^{k_B} = 16 = S_B$
Bob computes
$B = 2^{k_B} = 7$
Bob sends
$B = 7$
Amir receives
$B = 7$
Amir computes his secret key
$B^{k_A} = 16 = S_A$
$S_A = S_B$!!
Shared Secret Key
quantumformalism.com

QUANTUM FORMALISM

GitHub: github.com/quantumformalism

YouTube: youtube.com/ZaikuGroup

Discord: discord.gg/SPcmcsXMD2

Twitter: twitter.com/ZaikuGroup

LinkedIn: linkedin.com/company/zaikugroup