# Security in Cyber Physical System
# Tutorial # 1

May 4, 2023

Roy, Akash | CS22M007
M.Tech CS | Indian Institute of Technology, Madras

1. What are the mathematical properties that are used for the secure exchange of keys (hint: in terms of symmetry equivalence etc.)?

**Ans:** For symmetry equivalence during the key exchange we have the followings a generator number $g$, a large prime number $n$, the two exchanging parties have two private keys $a, b$.

The goal is to establish a secret key that's same for both the parties (symmetric key exchange).

Suppose Alice is a party that has private key $a$, Bob is another party who has private key $b$. Alice will compute $g^a \bmod n$. Bob will compute $g^b \bmod n$. These two can be exchanged via public non-encrypted channel because finding what is $a$ from $g^a \bmod n$ is computationally extremely hard.

Now Alice has $g^b \bmod n$, multiplying with $g^a \bmod n$, Alice will get $g^{ab} \bmod n$. Similarly Bob will multiply $g^a \bmod n$ with $g^b \bmod n$, then Bob will get $g^{ab} \bmod n$.

Now this number $g^{ab} \bmod n$ is a secret value that is not in the public domain and can not be derived from all the variables available in the public domain. Thus giving us a symmetric key $g^{ab} \bmod n$.

So the properties are following

- Given a function $f$, and two keys $a, b$, and some operation op, $f(a)$ op $f(b) = f(b)$ op $f(a)$
- $f^{-1}$ is not easy to calculate.

2. Discuss how the above function can be used as your algorithm for the secure exchange of keys.

**Ans:** Suppose I've one function $f$ and have the following properties

- Given a function $f$, and two keys $a, b$, and some operation op, $f(a)$ op $f(b) = f(b)$ op $f(a)$
- $f^{-1}$ is not easy to calculate.

Now our key-exchange algorithm would be the following

**Algorithm 1:** KEY-EXCHANGE ALGORITHM

**Input:** Private variable $a$ for Alice and variable $b$ for Bob, and one suitable operation OP

1 Calculate $f(a)$ from Alice's end.
2 Calculate $f(b)$ from Bob's end.
3 Exchange $f(a)$ and $f(b)$ with each other
4 Use $f(a)$ OP $f(b)$ as the symmetric key for encryption.