Cryptography Session No.7

Summary 27-07-2022

- If we have to transfer some data between “A” to “B” and we use a symmetric key to transfer data then there is a high chance a hacker will be able to sniff my key and as well the encrypted data, Now with the key, hacker can decrypt our data and get our original plain text. So here the problem is not with the symmetric key, Here the problem is how we are exchanging the “Key” between “A” and “B”. So to solve this challenge we use **Asymmetric Keys**.

- We have one more challenge, if “A” needs to communicate data with “B”, “C”, “D”, and like this with 1000’s users (*One to many communication*), then “A” will need the symmetric keys of all thousands of users, Now this is a big problem, First problem is how we can get the symmetric keys of these 1000’s user securely? Even if we get the keys managing these many keys will be very hard, If we compare it with the Gmail server then it has to communicate with billions of users at a time, and in this we will face a lot of issues, to solve this issue also we can use asymmetric key encryption.