1. A close-up of a sign

   Description automatically generated
2. Earlier lecture, we discussed the hash function which takes hash key too along with data to generate MAC Hash.   
   But the main point was that both sides receiver and sender use the same hash key.
3. Let’s talk about **Asymmetric keys**.
4. What is a pair of asymmetric keys?
5. Asymmetric Key is pair of two keys 🡺 Private and Public.
   1. Usually, they have same length but yes they are different.
   2. Private key is kept secret at one place.
   3. Only owner of this pair of key knows the private key.
   4. Public key can be communicated with anyone in the world..
6. **Different purposes of Private and Public Key**:
   1. **They can be used for data encryption**:
      1. Public key is used to encrypt data.
      2. Only the owner of the private key can decrypt data using that private key.
   2. **Another use case is to sign data using private key**.
      1. The owner of the private key signs data using private key (In other words, creates hash).
      2. The one having corresponding public key can verify the signature using the public key.
7. In next lecture, let us discuss encryption using asymmetric key.