Key Management Approaches

- The primary goal of key management is to share a secret (some information) among a specified set of participants
- There are several methods that can be employed to perform this operation, all of them requiring varying amounts of initial configuration, communication, and computation.
- The main approaches to key management are key predistribution, key transport, key arbitration, and key agreement.

- **Key Predistribution:**
- Key predistribution, as the name suggests, involves distributing keys to all interested parties before the start of communication.
- This method involves much less communication and computation, but all participants must be known *a priori*, during the initial configuration.
- Once deployed, there is no mechanism to include new members in the group or to change the key.
- As an improvement over the basic predistribution scheme, sub-groups may be formed within the group, and some communication can be restricted to a subgroup.
- However, the formation of sub-groups is also an *a priori* decision with no flexibility during the operation.

- **Key Transport:**
- In key transport systems, one of the communicating entities generates keys and transports them to the other members. The simplest scheme assumes that a shared key already exists among the participating members.
- This prior shared key is used to encrypt a new key and is transmitted to all corresponding nodes.
- Only those nodes which have the prior shared key can decrypt it. This is called the key encrypting key (KEK) method.
- However, the existence of a prior key cannot always be assumed. If the public key infrastructure (PKI) is present, the key can be encrypted with each participant's public key and transported to it. This assumes the existence of a TTP, which may not be available for ad hoc wireless networks.

- **Key Arbitration:**
- Key arbitration schemes use a central arbitrator to create and distribute keys among all participants. Hence, they are a class of key transport schemes.
- Networks which have a fixed infrastructure use the AP as an arbitrator, since it does not have stringent power or computation constraints.
- In ad hoc wireless networks, the problem with implementation of arbitrated protocols is that the arbitrator has to be powered on at all times to be accessible to all nodes.

- **Key Agreement**
- Most key agreement schemes are based on asymmetric key algorithms.
- They are used when two or more people want to agree upon a secret key, which will then be used for further communication.
- Key agreement protocols are used to establish a secure context over which a session can be run, starting with many parties who wish to communicate and an insecure channel.
- In group key agreement schemes, each participant contributes a part to the secret key. These need the least amount of pre-configuration, but such schemes have high computational complexity.
- The most popular key agreement schemes use the Diffie-Hellman exchange, an asymmetric key algorithm based on discrete logarithms