CipherSuite Configuration and Key Generation

- **CipherSuite Initialization**
  - where you define the KEM,KDF,AEAD
- **Public and Private Key generation**
  - for sender and recipient
- **Sender & Recipient Context**
  - Different Configuration for different modes
- **Encryption & Description**
  - Seal(msg,aad)
  - Open(enc,aad)

Cryptographic Essentials

- **KEM (Key encapsulation Mechanism)**
  - Allow Secure key exchange
- **KDF (Key Derivation function)**
  - Used to derive key
- **AEAD (Authentication Encryption and Additional Data)**
  - Secure data from alteration
- **PSK (Pre-Shared Key)**
  - held by both sender & recipient
- **Info**
  - Application Supplied Information
- **Enc**
  - byte string of encapsulated key received from a sender
- **Aad**
  - Additional authenticated data as bytes fed by an application.

Sender & Recipient Context with Modes

- **Base**
  - **Sender Context**
    - Recipient Public key
  - **Recipient Public Key**
    - Encapsulated key from sender
    - Recipient Private key
- **PSK**
  - **Sender Context**
    - Recipient Public key
    - Pre-Shared key
  - **Recipient Public Key**
    - Encapsulated key from sender
    - Recipient Private key
    - Pre-Shared Key
- **Auth**
  - **Sender Context**
    - Recipient Public key
    - Sender Key
  - **Recipient Public Key**
    - Encapsulated key from sender
    - Recipient Private key
    - Sender's Public Key
- **Auth Psk**
  - **Sender Context**
    - Recipient Public key
    - Sender Key
    - Pre-Shared Key
  - **Recipient Public Key**
    - Encapsulated key from sender
    - Recipient Private key
    - Sender's Public Key
    - PSK