Answers for Session 4c- Attacks and Vulnerabilities in Wireless Networks

1.Where/How will PMK come from/prepared?

PMK is generated from the passphrase that is present with both AP and the client
Below are the steps that are followed to generate the PMK for personal security:

- Passphrase is known to both AP and supplicant.
- PSK Gets generated from the Passphrase from the following function. We need passphrase and SSID to generate the PSK.
  PSK = pbkdf2.pbkdf2(str.encode(passphrase), str.encode(SSID), 4096, 32)
- PMK gets generated from the below function which uses HMAC-SHA1 to encode the data. If an 802.1X EAP exchange was carried out, the PMK is derived from the EAP parameters provided by the authentication server.

  PMK = PBKDF2(HMAC−SHA1, PSK, SSID, 4096, 256

2.How's this PRF work in the password dictionary

Pseudo-random functions (PRFs) are an interesting and powerful tool in cryptography, used to generate seemingly random outputs from deterministic inputs. While they aren't truly random, their outputs appear statistically random and unpredictable, making them useful for various security purposes.