In WPA2/WPA3 Personal mode, the passphrase (PSK) is used to derive the Pairwise Master Key (PMK) using a key derivation function (e.g., PBKDF2 in WPA2, or SAE in WPA3).

The PMK must be identical on both the client and AP for the 4-way handshake to succeed.

A wrong passphrase results in a different PMK, which affects the derivation of the Pairwise Transient Key (PTK) and the Message Integrity Code (MIC) used in the handshake.

## What Happens During the 4-Way Handshake with a Wrong Passphrase

**The 4-way handshake involves four messages to authenticate the client and AP and establish session keys. If the client uses a wrong passphrase**

1. **Message 1: AP to Client**
    - The AP sends a random nonce (ANonce) to the client.
    - Impact of Wrong Passphrase: No issue yet, as the client hasn't used the passphrase. The client receives the ANonce and prepares to compute the PTK.
2. **Message 2: Client to AP**
    - The client uses the wrong passphrase to derive an incorrect PMK, which it then uses (along with ANonce, its own nonce SNonce, and other parameters like MAC addresses) to compute an incorrect PTK.
    - The client generates a MIC (using the Key Confirmation Key, KCK, from the incorrect PTK) and sends the SNonce and MIC to the AP.
    - Impact of Wrong Passphrase:
        - The AP, using the correct PMK (derived from the correct passphrase), computes the PTK with the same ANonce, SNonce, and other parameters.
        - The AP verifies the client's MIC using its own PTK. Since the client's PTK (and thus KCK) is based on a wrong PMK, the MIC will not match.
        - The AP detects the mismatch and typically rejects the handshake, sending an error or terminating the process.
3. **Message 3: AP to Client (if Handshake Continues)**
    - If the AP continues (unlikely, as it may abort after Message 2's MIC failure), it sends the Group Temporal Key (GTK) encrypted with its PTK's Key Encryption Key (KEK) and a MIC.
    - Impact of Wrong Passphrase:
        - The client, using its incorrect PTK, cannot decrypt the GTK or verify the **AP's** MIC (since its KCK is wrong).
        - The client will fail to validate Message 3, causing the handshake to fail at this stage if it hasn't already.
4. **Message 4: Client to AP**
    - If the handshake reaches this point (rare due to earlier failures), the client sends a final acknowledgment with a MIC, which again will be invalid due to the incorrect PTK.
    - Impact of Wrong Passphrase: The AP rejects the invalid MIC, and the handshake fails.

## Outcome of a Wrong Passphrase

- **Handshake Failure:** The 4-way handshake will not complete because the MICs generated by the client and AP will not match, as they are based on different PTKs derived from different PMKs.
- **Connection Denied:** The client is unable to authenticate with the AP and cannot join the Wi-Fi network. The user typically sees an error like “Incorrect password” or “Connection failed.”
- **No Data Exposure:** The wrong passphrase does not compromise the network’s security, as the PMK and session keys are never transmitted, and the handshake ensures mutual authentication fails if the PMK is incorrect.

## Why This Happens

- The PMK is the root of trust in the 4-way handshake. A wrong passphrase creates a different PMK, leading to:
    - An incorrect PTK, which includes the KCK (for MICs), KEK (for GTK encryption), and Temporal Key (TK, for data encryption).
    - Mismatched MICs, which are cryptographic proofs of PMK knowledge, ensuring neither party can proceed without the correct PMK.
- In WPA3, the Simultaneous Authentication of Equals (SAE) process (preceding the 4-way handshake) further ensures that a wrong passphrase prevents PMK agreement even before the handshake begins, adding an extra layer of protection.