Exercise 4: Security analysis on IKE Auth:

(a) Try to find a man-in-the-middle attack on the "IKE AUTH" exchange with the modification that the data fields over which the authentication apyloads are generated such that $\boldsymbol{AUTH_i = Sig_{ski_i}(N_r)}$ and $\boldsymbol{AUTH_r = Sig_{ski_r}(N_i)}$, assume certificates are exchanged.

The IKE AUTH exchange relies on the Initiator and Responder binding their private key with their ID. This exchange achieves the binding by first generating the confirmation keys SK_{pi} and SK_{pr}, and then binding these keys to the ID of the initiator and responder, respectively. Each respective binding is signed by either the initiator or responder's private key, ensuring that they can validate each other's identity and establish mutual connection.

$$AUTH_i = Sig_{sk_i}(INIT, N_r, PRF(SK_{pi}, ID_i))$$
$$AUTH_r = Sig_{sk_r}(INIT, N_i, PRF(SK_{pr}, ID_r))$$

In the case of this question, the initiator and responder only sign the nonce of the other party as follows:

$$AUTH_i = Sig_{sk_i}(N_r)$$
$$AUTH_r = Sig_{sk_r}(N_i)$$

As a result, the initiator and responder's private key is not bound to their IDs and therefore no mutual authentication is established. Additionally, since the certificates are already exchanged, there is no additional identity verification and authentication at the AUTH stage. The security of IKE becomes solely reliant on $KE_i = g^i$ and $KE_r = g^r$, which are exchanged in the IKE INIT phase to establish the pre-secret master key and generate the various keys in the subsequent exchanges. Therefore, a simple man-in-the-middle attack on any Diffie Hellman key exchange applies in this situation, where the attacker may intercept communications during the key establishment procedure. The following method in Figure 1 describes MITM attacks on any DH key exchange:

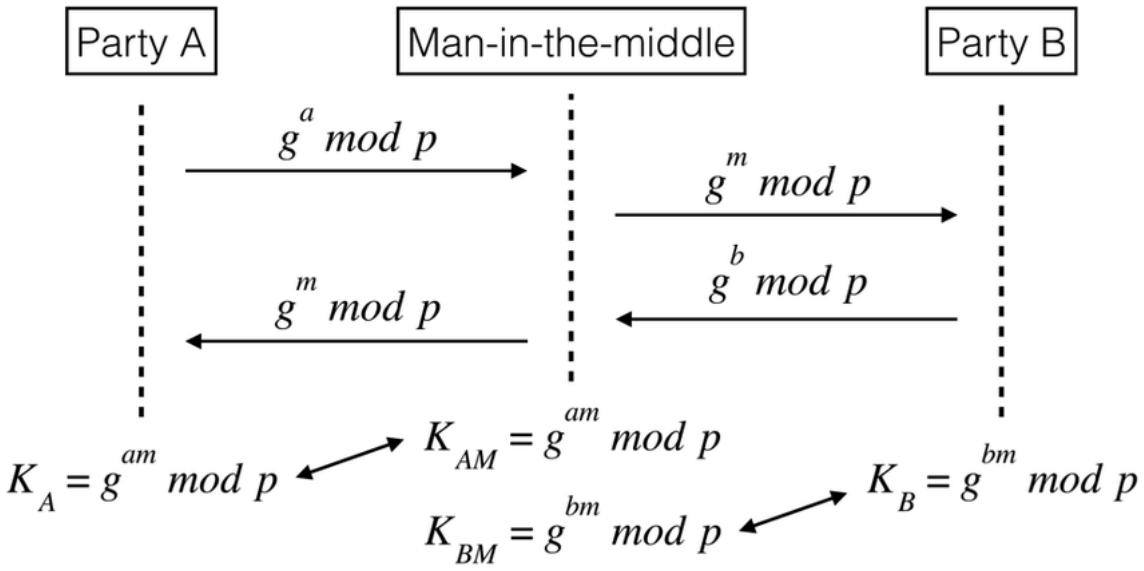

Figure 1 – MITM attack during DH exchange - https://www.researchgate.net/figure/The-man-in-the-middle-attacks-during-key-exchange-procedure_fig6_313738303

In Figure 1, party A is the initiator and party B is the responder. The attacker can attack the IKE AUTH exchange since the initiator and responder cannot verify the identity associated with the pre-secret master key.

(b) Try to explore possibilities to conduct a dictionary attack in IKEv2, when the pre-shared secret S_{pre} is a password with binary length 8 bits. (Hint: A failed execution may expose a value AUTH and the data it is protecting)

Attackers must wait initially for the victim to initiate an IKE exchange with a responder during an offline dictionary attack. The attacker will intercept the ClientHello message and prevent it from reaching the responder – the attacker will acts as the responder using IP spoofing and perform each of the necessary exchanges until message m5 is received from the victim as shown in Figure 2 below:

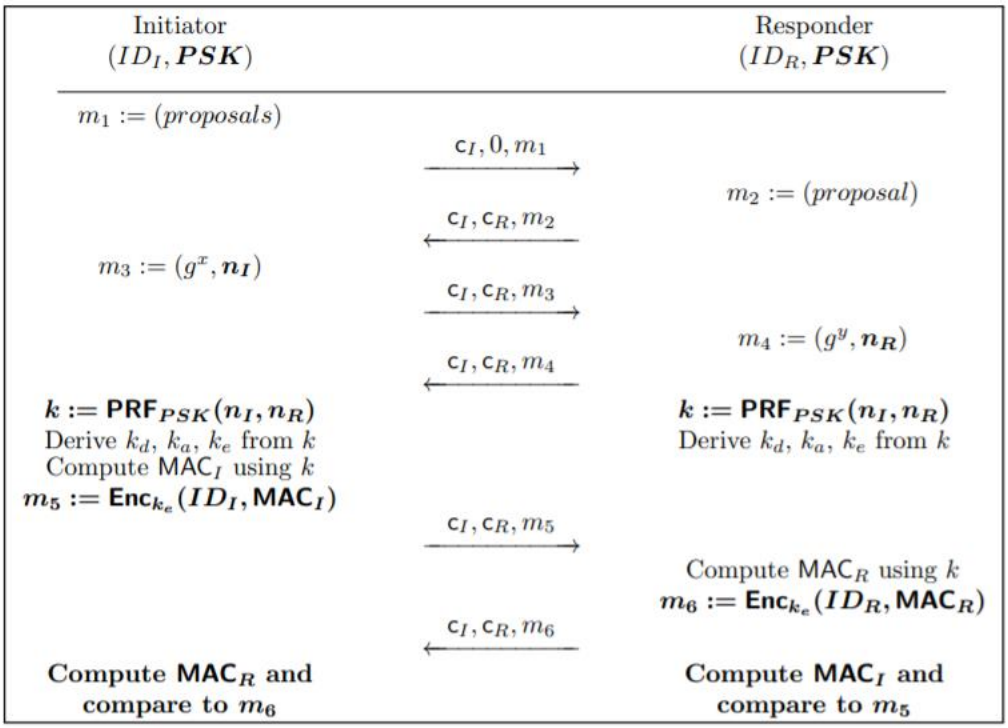

Figure 2 – IKEv2 offline dictionary attack exchanges - The Dangers of Key Reuse: Practical Attacks on IPsec IKE, pp. 13–14

Once m5 is received, the attacker has the ID and the MAC of the inititator, encrypted using k_e derived from $k = PRF_{PSK}(n_i, n_R)$, where PSK is the pre-shared key. ID_I is easily determined given it is usually assigned the IP address of the initiator. Given that the pre-shared key is 8 bits in length, an iterative offline dictionary attack need only to iterate a total of 256 permutations. For each PSK between 0 and 255, inclusive, k and k_e can be derived and m5 can be decrypted. The k_e value that decrypts m5 such that ID_I is the IP address, or another ID that the attacker knows, reveals the corresponding k and PSK values that the attacker needs. Once determined, the attacker can derive the other keys easily. This attack is made possible given the plaintext of m5 has a known structure that begins with ID_I, a known value for the attacker.