1.1. The attack trace found by OFMC shows that the communication between A and B in this protocol is intercepted by an intruder who impersonates B, thus, performing a man in the middle attack. Therefore, A uses the public key of the intruder to encrypt its identity, intruder's identity, number of request, and a symmetric key known to A. This encrypted information is sent to the intruder who, upon decrypting, makes a few changes such as excluding itself from the message and adds B's identity instead and creates a new request number and a symmetric key and forwards it to B (a web server), encrypting it using B's public key. This step shows that B will presume that the message was sent from A since it includes A's identity. Furthermore, the protocol requires A to authenticate itself to B using a trusted third party s with whom A shares a secret password. Thus, using the symmetric key sent by the intruder, B encrypts the identities of A, itself, s, and a request ID and sends it to the intruder. The intruder forwards this message to A but replaces the identity of B and the request ID with its ID and a forged request ID and encrypts it using the symmetric key sent by A earlier. The subsequent steps in the protocol requires A to communicate with s so that the latter can authenticate the former to B. These transmissions are again intercepted by the intruder who first forwards the message from A to s and then instead of s forwarding the message to B, sends it to the intruder and encrypts it using the public key of B. Upon decrypting, B can verify the message with the assumption that it is indeed sent from s since the identity of s and A are encrypted using the private key of s (this is also a step in the protocol). Hence, B presumes that the intruder is A and, hence, sends confidential data/information to the intruder. In conclusion, the attack is a result of weak authentication.

1.2. As seen from the attack trace, B and s can not properly authenticate A nor themselves to each other, upon receiving and transmitting messages. This is where intruder intercepts and performs the attack. To circumvent this issue and prevent the intruder from impersonating an entity, using the password shared between A and s (it can be safely assumed for now that the password is cryptographically strong), A can encrypt in a message the identity of B, a request ID generated for this session, along with its own and s identity. Since this message can only be decrypted by s, upon reception s can clearly see the identity of B and not the intruder along with a request ID generated from a previous session. Therefore, s will be able to determine that this message was not from A but an intruder. Likewise, when s is communicating with B, the former can follow similar steps as A did i.e. adding the identity of B and the same request ID from previous session and encrypt it using the public key of B. Thus, B can also authenticate the server.

1.3. Since the password shared between A and s is not cryptographically strong enough, OFMC finds that it is easily guessed by the intruder and, therefore, all the communication between A and s is compromised.

1.4. Any message that A transmits initially can potentially be compromised and known to the intruder. However, to communicate with s, A could encrypt an already encrypted message (albeit with a weak password) with the public key of s. Furthermore, the message can include a nonce generated by A and a request ID for this specific session. Even if the intruder gets a hold of this message and impersonates A later on, upon reception s can determine that the request ID is indeed from a previous session and the communicating entity is an intruder and not A.