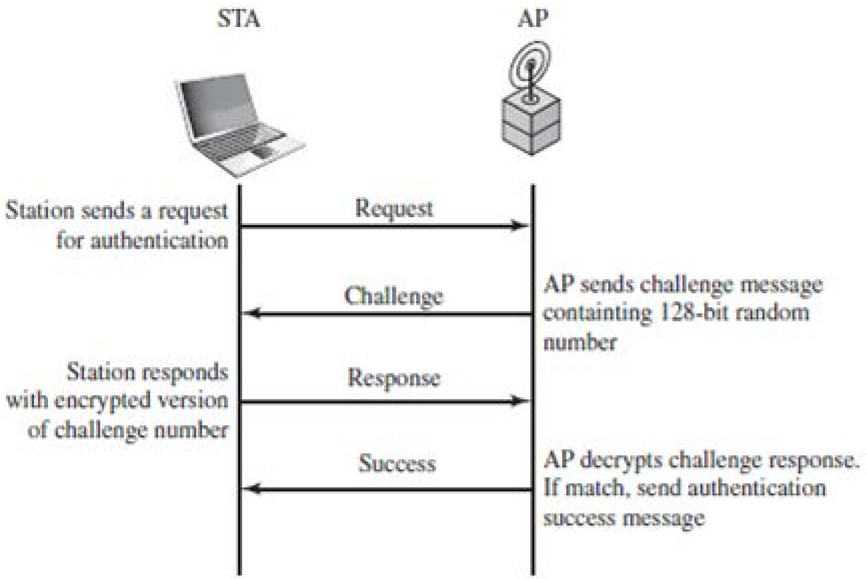
Prior to the introduction of IEEE 802.11i, the security scheme for IEEE 802.11 was Wired Equivalent Privacy (WEP). WEP assumed all devices in the network share a secret key. The purpose of the authentication scenario is for the STA to prove that it possesses the secret key. Authentication proceeds as shown in the figure below. The STA sends a message to the AP requesting authentication. The AP issues a challenge, which is a sequence of 128 random bytes sent as plaintext. The STA encrypts the challenge with the shared key and returns it to the AP. The AP decrypts the incoming value and compares it to the challenge that it sent. If there is a match, the AP confirms that authentication has succeeded.


STA
AP
Station sends a request for authentication
Request
Challenge
AP sends challenge message containting 128-bit random number
Station responds with encrypted version of challenge number
Response
Success
AP decrypts challenge response. If match, send authentication success message

a. What are the benefits of this authentication scheme?

b. This authentication scheme is incomplete. What is missing and why is this important? Hint: The addition of one or two messages would fix the problem.

c. What is a cryptographic weakness of this scheme?

Your Answer:

a. It is a quicker method of authentication since it carries simpler encryption practices. There is basic access control since only stations with the proper shared secret key can authenticate. There are also random challenges making infiltration for an attacker harder since it is completely randomized.

b. It is missing both challenge protection and mutual authentication. An attacker could easily intercept the challenge since it is plaintext. They could also recover the secret key since they can capture both this and the encrypted response. One sided authentication from the client to the AP opens vulnerabilities.

c. The encryption is rather weak due to it's simplicity. The visibility the hacker has on the encryption process opens the vulnerabilities that exist with the scheme. They can see between the plaintext challenge and the encrypted response and the key could easily be cracked since there is also weak key management.