What are some of the weaknesses of the WEP scheme? Check all that apply. **1 / 1 point**

- [x] Its use of the RC4 stream cipher

Correct
You nailed it! The RC4 stream cipher had a number of design flaws and weaknesses. WEP also used a small IV value, causing frequent IV reuse. Lastly, the way that the encryption keys were generated was insecure.

- [ ] Its use of ASCII characters for passphrases
- [x] Its poor key generation methods

Correct
You nailed it! The RC4 stream cipher had a number of design flaws and weaknesses. WEP also used a small IV value, causing frequent IV reuse. Lastly, the way that the encryption keys were generated was insecure.

- [x] Its small IV pool size

Correct
You nailed it! The RC4 stream cipher had a number of design flaws and weaknesses. WEP also used a small IV value, causing frequent IV reuse. Lastly, the way that the encryption keys were generated was insecure.

2. What symmetric encryption algorithm does WPA2 use? **1 / 1 point**

- ( ) RSA
- ( ) DES
- ( ) DSA
- (•) AES

Correct
Great work! WPA2 uses CCMP. This utilizes AES in counter mode, which turns a block cipher into a stream cipher.

3. How can you reduce the likelihood of WPS brute-force attacks? Check all that apply. **1 / 1 point**

- [ ] Update firewall rules.
- [x] Disable WPS.

Correct
Exactly! Ideally, you should disable WPS entirely if you can. If you need to use it, then you should use a lockout period to block connection attempts after a number of incorrect ones.

- [x] Implement lockout periods for incorrect attempts.

Correct
Exactly! Ideally, you should disable WPS entirely if you can. If you need to use it, then you should use a lockout period to block connection attempts after a number of incorrect ones.

- [ ] Use a very long and complex passphrase.

4. Select the most secure WiFi security configuration from below: **1 / 1 point**

- ( ) WEP 128 bit
- (•) WPA2 enterprise
- ( ) WPA2 personal
- ( ) WPA enterprise
- ( ) None
- ( ) WPA personal

Correct
Exactly right! WPA2 Enterprise would offer the highest level of security for a WiFi network. It offers the best encryption options for protecting data from eavesdropping third parties, and does not suffer from the manageability or authentication issues that WPA2 Personal has with a shared key mechanism. WPA2 Enterprise used with TLS certificates for authentication is one of the best solutions available.