Describe IV (Initialization Vector) attacks on WEP encryption. How do these attacks exploit the weaknesses in WEP's encryption process, and what are the consequences for security?

Answer: During an IV attack on WEP encryption, the IV is combined with the secret key to encrypt data that's about to be transmitted. This would allow a threat actor/ attacker to be able to decrypt any encrypted information over the network.

Discuss the use of Advanced Encryption Standard (AES) in WPA2 encryption. How does AES improve security, and why is it considered stronger than TKIP?

Answer: The good thing about AES is that it provides more security because it uses a key size of up to 256 bits. The larger the size of the key, the more security it provides, as it is hard for intruders to break long keys. AES provides factor authentication and verification keys, which enhance the data security.

Describe the security enhancements introduced in WPA3. How does WPA3 address previous vulnerabilities, and what features make it a more robust option for Wi-Fi security?

Answer: The AES-GCM encryption algorithm used in WPA3 provides enhanced security by combining encryption and authentication, ensuring the integrity and confidentiality of Wi-Fi communications. It offers a higher level of encryption strength and protection against unauthorized access and interception of data.