Encryption Scheme against Eavesdropping Adversary

1. This encryption scheme involves two parties: the sender (Alice) and the receiver (Bob). Alice wants to send a message to Bob securely.
2. Alice and Bob agree on a **secret key** that will be used to encrypt and decrypt messages. This key should be kept secret from any potential eavesdropper.
3. Alice encrypts the message using the secret key. The ciphertext is then sent over an insecure communication channel.
4. An eavesdropping adversary (Eve) intercepts the ciphertext and tries to decrypt it without knowing the secret key.
5. Because the encryption scheme is secure, Eve is unable to decrypt the message without the secret key. This is because the encryption algorithm is designed in such a way that it is mathematically difficult to reverse the encryption process without the key.
6. Even if Eve is able to intercept multiple ciphertexts, she cannot learn anything about the secret key or the plaintext message from them. This is because the encryption scheme is designed in such a way that each ciphertext is unique and provides no information about the underlying plaintext or key.
7. Bob receives the ciphertext and decrypts it using the secret key that he and Alice previously agreed upon. Because he has the secret key, he is able to recover the original plaintext message.
8. Therefore, **the encryption scheme is secure against an eavesdropping adversary**. As long as the secret key is kept secret, an eavesdropper cannot learn anything about the plaintext message from the ciphertext.