Network Security HW 18

<!-- pagebreak -->

Network Security HW 18

David Ayeke April 10. 2017

1. The STA should send a nonce as well.
2. The ciphertext is sent in plaintext. The attacker now has both the challenge and the response.
3. Once a challenge and response are recorded in play text, we can xor the two to get the key stream. We can use keystream and iv to encrypt any subsequent challenges