Bezpieczeństwo protokołów sieciowych, ćwiczenie 1

Maciej Grześkowiak

22 października 2020

Zobowiązanie bitowe

Zadanie 1: (10pkt)

1. Zaimplementuj protokół zobowiązania bitowego.
2. Protokół powinien działać w sieci (między dwoma urządzeniami).
3. Wykorzystaj bibliotekę `openssl`.
4. Termin realizacji 4 listopada 2020 roku.

Zobowiązanie bitowe

ALICE: Podejmuje decyzję, etap 1

1. wybiera losowo swój bit b
2. wybiera losowo ciągi A i B
3. oblicza $H(ABb) = Y$
4. wysyła ciagi A i Y do Boba

Zobowiązanie bitowe

ALICE: Odkrywa decyzję, etap 2

1. wysyła ciągi A, B i b do Boba

Zobowiązanie bitowe

BOB: Sprawdza zobowiązanie Alice, etap 3

1. porównuje otrzymane ciągi A
2. oblicza $H(ABb)$ i porównuje z Y
3. jeśli powyższe ciągi są równe, to uznaje bit b Alice