Cezary Troska
Systemy Rozproszone
Uniwersytet Wrocławski

20 czerwca 2021

Zadanie 5

Dlaczego na rys. 9.9 (plansza 58) nie jest konieczne, aby centrum rozprowadzania kluczy (KDC) miało pewność, że rozmawia z Ają, kiedy otrzymuje ono zamówienie na klucz tajny, który Aja będzie użytkować wspólnie z Benkiem?

Otrzymany klucz do komunikacji między Ają i Benkiem będzie zaszyfrowany za pomocą odpowiednich kluczy publicznych. Oznacza to, że przekazanie klucza przeznaczonego dla Aji komuś, kto nie jest Ają nie stwarza zagrożenia, ponieważ ta osoba nie będzie w stanie go odczytać bez klucza prywatnego Aji.

Zadanie 9

Wymyśl prosty protokół uwierzytelniania, używający podpisów w kryptosystemie z kluczem jawnym.

Na potrzeby prezentacji protokołu załóżmy, że Benek chce się uwierzetelnić przed Ają. Aby to zrobić, bierze jej klucz jawny, podpisuje go za pomocą swojego klucza prywatnego i wysyła. Aja otrzymuje wiadomość i stara się ją odczytać za pomocą znanych kluczy publicznych. Każdy wynik próby odczytania zestawia ze swoim kulczem publicznym. Gdy porównywane wartości będą się zgadzać, Aja wie, że ma do czynienia z właścicielem klucza publicznego, jakiego użyła do odszyfrowania wiadomości. Oznacza to, że Benek będzie poprawnie rozpoznany, jeśli Aja znała jego klucz publiczny.