Bezpieczeństwo protokołów sieciowych, ćwiczenia 4

Maciej Grześkowiak

26 listopada 2020

Zadanie nr 3, 20 pkt.

ALICE

1. Alice generuje klucz tajny k_A i klucz publiczny K_A do algorytmu RSA,
2. Alice generuje klucz tajny k'_A i klucz publiczny K'_A do algorytmu DSA,
3. Alice podpisuje K_A kluczem k'_A algorytmem DSA

$$s = DSA_{k'_A}(K_A)$$

4. Alice wysyła $[K'_A, K_A, s]$ do Boba

Zadanie nr 3, 20 pkt.

BOB

1. Bob weryfikuje $[K_A, s]$ kluczem K'_A,
2. Bob ustala M,
3. Bob oblicza $RSA_{K_A}(M) = C$,
4. Bob wysyła C do Alice.

Zadanie nr 3, 20 pkt.

ALICE

1. Alice oblicza $RSA_{k_A}(C) = M$,