Bezpieczeństwo protokołów sieciowych, ćwiczenia 3

Maciej Grześkowiak

5 listopada 2020

Symetryczny protokół szyfrownia

Alice i Bob

1. Alice i Bob ustalają (E, D), dwa szyfry do wyboru,
2. Alice i Bob ustalają wspólny sekret S za pomocą protokołu Diffiego-Hellmana,
3. Alice i Bob generują klucz tajny K z sekretu S
4. Alice ustala M, plik z dysku,
5. Alice oblicza $E_K(M) = C$,
6. Alice wysyła C do Boba
7. Bob oblicza $M = D_K(C)$

Protokół Diffiego Hellmana

Alice i Bob

1. Alice generuje liczbę pierwszą p, $g < p$ oraz $x_A < p$,
2. Alice oblicza $y_A = g^{x_A} \pmod{p}$,
3. Alice wysyła do Boba (p, g, y_A)
4. Bob losuje $x_B < p$
5. Bob oblicza $y_B = g^{x_B} \pmod{p}$
6. Bob wysyła do Alice y_B
7. Alice oblicza $S = y_B^{x_A} \pmod{p}$
8. Bob oblicza $S = y_A^{x_B} \pmod{p}$