Bezpieczeństwo protokołów sieciowych, ćwiczenia 5

Maciej Grześkowiak

14 stycznia 2021

Algorytm podpisu RSA, Generowanie kluczy

ALICE

1. Losuje liczby pierwsze p, q, $p \neq q$,
2. Oblicza $n = pq$ oraz $\varphi(n) = (p-1)(q-1)$,
3. Losuje $e < \varphi(n)$, $(e, \varphi(n)) = 1$,
4. Oblicza d takie, że $ed = 1 \pmod{\varphi(n)}$,
5. Ustala $K_A = (n, e)$ klucz publiczny do weryfikacji
6. Ustala $k_A = (n, d)$ klucz tajny do podpisu,

Algorytm podpisu RSA, Podpisywanie

Dane $k_A = (n, d)$ - klucz tajny, H - funkcja hashująca.

ALICE

1. Ustala M,
2. Oblicza $h = H(M)$,
3. Oblicza $s = h^d \pmod{n}$,
4. Podpis Alice pod M, to s,
5. Wysyła M, s do Boba.

Algorytm podpisu RSA, Weryfikacja

BOB $K_A = (n, e)$ - klucz publiczny, M, s, H - funkcja hashująca.

BOB

1. Oblicza $h' = H(M)$,
2. Oblicza $h = s^e \pmod{n}$
3. Bob akceptuje podpis jeśli $h = h'$.

Algorytm ślepego podpisu RSA

BOB $K_B = (n, e)$ - klucz publiczny,
$k_B = (n, d)$ klucz tajny do podpisu,
H - funkcja hashująca.

BOB

1. Wysyła $K_B = (n, e)$ do Alice

Algorytm ślepego podpisu RSA

ALICE M - wiadoność
H - funkcja hashująca.

ALICE

2. Odbiera $K_B = (n, e)$ od Boba
3. Losuje k, $(k, n) = 1$,
4. Oblicza $h = H(M)$,
5. Zakrywa h, tzn. oblicza $y = hk^e \pmod{n}$,
6. Wysyła y do Boba,

Algorytm ślepego podpisu RSA

BOB $K_B = (n, e)$ - klucz publiczny,
$k_B = (n, d)$ klucz tajny do podpisu,
H - funkcja hashująca.

BOB

7. Odbiera y od Alice,
8. Ślepo podpisuje y, tzn. oblicza $z = y^d \pmod{n}$
9. Wysyła z do Alice.

Algorytm ślepego podpisu RSA

ALICE M - wiadoność
H - funkcja hashująca.

ALICE

10. Odbiera z od Boba,
11. Odkrywa podpis Boba, tzn. oblicza $s = zk^{-1} \pmod{n}$,
12. Weryfikuje podpis $[M, s]$,
13. Jeśli weryfikacja jest poprawna, to s jest ślepym podpisem Boba pod M.

ad 2-6, Algorytm ślepego podpisu RSA

ALICE M - wiadoność
H - funkcja hashująca.

ALICE

2. Przygotowuje M_i, $i = 1, \ldots, 100$
3. Losuje k_i, $(k_i, n) = 1$, $i = 1, \ldots, 100$
4. Oblicza $h_i = H(M_i)$, $i = 1, \ldots, 100$
5. Zakrywa h_i, tzn. oblicza $y_i = h_i k_i^e \pmod{n}$,
6. Wysyła y_i do Boba, $i = 1, \ldots, 100$

Algorytm ślepego podpisu RSA

BOB $K_A = (n, e)$ - klucz publiczny,
$k_A = (n, d)$ klucz tajny do podpisu,
H - funkcja hashująca.

BOB

6.1. Odbiera y_i od Alice, $i = 1, \ldots, 100$

6.2. Losuje $j \in \{1, 2, \ldots, 100\}$

6.3. Wysyła j do Alice

ad 2-6, Algorytm ślepego podpisu RSA

ALICE M - wiadoność
H - funkcja hashująca.

ALICE

6.4. Odbiera j

6.5. Wysyła M_i, k_i, $i = 1, \ldots, 100$, $i \neq j$ do Boba

Algorytm ślepego podpisu RSA

BOB $K_A = (n, e)$ - klucz publiczny,
$k_A = (n, d)$ klucz tajny do podpisu,
H - funkcja hashująca.

BOB

6.6. Odbiera M_i, k_i, od Alice, $i = 1, \ldots, 100$,

6.7. Oblicza $h'_i = H(M_i)$, $i = 1, \ldots, 100$, $i \neq j$,

6.8. Oblicza $h_i = y_i(k_i^e)^{-1} \pmod{n}$, $i = 1, \ldots, 100$, $i \neq j$,

6.9. Jeśli $h'_i = h_i$, $i = 1, \ldots, 100$, $i \neq j$, to Bob przechodzi do kroku 8 z $y = y_j$,