Lista Nr 03, ćwiczenia

(wyk. 22,23.X.08r)

Kryptografia z kluczem publicznym RSA

1. Opis ogólny:

- **(a)** A i B to dwie strony, które chcą do siebie przesyłać wiadomości;
- **(b)** Każda strona ma klucz publiczny (e_A, n_A), (e_B, n_B) znany wszystkim użytkownikom i klucz sekretny (d_A, n_A), (d_B, n_B) znany tylko im;
- **(c)** $\mathcal{D} = Z_n$ jest zbiorem dozwolonych wiadomości;
- **(d)** Klucze definiują funkcje: $P_A, P_B, S_A, S_B : \mathcal{D} \longrightarrow \mathcal{D}$ takie, że P_A jest odwrotna do S_A i P_B jest odwrotna do S_A, tzn. $M = P_A S_A(M) = S_A P_A(M)$ i $M = P_B S_B(M) = S_B P_B(M)$ dla $M \in \mathcal{D}$.

2. Tworzenie klucza publicznego (e, n) i klucza sekretnego (d, n):

- **(a)** Wybieramy dwie duże liczby pierwsze p i q.
- **(b)** Obliczamy $n = pq$ i $\phi(n) = (p-1)(q-1)$.
- **(c)** Wybieramy niedużą liczbę nieparzystą e względnie pierwszą z $\phi(n)$.
- **(d)** Obliczamy liczbę $d < n$ taką, że

$$ed =_{\phi(n)} 1.$$

- **(e)** Publikujemy parę (e, n) jako klucz publiczny.
- **(f)** Trzymamy w sekrecie parę (d, n) jako klucz sekretny.

3. Kodowanie i dekodowanie:

- **(a)** $\mathcal{D} = Z_n = \{0, 1, 2, \ldots, n-1\}$ jest zbiorem dopuszczalnych wiadomości.
- **(b)** Kodowanie dla $M \in \mathcal{D}$ jest określone następująco:

$$P(M) = M^e \bmod n.$$

- **(c)** Dekodowanie dla $M \in \mathcal{D}$ jest określone następująco:

$$S(M) = M^d \bmod n.$$

Zad. 1 Uzasadnić (pkt. 2d), istnienie jedynej liczby d spełniającej $ed =_{\phi(n)} 1$.

Zad. 2 Dlaczego ze znajomości rozkładu $n = pq$, gdzie p, q – liczby pierwsze, łatwo można wyznaczyć liczbę sekretną d.

Zad. 3 Sprawdzić poprawność przedstawionego protokołu RSA, tzn. że dla $M \in Z_n$ zachodzi $PS(M) = SP(M) = M$.

Komentarz:

Fakty przedstawione na listach ćwiczeniowych Nr 01 – 03 są ogólnie znane, tym niemniej należy zaznaczyć, że przy opracowaniu wymienionych list korzystałem z materiałow do wykładu J. Cichonia [1] oraz M. Zawadowskiego [2].

Literatura

[1] J. Cichoń, Wstęp do informatyki (wersja robocza), 15.IX.08r: skrypt dostępny jest na stronie WWW autora, 2005,

WPPT Politechniki Wrocławskiej.

[2] M. Zawadowski, Wykład ze wstępu do informatyki (rok 2007–2008), 15.IX.08r: skrypt dostępny jest na stronie WWW autora, 14.I.2008,

WMIiM Uniwersytetu Warszawskiego.

Wrocław, dnia 21/10/2008