3.03.03

BDC- Infrastruktura Klucza Publicznego, 2003
WPPT, Politechnika Wrocławska

Lista nr 2

1. RSA-reprezentacje są definiowane nieco podobnie do reprezentacji DL: ustalamy $n = pq$, liczbę v względnie pierwszą z $\varphi(n)$, oraz $g_1, \ldots, g_l$. Mówimy, że h ma reprezentację $x_1, \ldots, x_{l+1}$, gdy
$$h = \prod_{i=1}^{l} g_i^{x_i} \cdot x_{l+1}^{v} \bmod n$$
oraz $x_i < v$ dla $i \leq l$.
Pokaż, że łatwo jest znaleźć element h mający reprezentację postaci $(x_1, \ldots, x_l, -)$, natomiast mając h' nie jest możliwe znalezienie jego reprezentacji bez złamania RSA.

2. - Pokazać, że z dwu RSA-reprezentacji tego samego h można obliczyć RSA-reprezentację dla 1.

   - Pokazać, że jeśli Alicja może dostać od Boba RSA-reprezentacje 1 dla podanych mu $g_1, \ldots, g_l$, to odpowiednio postępując może deszyfrować kryptogramy zbudowane przy pomocy klucza publicznego v (liczba v, zgodnie z oznaczeniami jest używana do budowania RSA-reprezentacji).

   Wskazówka: Alicja definiuje $g_i = h^{r_i} s_i^v$ dla $i = 1, \ldots l$, z algorytmu Euklidesa oblicza e, f takie, że $(e \sum r_i x_i) + fv = 1$, a następnie oblicza $h^f (x_{l+1} \prod s_i^{x_i})^{-e}$.
   Jakie praktyczne wnioslu płyną z rozwiązania tego zadania?

3. Istnienie klucza prywatnego odpowiadającego v w przypadku RSA-reprezentacji może potencjalnie nieść zagrożenia dla certyfikatów klucza prywatnego (w przypadku systemu opartego na dyskretnym logarytmie takiej „zapadki“ nie ma). Zbadać, czy takowe niebezpieczeństwa istotnie mogą się pojawić.

4. Porównać złożoność obliczeniową utworzenia liczby wraz z DL-reprezentacja i liczby z RSA-reprezentacją. W którym wypadku da się zmniejszyć koszt obliczeń bez kompromisu pod względem bezpieczeństwa?

5. Zaprojektuj protokół, w którym Alicja dowodzi Bobowi, że zna RSA-reprezentację liczby h bez zdradzania informacji o tej reprezentacji. (w istocie chodzi o dowód z wiedzą zerową, ale trzeba formalnie dowodzić tej własności dla zaprojektowanego rozwiązania).

/-/ Mirosław Kutyłowski