Lista zadań. Nr 7. 17 kwietnia 2005

Kryptografia

IIUWr.

1. (2pkt) Przyjmijmy, że Bob, używając schematu ElGamala podpisuje dwie wiadomoœci x_1 i x_2 podpisami (γ, δ_1) i (γ, δ_2), odpowiednio. (w obu podpisach powtarza się wartość γ). Załóżmy także, że $NWD((\delta_1 - \delta_2, p-1) = 1$.
   - Opisz, jak można efektywnie obliczyć k na podstawie przedstawionej wyżej informacji.
   - Opisz, jak można w tej sytuacji złamać schemat podpisu.
   - Niech $p = 31847$, $g = 5$ i $\beta = 25703$. Oblicz k i a, wiedząc, że podpis $(23972, 31396)$ złożono pod wiadomością $x = 8990$, a podpis $(23972, 20481)$ - pod wiadomością $x = 31415$.

2. (2pkt) Załóżmy, że Ewa dysponuje wykonanym przez Boba (według schematu ElGamala) podpisem $\gamma, \delta)$ pod wiadomością x. Wykaż, że następująca procedura pozwala Ewie podpisać kolejne wiadomości.

   Niech $0 \le h, i, j \le p-2$ oraz $NWD(h\gamma - j\delta, p-1) = 1$. Oblicz

   $$\lambda = \gamma^h g^i \beta^j \bmod p$$

   $$\mu = \delta\lambda(h\gamma - j\delta)^{-1} \bmod (p-1)$$

   $$x' = \lambda(hx + i\delta)(h\gamma - j\delta)^{-1} \bmod (p-1)$$

   Obliczenia $(h\gamma - j\delta)^{-1}$ są wykonywane mod $(p-1)$. Podpisem pd x' jest para (λ, μ).

3. (1pkt) Załóżmy, że Bob stosuje schemat podpisu ElGamala przy $p = 467$, $g = 2$ oraz $\beta = 132$. Przypuśćmy, że do wiadomości $x = 100$ dołączył podpis $(29, 51)$. Oblicz fałszywy podpis, który może wygenerowac Ewa, przyjmując $h = 102$, $i = 45$ oraz $j = 293$.

4. (2pkt) Rozważmy wariant schematu podpisów ElGamala, różniący się od oryginalnego sposobem obliczania δ. Teraz

   $$\delta = (x - k\gamma)a^{-1} \bmod (p-1).$$

   - Opisz, jak można teraz weryfikować podpis (γ, δ) pod wiadomością x używając publicznego klucza Boba.
   - Omów przewagę obliczeniową schematu zmodyfikowanego nad oryginalnym.
   - Porównaj krótko bezpieczeństwo obu schematów.

5. (2pkt) Udowodnij poprawność schematu DSS.

6. (1pkt) Wyznacz podpis pod wiadomością $x = 52$ wykonany według schematu DSS z wartościami $q = 101$, $p = 7879$, $g = 170$ $a = 75$, $\beta = 4567$ oraz $k = 49$. Prześledź weryfikację tego podpisu.