Lista zadań. Nr 8. 24 kwietnia 2005

Kryptografia

IIUWr.

1. (1pkt) Załóżmy, że Bob podpisał dwie k-bitowe wiadomości używając:
   - schematu Lamporta,
   - schematu Bosa-Chauma.

   Ile nowych wiadomości może podpisać teraz Ewa, która zna obydwa podpisy?

2. (1pkt) Jak wiadomo, algorytm RSA jest wykorzystywany zarówno w schemacie szyfrowania wiadomości, jak i podpisu. Zaproponuj schemat podpisu oparty na metodzie używanej w schemacie szyfrowania Rabina. Co możesz powiedzieć o bezpieczeństwie tego schematu?

3. Przypuśćmy, że Bob stosuje schemat podpisu niezaprzeczalnego Chauma-van Antwerpena z wartościami $p = 467$, $\alpha = 4$, $a = 101$ oraz $\beta = 449$. Załóżmy, że dociera do niego wiadomość $x = 157$ z podpisem $y = 25$ i chce on wykazać, że podpis jest sfałszowany. Niech wybranymi przez Alicję liczbami losowymi do protokołu wyrzeczenia będą $e_1 = 46$, $e_2 = 123$, $f_1 = 198$ i $f_2 = 11$. Oblicz pytania Alicji, c i d, oraz odpowiedzi Boba, C i D, i wykaż, że sprawdzian zgodności przeprowadzony przez Alicję zakończy się powodzeniem.

4. Schemat podpisów niepodrabialnych (autorstwa van Heysta i Petersena) wymaga trzech stron: centralnego autorytetu (CA), podpisującego Boba i weryfikującej Alicji.
   - CA wybiera:
     - p i q liczby pierwsze takie, że $p = 2q + 1$ i DLOG jest trudny w Z_p^*;
     - $\alpha \in Z_p^*$ - element rzędu q;
     - $a_0 \in \langle 1, q-1 \rangle$ i oblicza $\beta = \alpha^{a_0}$.

     Wartości p, q, α i β są publiczne i stałe. Wartość a_0 pozostaje tajna.
   - ustalając swój klucz $K = \langle \gamma_1, \gamma_2, a_1, a_2, b_1, b_2 \rangle$, Bob:
     - losuje wartości $a_1, a_2, b_1, b_2 \in Z_q$
     - oblicza $\gamma_i = \alpha^{a_i} \beta^{b_i}$ dla $i = 1, 2$.

     Wartości a_1, a_2, b_1, b_2 pozostają prywatne, z γ_1 i γ_2 - publiczne.
   - Podpisując wiadomość $x \in Z_q$, Bob oblicza $sig_K(x) = \langle y_1, y_2 \rangle$, gdzie $y_i = a_i + xb_i \bmod q$, dla $i = 1, 2$.
   - Weryfikując podpis $y = \langle y_1, y_2 \rangle$ pod wiadomością x, Alicja sprawdza, czy

   $$\gamma_1 \gamma_1^x \equiv \alpha^{y_1} \beta^{y_2} (\bmod p)$$

   (a) Sprawdź, że procedura weryfikacji jest poprawna.

   (b) Uzasadnij stwierdzenie, że schemat van Heysta-Petersena jest schematem podpisów jednokrotnych

5. Mówimy, że dwa klucze $K = \langle \gamma_1, \gamma_2, a_1, a_2, b_1, b_2 \rangle$ i $K = \langle \gamma_1', \gamma_2', a_1', a_2', b_1', b_2' \rangle$ są *równoważne*, jeśli $\gamma_1 = \gamma_1'$ i $\gamma_2 = \gamma_2'$.

   (a) Pokaż, że dla dowolnego klucza K, klasa abstrakcji kluczy równoważnych z K liczy q^2 elementów.

(b) Pokaż, że dla dwóch równoważnych kluczy K i K' oraz dowolnej pary $\langle x, y\rangle$:

$$sig_K(x, y) \Leftrightarrow sig_{K'}(x, y).$$

(c) Niech K będzie kluczem i $y = sig_K(x)$. Pokaż, że istnieje dokładnie q kluczy K' równoważnych kluczowi K, takich, że $y = sig_{K'}(x)$.

(d) Niech K będzie kluczem i $y = sig_K(x)$ oraz $ver_K(x', y') =' \text{TAK}'$. Pokaż, że istnieje co najwyżej jeden klucz K' równoważny kluczowi K, taki, że $y = sig_{K'}(x)$ i $y' = sig_{K'}(x')$.

6. Udowodnij, że Bob, dysponując parą $\langle x, y\rangle$, taką, że

- $\langle x, y\rangle$ przechodzi weryfikację z kluczem Boba K,
- y nie został utworzony z x za pomocą klucza K, tj. $y \neq sig_K(x)$,

potrafi obliczyć a_0.

7. Rozważmy schemat podpisu niepodrabialnego van Heysta-Petersena z wartościami $p = 3467$, $\alpha = 4$, $a_0 = 1567$ oraz $\beta = 514$.

- Wyznacz wszystkie klucze $K = \langle\gamma_1, \gamma_2, a_1, a_2, b_1, b_2\rangle$, dla których $sig_K(42) = \langle 1118, 1449\rangle$.
- Przypuścmy, że $sig_K(42) = \langle 1118, 1449\rangle$ oraz $sig_K(969) = \langle 899, 471\rangle$. Nie używając wartości a_0 wyznacz wartość K.

8. Przypuśćmy, że Bob stosuje schemat podpisu niepodrabialnego van Heysta-Petersena z wartościami $p = 5087$, $\alpha = 25$ oraz $\beta = 1866$. Niech jego kluczem będzie

$$K = \langle 5065, 5076, 144, 874, 1873, 2345\rangle.$$

Przypuśćmy , że Bob stwierdził fałszywość podpisu $\langle 2219, 458\rangle$ pod wiadomością 4785.

(a) Pokaż, że sfałszowany podpis spełnia warunek weryfikacji, a więc jest ważnym podpisem.

(b) Opisz, w jaki sposób na podstawie tego podpisu Bob obliczy dowód fałszerstwa.