Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni **III-A Appello d'Esame 2012-13 – 13 settembre 2013**

Cognome e nome: *(stampatello)*
(firma leggibile)

Matricola:

NB: In ogni esercizio, ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo.

Domanda 1

(svolgere su questo foglio nello spazio assegnato) (7 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 113$, $\alpha = 6$, $\beta = \alpha^a \bmod p = 31$, tenendo segreto l'esponente a ($1 < a \leq p\text{-}2$).

a) Bob estrae il numero casuale segreto k (*nonce*) ($k \perp p\text{-}1$). Usando sempre questo stesso valore di k, Bob calcola le seguenti firme A_k per i rispettivi messaggi P_k:

$A_1 = (r_1, s_1) = (92, 4)$ $P_1 = 12$
$A_2 = (r_2, s_2) = (92, 44)$ $P_2 = 100$
$A_3 = (r_3, s_3) = (92, 12)$ $P_3 = 35$

Verificare che le tre firme siano valide.

VER: $\beta^r r^s \equiv \alpha^P \pmod p$

A_1 | $31^{92} \cdot 92^4 \bmod 113 = 56$; $6^{72} \bmod 113 = 56$ } $\Rightarrow A_1$ OK

A_2 | $31^{92} \, 92^{44} \bmod 113 \equiv 111$; $6^{100} \bmod 113 \equiv 111$ } $\Rightarrow A_2$ OK

A_3 | $31^{92} \, 92^{12} \bmod 113 = 81$; $6^{35} \bmod 113 = 40$ } $\Rightarrow A_3$ NO

b) Oscar intercetta i tre messaggi (P_k, A_k). Sulla base delle sole firme verificate valide, calcolare k e a (*attacco del nonce ripetuto*).

$s = k^{-1}(P - ar) \bmod (p-1) \rightarrow sk \equiv P - ar \pmod{p-1}$

$$\begin{cases} 4 \cdot k \equiv 12 - 4a \pmod{112} \\ 44 \cdot k \equiv 100 - 4a \pmod{112} \end{cases}$$

$40k \equiv 88 \pmod{112}$ $\quad \gcd(40, 112) = 8 \rightarrow$ 8 soluzioni

$5k \equiv 11 \pmod{14}$ $\quad 5^{-1} \bmod 14 = 5^5 \bmod 14 = 3$

$k_0 = 11 \cdot 3 \bmod 14 = 5$

$k_i = k_0 + 14i \bmod 112 \quad (i = 0, 1, \dots 7)$

$= 5, 19, 33, 47, 61, 75, 89, 103$

Dai dati pubblici: $r = \alpha^k \bmod p \rightarrow 6^k \bmod 113 = 92$

$\Rightarrow \boxed{k = 5}$

$4 \cdot 5 \equiv 12 - 92 \pmod{172}$

$92 \equiv 104 \pmod{172}$ $\quad mcd(92, 172) = 4 \Rightarrow$ 4 soluzioni

$92_3 \equiv 26 \pmod{28}$ $\quad 23^{-1} \bmod 28 = 23^{11} \bmod 28 = 11$

$a_0 = 26 \cdot 11 \bmod 28 = 6$

$a_i = a_0 + 28i \bmod 172 \quad (i = 0,1,2,3)$

$= 6, 34, 62, 90$

Dai dati pubblici:

$\beta = \alpha^a \bmod p \quad 6^a \bmod 173 = 37 \Rightarrow \boxed{a = 90}$

Domanda 2

(svolgere su questo foglio nello spazio assegnato) (6 punti)

Si consideri l'algoritmo di cifratura di Hill definito come

$$\mathbf{C}_i = \mathbf{P}_i \cdot \mathbf{K} + \mathbf{B} \mod 128$$

dove:

$\mathbf{C}_i$ = coppia i-esima di caratteri cifrati $[C_{1i}\ C_{2i}]$;
$\mathbf{P}_i$ = coppia i-esima di caratteri in chiaro $[P_{1i}\ P_{2i}]$;
$\mathbf{K}$, $\mathbf{B}$ = chiave di cifratura, con

$$\mathbf{K} = \begin{bmatrix} 1 & 10 \\ 20 & 101 \end{bmatrix} \qquad \mathbf{B} = [10 \quad 20].$$

a) Verificare che la chiave sia valida.

b) Decifrare il messaggio $\mathbf{C} = [1\ \ 2]$.

a) $\det(K) = 101 - 200 \mod 128 = 29 \quad \perp 128 \quad OK \ (\exists K^{-1})$

b) $P = (C - B) K^{-1}$

$$K^{-1} \equiv \frac{1}{29} \begin{pmatrix} 101 & -10 \\ -20 & 1 \end{pmatrix} \equiv \begin{pmatrix} 105 & 110 \\ 92 & 53 \end{pmatrix} \pmod{128}$$

$$29^{-1} \bmod 128 = 29^{63} \bmod 128 = 53$$

$$P = (1-10 \quad 2-20) \begin{pmatrix} 105 & 110 \\ 92 & 53 \end{pmatrix} \equiv (119 \quad 110) \begin{pmatrix} 105 & 110 \\ 92 & 53 \end{pmatrix} \equiv (87 \quad 104) \pmod{128}$$

Verifica: $PK + B = (87 \quad 104) \begin{pmatrix} 1 & 10 \\ 10 & 101 \end{pmatrix} + (10 \quad 20) = (1 \quad 2) \quad OK$

$= C$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **III-A Appello d'Esame 2012-13 – 13 settembre 2013**

Cognome e nome: *(stampatello)* *(firma leggibile)*

Matricola:

Domanda 3

(svolgere su questo foglio nello spazio assegnato) (6 punti)

La *Trusted Authority* TA adotta lo *Schema di Blom* per distribuire chiavi simmetriche a tre utenti A, B e C e pubblica $p = 997$. Gli identificativi pubblici dei tre utenti sono rispettivamente $r_A = 111$, $r_B = 222$, $r_C = 333$.

a) Per i tre utenti, TA sceglie e tiene segreti $a = 501$, $b = 955$, $c = 370$. Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$a_A = a + b r_A \bmod p = 824$ $\quad a_B = a + b r_B \bmod p = 150$ $\quad a_C = a + b r_C \bmod p = 473$

$b_A = b + c r_A \bmod p = 151$ $\quad b_B = b + c r_B \bmod p = 344$ $\quad b_C = b + c r_C \bmod p = 537$

$g_A(x) = a_A + b_A x$ $\quad K_{AB} = g_A(r_B) = 448$

$g_B(x) = a_B + b_B x$ $\quad K_{AC} = g_A(r_C) = 260$

$g_C(x) = a_C + b_C x$ $\quad K_{BC} = g_B(r_C) = 47$

b) Per i tre utenti, TA sceglie e tiene segreti a, b, c. Gli utenti A e B si accordano e si scambiano le informazioni $a_A = 271$, $b_A = 117$, $a_B = 419$, $b_B = 565$.
- Calcolare i parametri segreti a, b, c.
- Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$$a_A = \begin{cases} a + b\,111 \bmod 997 = 271 \rightarrow b \equiv 666 \pmod{997} \\ a_B = a + b\,222 \bmod 997 = 419 \nearrow a \equiv 123 \pmod{997} \\ b_A = b + c\,111 \bmod 997 = 117 \quad c \equiv 22 \pmod{997} \end{cases}$$

$$b = 111^{-1} \cdot 148 \bmod 997 = 503 \cdot 148 \bmod 997 = 666$$

$$a = 419 - 666 \cdot 222 \bmod 997 = 123$$

$$c = (117 - 666)\,111^{-1} \bmod 997 = 22$$

$$111^{-1} \bmod 997 = 503$$

$$K_{AB} = 323$$

$$K_{AC} = 349$$

$$K_{BC} = 131$$

Cognome e nome: *(stampatello)*
(firma leggibile)

Matricola:

Domanda 4

(svolgere su questo foglio nello spazio assegnato) (6 punti)

Si presentino protocolli di *distribuzione di chiave simmetrica*, con e senza *autenticazione*. In particolare:

a) precisare che differenza c'è tra *symmetric key agreement* e *symmetric key distribution*;

b) citare (senza dettagliare) un esempio di protocollo di *distribuzione di chiave simmetrica senza autenticazione*;

c) citare (senza dettagliare) due esempi di protocolli di *distribuzione di chiave simmetrica con autenticazione*, precisando come viene risolto il problema di impedire i *replay attack*;

d) descrivere il protocollo di *Needham-Schroeder*, nella versione con utilizzo di chiave simmetrica verso la TA.

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (11 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) In un *firewall*, spiegare in cosa consistono e per cosa si differenziano *rule set* basati su *default policy* di tipo *deny-all* e di tipo *allow-all*. *(3 punti)*

2) Definire le proprietà *fortemente resistente alle collisioni* e *debolmente resistente alle collisioni* di una funzione di hash. *(3 punti)*

Cognome e nome: *(stampatello)*
(firma leggibile)

Matricola:

3) In una infrastruttura a chiave pubblica (PKI), in che modo una *Certification Authority* certifica l'identità di un soggetto? Quali sono le tre informazioni chiave contenute in un certificato di identità? *(3 punti)*

4) Calcolare 1/500 mod 977 per mezzo dell'Algoritmo di Euclide Esteso. *(2 punti)*

$977 = 1 \cdot 500 + 477$ $\quad x_0 = 0 \quad x_1 = 1$ $\quad \Rightarrow 500^{-1} \bmod 977 = 170$

$500 = 1 \cdot 477 + 23$ $\quad x_2 = -1$

$477 = 20 \cdot 23 + 17$ $\quad x_3 = 2$ $\quad 170 \cdot 500 \bmod 977 = 1$

$23 = 1 \cdot 17 + 6$ $\quad x_4 = -41$

$17 = 2 \cdot 6 + 5$ $\quad x_5 = 43$

$6 = 1 \cdot 5 + 1$ $\quad x_6 = -127$

$5 = 5 \cdot 1 + 0$ $\quad x_7 = 170$