Sicurezza delle Reti

Prof. Stefano Bregni — **I Appello d'Esame 2016-17 – 27 giugno 2017**

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) (6 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 149$, $\alpha = 8$, $\beta = \alpha^a \bmod p = 37$, 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:

$A_1 = (r_1, s_1) = (84, 124)$ $\quad P_1 = 20$
$A_2 = (r_2, s_2) = (84, 33)$ $\quad P_2 = 40$
$A_3 = (r_3, s_3) = (84, 88)$ $\quad P_3 = 60$

Verificare che le tre firme siano valide.

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

A_1 $\left| \begin{array}{l} 37^{84} 84^{124} \equiv 25 \\ 8^{20} \equiv 25 \end{array} \right\} \Rightarrow$ OK $\quad (\bmod 149)$

A_2 $\left| \begin{array}{l} 37^{84} 84^{33} \equiv 52 \\ 8^{40} \equiv 29 \end{array} \right\} \Rightarrow$ NO

A_3 $\left| \begin{array}{l} 37^{84} 84^{88} \equiv 129 \\ 8^{60} \equiv 129 \end{array} \right\} \Rightarrow$ OK

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*).

$P_1 = 20 \quad A_1 = (84, 124)$

$P_3 = 60 \quad A_3 = (84, 88)$

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

$$\begin{cases} 124k \equiv 20 - a84 \pmod{148} \\ 88k \equiv 60 - a84 \pmod{148} \end{cases}$$

$36k \equiv -40 \equiv 108 \pmod{148} \quad \text{mcd}(36, 148) = 4 \Rightarrow 4 \text{ soluzioni}$

$9k \equiv 27 \pmod{37} \quad 9^{-1} \equiv 33 \pmod{37}$

$\Rightarrow k_0 \equiv 27 \cdot 33 \equiv 3 \pmod{37}$

$k_i = 3, 40, 77, 110 \pmod{148}$

$\Rightarrow \boxed{k = 77}$

Dai dati pubblici: $r = \alpha^k \bmod p$

$\beta^{77} \equiv 84$ ok

$124 \cdot 77 \equiv 20 - a \cdot 84 \pmod{148}$

$a84 \equiv 92 \pmod{148} \quad \text{mcd}(84, 148) = 4 \Rightarrow 4 \text{ soluzioni}$

$a21 \equiv 23 \pmod{37} \quad 21^{-1} \equiv 30 \pmod{37}$

$\Rightarrow a_0 \equiv 23 \cdot 30 \equiv 24 \pmod{37}$

$a_i \equiv 24, 61, 98, 135$

Dai dati pubblici:

$B \equiv \alpha^a \pmod p$

$8^{24} \equiv 37 \pmod{749}$

$\Rightarrow \boxed{a = 24}$

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (5 punti)

Bob adotta il *sistema di firma elettronica RSA*. Pubblica il modulo $n = 5353$ e l'esponente di cifratura $e = 2137$.

a) Verificare la correttezza dei dati forniti in base alle ipotesi del metodo RSA.

b) Calcolare la firma di Bob A per il messaggio $m = 100$.

a) $n = 5353 = 53 \cdot 101$ (primi)

$\varphi(n) = 52 \cdot 100 = 5200 = 2^4 5^2 \cdot 13$ $\quad e \perp \varphi(n)$

$\varphi[\varphi(n)] = 1920$

b) $d = e^{-1} \bmod \varphi(n) = e^{\varphi[\varphi(n)]-1} \bmod \varphi(n) = 2137^{1919} \bmod 5200$

Meglio usare l'algoritmo di Euclide Esteso:

$5200 = 2 \cdot 2137 + 926$ $\quad X_0 = 0 \quad X_1 = 1$

$2137 = 2 \cdot 926 + 285$ $\quad X_2 = -q_1 X_1 + X_0 = -2$

$926 = 3 \cdot 285 + 71$ $\quad X_3 = -q_2 X_2 + X_1 = 5$

$285 = 4 \cdot 71 + 1$ $\quad X_4 = -q_3 X_3 + X_2 = -17$

$71 = 71 \cdot 1 + \phi$ $\quad X_5 = -q_4 X_4 + X_3 = 73$

$\Rightarrow d = 73$

Verifica: $73 \cdot 2137 \bmod 5200 = 1$

$A = m^d \bmod n = 100^{73} \bmod 5353 = 3332$

Domanda 3
(svolgere su questo foglio nello spazio assegnato) (6 punti)

Alice e Bob adottano il protocollo di *Diffie-Hellman* per l'instaurazione della loro chiave simmetrica K_{AB}. Alice pubblica $p = 163$ e inizialmente $\alpha = 4$. Alice sceglie $1 \le x \le p-2$ (segreto). Bob sceglie $1 \le y \le p-2$ (segreto).

a) Alice verifica la correttezza dei dati secondo le ipotesi di Diffie-Hellman. Nel caso $\alpha = 4$ non risulti una scelta valida, Alice si corregge e pubblica invece un valore valido scelto nell'insieme $\alpha = \{3, 4, 5, 6\}$. Se nessuna di queste scelte risultasse valida, Alice e Bob rinunceranno a proseguire (e l'esercizio termina qui).

Test $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $\quad p-1 = 162 = 2 \cdot 3^4$

$\alpha = 4$ $\left\{ 4^{81} \equiv 1 \pmod{163} \right\} \Rightarrow$ NO

$\alpha = 3$ $\left\{ \begin{array}{l} 3^{81} \equiv 162 \\ 3^{54} \equiv 58 \end{array} \right\} \Rightarrow$ OK $\Rightarrow \alpha = 3$ (unico elem. primitivo dell'insieme)

b) Oscar osserva i numeri scambiati da Alice e Bob:

Alice ➔ Bob: $\alpha^x \equiv 162 \pmod p$

Alice ← Bob: $\alpha^y \equiv 13 \pmod p$

Sulla base delle informazioni conosciute da Oscar, calcolare gli esponenti segreti x e y e la chiave K_{AB}.

$x \equiv 81 \pmod{163}$ (per tentativi o BSGS)

$y \equiv 39 \pmod{163}$ (e dal punto a))

$K_{AB} = \alpha^{xy} \bmod p = 3^{81 \cdot 39} \equiv 162 \pmod{163}$

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

Matricola:

Domanda 4
(svolgere su questo foglio nello spazio assegnato) (5 punti)

Una Trusted Authority (TA) rilascia ad Alice (A) il *certificato* $C_A = (A, K_A, \{h(A, K_A)\}_{K_{TA}^{-1}})$, ove

- cifratura e firma sono RSA con $n = 3337$;
- la chiave pubblica della TA è $K_{TA} = 57$;
- la chiave pubblica di Alice è $K_A = 2615$;
- l'identificativo di Alice è $A = 257$ (con il vincolo A primo);
- la funzione di hash $h = h(x,y)$ è definita per $h, x, y \in \mathbb{Z}_n$ come

$$h = h(x, y) = \Big(x \oplus \mathrm{SL}_3(y) \oplus \big(x^{-1} \bmod \varphi(n)\big)\Big) \bmod n$$

ove SL_k = scorrimento ciclico a sinistra di k posizioni;
x, y, h parole di b bit (determinare b come il valore minimo necessario per esprimere i valori richiesti).

a) Verificare la correttezza dei dati forniti secondo le ipotesi di RSA.

b) Calcolare il certificato C_A rilasciato da TA.

c) Verificare l'autenticità del certificato C_A.

a) $n = 3337 = 47 \cdot 71$ $\varphi(n) = 3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ $\varphi[\varphi(n)] = 1056$

$K_{TA} = 57 \perp 3220$ ok $K_A = 2615 \not\perp 3220$ No! $A = 257$ primo

$\Rightarrow \nexists K_A^{-1}$ $b = 12$

b) $K_{TA}^{-1} = 57^{-1} \bmod 3220 \equiv 113$ (con Euclide Esteso)

$A = 257 = 0001\ 0000\ 0001$

$K_A = 2615 = 1010\ 0011\ 0111$ $SL_3(K_A) = 0001\ 1011\ 1101$

$A^{-1} = 257^{-1} \bmod 3220 \equiv 213$ (con Euclide Esteso)

$= 0000\ 1101\ 0101$

$h = h(A, K_A) =$ 0001 0000 0001 ⊕ A

0001 1011 1101 ⊕ $SL_3(A)$

0000 1101 0101 A^{-1}

0000 0110 1001

$= 105$

$\{h\}_{K_{TA}^{-1}} = 105^{113} \bmod 3337 = 986$

$\Rightarrow C_A = (257, 2615, 986)$

c) Deve essere $986^{57} \equiv 105 \pmod{n}$ OK

$\{\{h\}_{K_{TA}^{-1}}\}_{K_{TA}} = h$

Sicurezza delle Reti
Prof. Stefano Bregni **I Appello d'Esame 2016-17 – 27 giugno 2017**

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

Matricola:

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (14 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) Per determinare se l'equazione $x^2 \equiv -a \pmod{p}$ ha soluzione, con $p = 2473$ primo, si calcola il simbolo di Legendre corrispondente e si ottiene $(a/p) = -1$. Cosa si conclude? L'equazione $x^2 \equiv -a \pmod{p}$ ha soluzione? E l'equazione $x^2 \equiv a \pmod{p}$? Motivare la risposta. *(2 punti)*

$x^2 \equiv a \pmod{p}$ non ha soluzione

$x^2 \equiv -a \pmod{p}$ mentre $(p \equiv 1 \pmod{4})$

2) Si considerino le funzioni di cifratura doppia $C = E_{K_2}(E_{K_1}(P))$ e sua decifratura $P = D_{K_1}(D_{K_2}(C))$, con due chiavi K_1 e K_2 ciascuna di lunghezza $n = 32$ bit, $P \in \mathbb{Z}_{256}$, $C \in \mathbb{Z}_{256}$. Si intende tentare un attacco *Meet-in-the-Middle* per trovare la coppia di chiavi K_1, K_2. *(2 punti)*

- Quali informazioni è necessario conoscere per eseguire l'attacco? L'attacco ha sempre successo?
- Si indichi con E il peso computazionale di una operazione di cifratura semplice $E_K(X)$, uguale al peso di una decifratura $D_K(X)$. Quanti calcoli sono necessari (in termini di E) per completare l'attacco con successo?
- Quale occupazione di memoria [byte] è necessaria per completare l'attacco con successo?

Numero operazioni: tra $2^{32} \cdot E$ e $2^{33} \cdot E$ $(10^9 \div 2 \cdot 10^9)$

Occupazione memoria: 1 Gbyte ÷ 2 Gbyte (+1 Byte :))

3) Descrivere sinteticamente il *Test di Primalità di Solovay-Strassen.* *(2 punti)*

4) Definire la proprietà *debolmente resistente alle collisioni* di una funzione di hash. Perché questa proprietà è più facile da soddisfare della proprietà *fortemente resistente alle collisioni*? *(2 punti)*

5) Descrivere lo *Schema di Lamport* per l'autenticazione di un host A da parte di un server B, precisando quali informazioni sono pubbliche o trasferite in chiaro, e quali altre sono private e memorizzate in A o B. *(3 punti)*

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

Matricola:

6) Trovare i fattori primi di $n = 15229$ attraverso l'*Algoritmo di Fattorizzazione p−1* di Pollard con base $a = 2$. *(3 punti)*

$b_1 \equiv 2 \pmod{15229}$

$b_2 \equiv 2^2 \equiv 4$ $\quad MCD(3, n) = 1$

$b_3 \equiv 4^3 \equiv 64$ $\quad MCD(63, n) = 1$

$b_4 \equiv 64^4 \equiv 10087$ $\quad MCD(10086, n) = 1$

$b_5 \equiv 10087^5 \equiv 11057$ $\quad MCD(11056, n) = 1$

$b_6 \equiv 11057^6 \equiv 11350$ $\quad MCD(11349, n) = 97$

$\Rightarrow p = 97$

$q = n/p = 157$