Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni **IV Appello d'Esame 2014-15 – 17 luglio 2015**

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 $p = 107$, $\alpha = 7$, $\beta = \alpha^a \bmod p = 72$, tenendo segreto l'esponente a $(1 < a \leq p\text{-}2)$.

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

$A_1 = (r_1, s_1) = (67, 58)$ $P_1 = 61$
$A_2 = (r_2, s_2) = (67, 31)$ $P_2 = 62$
$A_3 = (r_3, s_3) = (67, 100)$ $P_3 = 63$

Verificare che le tre firme siano valide.

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

A_1 $\left| \begin{array}{l} 72^{67}\ 67^{58} \equiv 38 \\ 7^{61} \equiv 38 \end{array} \right\} \Rightarrow$ OK $\pmod{107}$

A_2 $\left| \begin{array}{l} 72^{67}\ 67^{31} \equiv 105 \\ 7^{62} \equiv 52 \end{array} \right\} \Rightarrow$ NO

A_3 $\left| \begin{array}{l} 72^{67}\ 67^{100} \equiv 43 \\ 7^{63} \equiv 43 \end{array} \right\} \Rightarrow$ 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*).

$P_1 = 61 \quad A_1 = (67, 58)$

$P_3 = 63 \quad A_3 = (67, 100)$

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

$$\begin{cases} 58k \equiv 61 - 67a \pmod{106} \\ 100k \equiv 63 - 67a \pmod{106} \end{cases}$$

$42k \equiv 2 \pmod{106} \qquad \mathrm{mcd}(42, 106) = 2 \Rightarrow 2$ soluzioni

$21k \equiv 1 \pmod{53} \qquad 21^{-1} \bmod 53 = 48$

$k_0 = 48$

$k_1 = 48 + 53 = 101$

$\Rightarrow k = 101$

Dai dati pubblici:

$r = \alpha^k \bmod p$

$7^{48} \bmod 107 = 40$

$7^{101} \bmod 107 = 67$ ok

$58 \cdot 101 \equiv 61 - 67a \pmod{106}$

$67a \equiv 33 \pmod{106} \qquad \mathrm{mcd}(67, 106) = 1 \Rightarrow 1$ soluzione

$67^{-1} \bmod 106 = 79$

$a = 33 \cdot 79 \bmod 106 = 97$

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

Matricola:

Domanda 2

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

Calcolare il logaritmo discreto $\text{Log}_\alpha(\beta)$ soluzione dell'equazione $\alpha^x \equiv \beta \pmod p$ per $p = 89$, $\alpha = 7$, $\beta = 53$, applicando l'algoritmo *Baby Step Giant Step*. Prima di tutto, verificare se esiste certamente una soluzione.

Se $\alpha = 7$ è una radice primitiva di $\mathbb{Z}_p^* \Rightarrow$ esiste 1 soluzione per $\forall \beta$

$p - 1 = 88 = 2^3 \cdot 11$

$\begin{cases} 7^8 \bmod 89 = 4 \\ 7^{44} \bmod 89 = 15 \end{cases} \Rightarrow \alpha = 7$ radice prim.

$N = \lceil \sqrt{p-1} \rceil = 10$

j	α^j	k	$\beta\alpha^{-Nk} = 53 \cdot 7^{-10k}$
0	1	0	53
1	7	(1)	(87)
2	49	2	
3	76		
4	(87)		
5	75		
6	80		
7	26		
8	4		
9	28		
10	18		

$\alpha^{-1} \bmod p = 7^{87} \bmod 89 = 51$

$\Rightarrow \alpha^j \equiv \beta\alpha^{-Nk} \pmod p$ per $j = 4, k = 1$

$\alpha^{j+Nk} \equiv \beta \pmod p \Rightarrow x = j + Nk = 14$

Verifica $7^{14} \equiv 53 \bmod 89$

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

Matricola:

Domanda 3

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

Si consideri il campo GF(2^8) = $\mathbb{Z}_2(x)$ mod ($x^8+x^4+x^3+x+1$).

Si segua la notazione usuale: gli elementi E*k* sono numerati con $k = 0, 1, \ldots$; l'indice k, espresso in forma binaria, rappresenta i coefficienti del polinomio corrispondente (bit più significativo = coefficiente di grado più alto).

Calcolare 1 / E128 in GF(2^8) eseguendo tutte le operazioni sulle rappresentazioni polinomiali degli elementi e applicando l'Algoritmo di Euclide Esteso. Esprimere il risultato finale con la notazione E*k*.

$E128: a(x) = x^7$

1) $m(x) = q_1(x)\,a(x) + r_1(x)$

$q_1(x) = x$

$r_1(x) = x^4+x^3+x+1$

$x^8+x^4+x^3+x+1 \;|\; x^7$

$x^8 \qquad\qquad\quad |\; x$

x^4+x^3+x+1

2) $a(x) = q_2(x)\,r_1(x) + r_2$

$q_2(x) = x^3+x^2+x$

$r_2(x) = x$

$x^7 \;|\; x^4+x^3+x+1$

$x^4+x^6+x^4+x^3 \;|\; x^3+x^2+x$

$x^6+x^4+x^3+x^2$

$x^6+x^5+x^3+x^2$

$x^5+x^4+x^2$

$x^5+x^4+x^2+x$

x

3) $r_1(x) = q_3(x) r_2(x) + r_3(x)$

$q_3(x) = x^3 + x^2 + 1$

$r_3(x) = 1$

$$\begin{array}{r|l} x^4 + x^3 + x + 1 & x \\ \hline x^4 & x^3 + x^2 + 1 \\ \hline x^3 + x + 1 & \\ x^3 & \\ \hline x + 1 & \\ x & \\ \hline 1 & \end{array}$$

$X_0 = 0 \quad X_1 = 1$

$X_2 = -q_1(x) X_1 + X_0 = x$

$X_3 = -q_2(x) X_2 + X_1 = (x^3 + x^2 + x) x + 1 = x^4 + x^3 + x^2 + 1$

$X_4 = -q_3(x) X_3 + X_2 = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + 1) + x$

$= x^7 + x + 1$

In notazione binaria: $10000011 =$

$= \text{E}131$

Verifica: $x^7 (x^7 + x + 1) = x^{14} + x^8 + x^7$

$(x^{14} + x^8 + x^7) \bmod (x^8 + x^4 + x^3 + x + 1) = 1$

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

Matricola:

Domanda 4

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

a) Che differenza c'è tra i protocolli di *symmetric key agreement* e *symmetric key distribution*?

b) In cosa consiste un *replay attack* ai protocolli precedenti?

c) Come possono essere impediti i *replay attack*? Citare (senza dettagliare) due esempi di protocolli che impediscono questi attacchi precisando come.

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (13 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) Ricavare la sequenza binaria pseudo-casuale generata dall'algoritmo *Blum-Blum-Shab* per $p = 23$, $q = 31$, $x = 5$ e determinarne il periodo P. *(2 punti)*

i	x_i	b_i
0	25	1
1	625	1
2	614	0
3	532	0
4	676	0
5	656	0
6	397	1
7	36	0
8	583	1
9	501	1
10	25	1

$P = 10$

$n = pq = 23 \cdot 31 = 713$

$x_0 = x$

$x_i = x_{i-1}^2 \bmod n$

2) Definire il problema del Logaritmo Discreto in un campo finito GF(p^n). *(2 punti)*

3) 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)*

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

Matricola:

4) Descrivere il *Test di Primalità di Fermat*. Cos'è un *Numero di Carmichael*? *(2 punti)*

5) Esprimere il *Problema Computazionale di Diffie-Hellman*. Saper risolvere il problema del logaritmo discreto è condizione necessaria o sufficiente per la risoluzione di questo Problema? *(2 punti)*

6) Cos'è una *One-Time Password*? Come può essere generata in un *meccanismo di autenticazione a Sfida e Risposta*? Fare un esempio. *(3 punti)*