Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **VI Appello d'Esame 2013-14 – 17 settembre 2014**

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 $p = 149$, $\alpha = 8$, $\beta = \alpha^a \bmod p = 127$, 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:

$A_1 = (r_1, s_1) = (75, 2)$ $\quad P_1 = 10$
$A_2 = (r_2, s_2) = (75, 124)$ $\quad P_2 = 20$
$A_3 = (r_3, s_3) = (75, 94)$ $\quad P_3 = 30$

Verificare che le tre firme siano valide.

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

A_1

$$\left.\begin{array}{l} 127^{75} \cdot 75^{2} \bmod 149 = 69 \\ \beta^{10} \bmod 149 = 144 \end{array}\right\} \Rightarrow \text{NO}$$

A_2

$$\left.\begin{array}{l} 127^{75} \cdot 75^{124} \bmod 149 = 25 \\ \beta^{20} \bmod 149 = 25 \end{array}\right\} \Rightarrow \text{OK}$$

A_3

$$\left.\begin{array}{l} 127^{75} \cdot 75^{94} \bmod 149 = 24 \\ \beta^{30} \bmod 149 = 24 \end{array}\right\} \Rightarrow \text{OK}$$

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*).

$P_2 = 20 \quad A_2 = (75, 124)$

$P_3 = 30 \quad A_3 = (75, 94)$

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

$$\begin{cases} 124k \equiv 20 - 75a \pmod{148} \\ 94k \equiv 30 - 75a \pmod{148} \end{cases}$$

$30k \equiv -10 \pmod{148} \quad \gcd(30, 148) = 2 \rightarrow$ 2 soluzioni

$15k \equiv -5 \pmod{148} \quad 15^{-1} \bmod 74 = 5$

$k_0 \equiv (-5) \cdot 5 \bmod 74 \equiv 49 \pmod{148}$

$k_1 \equiv k_0 + 74 \equiv 123 \pmod{148}$

Dati noti pubblici:

$r = \alpha^k \bmod p \rightarrow 5^k \bmod 149 = 75$

$\Rightarrow k = 49$

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

Matricola:

$94K \equiv 30 - 975 \pmod{148}$

$94 \cdot 49 \equiv 30 - 975 \pmod{148}$

$975 \equiv 12 \pmod{148}$ $\quad \gcd(75, 148) = 1 \rightarrow$ 1 soluzione

$75^{-1} \bmod 148 = 75$

$q \equiv 12 \cdot 75 \pmod{148}$

$q \equiv 12$

Domanda 2

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

Bob adotta il *sistema di cifratura a chiave pubblica RSA*. Pubblica il modulo $n = 3953$ e l'esponente di cifratura $e = 1225$.

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

b) Alice trasmette il messaggio cifrato $C = 100$. Calcolare il messaggio in chiaro P.

a) $n = 3953 = 59 \cdot 67$ (per tentativi)

$\varphi(n) = 58 \cdot 66 = 3828 = 2^2 \cdot 3 \cdot 11 \cdot 29$ $e \perp \varphi(n)$ OK

$\varphi[\varphi(n)] = 1120$

b) $d = e^{-1} \bmod \varphi(n) = e^{\varphi[\varphi(n)]-1} \bmod \varphi(n) = 1225^{1119} \bmod 3828$

Meglio usare l'algoritmo di Euclide Esteso:

$3828 = 3 \cdot 1225 + 153$

$1225 = 8 \cdot 153 + 1$

$153 = 153 \cdot 1 + 0$

$x_0 = 0 \quad x_1 = 1$

$x_2 = -q_1 x_1 + x_0 = -3$

$x_3 = -q_2 x_2 + x_1 = 25$

$\Rightarrow d = 25$

Verifica $25 \cdot 1225 \bmod 3828 = 1$

$P = C^d \bmod n = 100^{25} \bmod 3953 = 122$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **VI Appello d'Esame 2013-14 – 17 settembre 2014**

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

Matricola:

Domanda 3
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Cos'è un elemento primitivo $\alpha \in \mathbb{Z}_p^*$?

b) Qual è l'ordine dell'elemento $\alpha = 11$? E' un elemento primitivo di $\mathbb{Z}_{23}^*$?

$11^2 \equiv 6 \pmod{23}$
$11^{11} \equiv 22 \pmod{23}$
$\Rightarrow \alpha = 11$ elem. prim.

$\mathrm{Ord}(11) = 22$

c) Qual è l'ordine dell'elemento $\alpha = 13$? E' un elemento primitivo di $\mathbb{Z}_{23}^*$?

$13^2 \equiv 8 \pmod{23}$
$13^{11} \equiv 1 \pmod{23}$
$\Rightarrow \alpha = 13$ non elem. prim.

$\mathrm{Ord}(13) = 11$

d) Trovare ed elencare in ordine crescente i residui quadratici a_q dell'insieme $\mathbb{Z}_{23}^*$, cioè gli elementi $a \in \mathbb{Z}_{23}^*$: $a \equiv (\pm b)^2 \pmod{23}$, con $b \in \mathbb{Z}_{23}^*$.

b	$a_q = (\pm b)^2$
1	$1^2 \equiv 1$
2	$2^2 \equiv 4$
3	$3^2 \equiv 9$
4	16
5	2
6	13
7	3
8	18
9	12
10	8
11	6

$a_q = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$

Domanda 4

(svolgere su questo foglio nello spazio assegnato) (5 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 $(E128)^2 + E24$ in GF(2^8) eseguendo tutte le operazioni sulle loro rappresentazioni binarie.

$X_0 = E128 = 10000000$ $\quad E24 = 00011000$ $\quad E128 = 10000000$

$M = 100011011$

$X_1 = (10000000) \cdot (00000010) = 10000000$

100011011

000011011

$X_2 = (00011011) \cdot (\quad\quad) = 00110110$

$X_3 = (00110110) \cdot (\quad\quad) = 01101100$

$X_4 = (01101100) \cdot (\quad\quad) = 11011000$

$X_5 = (11011000) \cdot (\quad\quad) = 11011000$

100011011

010101011

$X_6 = (10101011) \cdot (\quad\quad) = 10101110$

100011011

001001101

$X_7 = (01001101) \cdot (\quad\quad) = 10011010$

$E128 \cdot E128 + E24 = X_7 + E24 = 10011010$

$= 00011000$

$10000010 \rightarrow E130$

Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **VI Appello d'Esame 2013-14 – 17 settembre 2014**

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) Calcolare 1/23 mod 317 per mezzo dell'Algoritmo di Euclide Esteso. *(2 punti)*

K	$q_K \cdot r_{K-1} + r_K$
1	$317 = 13 \cdot 23 + 18$
2	$23 = 1 \cdot 18 + 5$
3	$18 = 3 \cdot 5 + 3$
4	$5 = 1 \cdot 3 + 2$
5	$3 = 1 \cdot 2 + 1$
6	$2 = 2 \cdot 1 + 0$

$x_0 = 0 \quad x_1 = 1$

$x_2 = -q_1 x_1 + x_0 = -13 = 304$

$x_3 = -q_2 x_2 + x_1 = 14$

$x_4 = -q_3 x_3 + x_2 = -55 = 262$

$x_5 = -q_4 x_4 + x_3 = 69$

$x_6 = -q_5 x_5 + x_4 = -124 = 193$

2) Si consideri il meccanismo di memorizzazione cifrata (tramite una funzione unidirezionale $f(x)$) delle password in un file pubblico per il controllo dell'accesso a un sistema. Si descriva in cosa consiste un *attacco del vocabolario*, il meccanismo del *salt* e come il suo utilizzo contrasta questi attacchi. *(4 punti)*

3) In un *firewall*, spiegare in cosa consistono e per cosa si differenziano i *Packet Filter statici* e *dinamici*, riferendosi al caso in cui si desideri filtrare traffico UDP e TCP. *(3 punti)*

4) Descrivere la procedura di cifratura di un flusso di byte in chiaro $\{p_i\}$ basata sull'applicazione ripetuta di una funzione di hash $h(x)$, secondo una modalità analoga a OFB. *(3 punti)*

5) Si consideri una successione binaria pseudo casuale PRBS generata attraverso un Linear Feedback Shift Register di ordine m, avente polinomio caratteristico $P(x)$ di grado m. Qual è il periodo massimo che può avere la successione? Dare una condizione sufficiente perché il periodo abbia effettivamente tale valore massimo. *(2 punti)*