Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni **Appello ex-"Prova in Itinere" – 8 febbraio 2013**

Cognome e nome: *(stampatello)*

(firma leggibile)

Matricola:

NB1: 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 $p = 113$, $\alpha = 7$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 29$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 7$ non risultasse una scelta valida, Bob userà invece $\alpha = 6$ (da verificare). Se anche questa scelta non risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Bob estrae il numero casuale segreto (*nonce*) $k = 51$. Per questo valore di k, calcolare la firma A $=(r,s)$ del messaggio $P = 101$.

c) Verificare se anche la firma $A' = (r', s') = (103, 46)$ è valida per lo stesso messaggio $P = 101$.

a) p primo $1 < a \leq p-2$ $k \perp p-1$ α elem. prim. di $\mathbb{Z}_p^*$ $p-1 = 112 = 2^4 \cdot 7$

Test se α elem. primitivo : $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$

$$\left.\begin{array}{l} 7^{56} \equiv 1 \pmod{113} \\ 7^{16} \equiv 49 \pmod{113} \end{array}\right\} \Rightarrow \alpha = 7 \text{ NO}$$

$$\left.\begin{array}{l} 6^{56} \equiv 112 \\ 6^{16} \equiv 30 \end{array}\right\} \Rightarrow \alpha = 6 \text{ OK elem. primitivo di } \mathbb{Z}_{113}^*$$

$$\beta = \alpha^a \bmod p = 6^{29} \bmod 113 = 23$$

b) $r = \alpha^{K} \bmod p = 6^{51} \bmod 113 = 70$

$s = K^{-1}(P - ar) \bmod (p-1) = 11\,(101 - 29 \cdot 70) \bmod 112 = 61$

$K^{-1} \bmod (p-1) = 51^{-1} \bmod 112 = 51^{47} \bmod 112 = 11$

verifica: $11 \cdot 51 \bmod 112 = 1$

c) $\beta^{r} r^{s} \equiv \alpha^{P} \bmod p$?

$$\left.\begin{array}{l} 23^{103} \cdot 103^{46} \bmod 113 = 101 \\ 6^{101} \bmod 113 = 101 \end{array}\right\} \Rightarrow ok$$

$\left(A' = (103, 46) \text{ calcolata con } K = 3 \right)$

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (6 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 $n = 221$;
- la chiave pubblica della TA sia $K_{TA} = 35$;
- la chiave pubblica di Alice sia $K_A = 25$;
- l'identificativo di Alice sia $A = 200$;
- la funzione di hash $h = h(x,y)$ sia definita per $h, x, y \in \mathbb{Z}_n$ come
  $$h = h(x,y) = (x \oplus SL_3(y) \oplus SL_4(y)) \bmod n$$
  con SL_k = scorrimento ciclico a sinistra di k posizioni;
  x, y, h parole di 8 bit.

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) $n = 221 = 13 \cdot 17 \quad \varphi(n) = 192 = 2^6 \cdot 3 \quad \varphi[\varphi(n)] = 64$

$35 \perp 192 \quad 25 \perp 192 \quad 200 \in \mathbb{Z}_{221}$

b) $K_{TA}^{-1} = 35^{-1} \bmod 192 = 35^{63} \bmod 192 = 11$

$A = 200 = 11001000_2 \qquad SL_3(K_A) = 11001000$

$K_A = 25 = 00011001_2 \qquad SL_4(K_A) = 10010001$

$$h = \begin{array}{r} 11001000 \oplus \\ 11001000 \oplus \\ 10010001 = \\ \hline 10010001 \end{array} = 145$$

$\{h\}_{K_{TA}^{-1}} = h^{K_{TA}^{-1}} \bmod n = 145^{11} \bmod 221 = 202$

$\Rightarrow C_A = (200, 25, 202)$

c) Decifrare $202^{35} \bmod 221 = 145$ OK

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

Matricola:

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

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

Si segua la notazione usuale: gli elementi Ek 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)

a) Calcolare E6 + E7.

b) ~~Calcolare~~ E6 × E7.

c) Calcolare l'inverso dell'elemento E7 applicando l'Algoritmo di Euclide Esteso al polinomio corrispondente.

a) $110 \oplus 111 = 001 \qquad \underline{E1}$

b) $(x^2+x)(x^2+x+1) \bmod (x^3+x+1) =$

$= (x^4+x) \bmod (x^3+x+1) = x^2 \qquad \underline{E4}$

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

c) $E7 : x^2+x+1 \qquad a^{-1} \bmod b \qquad a = x^2+x+1$
$b = x^3+x+1$

$b = q_1 \cdot a + r_1 \qquad x^3+x+1 = (x+1)(x^2+x+1)+x$

$a = q_2 \cdot r_1 + r_2 \qquad x^2+x+1 = (x+1)x + 1$

$X_0 = 0 \quad X_1 = 1$

$X_2 = -q_1 X_1 + X_0 = -(x+1) = x+1$

$X_3 = -q_2 X_2 + X_1 = (x+1)(x+1)+1 = x^2 \qquad \underline{E7^{-1} = E4}$

$$
\begin{array}{l|l}
x^3 + x + 1 & x^2 + x + 1 \\ \cline{2-2}
x^3 + x^2 + x & x + 1 \\ \cline{1-1}
x^2 + 1 & \\
x^2 + x + 1 & \\ \cline{1-1}
\quad x &
\end{array}
$$

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

Matricola:

Domanda 4
(svolgere su questo foglio nello spazio assegnato) (6 punti)

a) Cos'è una funzione di *hash*? Qual è l'ingresso? Qual è l'uscita? A cosa serve?

b) Definire la proprietà di *unidirezionalità* di una funzione di hash.

c) Definire la proprietà di una funzione di hash *fortemente resistente alle collisioni.*

d) Definire la proprietà di una funzione di hash *debolmente resistente alle collisioni.*

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (12 punti)

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

---

1) Calcolare l'inverso a^{-1} di $a \equiv 100 \pmod{999}$ applicando il Teorema di Eulero e quindi l'algoritmo di *Square & Multiply* per il calcolo della potenza. *(2 punti)*

$a^{-1} \equiv a^{\varphi(n)-1} \mod n$

$\varphi(999) = 648$

$a^{-1} \equiv 100^{647} \pmod{999} \equiv 10$

Ver. $100 \cdot 10 \mod 999 = 1$

$647 = 1010000111_2$

1	$1^2 \cdot 100$	$\equiv 100$	(mod 999)
0	100^2	$\equiv 10$	( )
1	$10^2 \cdot 100$	$\equiv 10$	( )
0	10^2	$\equiv 100$	( )
0	100^2	$\equiv 10$	( )
0	10^2	$\equiv 100$	( )
0	100^2	$\equiv 10$	( )
1	$10^2 \cdot 100$	$\equiv 10$	( )
1	$10^2 \cdot 100$	$\equiv 10$	( )
1	$10^2 \cdot 100$	$\equiv 10$	( )

---

2) Trovare ed elencare in ordine crescente i *residui quadratici* a_q dell'insieme $\mathbb{Z}_p^*$ per $p = 17$, cioè gli elementi $a \in \mathbb{Z}_p^*$ | : $a \equiv (\pm b)^2 \pmod{p}$, con $b \in \mathbb{Z}_p^*$. *(2 punti)*

b	a_q	
1	$1^2 \equiv 1$	(mod 17)
2	$2^2 \equiv 4$	(")
3	$3^2 \equiv 9$	(")
4	$4^2 \equiv 16$	(")
5	$5^2 \equiv 8$	(")
6	$6^2 \equiv 2$	(")
7	$7^2 \equiv 15$	(")
8	$8^2 \equiv 13$	(")

$a_q = \{1, 2, 4, 8, 9, 13, 15, 16\}$

Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **Appello ex-"Prova in Itinere" – 8 febbraio 2013**

Cognome e nome: *(stampatello)*

(firma leggibile)

Matricola:

3) Enunciare il *Test di Primalità di Fermat*. Cos'è un numero *pseudoprimo forte*? *(3 punti)*

4) Si consideri un algoritmo di cifratura simmetrica $E_K(P)$ con chiave K di lunghezza n bit. La cifratura doppia $E_{K_2}[\ E_{K_1}(P)\ ]$, con due chiavi K_1, K_2 applicate successivamente, offre una sicurezza equivalente all'impiego di una chiave di lunghezza doppia $2n$? Fare un esempio in cui questo è vero e uno in cui non lo è. *(2 punti)*

5) A cosa serve il protocollo di Diffie-Hellmann? Illustrarlo. *(3 punti)*