Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **I Appello d'Esame 2014-15 – 13 febbraio 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) (7 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 107$, $\alpha = 5$, $\beta = \alpha^a \bmod p = 66$, 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:

$A_1 = (r_1, s_1) = (84, 74)$ $\quad P_1 = 14$
$A_2 = (r_2, s_2) = (84, 23)$ $\quad P_2 = 15$
$A_3 = (r_3, s_3) = (84, 40)$ $\quad P_3 = 16$

Verificare che le tre firme siano valide.

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

A_1 $\begin{cases} 66^{84}\, 84^{74} \equiv 27 \\ 5^{14} \equiv 11 \end{cases} \Rightarrow$ NO $\pmod{107}$

A_2 $\begin{cases} 66^{84}\, 84^{23} \equiv 55 \\ 5^{15} \equiv 55 \end{cases} \Rightarrow$ OK

A_3 $\begin{cases} 66^{84}\, 84^{40} \equiv 61 \\ 5^{16} \equiv 61 \end{cases} \Rightarrow$ 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*).

$P_2 = 15 \quad A_2 = (84, 23)$

$P_3 = 16 \quad A_3 = (84, 40)$

$S = K^{-1}(P - ar) \bmod (p-1) \rightarrow SK \equiv P - ar \pmod{p-1}$

$$\begin{cases} 23K \equiv 15 - a84 \pmod{106} \\ 40K \equiv 16 - a84 \pmod{106} \end{cases}$$

$17K \equiv 1 \pmod{106}$ $17 \perp 106 \Rightarrow$ 1 soluzione $17^{-1} \bmod 106 = 17^{51} \bmod 106 \equiv$
$\equiv 25$

$\Rightarrow \boxed{K = 25}$

$23 \cdot 25 \equiv 15 - a84 \pmod{106}$

$a84 \equiv 76 \pmod{106}$ $\gcd(84, 106) = 2 \Rightarrow$ 2 soluzioni

$a42 \equiv 38 \pmod{53}$ $42^{-1} \bmod 53 = 42^{51} \bmod 53 = 24$

$a_0 = 38 \cdot 24 \bmod 53 = 11$

$a_1 = a_0 + 53 = 64$

Dai dati pubblici:

$\beta = \alpha^a \bmod p \rightarrow 5^a \bmod 107 = 66$

$\Rightarrow \boxed{a = 11}$

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

Matricola:

Domanda 2

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

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 197$, $\alpha = 5$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 128$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 5$ non risultasse una scelta valida, Bob userà invece $\alpha = 6$, oppure ancora $\alpha = 7$ (da verificare). Se anche queste scelte non risultassero valide, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 64$ e spedisce il messaggio $P_1 = 20$. Calcolare il messaggio cifrato $C_1 = (r_1, t_1)$.

c) Alice estrae un nuovo numero casuale segreto (*nonce*) k e, usando sempre questo stesso valore, spedisce i messaggi P_2, P_3, P_4. Oscar intercetta i messaggi cifrati $C_2 = (r_2, t_2) = (138, 52)$, $C_3 = (r_3, t_3) = (138, 73)$, $C_4 = (r_4, t_4) = (138, 168)$ e, per altra via, viene a sapere che $P_2 = 50$. Calcolare P_3 e P_4.

a) p primo: $1 < a \leq p-2$ $\quad p-1 = 196 = 2^2 \cdot 7^2$

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

$5^{98} \equiv 196$
$5^{28} \equiv 114$
$\Rightarrow$ SI $\quad \alpha = 5$

$\beta = \alpha^a \bmod p = 5^{128} \bmod 197 = 105$

b) $r_1 = \alpha^k \bmod p = 5^{64} \bmod 197 = 156$

$t_1 = \beta^k P_1 \bmod p = 105^{64} \cdot 20 \bmod 197 = 45$

$\Rightarrow C_1 = (156, 45)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $\quad t_2^{-1} = 52^{-1} \equiv 72 \pmod{197}$

$P_3 = P_2 \frac{t_3}{t_2} \bmod p = 50 \cdot 73 \cdot 72 \bmod 197 = 2$

$P_4 = P_2 \frac{t_4}{t_2} \bmod p = 50 \cdot 168 \cdot 72 \bmod 197 = 10$

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

Matricola:

Domanda 3

(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 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).

Calcolare il prodotto degli elementi E18 × E127 in GF(2^8) eseguendo tutte le operazioni sulle loro rappresentazioni binarie.

Meglio E127 x E18

E127 = 01111111
E18 = 00010010
m = 100011011

X_0 = E127 = 01111111

$X_1 = (01111111) \cdot (00100010) = 11111110$

$X_2 = (11111110) \cdot (\quad) = 111111100$
100011011
11100111

$X_3 = (11100111) \cdot (\quad) = 111001110$
100011011
11010101

$X_4 = (11010101) \cdot (\quad) = 110101010$
100011011
10111001

E127 x E18 = $X_1 + X_4$ = 11111110
10111001
01001111 = E79

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* $y = h(x)$?

b) Si consideri la funzione SHA-256 (SHA-2 nella versione a 256 bit). Dato un hash h_1, quanti sono i messaggi m di lunghezza massima 1 kbyte (k = 1024×) tali per cui $h(m) = h_1$?

c) Verificare se la funzione $h(x) = x^2 \bmod n$, con n composto e difficile da fattorizzare, gode della proprietà *fortemente resistente alle collisioni*.

d) Verificare se la funzione $h(x) = x^2 \bmod n$, con n composto e difficile da fattorizzare, gode della proprietà *debolmente resistente alle collisioni*.

b) $|m| = 2^{8193} - 2$ $|h| = 2^{256}$ $\rightarrow \sim 2^{7937}$

c) no: basta che $x_1 = x_2 + n$ $(x_1 = \pm x_2 + kn)$

d) no: dato x_1, $x_2 = -x_1$

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) Esprimere la definizione di *Simbolo di Jacobi*. *(2 punti)*

2) Determinare se l'equazione $x^2 \equiv 15 \pmod{997}$ ha soluzione, tramite il calcolo del simbolo di Legendre corrispondente. *(2 punti)*

$p = 997$ primo

$$\left(\frac{15}{997}\right) = \left(\frac{997}{15}\right) = \left(\frac{7}{15}\right) = \left(\frac{7}{3}\right)\left(\frac{7}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = 1 \cdot (-1) = -1$$

$\Rightarrow$ non ha soluzione

3) Cos'è un elemento primitivo $\alpha \in \mathbb{Z}_p^*$? *(2 punti)*

4) Quali sono le tre informazioni fondamentali contenute in un *certificato di identità* in una PKI? Precisare il meccanismo di autenticazione e dove si reperiscono le chiavi utilizzate. *(2 punti)*

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

Matricola:

5) Cos'è un cifrario monoalfabetico? E un cifrario polialfabetico? *(1 punto)*

6) Descrivere sommariamente l'*algoritmo AES*. Specificare: *(4 punti)*
- lunghezza delle chiavi;
- ruolo e funzioni dei *round* (ingresso, uscita, *layer*);
- funzioni dei singoli *layer*.