Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **II Appello d'Esame 2013-14 – 3 marzo 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) (5 punti)

Alice e Bob adottano il protocollo di *Diffie-Hellman* per lo scambio della chiave. Alice pubblica $p = 139$ e inizialmente $\alpha = 4$. Alice sceglie $x = 57$ (segreto). Bob sceglie $y = 12$ (segreto). Oscar si interpone e sceglie $z = 2$ (attacco *man in the middle*).

a) Alice verifica la correttezza dei dati forniti 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 $\alpha = \{3, 4, 5, 6, 7, 8, 9, 10\}$. Se nessuna di queste scelte risultasse valida, Alice e Bob rinunceranno a proseguire (e l'esercizio termina qui).

p primo $1 < x, y, z \le p-2$ Test se α elem. primitivo: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$

$p-1 = 138 = 2 \cdot 3 \cdot 23$

$\alpha = 4$ $4^{69} \equiv 1$, $4^{46} \equiv 42$, $4^{6} \equiv 65$ $\Rightarrow$ NO

$\alpha = 3$ $3^{69} \equiv 138$, $3^{46} \equiv 42$, $3^{6} \equiv 34$ $\Rightarrow$ OK

$\alpha = 5, 6, 7, 8, 9, 10$ NO

b) Calcolare i numeri scambiati tra Alice, Bob e Oscar e le chiavi K_A e K_B condivise rispettivamente tra Oscar e Alice e tra Oscar e Bob.

6) $A \to O \quad \alpha^x \bmod p = 3^{57} \bmod 139 = 60$

$B \to O \quad \alpha^y \bmod p = 3^{12} \bmod 139 = 44$

$O \to A$, $O \to B$ $\quad \alpha^z \bmod p = 3^2 \bmod 139 = 9$

Alice calcola: $K_A = 9^{57} \bmod 139 = 125$

Bob calcola: $K_B = 9^{12} \bmod 139 = 129$

Oscar calcola: $K_A = 60^2 \bmod 139 = 125$

$K_B = 44^2 \bmod 134 = 129$

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (7 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 109$, $\alpha = 6$, $\beta = \alpha^a \bmod p = 48$, 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:

$A_1 = (r_1, s_1) = (42, 74)$ $\quad P_1 = 106$
$A_2 = (r_2, s_2) = (42, 99)$ $\quad P_2 = 10$
$A_3 = (r_3, s_3) = (42, 28)$ $\quad P_3 = 56$

Verificare che le tre firme siano valide.

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

A_1 | $48^{42} \cdot 42^{74} \bmod 109 = 106$; $6^{106} \bmod 109 = 106$ } $\Rightarrow$ OK

A_2 | $48^{42} 42^{99} \bmod 109 = 55$; $6^{90} \bmod 109 = 61$ } $\Rightarrow$ NO

A_3 | $48^{42} \cdot 42^{28} \bmod 109 = 73$; $6^{56} \bmod 109 = 73$ } $\Rightarrow$ 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*).

$P_1 = 106 \quad A_1 = (42, 74)$

$P_2 = 56 \quad A_2 = (42, 28)$

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

$$\begin{cases} 74k \equiv 106 - a42 \pmod{108} \\ 28k \equiv 56 - a42 \pmod{108} \end{cases}$$

$46k \equiv 50 \pmod{108} \quad \text{mcd}(46, 108) = 2 \rightarrow$ 2 soluzioni

$23k \equiv 25 \pmod{54} \quad 23^{-1} \bmod 54 = 47$

$k_0 \equiv 25 \cdot 47 \bmod 54 = 41 \pmod{108}$

$k_1 = k_0 + 54 = 95 \pmod{108}$

Dei dati pubblici:

$r = a^k \bmod p \rightarrow 6^k \bmod 109 = 42$

$\Rightarrow \boxed{k = 41}$

$28\,K \equiv 56 - a\,42 \pmod{128}$

$28 \cdot 41 \equiv 56 - a\,42 \pmod{128}$

$a\,42 \equiv 96 \pmod{128}$ $\quad mcd(42, 128) = 6 \rightarrow$ 6 soluzioni

$a\,7 \equiv 16 \pmod{128}$ $\quad 7^{-1} \bmod 128 = 13$

$a_0 = 13 \cdot 16 \bmod 128 = 80$

$a_i \equiv a_0 + \frac{i}{6} 128 \quad (i = 1, \dots 5)$ $\quad a_i = 28, 46, 64, 82, 100$

Dai tasti pubblici:

$\beta = \alpha^a \bmod p \rightarrow 5^a \bmod 109 = 48$

$\Rightarrow \boxed{a = 64}$

Domanda 3

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

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 149$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 77$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 3$ non risultasse una scelta valida, Bob userà invece $\alpha = 4$, oppure ancora $\alpha = 5$ (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*) $k = 86$ e spedisce il messaggio $P = 100$. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob, per un errore di trasmissione, riceve $C' = (r', t') = (44, 55)$. Calcolare il messaggio decifrato da Bob P'.

a) p primo $1 < a \leq p-2$ Tgt se α elem. prim. di Z_p^*: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$

$3^{74} \equiv 148$
$3^4 \equiv 81$ $\Rightarrow$ ok $\alpha = 3$

$\beta = \alpha^a \bmod p = 3^{77} \bmod 149 = 122$

b) $r = \alpha^K \bmod p = 3^{86} \bmod 149 = 42$

$t = \beta^K \cdot P \bmod p = 122^{86} \cdot 100 \bmod 149 = 73$

$C = (42, 73)$

c) $C' = (r', t') = (44, 55)$

$P' = t' \cdot r'^{-a} \bmod p = 55 \cdot 44^{71} \bmod 149 = 113$

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

Matricola:

Domanda 4
(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).

a) Calcolare il prodotto degli elementi E31 × E33 in GF(2^8) eseguendo tutte le operazioni sulle loro rappresentazioni binarie.

a) E31 = 00011111 M = 100011011

E33 = 00100001

X_0 = E31 = 00011111

X_1 = (00011111) · (00000010) = 00111110

X_2 = (00111110) · (") = 01111100

X_3 = (01111100) · (") = 11111000

X_4 = (11111000) · (") = 111110000

100011011

11101011

X_5 = (11101011) · (") = 111010110

100011011

11001101

E31 · E33 = X_0 + X_5 = 00011111

11001101

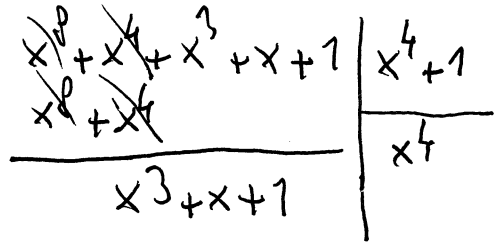
11010010 = E210

b) Calcolare l'inverso dell'elemento E17 (ossia $a(x) = x^4+1$) in GF(2^8) applicando l'Algoritmo di Euclide Esteso al polinomio corrispondente.

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

$q_1(x) = x^4$

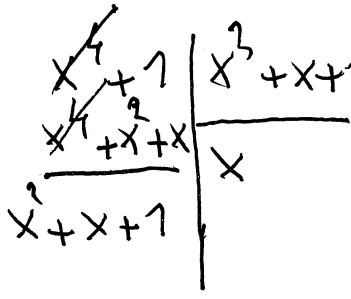
$r_1(x) = x^3+x+1$



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

$q_2(x) = x$

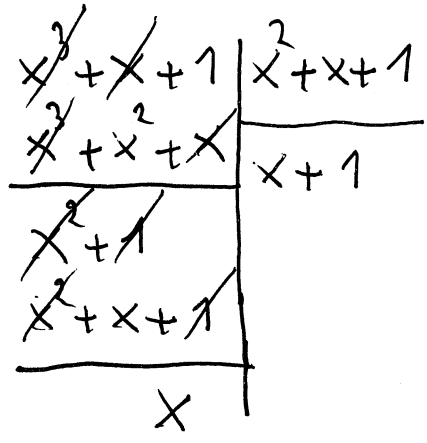
$r_2(x) = x^2+x+1$



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

$q_3(x) = x+1$

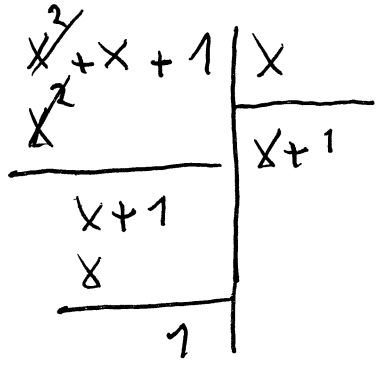
$r_3(x) = x$



4) $r_2(x) = q_4(x)\,r_3(x) + r_4(x)$

$q_4(x) = x+1$

$r_4(x) = 1$



$X_0 = 0 \quad X_1 = 1$

$X_2 = -q_1(x)X_1 + X_0 = x^4$

$X_3 = -q_2(x)X_2 + X_1 = x^5 + 1$

$X_4 = -q_3(x)X_3 + X_2 = -(x+1)(x^5+1) + x^4 = x^6 + x^5 + x^4 + x + 1$

$X_5 = -q_4(x)X_4 + X_3 = -(x+1)(x^6+x^5+x^4+x+1) + x^5 + 1 =$

$= x^7 + x^5 + x^4 + x^2$

In binario: 10110100 = E18O

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

Matricola:

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) Descrivere sommariamente come è stata costruita la S-Box nell'algoritmo Rijndael. In quale layer viene utilizzata? *(2 punti)*

2) Trovare tutte le soluzioni dell'equazione $13^x \equiv 2 \pmod{19}$ *(2 punti)*

$x \equiv 11 \pmod{18}$

3) Cos'è un numero *pseudoprimo* per la base *a*? *(2 punti)*

4) Descrivere un attacco del compleanno che miri a firmare validamente un documento fraudolento. *(3 punti)*

5) Descrivere un *ruleset* statico (*packet filter*) di un firewall. *(3 punti)*