Sicurezza delle Reti

Prof. Stefano Bregni — **II Appello d'Esame 2016-17 – 17 luglio 2017**

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 $p = 179$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 72$.

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 un valore valido scelto nell'insieme $\alpha = \{4, 5, 6\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Bob estrae il numero casuale segreto (*nonce*) $k = 129$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 12$.

c) Verificare se anche la firma $A' = (r', s') = (35, 128)$ è valida per lo stesso messaggio $P = 12$. Se è valida, calcolare il valore di k per cui è stata calcolata da Bob.

a) p primo $1 < a < p-2$ $k \perp p-1$ α elem. primitivo di $\mathbb{Z}_p^*$

Test se α elem. primitivo $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $p-1 = 178 = 2 \cdot 89$

$3^{89} \equiv 1$, 3^2 $\Rightarrow$ $\alpha = 3$ NO

$4^{89} \equiv 1$, 4^2 $\Rightarrow$ NO

$5^{89} \equiv 1$, 5^2 $\Rightarrow$ NO

$6^{89} \equiv 178$, $6^2 \equiv 36$ $\alpha = 6$ SI $\Rightarrow$ $\alpha = 6$ elem. primitivo di $\mathbb{Z}_{179}^*$

$\beta = \alpha^a \bmod p = 6^{72} \bmod 179 = 22$

b) $r = \alpha^K \bmod p = 6^{129} \bmod 179 = 90$

$S = K^{-1}(P - ar) \bmod (p-1) = 11(12 - 72 \cdot 90) \bmod 178 = 132$

$K^{-1} \bmod (p-1) = 129^{-1} \bmod 178 = 69$ (con Euclide E.)

Verifica: $129 \cdot 69 \bmod 178 \equiv 1$

c) $\beta^r r^S \equiv \alpha^P \pmod p$

$22^{35}\ 35^{128} \bmod 179 = 31$
$6^{92} \bmod 179 \equiv 31$
$\Rightarrow$ OK

$A' = (35, 128)$ prima validità di $P=12$

$SK \equiv P - ar \pmod{178}$

$128\,K \equiv 12 - 72 \cdot 35 \pmod{178}$

$128\,K \equiv 162 \pmod{178}$ $\quad MCD(128, 172) = 2 \rightarrow$ 2 soluzioni

$64\,K \equiv 81 \pmod{89}$ $\quad 64^{-1} \equiv 32 \pmod{89}$

$\rightarrow K_0 \equiv 32 \cdot 81 \equiv 11 \pmod{89}$

$K_1 \equiv 11, 100 \pmod{178}$

Dai dati pubblici:

$r = \alpha^K \bmod p$

$\Rightarrow K = 11$

Sicurezza delle Reti
Prof. Stefano Bregni — **II Appello d'Esame 2016-17 – 17 luglio 2017**

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (6 punti)

Si consideri l'algoritmo di cifratura di Hill definito come

$$\mathbf{C}_i = \mathbf{P}_i \cdot \mathbf{K} + \mathbf{B} \mod 16$$

dove:

$\mathbf{C}_i$ = coppia i-esima di caratteri cifrati $[C_{1i}\ C_{2i}]$;
$\mathbf{P}_i$ = coppia i-esima di caratteri in chiaro $[P_{1i}\ P_{2i}]$;
$\mathbf{K}$, $\mathbf{B}$ = chiave di cifratura, con

$$\mathbf{K} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \qquad \mathbf{B} = [b_1 \quad b_2].$$

Effettuare un *attacco di tipo testo in chiaro noto*, con

$$\mathbf{P} = [1\ \ 2\ \ 3\ \ 3\ \ 4\ \ 4] \qquad \mathbf{C} = [14\ \ 3\ \ 10\ \ 4\ \ 13\ \ 10]$$

e ricavare la chiave $\mathbf{K}$, $\mathbf{B}$.

Per i valori ricavati di $\mathbf{K}$ e $\mathbf{B}$,
- esiste un solo $\mathbf{C}$ che corrisponde a un certo $\mathbf{P}$?
- esiste un solo $\mathbf{P}$ che corrisponde a un certo $\mathbf{C}$?

Giustificare le risposte.

$$\begin{cases} C_1 = P_1 K + B \\ C_2 = P_2 K + B \\ C_3 = P_3 K + B \end{cases} \qquad \begin{pmatrix} C_1 - C_3 \\ C_2 - C_3 \end{pmatrix} \equiv \begin{pmatrix} P_1 - P_3 \\ P_2 - P_3 \end{pmatrix} K \pmod{16}$$

$$\begin{pmatrix} 1 & 9 \\ 13 & 10 \end{pmatrix} \equiv \underbrace{\begin{pmatrix} -3 & -2 \\ -1 & -1 \end{pmatrix}}_{P} K \pmod{16} \qquad \det P = 1 \qquad 1^{-1} \equiv 1$$

$$P^{-1} \equiv 1 \cdot \begin{pmatrix} 15 & 2 \\ 1 & 13 \end{pmatrix} \pmod{16}$$

$$K \equiv \begin{pmatrix} 15 & 2 \\ 1 & 13 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 13 & 10 \end{pmatrix} \equiv \begin{pmatrix} 9 & 11 \\ 10 & 11 \end{pmatrix} \pmod{16}$$

$\det K = 5 \quad 5 \perp 16 \Rightarrow \exists K^{-1}$ corrispondenza biunivoca tra P e C

$$B \equiv C_1 - P_1 K \equiv (14\ 3) - (1\ 2)\begin{pmatrix} 9 & 11 \\ 10 & 11 \end{pmatrix} \equiv (1\ 2) \pmod{16}$$

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 E17 × E63 in GF(2^8) eseguendo tutte le operazioni sulle loro rappresentazioni binarie.

Meglio calcolare E63 × E17

E63 = 01111111
E17 = 00010001
Π = 100011011

X_0 = E63 = 01111111

X_1 = (01111111) · (00000010) = 11111110

X_2 = (11111110) · (——) = 11111100

X_3 = (11111100) · (——) = 111111000
100011011
11100011

X_4 = (11100011) · (——) = 11100110
100011011
11011101

E63 × E17 = $X_0 + X_4$ = 01111111
11011101
11100010 = E226

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

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 163$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 83$.

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 un valore valido scelto nell'insieme $\alpha = \{4, 5, 6\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 112$ e spedisce il messaggio $P_1 = 100$. 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 $C_2 = (r_2, t_2) = (96, 130)$, $C_3 = (r_3, t_3) = (96, 86)$, $C_4 = (r_4, t_4) = (96, 11)$ e, per altra via, viene a sapere che $P_2 = 20$. Calcolare P_3 e P_4.

a) p primo $1 < \alpha < p-2$ $p-1 = 162 = 2 \cdot 3^4$

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

$\left.\begin{array}{l} 3^{81} \equiv 162 \pmod{163} \\ 3^{54} \equiv 58 \end{array}\right\} \Rightarrow$ ok $\alpha = 3$ elem. primitivo di Z_p^*

$\beta = \alpha^a \bmod p = 3^{83} \bmod 163 = 154$

b) $r_1 = \alpha^k \bmod p = 3^{112} \bmod 163 = 111$

$t_1 = \beta^k P \bmod p = 154^{112} \cdot 100 \bmod 163 = 146$ $\Rightarrow C_1 = (111, 146)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $t_2^{-1} = 130^{-1} \equiv 79 \pmod{163}$

$P_3 = P_2 \frac{t_3}{t_2} \bmod p = 20 \cdot 86 \cdot 79 \bmod 163 = 101$

$P_4 = P_2 \frac{t_4}{t_2} \bmod p = 20 \cdot 11 \cdot 79 \bmod 163 = 102$

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

Matricola:

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) Cos'è un *elemento primitivo* $\alpha \in \mathbb{Z}_p^*$? Quanti sono gli elementi primitivi di $\mathbb{Z}_{1109}^*$? Qual è l'*ordine* dell'elemento $\alpha = 4$ in $\mathbb{Z}_{1109}^*$? *(3 punti)*

$p = 1109$ primo. $\varphi(p-1)$ elem. primitivi

$p-1 = 1108 = 2^2 \cdot 277$ $\quad \varphi(p-1) = 552$

$\alpha^2 \equiv 16 \pmod{1109}$

$\alpha^4 \equiv 256$

$\alpha^{277} \equiv 1108 \equiv -1$

$\alpha^{554} \equiv 1$ $\quad \Rightarrow \text{ord}_{1109}(\alpha = 4) = 554$

---

2) Si consideri la sequenza binaria pseudo-casuale $\{x_i\}$ generata dall'algoritmo *Blum-Blum-Shab* per $p = 83$, $q = 139$. In base alla teoria, qual è il valore massimo che può assumere il suo periodo $P = \pi(x_0)$ per valori arbitrari del seme $x_0 = x^2 \in \mathbb{Z}_n$? Si ricorda che $\pi(x_0)$ divide $\lambda(\lambda(n))$, dove $\lambda(n) := \text{mcm}\left(\left\{\varphi\left(p_i^{a_i}\right)\right\}\right)$ è la Funzione di Charmichael. *(2 punti)*

$\lambda(n) = \text{mcm}(82, 138) = 2 \cdot 3 \cdot 23 \cdot 41 = 5658$

$82 = 2 \cdot 41$

$138 = 2 \cdot 3 \cdot 23$

$\lambda(\lambda(n)) = \lambda(5658) = \text{mcm}(1, 2, 22, 40) =$

$22 = 2 \cdot 11$

$40 = 2^3 \cdot 5$

$= 2^3 \cdot 5 \cdot 11 = 440$

$\Rightarrow \max \pi(x_0) = 440$

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

Matricola:

3) Descrivere la procedura di autenticazione e cifratura di un messaggio PGP inviato da Alice a Bob basato sugli algoritmi RSA, 3DES, SHA, DSA (firma El Gamal). *(3 punti)*

4) A cosa serve il Protocollo di Needham-Schroeder? Chi sono gli interlocutori del protocollo? Qual è la sua caratteristica principale e come evita i *replay attack*? *(3 punti)*

5) Descrivere l'*attacco dell'intruso* al Protocollo di Instaurazione della Chiave di Diffie-Hellman. Come è possibile ostacolarlo? *(2 punti)*