Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **V Appello d'Esame 2013-14 – 1 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) (6 punti)

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 101$, $\alpha = 5$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 32$.

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 $P_1 = 50$. 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 $C_2 = (r_2, t_2) = (39, 5)$, $C_3 = (r_3, t_3) = (39, 82)$, $C_4 = (r_4, t_4) = (39, 76)$ e, per altra via, viene a sapere che $P_2 = 16$. Calcolare P_3 e P_4.

a) p primo $1 < a \leq p-2$ $\quad p-1 = 100 = 2^2 \cdot 5^2$

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

$5^{50} \equiv 1$, $5^{20} \equiv$ $\Rightarrow$ NO $\quad 6^{50} \equiv 1$, $6^{20} \equiv$ $\Rightarrow$ NO $\quad 7^{50} \equiv 100$, $7^{20} \equiv 84$ $\Rightarrow$ OK $\quad \alpha = 7$

$\beta = \alpha^a \bmod p = 7^{32} \bmod 101 = 92$

b) $r_1 = \alpha^k \bmod p = 7^{64} \bmod 101 = 81$

$t_1 = \beta^k P_1 \bmod p = 92^{64} \cdot 50 \bmod 101 = 67$

$\Rightarrow C_1 = (81, 67)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$

$t_2^{-1} = 5^{-1} \equiv 81 \pmod{101}$

$P_3 = P_2 \frac{t_3}{t_2} \bmod p = 16 \cdot 82 \cdot 81 \bmod 101 = 20$

$P_4 = P_2 \frac{t_4}{t_2} \bmod p = 16 \cdot 76 \cdot 81 \bmod 101 = 21$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **V Appello d'Esame 2013-14 – 1 settembre 2014**

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

Matricola:

Domanda 2

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

La *Trusted Authority* TA adotta lo *Schema di Blom* per distribuire chiavi simmetriche a tre utenti A, B e C e pubblica $p = 569$. Gli identificativi pubblici dei tre utenti sono rispettivamente $r_A = 25$, $r_B = 26$, $r_C = 27$.

a) Per i tre utenti, TA sceglie e tiene segreti $a = 501$, $b = 369$, $c = 111$. Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$a_A = a + b r_A \bmod p = 53$ $\quad a_B = a + b r_B \bmod p = 422$ $\quad a_C = a + b r_C \bmod p = 222$

$b_A = b + c r_A \bmod p = 299$ $\quad b_B = b + c r_B \bmod p = 410$ $\quad b_C = b + c r_C \bmod p = 527$

$g_A(x) = a_A + b_A x$ $\quad K_{AB} = g_A(r_B) = 430$

$g_B(x) = a_B + b_B x$ $\quad K_{AC} = g_A(r_C) = 160$

$g_C(x) = a_C + b_C x$ $\quad K_{BC} = g_B(r_C) = 112$

b) Per i tre utenti, TA sceglie e tiene segreti a, b, c. Gli utenti A e B si accordano e si scambiano le informazioni $a_A = 510$, $b_A = 201$, $a_B = 530$, $b_B = 231$.
- Calcolare i parametri segreti a, b, c.
- Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$$a_A = \begin{cases} a + b25 \bmod 569 = 510 & b \equiv 20 \pmod{569} \\ a + b26 \bmod 569 = 530 & a \equiv 10 \pmod{569} \\ b + c25 \bmod 569 = 201 & c = 30 \pmod{569} \end{cases}$$

$b \equiv 20 \pmod{569}$

$25^{-1} \equiv 478 \pmod{569}$

$a \equiv 530 - 20 \cdot 26 \equiv 10 \pmod{569}$

$c \equiv (201 - 20) \cdot 25^{-1} \pmod{569}$

$\equiv 30$

$K_{AB} = 46$

$K_{AC} = 247$

$K_{BC} = 508$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **V Appello d'Esame 2013-14 – 1 settembre 2014**

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

Matricola:

Domanda 3

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

Si consideri l'algoritmo di cifratura di Hill definito come

$$\mathbf{C}_i = \mathbf{P}_i \cdot \mathbf{K} + \mathbf{B} \mod 32$$

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

$$\mathbf{P} = [1\ \ 3\ \ 2\ \ 4\ \ 3\ \ 8] \qquad \mathbf{C} = [1\ \ 5\ \ 2\ \ 6\ \ 3\ \ 2]$$

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 al $\mathbf{P}$ assegnato? Perché? La chiave ricavata è valida?

$$\begin{cases} C_1 = P_1 K + B \\ C_2 = P_2 K + B \\ C_3 = P_3 K + B \end{cases} \qquad \begin{pmatrix} C_1 - C_3 \\ C_2 - C_3 \end{pmatrix} \equiv \begin{pmatrix} P_1 - P_3 \\ P_2 - P_3 \end{pmatrix} K \pmod{32}$$

$$\begin{pmatrix} -2 & 3 \\ -1 & 4 \end{pmatrix} \equiv \begin{pmatrix} -2 & -5 \\ -1 & -4 \end{pmatrix} K \pmod{32} \qquad K = \begin{pmatrix} -2 & -5 \\ -1 & -4 \end{pmatrix}^{-1} \begin{pmatrix} -2 & 3 \\ -1 & 4 \end{pmatrix}$$

$$\det \begin{pmatrix} -2 & -5 \\ -1 & -4 \end{pmatrix} \equiv 3 \qquad \begin{pmatrix} -2 & -5 \\ -1 & -4 \end{pmatrix}^{-1} \equiv 11 \begin{pmatrix} -4 & 5 \\ 1 & -2 \end{pmatrix} \pmod{32} \qquad 3^{-1} \equiv 11 \pmod{32}$$

$$\equiv \begin{pmatrix} 20 & 23 \\ 11 & 10 \end{pmatrix}$$

$$K = \begin{pmatrix} 20 & 23 \\ 11 & 10 \end{pmatrix} \begin{pmatrix} -2 & 3 \\ -1 & 4 \end{pmatrix} \equiv \begin{pmatrix} 1 & 24 \\ 0 & 9 \end{pmatrix} \pmod{32}$$

$\det K = 9 \qquad \mathrm{mcd}(9, 32) = 1 \Rightarrow \exists\, K^{-1}$

$$B = C_1 - P_1 K \equiv (1\ 5) - (1\ 3)\begin{pmatrix} 1 & 24 \\ 0 & 9 \end{pmatrix} \equiv (1\ 5) - (1\ 19) \equiv (0\ 18) \pmod{72}$$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni

V Appello d'Esame 2013-14 – 1 settembre 2014

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 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 E5 / E9 in GF(2^8) eseguendo tutte le operazioni sulle rappresentazioni polinomiali degli elementi e applicando l'Algoritmo di Euclide Esteso per calcolare l'inverso. Esprimere il risultato finale con la notazione Ek.

$E9 \triangleq a(x) = x^3+1$

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

$q_1(x) = x^5+x^2+x+1$

$r_2(x) = x^2$

$x^8+x^4+x^3+x+1 \;\big|\; x^3+1$

x^8+x^3

x^5+x^2+x+1

$x^5+x^4+x^3+x+1$

x^5+x^2

$x^4+x^3+x^2+x+1$

x^4+x

x^3+x^2+1

x^3+1

x^2

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

$q_2(x) = x$

$r_2(x) = 1$

$x^3+1 \;\big|\; x^2$

x^3 | x

1

$X_0 = 0 \quad X_1 = 1$

$X_2 = -q_1(x) X_1 + X_0 = x^5 + x^2 + x + 1$

$X_3 = -q_2(x) X_2 + X_1 = x^6 + x^3 + x^2 + x + 1$

In binario: $01001111 = E7g$

$E5/Eg = E5 \cdot E7g = (x^2+1)(x^6+x^3+x^2+x+1)$

$= x^8 + x^6 + x^5 + x^4 + x + 1 \equiv x^6 + x^5 + x^3$ (mod $m(x)$)

$= 01101000 = E104$

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) Ricavare la sequenza binaria pseudo-casuale generata dall'algoritmo *Blum-Blum-Shab* per $p = 19$, $q = 31$, $x = 9$ e determinarne il periodo P. *(2 punti)*

i	x_i	b_i
0	81	1
1	82	0
2	245	1
3	536	0
4	453	1
5	237	1
6	214	0
7	443	1
8	112	0
9	175	1
10	586	0
11	9	1
12	81	1

$P = 12$

2) Quali informazioni contiene un *certificato di identità* di una PKI? Cosa garantisce? Con che chiave l'utente verifica la validità della firma di un certificato ricevuto? Se la firma risulta valida, mi posso fidare delle informazioni garantite dal certificato? *(3 punti)*

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

4) Descrivere il funzionamento di un *firewall* realizzato per mezzo di un *application proxy*. *(3 punti)*

5) Enunciare il *Teorema Cinese del Resto*. *(2 punti)*