Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni **VI Appello d'Esame 2014-15 – 22 settembre 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) (5 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 103$, $\alpha = 5$, $\beta = \alpha^a \bmod p = 84$, 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:

$A_1 = (r_1, s_1) = (45, 59)$ $P_1 = 50$
$A_2 = (r_2, s_2) = (45, 91)$ $P_2 = 51$
$A_3 = (r_3, s_3) = (45, 19)$ $P_3 = 52$

Verificare che le tre firme siano valide.

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

A_1 $\left| \begin{array}{l} 84^{45} 45^{59} \equiv 41 \\ 7^{50} \equiv 41 \end{array} \right\} \Rightarrow$ OK $\pmod{103}$

A_2 $\left| \begin{array}{l} 84^{45} 45^{91} \equiv 58 \\ 7^{51} \equiv 102 \end{array} \right\} \Rightarrow$ NO

A_3 $\left| \begin{array}{l} 84^{45} 45^{19} \equiv 98 \\ 7^{52} \equiv 98 \end{array} \right\} \Rightarrow$ 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*).

$P_1 = 50 \quad A_1 = (45, 59)$

$P_3 = 52 \quad A_3 = (45, 19)$

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

$$\begin{cases} 59k \equiv 50 - a45 \pmod{102} \\ 19k \equiv 52 - a45 \pmod{102} \end{cases}$$

$40k \equiv 100 \pmod{102} \quad mcd(40, 102) = 2 \Rightarrow 2$ soluzioni

$20k \equiv 50 \pmod{51} \quad 20^{-1} \equiv 23 \pmod{51}$

$k_0 = 23 \cdot 50 \bmod 51 = 28$

$k_1 = k_0 + 51 = 79$

Dai dati pubblici: $r = \alpha^k \bmod p$

$5^{28} \bmod 103 = 58$

$5^{79} \bmod 103 = 45 \Rightarrow$ **$k = 79$**

$19 \cdot 79 \equiv 52 - a45 \pmod{102}$

$45a \equiv 81 \pmod{102} \quad mcd(45, 102) = 3 \Rightarrow 3$ soluzioni

$15a \equiv 27 \pmod{34} \quad 15^{-1} \equiv 25 \pmod{34}$

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

Matricola:

$a_0 = 29$

$a_1 = a_0 + 34 = 63$

$a_2 = a_0 + 2 \cdot 34 = 97$

Dai dati pubblici: $\beta = \alpha^a \bmod p$

$5^{29} \bmod 103 = 84 \Rightarrow (a = 29)$

Domanda 2

(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 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).

Calcolare il prodotto degli elementi E32 × E223 in GF(2^8) eseguendo tutte le operazioni sulle loro rappresentazioni binarie.

Meglio calcolare E223 × E32

E223 = 11011111

E32 = 00100000

M = 100011011

X_0 = E223 = 11011111

$X_1 = (11011111) \cdot (00000010) = 110111110$

100011011

10100101

$X_2 = (10100101) \cdot (\quad\quad) = 101001010$

100011011

01010001

$X_3 = (01010001) \cdot (\quad\quad) =$ 10100010

$X_4 = (10100010) \cdot (\quad\quad) = 101000100$

100011011

01011111

$X_5 = (01011111) \cdot (\quad\quad) = 10111110$

$E223 \times E32 = X_5 = 10111110 = E190$

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

Matricola:

Domanda 3

(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 $p = 571$. Gli identificativi pubblici dei tre utenti sono rispettivamente $r_A = 11$, $r_B = 22$, $r_C = 33$.

a) Per i tre utenti, TA sceglie e tiene segreti $a = 100$, $b = 200$, $c = 300$. Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$a_A = a + b r_A \bmod p = 16$ $\quad a_B = a + b r_B \bmod p = 503$ $\quad a_C = a + b r_C \bmod p = 419$

$b_A = b + c r_A \bmod p = 74$ $\quad b_B = b + c r_B \bmod p = 519$ $\quad b_C = b + c r_C \bmod p = 393$

$g_A(x) = a_A + b_A x$ $\quad K_{AB} = g_A(r_B) = 502$

$g_B(x) = a_B + b_B x$ $\quad K_{AC} = g_A(r_C) = 174$

$g_C(x) = a_C + b_C x$ $\quad K_{BC} = g_B(r_C) = 500$

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 $a_A = 440$, $b_A = 141$, $a_B = 210$, $b_B = 251$.
- Calcolare i parametri segreti a, b, c.
- Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$$\begin{cases} a_A = a + b11 \bmod 571 = 440 & b \equiv 31 \pmod{571} \\ a_B = a + b22 \bmod 571 = 210 & a \equiv 99 \ (\text{—}) \\ b_A = b + c11 \bmod 571 = 141 & c \equiv 10 \ (\text{—}) \end{cases}$$

$$11\,b \equiv 341 \pmod{571} \qquad 11^{-1} \equiv 52 \pmod{571}$$

$$b \equiv 31$$

$$a \equiv 210 - 31 \cdot 22 \equiv 99 \pmod{571}$$

$$c \equiv (141 - 31)\,52 \equiv 10 \pmod{571}$$

$$K_{AB} = 116$$

$$K_{AC} = 525$$

$$K_{BC} = 499$$

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

Matricola:

Domanda 4

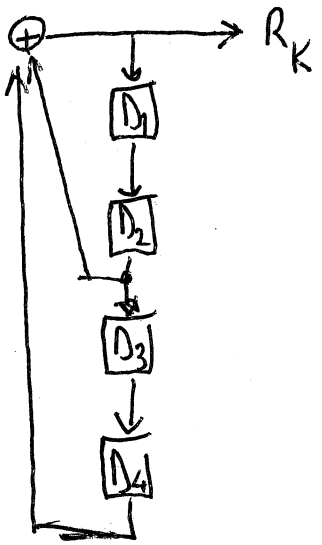
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Si disegni lo schema di uno *scrambler autosincronizzante* avente polinomio caratteristico $P(x) = 1+x^2+x^4$, alimentato con tutti "0" e utilizzato come generatore di sequenza PRBS. Si indichino la sequenza binaria in ingresso con $\{I_k\} \equiv \{0\}$ e la sequenza binaria in uscita con $\{R_k\}$.

b) Si inizializzi lo scrambler con tutti "1" negli elementi di ritardo D_i. Ricavare la sequenza PRBS $\{R_k\}$ generata all'uscita, evidenziando la sua periodicità. Qual è il periodo P della sequenza?

c) Verificare se il polinomio $P(x)$ è irriducibile.

a)



b)

Pass K	I_K	D_{1K}	D_{2K}	D_{3K}	D_{4K}	R_K
0	0	1	1	1	1	0
1	0	0	1	1	1	0
2	0	0	0	1	1	1
3	0	1	0	0	1	1
4	0	1	1	0	0	1
5	0	1	1	1	0	1
6	0	1	1	1	1	0
7	0					

$P=6$

c) $P(x) = 1 + x^2 + x^4$

Divisibile per x? NO

Divisibile per $(x+1)$ NO

$$x^4+x^2+1 \;\big|\; x+1$$
$$x^4+x^3 \quad\quad x^3+x^2$$
$$x^3+x^2+1$$
$$x^3+x^2$$
$$1$$

Riducibile ph x^2+x+1? SI

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

$\Rightarrow P(x)=(x^2+x+1)^2$ non irriducibile

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **VI Appello d'Esame 2014-15 – 22 settembre 2015**

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

Matricola:

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (**16** *punti*)

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

1) L'equazione $x^2 \equiv 17 \pmod{199}$ ha soluzione? Se la risposta è sì, calcolarne le radici, altrimenti risolvere $x^2 \equiv -17 \equiv 182 \pmod{199}$. *(2 punti)*

199 primo → l'eq. ha soluzione se $17^{\frac{199-1}{2}} \equiv 1 \pmod{199}$

$17^{99} \bmod 199 = -1 \Rightarrow$ NO

$199 \equiv 3 \pmod 4 \Rightarrow$ l'eq $x^2 \equiv -17 \pmod{199}$ ha radici

$x = \pm 17^{\frac{199+1}{4}} \bmod 199 = \pm 17^{50} \bmod 199 = \pm 111$

$\Rightarrow x_{1,2} \equiv \pm 111 \pmod{199}$

2) Un sergente mette i suoi soldati in fila su 10 colonne, ma ne avanza uno. Allora prova a metterli in fila su 11 colonne, ma ne avanzano due. Allora li manda tutti via, ordinando loro di farsi i conti da soli e di farsi trovare in fila la mattina dopo alle 4:00 in modo che non ne avanzi nessuno. La mattina dopo, i soldati attendono il sergente allineati su 3 colonne tutti sorridenti. Quanti sono? *(2 punti)*

$x = 1 + k10 \equiv 2 \pmod{11}$

$k10 \equiv 1 \pmod{11} \rightarrow k = 10$ $\qquad 10^{-1} \equiv 10 \pmod{11}$

$\Rightarrow x \equiv 1 + 100 \equiv 101 \pmod{110}$

$x = 101 + n110 \equiv 0 \pmod 3$

$2 + n \cdot 2 \equiv 0 \pmod 3$ $\qquad n2 \equiv 1 \pmod 3 \rightarrow n = 2$

$\Rightarrow x \equiv 321 \pmod{330}$

3) Descrivere il principio di un *cifrario a permutazione* su blocchi di *n* simboli. Si tratta di un cifrario mono- o poli-alfabetico? In cosa consiste la sua chiave? Quante sono le chiavi possibili, nel caso i simboli siano parole di 4 bit?*(2 punti)*

4) Cosa garantisce un'*Autorità di Certificazione*? Come mi garantisce che il certificato che mi presenta sia proprio suo?*(2 punti)*

5) Cos'è un *Bit Interleaved Parity (BIP) Code*? A che scopo è stato proposto? A che scopo mettere l'*interleaving*? Se lo utilizzo come *hash*, un BIP è o non è *unidirezionale* (resistente alla contro-immagine)? Perché? *(3 punti)*

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

Matricola:

6) Perché firmare l'*hash* del messaggio e non il messaggio originale? Perché utilizzare un *hash* di 16 bit non è una buona idea? Come realizzare un attacco a una firma su *hash* a 16 bit? *(2 punti)*

7) Descrivere le proprietà di *diffusione* e *confusione*, che secondo Claude Shannon un buon crittosistema dovrebbe avere per ostacolarne l'analisi. *(2 punti)*