# Mobilità e Sicurezza delle Reti

**Prof. Stefano Bregni** — **III Appello d'Esame 2014-15 – 3 luglio 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) (6 punti)*

a) Cos'è un *elemento primitivo* $\alpha \in \mathbb{Z}_p^*$?

b) Trovare ed elencare in ordine crescente i primi 4 elementi primitivi di $\mathbb{Z}_{31}^*$.

Test: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$

$\varphi(30) = 8$ elem. prim.

$\alpha = \{3, 11, 12, 13, \dots\}$

$2^{15} \equiv 1$, $2^{10} \equiv$, $2^6 \equiv$

$3^{15} \equiv 30$, $3^{10} \equiv 25$, $3^6 \equiv 16$

$4^{15} \equiv 1$, $4^{10} \equiv$, $4^6 \equiv$

$5^{15} \equiv 1$, $5^{10} \equiv$, $5^6 \equiv$

$6^{15} \equiv 30$, $6^{10} \equiv 25$, $6^6 \equiv 1$

$7^{15} \equiv 1$, $7^{10} \equiv$, $7^6 \equiv$

$8^{15} \equiv 1$, $8^{10}$, $8^6$

$9^{15} \equiv 1$, $9^{10}$, $9^6$

$10^{15} \equiv 1$, $10^{10} \equiv 11$, $10^6$

$11^{15} \equiv 30$, $11^{10} \equiv 5$, $11^6 \equiv 4$

$12^{15} \equiv 30$, $12^{10} \equiv 25$, $12^6 \equiv 2$

$13^{15} \equiv 30$, $13^{10} \equiv 5$, $13^6 \equiv 16$

c) Qual è l'*ordine* dell'elemento $\alpha = 6$?

$\mathrm{Ord}(6) = 6$

**Domanda 2**

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

Alice e Bob adottano un *sistema di firma cieca RSA*. Alice pubblica il modulo $n = 551$ e l'esponente di cifratura $e = 17$. Bob estrae il numero casuale segreto (*nonce*) $k = 12$ e chiede ad Alice di firmare ciecamente il messaggio $P = 500$.

a) Verificare la correttezza dei dati forniti secondo le ipotesi del metodo di firma cieca RSA.

b) Calcolare i messaggi scambiati da Alice e Bob e la firma $A$ del messaggio $P$.

a) $n = 551 = 19 \cdot 29$ $\varphi(n) = 504 = 2^3 \cdot 3^2 \cdot 7$ $\varphi[\varphi(n)] = 144$

$k \perp n$ ok $e \perp \varphi(n)$ ok

b) $d = e^{-1} \bmod \varphi(n) = 17^{143} \bmod 504 = 89$ (meglio Euclide Esteso) Ⓐ

Bob → Alice: $t = k^e P \bmod n = 12^{17} \cdot 500 \bmod 551 = 200$

Alice → Bob: $s = t^d \bmod n = 200^{89} \bmod 551 = 192$

Bob calcola la firma: $A = s/k \bmod n = 192 \cdot 46 \bmod 551 = 16$

dove $k^{-1} \bmod n = 12^{503} \bmod 551 \equiv 46 \pmod{551}$

(meglio Euclide Esteso) Ⓑ

Verifica: $A = P^d \bmod n = 500^{89} \bmod 551 = 16 = A$ calcolato come sopra

(A) $524 = 29 \cdot 17 + 11$ $\quad x_0 = 0 \quad x_1 = 1$

$17 = 1 \cdot 11 + 6$ $\quad x_2 = -29$

$11 = 1 \cdot 6 + 5$ $\quad x_3 = 30$

$6 = 1 \cdot 5 + 1$ $\quad x_4 = -59$

$5 = 5 \cdot 1 + 0$ $\quad x_5 = 89$

(B) $551 = 45 \cdot 12 + 11$ $\quad x_0 = 0 \quad x_1 = 1$

$12 = 1 \cdot 11 + 1$ $\quad x_2 = -45$

$11 = 11 \cdot 1 + 0$ $\quad x_3 = 46$

**Domanda 3**

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

Si consideri l'algoritmo di cifratura di Hill definito come

$$\mathbf{C}_i = \mathbf{P}_i \cdot \mathbf{K} + \mathbf{B} \mod 27$$

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

$$\mathbf{P} = [10 \quad 16 \quad 11 \quad 16 \quad 20 \quad 20] \qquad \mathbf{C} = [11 \quad 16 \quad 12 \quad 0 \quad 20 \quad 26]$$

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 $\mathbf{C}$?

$$\begin{cases} C_1 = P_1 K + B \\ C_2 = P_2 K + B \\ C_3 = P_3 K + B \end{cases} \qquad \begin{pmatrix} C_1 - C_3 \\ C_2 - C_3 \end{pmatrix} \equiv \begin{pmatrix} P_1 - P_3 \\ P_2 - P_3 \end{pmatrix} K \pmod{27}$$

$$\begin{pmatrix} 18 & 17 \\ 19 & 1 \end{pmatrix} \equiv \begin{pmatrix} 17 & 23 \\ 18 & 23 \end{pmatrix} K \pmod{27} \longrightarrow K = \begin{pmatrix} 17 & -4 \\ 18 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 18 & 17 \\ 19 & 1 \end{pmatrix}$$

$$\det \begin{pmatrix} 17 & -4 \\ 18 & -1 \end{pmatrix} = 4 \qquad \begin{pmatrix} 17 & 23 \\ 18 & 23 \end{pmatrix}^{-1} \equiv 7 \begin{pmatrix} 23 & 4 \\ 9 & 17 \end{pmatrix} \pmod{27} \qquad 4^{-1} \equiv 7 \pmod{27}$$

$$\equiv \begin{pmatrix} -1 & 1 \\ 9 & 11 \end{pmatrix}$$

$$K = \begin{pmatrix} -1 & 1 \\ 9 & 11 \end{pmatrix} \begin{pmatrix} 18 & 17 \\ 19 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 11 \\ 20 & 2 \end{pmatrix} \pmod{27}$$

$\det K = 25$ N.B. $\mathrm{mcd}(25, 27) = 1 \Rightarrow \exists\, K^{-1}$

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

**Matricola:**

$$B = C_1 - P_1 K \equiv (11\ 6) - (10\ 16)\begin{pmatrix} 1 & 11 \\ 20 & 2 \end{pmatrix} = (11\ 16) - (33\ 7) = (5\ 9)$$

**Domanda 4**

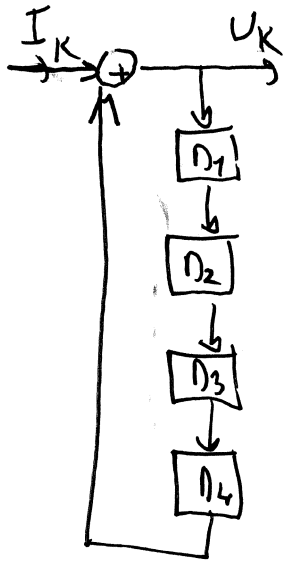
*(svolgere su questo foglio nello spazio assegnato) (5 punti)*

a) Si disegni lo schema di uno *scrambler autosincronizzante* avente polinomio caratteristico $P(x) = 1+x^4$. Si indichi la sequenza binaria in ingresso con $\{I_k\}$, la sequenza binaria in uscita con $\{U_k\}$.

b) Si inizializzi lo scrambler con tutti "1" negli elementi di ritardo $D_i$. Lo si alimenti con una sequenza dati composta da tutti "1" in ingresso. Ricavare la sequenza restituita all'uscita $\{U_k\}$, evidenziando la sua periodicità. Qual è il periodo $P$ della sequenza?

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

a)




b)

| Passo K | $I_k$ | $D_{1k}$ | $D_{2k}$ | $D_{3k}$ | $D_{4k}$ | $U_k$ | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 0 | |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | |
| 2 | 1 | 0 | 0 | 1 | 1 | 0 | |
| 3 | 1 | 0 | 0 | 0 | 1 | 0 | |
| 4 | 1 | 0 | 0 | 0 | 0 | 1 | |
| 5 | 1 | 1 | 0 | 0 | 0 | 1 | |
| 6 | 1 | 1 | 1 | 0 | 0 | 1 | |
| 7 | 1 | 1 | 1 | 1 | 0 | 1 | |
| 8 | 1 | 1 | 1 | 1 | 1 | 0 | $P=8$ |

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

- non divisibile per $x$
- divisibile per $x+1$
  → è divisibile

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

$$P(x) = (x+1)(x^3+x^2+x+1)$$

non irriducibile

**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)** Calcolare 3/55 mod 131 per mezzo dell'Algoritmo di Euclide Esteso. *(2 punti)*

| $k$ | $q_k \cdot r_{k-1} + r_k$ | $x_k$ |
|---|---|---|
| | | $x_0 = 0$ |
| 1 | $131 = 2 \cdot 55 + 21$ | $x_1 = 1$ |
| 2 | $55 = 2 \cdot 21 + 13$ | $x_2 = -2$ |
| 3 | $21 = 1 \cdot 13 + 8$ | $x_3 = 5$ |
| 4 | $13 = 1 \cdot 8 + 5$ | $x_4 = -7$ |
| 5 | $8 = 1 \cdot 5 + 3$ | $x_5 = 12$ |
| 6 | $5 = 1 \cdot 3 + 2$ | $x_6 = -19$ |
| 7 | $3 = 1 \cdot 2 + 1$ | $x_7 = 31$ |
| 8 | $2 = 2 \cdot 1 + 0$ | $x_8 = -50 \equiv 81$ |

$3 \cdot 55^{-1} \equiv 3 \cdot 81 \equiv 112 \pmod{131}$

**2)** Come è stata costruita la tabella S-Box nell'Algoritmo Rijndael? *(2 punti)*

**3)** Enunciare il *Teorema Cinese del Resto* generalizzato a $K$ congruenze. *(2 punti)*

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

**Matricola:**

**4)** Fare un esempio di *Linear Feedback Shift Register* utilizzato per generare una sequenza di bit pseudo-casuali. Quale può essere il periodo massimo della sequenza generata? *(2 punti)*

**5)** 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 i caratteri di un alfabeto di 26 caratteri? *(2 punti)*

**6)** Cosa è SHA? A cosa serve? Quale risultato producono SHA-1 e SHA-2? *(3 punti)*