Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni **I Appello d'Esame 2013-14 – 14 febbraio 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)

a) Trovare ed elencare in ordine crescente gli elementi primitivi di $\mathbb{Z}_{19}^*$.

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

$\varphi(18) = 6$ elem. primitivi

$\checkmark \begin{cases} 2^9 \equiv 18 \\ 2^6 \equiv 7 \end{cases}$ $\begin{cases} 8^9 \equiv \\ 8^6 \equiv \end{cases}$ $\times \begin{cases} 14^9 \equiv 18 \\ 14^6 \equiv 7 \end{cases}$

$\times \begin{cases} 3^9 \equiv 18 \\ 3^6 \equiv 7 \end{cases}$ $\begin{cases} 9^9 \equiv \\ 9^6 \equiv \end{cases}$ $\times \begin{cases} 15^9 \equiv 18 \\ 15^6 \equiv 11 \end{cases}$

$\Rightarrow \alpha = \{2, 3, 10, 13, 14, 15\}$

$\begin{cases} 4^9 \equiv \\ 4^6 \equiv \end{cases}$ * $\times \begin{cases} 10^9 \equiv 18 \\ 10^6 \equiv 11 \end{cases}$ $\begin{cases} 16^9 \equiv \\ 16^6 \equiv \end{cases}$

$\begin{cases} 5^9 \equiv 1 \\ 5^6 \equiv \end{cases}$ $\begin{cases} 11^9 \equiv 1 \\ 11^6 \equiv \end{cases}$ $\begin{cases} 17^9 \equiv \\ 17^6 \equiv \end{cases}$

$\begin{cases} 6^9 \equiv 1 \\ 6^6 \equiv \end{cases}$ $\begin{cases} 12^9 \equiv 18 \\ 12^6 \equiv 1 \end{cases}$

$\begin{cases} 7^9 \equiv 1 \\ 7^6 \equiv \end{cases}$ $\times \begin{cases} 13^9 \equiv 18 \\ 13^6 \equiv 11 \end{cases}$

b) Qual è l'*ordine* dell'elemento $\alpha = 11$?

$11^2 \equiv 7 \pmod{19}$

$11^3 \equiv 1 \Rightarrow Ord(11) = 3$

c) Qual è l'*ordine* dell'elemento $\alpha = 13$?

$\alpha = 13$ elem. prim. $\Rightarrow Ord(13) = 18$

d) Trovare ed elencare in ordine crescente i residui quadratici a_q dell'insieme $\mathbb{Z}_{19}^*$, cioè gli elementi $a \in \mathbb{Z}_{19}^* \mid$: $a \equiv (\pm b)^2$ (mod 19), con $b \in \mathbb{Z}_{19}^*$.

b	a_q
1	$1^2 \equiv 1$ (mod 19)
2	$2^2 \equiv 4$
3	$3^2 \equiv 9$
4	$4^2 \equiv 16$
5	$5^2 \equiv 6$
6	$6^2 \equiv 17$
7	$7^2 \equiv 11$
8	$8^2 \equiv 7$
9	$9^2 \equiv 5$

$a_q = \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$

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 $[P_{1i} \;\; P_{2i}]$;
K, **B** = chiave di cifratura, con

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

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

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

e ricavare la chiave **K**, **B**.

Per i valori ricavati di **K** e **B**, esiste un solo **C** che corrisponde a **P**? esiste un solo **P** che corrisponde a **C**?

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

$$\begin{pmatrix} -2 & 1 \\ -2 & 2 \end{pmatrix} \equiv \begin{pmatrix} 1 & -2 \\ 3 & -3 \end{pmatrix} K \pmod{16} \qquad K = \begin{pmatrix} 1 & -2 \\ 3 & -3 \end{pmatrix}^{-1} \begin{pmatrix} -2 & 1 \\ -2 & 2 \end{pmatrix}$$

$$\det \begin{pmatrix} 1 & -2 \\ 3 & -3 \end{pmatrix} = 3 \qquad \begin{pmatrix} 1 & -2 \\ 3 & -3 \end{pmatrix}^{-1} \equiv 11 \begin{pmatrix} -3 & 2 \\ -3 & 1 \end{pmatrix} \pmod{16} \qquad 3^{-1} \equiv 11 \pmod{16}$$

$$\equiv \begin{pmatrix} -1 & 6 \\ -1 & 11 \end{pmatrix}$$

$$K = \begin{pmatrix} -1 & 6 \\ -1 & 11 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ -2 & 2 \end{pmatrix} \equiv \begin{pmatrix} 2 & 0 \\ 4 & -1 \end{pmatrix} \equiv \begin{pmatrix} 6 & 11 \\ 12 & 5 \end{pmatrix} \pmod{16}$$

$\det K = 10$ NB: $\mathrm{mcd}(10, 16) = 2 \Rightarrow \nexists\, K^{-1}$

$$B = C_1 - P_1 K \equiv (1 \;\; 2) - (3 \;\; 2) \begin{pmatrix} 6 & 11 \\ 12 & 5 \end{pmatrix} \equiv (1 \;\; 2) - (10 \;\; 11) = (7 \;\; 7)$$

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

Matricola:

Domanda 3

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

Si consideri il campo GF(8) = $\mathbb{Z}_2(x)$ mod (x^3+x+1).

Si segua la notazione usuale: gli elementi Ek sono numerati con $k = 0, 1, ...$; l'indice k, espresso in forma binaria, rappresenta i coefficienti del polinomio corrispondente (bit più significativo = coefficiente di grado più alto).

a) Quanti sono gli elementi di GF(8)*? Giustificare la risposta.

7

b) Qual è l'ordine dell'elemento E5? Giustificare la risposta.

7

c) Verificare la risposta data al punto precedente, completando la seguente tabella:

$(E5)^1$	$(x^2+1)^1$	$\equiv$	x^2+1	E5
$(E5)^2$	$(x^2+1)^2$	$\equiv$	x^2+x+1	E7
$(E5)^3$	$(x^2+1)^3$	$\equiv$	x^2+x	E6
$(E5)^4$	$(x^2+1)^4$	$\equiv$	$x+1$	E3
$(E5)^5$	$(x^2+1)^5$	$\equiv$	x^2	E4
$(E5)^6$	$(x^2+1)^6$	$\equiv$	x	E2
$(E5)^7$	$(x^2+1)^7$	$\equiv$	1	E1
$(E5)^8$	$(x^2+1)^8$	$\equiv$		

d) Calcolare l'inverso dell'elemento E3 applicando l'Algoritmo di Euclide Esteso al polinomio corrispondente.

$E3 : x+1$

$a^{-1} \bmod b$

$a = x+1$

$b = x^3+x+1$

- $b = q_1 a + r_1$
- $a = q_2 r_1 + r_2$

~~

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

$$
\begin{array}{l|l}
x^3+x+1 & x+1 \\
\cline{2-2}
x^3+x^2 & x^2+x \\
\hline
x^2+x+1 & \\
x^2+x & \\
\hline
\quad 1 &
\end{array}
$$

$X_0 = 0 \quad X_1 = 1$

$X_2 = -q_1 X_1 + X_0 =$

$\boxed{= x^2+x} = a^{-1}(x)$

$E3^{-1} = E6$

Verifica: $(x+1)(x^2+x) = x^3 + \cancel{x^2} + \cancel{x^2} + \cancel{x} \equiv 1 \quad (\bmod (x^3+x+1))$

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

Matricola:

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 $p = 127$, $\alpha = 5$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 64$.

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 $\alpha = 6$ (da verificare). Se anche questa scelta non risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 110$ e spedisce il messaggio $P_1 = 12$. 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 $C_2 = (r_2, t_2) = (96, 13)$, $C_3 = (r_3, t_3) = (96, 121)$, $C_4 = (r_4, t_4) = (96, 62)$ e, per altra via, viene a sapere $P_2 = 25$. Calcolare P_3 e P_4.

a) p primo $1 \leq a \leq p-2$

Test se α elem. primitivo di $\mathbb{Z}_p^*$:

$p-1 = 126 = 2 \cdot 3^2 \cdot 7$

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

$$\left.\begin{array}{l} 5^{63} \equiv 126 \\ 5^{42} \equiv 1 \\ 5^{18} \equiv 64 \end{array}\right\} \Rightarrow \text{NO} \qquad \left.\begin{array}{l} 6^{63} \equiv 126 \\ 6^{42} \equiv 107 \\ 6^{18} \equiv 64 \end{array}\right\} \Rightarrow \text{OK} \quad (\alpha = 6)$$

$\beta = \alpha^a \bmod p = 6^{64} \bmod 127 = 121$

b) $r_1 = \alpha^K \bmod p = 6^{110} \bmod 127 = 72$

$t_1 = \beta^K P_1 \bmod p = 121^{110} \cdot 12 \bmod 127 = 102$

$C_1 = (72, 102)$

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

$t_2^{-1} \equiv 13^{125} \equiv 88 \pmod{127}$

$P_3 = P_2 \frac{t_3}{t_2} \bmod p = 121 \cdot 88 \cdot 25 \bmod 127 = 8$

$P_4 = P_2 \frac{t_4}{t_2} \bmod p = 62 \cdot 88 \cdot 25 \bmod 127 = 2$

Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni | **I Appello d'Esame 2013-14 – 14 febbraio 2014**

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) In una PKI, che informazioni contiene un *certificato di identità*? Con che chiave si verifica la validità della sua firma? Chi o cosa garantisce l'autenticità della firma verificata valida? *(2 punti)*

2) Descrivere le caratteristiche di un sistema Feistel. *(3 punti)*

3) Definire la proprietà di *unidirezionalità* di una funzione di hash. *(2 punti)*

4) Definire la proprietà *debolmente resistente alle collisioni* di una funzione di hash. Perché questa proprietà è più facile da soddisfare della proprietà *fortemente resistente alle collisioni*? *(2 punti)*

5) Come si può risolvere il problema di impedire i *replay attack* nei protocolli di *distribuzione di chiave simmetrica*? Illustrare in particolare il protocollo di *Needham-Schroeder*. *(3 punti)*