Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni **II Appello d'Esame 2014-15 – 2 marzo 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)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 199$, $\alpha = 7$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 56$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 7$ non risultasse una scelta valida, Bob userà invece $\alpha = 6$ (anch'esso da verificare). Se anche questa scelta non risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Bob estrae il numero casuale segreto (*nonce*) $k = 151$. Per questo valore di k, calcolare la firma $A = (r, s)$ del messaggio $P = 200$.

c) Verificare se anche la firma $A' = (r', s') = (44, 100)$ è valida per lo stesso messaggio $P = 200$.

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

Test se α elem. primitivo: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $\quad p-1 = 198 = 2 \cdot 3^2 \cdot 11$

$7^{66} \equiv 106$, $7^{99} \equiv 1$, $7^{18} \equiv 121$ $\Rightarrow$ $\alpha = 7$ NO

$6^{66} \equiv 92$, $6^{99} \equiv 198$, $6^{18} \equiv 63$ $\Rightarrow$ $\alpha = 6$ SI

tutti $\pmod{199}$

$\Rightarrow \alpha = 6$ elem. primitivo di $\mathbb{Z}_{199}^*$

$\beta = \alpha^a \bmod p = 6^{56} \bmod 199 = 126$

b) $r = \alpha^K \bmod p = 6^{151} \bmod 199 = 69$

$s = K^{-1}(P - qr) \bmod (p-1) = 139 \cdot (200 - 56 \cdot 69) \bmod 198 = 158$

$K^{-1} \bmod (p-1) = 151^{-1} \bmod 198 = 151^{59} \bmod 198 = 139$

Verifico: $151 \cdot 139 \bmod 198 = 1$ $\quad \varphi(198) = 60$

c) $\beta^r r^s \equiv \alpha^P \bmod p$

$$\left.\begin{aligned} 126^{44} \cdot 44^{100} \bmod 199 &= 36 \\ 6^{200} \bmod 199 &= 36 \end{aligned}\right\} \Rightarrow \text{OK}$$

Note: $A' = (44, 100)$ firma di $P = 200$ calcolata per $K = 13$)

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

Matricola:

Domanda 2

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

Si consideri il campo GF(16) = $\mathbb{Z}_2(x)$ mod (x^4+x^3+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).

a) Verificare se il polinomio $m(x) = x^4+x^3+1$ è irriducibile.

Div. X: NO

Div. $X+1$: NO

$x^4+x^3+1 \mid x+1$

$x^4+x^3 \mid x^3$

1

Div. X^2 NO

Div. X^2+1 NO

Div. X^2+X+1: NO

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

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

x^2+1

x^2+x+1

x

$\Rightarrow x^4+x^3+1$ irriducibile

b) Quale potrebbe essere l'ordine dell'elemento E5? Giustificare la risposta.

Al massimo $2^4-1=15$ (se E5 elem. generatore)

c) Verificare qual è effettivamente l'ordine dell'elemento E5 completando la seguente tabella:

$(E5)^1$	$(x^2+1)^1$	$\equiv$	x^2+1	E5
$(E5)^2$	$(x^2+1)^2$	$\equiv$	$x^4+1 \equiv x^3$	E8
$(E5)^3$	$(x^2+1)^3$	$\equiv$	$x^3(x^2+1) = x^5+x^3 \equiv x+1$	E3
$(E5)^4$	$(x^2+1)^4$	$\equiv$	$x^6 \equiv x^3+x^2+x+1$	E15
$(E5)^5$	$(x^2+1)^5$	$\equiv$	$x^3(x+1) \equiv x^4+x^3 \equiv 1$	E1 $\Rightarrow ord(x^2+1)=5$
$(E5)^6$	$(x^2+1)^6$	$\equiv$	x^2+1	E5
$(E5)^7$	$(x^2+1)^7$	$\equiv$		
$(E5)^8$	$(x^2+1)^8$	$\equiv$		
$(E5)^9$	$(x^2+1)^9$	$\equiv$		
$(E5)^{10}$	$(x^2+1)^{10}$	$\equiv$		
$(E5)^{11}$	$(x^2+1)^{11}$	$\equiv$		
$(E5)^{12}$	$(x^2+1)^{12}$	$\equiv$		
$(E5)^{13}$	$(x^2+1)^{13}$	$\equiv$		
$(E5)^{14}$	$(x^2+1)^{14}$	$\equiv$		
$(E5)^{15}$	$(x^2+1)^{15}$	$\equiv$		
$(E5)^{16}$	$(x^2+1)^{16}$	$\equiv$		
$(E5)^{17}$	$(x^2+1)^{17}$	$\equiv$		

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **II Appello d'Esame 2014-15 – 2 marzo 2015**

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

Matricola:

Domanda 3

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

Bob adotta il *sistema di cifratura a chiave pubblica RSA*. Pubblica il modulo $n = 8791$ e l'esponente di cifratura $e = 6243$.

a) Verificare la correttezza dei dati forniti in base alle ipotesi del metodo RSA.

b) Alice trasmette il messaggio cifrato $C = 10$. Calcolare il messaggio in chiaro P.

a) $n = 8791 = 59 \cdot 149$ (per tentativi) $\quad e = 6243 = 3 \cdot 2081$

$\varphi(n) = 8584 = 2^3 \cdot 29 \cdot 37 \quad e \perp \varphi(n)$ OK

$\varphi[\varphi(n)] = 4032$

b) $d = e^{-1} \bmod \varphi(n) = e^{\varphi[\varphi(n)]-1} \bmod \varphi(n) = 6243^{4031} \bmod 8584$

Meglio usare l'algoritmo di Euclide Esteso:

1	$8584 = 1 \cdot 6243 + 2341$	$x_0 = 0 \quad x_1 = 1$
2	$6243 = 2 \cdot 2341 + 1561$	$x_2 = -q_1 x_1 + x_0 = -1$
3	$2341 = 1 \cdot 1561 + 780$	$x_3 = -q_2 x_2 + x_1 = 3$
4	$1561 = 2 \cdot 780 + 1$	$x_4 = -q_3 x_3 + x_2 = -4$
5	$780 = 780 \cdot 1 + 0$	$x_5 = -q_4 x_4 + x_3 = 11$

$\Rightarrow d = 11$ Verifica: $6243 \cdot 11 \bmod 8584 = 1$

$P = C^d \bmod n = 10^{11} \bmod 8791 = 1430$

Domanda 4

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

a) Cos'è un *residuo quadratico* dell'insieme $\mathbb{Z}_p^*$?

b) Dopo avere calcolato tutti i residui quadratici a_q dell'insieme $\mathbb{Z}_{19}^*$, dire quali sono le radici quadrate di -2 (mod 19).

b	a_q
1	$1^2 \equiv 1 \pmod{19}$
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	$9^2 \equiv 5$

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

$\sqrt{17} \equiv \sqrt{-2} \equiv \pm 6 \equiv \{6, 13\}$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni

II Appello d'Esame 2014-15 – 2 marzo 2015

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) Determinare se l'equazione $x^2 \equiv -971 \pmod{997}$ ha soluzione, tramite il calcolo del simbolo di Legendre corrispondente. *(2 punti)*

p = 997 primo a = 971 primo

$$\left(\frac{971}{997}\right) = \left(\frac{997}{971}\right) = \left(\frac{26}{971}\right) = \left(\frac{2}{971}\right)\left(\frac{13}{971}\right) = (-1)\left(\frac{9}{13}\right) = -\left(\frac{13}{9}\right) = -\left(\frac{4}{9}\right) =$$

$$= -\left(\frac{4}{3}\right)^2 = -1 \Rightarrow \text{l'eq. ha soluzione}$$

2) Descrivere la procedura di cifratura di un flusso di byte in chiaro $\{p_i\}$ basata sull'applicazione iterativa di una funzione di hash $h(x)$ secondo una modalità analoga a OFB. *(2 punti)*

3) Definire il problema del Logaritmo Discreto in un campo finito GF(p^n). *(2 punti)*

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

5) Si considerino le funzioni di cifratura doppia $C = E_{K_2}(E_{K_1}(P))$ e decifratura $P = D_{K_1}(D_{K_2}(C))$ con due chiavi K_1 e K_2 ciascuna di lunghezza n bit. *(5 punti)*

- Può esistere una terza chiave K_3 tale che la cifratura doppia $C = E_{K_2}(E_{K_1}(P))$ sia equivalente a una cifratura singola $C = E_{K_3}(P)$? Spiegare un esempio in cui questo avviene e un esempio in cui questo non avviene.

- Supponiamo di avere intercettato una coppia P, C di messaggi rispettivamente in chiaro e cifrato doppio secondo il sistema sopraindicato. Descrivere la procedura di un attacco *Meet-in-the-Middle* per trovare la coppia di chiavi K_1, K_2. Quanti calcoli sono necessari?