Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **II Appello d'Esame 2012-13 – 11 luglio 2013**

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 cifratura a chiave pubblica RSA*. Pubblica il modulo $n = 323$ e l'esponente di cifratura $e = 17$.

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

b) Alice trasmette il messaggio cifrato $C = 55$. Calcolare il messaggio in chiaro P.

c) Alice vuole inviare il messaggio in chiaro $P = 55$. Calcolare il corrispondente messaggio cifrato C.

a) $n = 323 = 17 \cdot 19$ $\varphi(n) = 288 = 2^5 3^2$ $e \perp \varphi(n)$ OK

$\varphi[\varphi(n)] = 96$

b) $d = e^{-1} \bmod \varphi(n) = e^{\varphi[\varphi(n)]-1} \bmod \varphi(n) = 17^{95} \bmod 288 = 17$

Verifica: $17 \cdot 17 \bmod 288 = 1$ ok

$P = C^d \bmod n = 55^{17} \bmod 323 = 123$

c) $C = P^e \bmod n = 55^{17} \bmod 323 = 123$

Domanda 2

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

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 113$, $\alpha = 6$, $\beta = \alpha^a \bmod p = 37$, tenendo segreto l'esponente a ($1 < a \leq p\text{-}2$).

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

b) Bob estrae il numero casuale segreto k (*nonce*) ($k \perp p\text{-}1$). Usando entrambe le volte questo stesso valore di k, Bob calcola le firme $A_1 = (r_1, s_1) = (55, 62)$ e $A_2 = (r_2, s_2) = (55, 39)$, rispettivamente dei messaggi $P_1 = 7$ e $P_2 = 48$. Oscar intercetta A_1 e A_2. Calcolare k e a (*attacco del nonce ripetuto*).

a) $p = 113$ primo

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

$p - 1 = 112 = 2^4 \cdot 7$

$6^{56} \equiv 112 \pmod{113}$
$6^{16} \equiv 30 \pmod{113}$
$\Rightarrow$ OK $\alpha = 6$ elem. primitivo di $\mathbb{Z}_{113}^*$

$\beta = 6^a \bmod 113 = 37$

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

$\begin{cases} 62 \cdot k \equiv 7 - a55 \pmod{112} \\ 39 \cdot k \equiv 48 - a55 \pmod{112} \end{cases}$

$23^{-1} \bmod 112 = 23^{47} \bmod 112 = 39$

$23 \perp 112$

$k \cdot 23 \equiv 71 \pmod{112} \rightarrow k = 23^{-1} \cdot 71 \bmod 112 = (81)$

$a55 \equiv 7 - 62 \cdot 81 \equiv 25 \pmod{112}$

$\rightarrow a = 55^{-1} \cdot 25 \bmod 112 = (31)$

$55^{-1} \bmod 112 = 55^{47} \bmod 112 = 55$

$55 \perp 112$

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

Matricola:

Domanda 3

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

Si consideri il campo GF(2^8) = $\mathbb{Z}_2(x)$ mod ($x^8+x^4+x^3+x+1$).

a) Calcolare l'inverso dell'elemento $a(x) = x^3+1$ in GF(2^8) applicando l'Algoritmo di Euclide Esteso.

b) Verificare il risultato ottenuto moltiplicando $a(x) \cdot a^{-1}(x)$.

c) Tutti i polinomi che $\in$ GF(2^8) hanno un inverso? Perché?

a)

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

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

$r_1(x) = x^2$

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

$x^8 + x^5$ → $x^5 + x^2 + x + 1$

$x^8 + x^4 + x^3 + x + 1$

$x^5 + x^2$

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

$x^4 + x$

$x^3 + x^2 + 1$

$x^3 + 1$

x^2

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

$q_2(x) = x$

$r_2(x) = 1$

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

x^3 → x

1

$X_0 = 0 \quad X_1 = 1$

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

$X_3 = -q_2(x) X_2 + X_1 = x(x^5 + x^2 + x + 1) + 1 = x^6 + x^3 + x^2 + x + 1 = q^{-1}(x)$

b) Verifica: $(x^6 + x^3 + x^2 + x + 1)(x^3 + 1) = x^9 + x^5 + x^4 + x^2 + x + 1 \equiv$

$\equiv 1 \mod m(x)$

$$\begin{array}{l|l} x^9 + x^5 + x^4 + x^2 + x + 1 & x^8 + x^4 + x^3 + x + 1 \\ \hline x^9 + x^5 + x^4 + x^2 + x & x \\ \hline 1 & \end{array}$$

c) (vedi libro) Si tratta di ϕ

Domanda 4

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

La *Trusted Authority* TA adotta lo *Schema di Blom* per distribuire chiavi simmetriche a tre utenti A, B e C e pubblica $p = 227$. Gli identificativi pubblici dei tre utenti sono rispettivamente $r_A = 100$, $r_B = 101$, $r_C = 102$.

a) Per i tre utenti, TA sceglie e tiene segreti $a = 10$, $b = 15$, $c = 50$. Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$a_A = a + b r_A \bmod p = 148$ $a_B = a + b r_B \bmod p = 163$ $a_C = a + b r_C \bmod p = 178$

$b_A = b + c r_A \bmod p = 21$ $b_B = b + c r_B \bmod p = 71$ $b_C = b + c r_C \bmod p = 121$

$g_A(x) = a_A + b_A x$ $K_{AB} = g_A(r_B) = 226$

$g_B(x) = a_B + b_B x$ $K_{AC} = g_A(r_C) = 20$

$g_C(x) = a_C + b_C x$ $K_{BC} = g_B(r_C) = 141$

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 $a_A = 22$, $a_B = 88$, $b_A = 205$, $b_B = 77$.
- Calcolare i parametri segreti a, b, c.
- Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$$a_A = \begin{cases} a + b\,100 \bmod 227 = 22 \\ a + b\,101 \bmod 227 = 88 \\ b + c\,100 \bmod 227 = 205 \end{cases}$$

$a + b\,100 \bmod 227 = 22 \rightarrow b \equiv 66 \pmod{227}$

$a + b\,101 \bmod 227 = 88 \nearrow \quad a \equiv 5 \pmod{227}$

$100^{-1} \bmod 227 = 100^{225} \bmod 227 = 84$

$c \cdot 100 \equiv 139 \pmod{227}$

$c = 139 \cdot 84 \bmod 227 = 99 \rightarrow c \equiv 99 \pmod{227}$

$K_{AB} = 70$

$K_{AC} = 48$

$K_{BC} = 224$

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (14 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

---

1) Esprimere la definizione di *Simbolo di Legendre*. Calcolare $\left(\frac{100}{223}\right)$. *(2 punti)*

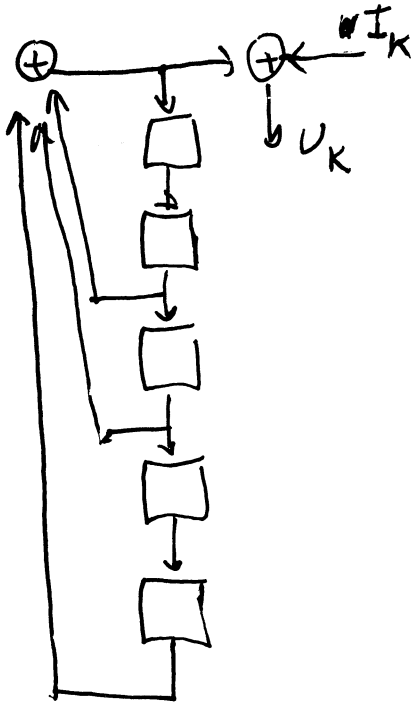
$\left(\frac{q}{p}\right) = \begin{cases} +1 & \text{se } x^2 \equiv q \pmod p \text{ ha soluzione} \\ -1 & \text{se } x^2 \equiv q \pmod p \text{ non ha soluzione} \end{cases}$

$\left(\frac{100}{223}\right) \equiv 100^{111} \pmod{223}$ 223 primo $100 \not\equiv 0 \pmod{223}$

$100^{111} \bmod 223 = 1$

---

2) Si disegni lo schema di uno *scrambler additivo* avente polinomio caratteristico $1+x^2+x^3+x^5$. Quale sarà al massimo il periodo della sequenza PRBS generata avendo tutti "0" all'ingresso? *(2 punti)*



$P = 2^5 - 1 = 31$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **II Appello d'Esame 2012-13 – 11 luglio 2013**

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

Matricola:

3) Calcolare 8751423^{65536} mod 131072. *(2 punti)*

$a^{\varphi(n)} \equiv 1 \pmod{n}$ se $a \perp n$

$\varphi(2^{17}) = 2^{16}$ $a \perp n$ perché a dispari e non multiplo di n

$\Rightarrow = 1$

4) Si considerino le funzioni Doppio-DES di cifratura $C = E_{K_2}(E_{K_1}(P))$ e decifratura $P = D_{K_1}(D_{K_2}(C))$ con due chiavi K_1 e K_2 ciascuna di lunghezza n bit. *(4 punti)*

- Esiste una terza chiave K_3 tale che la cifratura DES doppia $C = E_{K_2}(E_{K_1}(P))$ sia equivalente a una cifratura DES singola $C = E_{K_3}(P)$?

no

Supponiamo di avere intercettato una coppia P, C di messaggi rispettivamente in chiaro e cifrato Doppio-DES.

- In cosa consiste l'attacco a forza bruta per trovare la coppia K_1, K_2? Quanti calcoli sono necessari?

max 2^{2n} tentativi

- Si descriva l'attacco *Meet-in-the-Middle* per trovare la coppia K_1, K_2. Quanti calcoli sono necessari?

max $2 \cdot 2^n$ tentativi $= 2^{n+1}$

5) Si descriva lo *Schema di Lamport* per l'autenticazione di un host A da parte di un server B. Quale informazione è pubblica? Quale informazione è memorizzata (privata) in A? Quale informazione è memorizzata (privata) in B?*(4 punti)*