Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **III Appello d'Esame 2013-14 – 4 luglio 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)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 181$, $\alpha = 7$, $\beta = \alpha^a \bmod p$, 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 $\alpha = 10$ (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*) $k = 23$. Per questo valore di k, calcolare la firma $A = (r, s)$ del messaggio $P = 11$.

c) Verificare se anche la firma $A' = (r', s') = (112, 57)$ è valida per lo stesso messaggio $P = 11$.

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

Tst se α elem. primitivo: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $\quad p-1 = 180 = 2^2 \cdot 3^2 \cdot 5$

$7^{10} \equiv 180 \pmod{181}$
$7^{60} \equiv 1 \quad (\ \ )$
$7^{36} \equiv 1 \quad (\ \ )$
$\Rightarrow \alpha = 7$ NO

$10^{10} \equiv 180$
$10^{60} \equiv 48$
$10^{36} \equiv 42$
$\Rightarrow \alpha = 10$ OK

$\Rightarrow \alpha = 10$ elem. prim. di $\mathbb{Z}_{181}^*$

$\beta = \alpha^a \bmod p = 10^{56} \bmod 181 = 170$

b) $r = \alpha^k \bmod p = 10^{23} \bmod 191 = 57$

$s = k^{-1}(P - ar) \bmod (p-1) = 47 \cdot (11 - 56 \cdot 57) \bmod 190 = 73$

$k^{-1} \bmod (p-1) = 23^{-1} \bmod 190 = 23^{47} \bmod 190 = 47$

Verifica: $23 \cdot 47 \bmod 190 = 1$ $\quad \varphi(190) = 48$

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

$$\left.\begin{aligned} 170^{112} \cdot 112^{57} \bmod 191 &= 153 \\ 10^{11} \bmod 191 &= 153 \end{aligned}\right\} \Rightarrow \text{OK}$$

(Nota: $A' = (112, 57)$ firma di $P = 11$ calcolata con $K = 7$)

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

Matricola:

Domanda 2

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

Bob adotta il *sistema di cifratura a chiave pubblica RSA*. Pubblica il modulo $n = 2867$ e l'esponente di cifratura $e = 677$.

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

b) Alice trasmette il messaggio cifrato $C = 16$. Calcolare il messaggio in chiaro P.

a) $n = 2867 = 47 \cdot 61$ (primalità, fonte bonta)

$\varphi(n) = 2760 = 2^3 \cdot 3 \cdot 5 \cdot 23$ $\quad e \perp \varphi(n)$ OK

$\varphi[\varphi(n)] = 704$

b) $d = e^{-1} \bmod \varphi(n) = e^{\varphi[\varphi(n)]-1} \bmod \varphi(n) = 677^{703} \bmod 2760$

Meglio algoritmo Euclide Esteso:

$2760 = 4 \cdot 677 + 52$

$677 = 13 \cdot 52 + 1$

$52 = 52 + 1 + 0$

$x_0 = 0 \quad x_1 = 1$

$x_2 = -q_1 x_1 + x_0 = -4$

$x_3 = -q_2 x_2 + x_1 = 53 \Rightarrow d = 677^{-1} \bmod 2760 = 53$

Verifica: $53 \cdot 677 \bmod 2760 = 1$

$P = C^d \bmod n = 16^{53} \bmod 2867 = 972$

Domanda 3

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

Si consideri l'algoritmo di cifratura di Hill definito come

$$\mathbf{C}_i = \mathbf{P}_i \cdot \mathbf{K} + \mathbf{B} \mod 256$$

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

$$\mathbf{K} = \begin{bmatrix} 11 & 22 \\ 33 & 55 \end{bmatrix} \qquad \mathbf{B} = [50 \quad 100].$$

a) Verificare che la chiave sia valida.

b) Se possibile, decifrare il messaggio $\mathbf{C} = [100\ \ 101]$.

a) $\det(K) = 605 - 726 \bmod 256 \equiv 135$ $\perp 256$ ok $\exists K^{-1}$

b) $P = (C-B)K^{-1}$

$$K^{-1} = \frac{1}{135}\begin{pmatrix} 55 & -22 \\ -33 & 11 \end{pmatrix} \equiv \begin{pmatrix} 209 & 70 \\ 233 & 93 \end{pmatrix} \pmod{256}$$

$$135^{-1} \bmod 256 = 135^{127} \bmod 256 \equiv 55 \pmod{256}$$

Verifico $55 \cdot 135 \equiv 1 \pmod{256}$

$$P = (100-50 \quad 101-100)\begin{pmatrix} 209 & 70 \\ 233 & 93 \end{pmatrix} \equiv (50 \quad 1)\begin{pmatrix} 209 & 70 \\ 233 & 93 \end{pmatrix} \equiv (187 \quad 9) \pmod{256}$$

Verifica: $PK + B = (187\ 9)\begin{pmatrix} 11 & 22 \\ 33 & 55 \end{pmatrix} + (50\ 100) = (100\ 101) = C$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni
III Appello d'Esame 2013-14 – 4 luglio 2014

Cognome e nome:
(stampatello)
(firma leggibile)

Matricola:

Domanda 4
(svolgere su questo foglio nello spazio assegnato) (6 punti)

a) Cos'è una funzione di *hash*? A cosa serve? Cosa accetta in ingresso? Cosa produce in uscita?

b) Definire la proprietà di *unidirezionalità* di una funzione di hash.

c) Definire la proprietà *fortemente resistente alle collisioni* di una funzione di hash.

d) Definire la proprietà *debolmente resistente alle collisioni* di una funzione di hash. Giustificare il fatto che questa proprietà è più facile da soddisfare della proprietà *fortemente resistente alle collisioni*.

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) Esprimere la definizione di *Simbolo di Legendre*. Calcolare $\left(\frac{221}{223}\right)$. *(2 punti)*

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

$\left(\frac{221}{223}\right) = \left(\frac{-2}{223}\right) = (-2)^{111} \bmod 223 = -1$ (111 dispari)

2) Descrivere un attacco del compleanno che miri a firmare validamente un documento fraudolento. *(3 punti)*

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni

III Appello d'Esame 2013-14 – ~~16~~ 4 luglio 2014

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

Matricola:

3) Applicando il Teorema Cinese del Resto, trovare la congruenza equivalente a *(2 punti)*

$$\begin{cases} x \equiv 6 \pmod{15} \\ x \equiv 15 \pmod{16} \end{cases}$$

verificando le ipotesi.

$15 \nmid 16 \Rightarrow \exists$ la soluzione

$x = 6 + k15 \equiv 15 \pmod{16}$

$k15 \equiv 15 - 6 \pmod{16}$

$k \equiv 9 \cdot 15^{-1} \pmod{16}$

$15^{-1} \bmod 16 = 15^{\varphi} \bmod 16 = 15$

$k \equiv 9 \cdot 15 \pmod{16} \equiv 7$

$\Rightarrow x \equiv 6 + 7 \cdot 15 \pmod{15 \cdot 16}$

$x \equiv 111 \pmod{240}$

4) Siano noti $n = p \cdot q = 314869$ (prodotto di due primi distinti p, q) e $\varphi(n) = 313740$. Calcolare p e q. *(2 punti)*

$(x-p)(x-q) \equiv x^2 - (p+q)x + pq = 0$

$n - \varphi(n) + 1 = p + q$

$x^2 - 1130x + 314869 = 0$

$p, q = \dfrac{1130 \pm \sqrt{1130^2 - 4 \cdot 314869}}{2} = \begin{cases} 499 \\ 631 \end{cases}$

5) 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. *(3 punti)*

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

- Descrivere la procedura di un attacco a forza bruta per trovare la coppia di chiavi K_1, K_2. Quanti calcoli sono necessari?

max 2^{2n} tentativi

- Descrivere la procedura di un attacco *Meet-in-the-Middle* per trovare la coppia di chiavi K_1, K_2. Quanti calcoli sono necessari?

max $2 \cdot 2^{n}$ tentativi