Sicurezza delle Reti

Prof. Stefano Bregni — **IV Appello d'Esame 2018-19 – 21 gennaio 2020**

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) (7 punti)

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 139$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 129$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 3$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{4, 5\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 64$ e spedisce il messaggio $P = 28$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob riceve $C' = (r', t') = (36, 6)$. Calcolare il messaggio decifrato da Bob P'.

d) Calcolare per quale valore di k Alice ha calcolato $C' = E[P']$.

a) p primo $1 < a \leq p-2$ $p-1 = 138 = 2 \cdot 3 \cdot 23$ Tutti gli α elem. primi di $\mathbb{Z}_p^*$

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

$3^{69} \equiv 138$
$3^{46} \equiv 42$
$3^{6} \equiv 34$
$\Rightarrow$ $\alpha = 3$ ($\alpha = 4, 5$ No) OK

$\beta = \alpha^a \bmod p = 3^{129} \bmod 139 = 48$

b) $r = \alpha^k \bmod p = 3^{64} \bmod 139 = 4$

$t = \beta^k P \bmod p = 48^{64} \cdot 28 \bmod 139 = 25$ $\Rightarrow$ $C = (4, 25)$

c) $C' = (r', t') = (36, 6)$

$P' = t' \cdot r'^{-a} \bmod p = 6 \cdot 36^{9} \bmod 139 = 34$

d) $3^k \bmod 139 = 36$ $\rightarrow$ $k = 66$ (B565)

Domanda 2

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

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 109$, $\alpha = 6$, $\beta = \alpha^a \bmod p = 10$, tenendo segreto l'esponente a ($1 < a \leq p\text{-}2$).

a) Bob estrae il numero casuale segreto k (*nonce*) ($k \perp p\text{-}1$). Usando sempre questo stesso valore di k, Bob calcola le seguenti firme A_k per i rispettivi messaggi P_k:

$A_1 = (r_1, s_1) = (56, 61)$ $P_1 = 15$
$A_2 = (r_2, s_2) = (56, 61)$ $P_2 = 20$
$A_3 = (r_3, s_3) = (56, 103)$ $P_3 = 21$

Verificare che le tre firme siano valide.

$\beta^r r^s \equiv \alpha^P \pmod p$

A_1 | $10^{56}\ 56^{61} \equiv 77$; $6^{15} \equiv 77$ $\Rightarrow$ OK

A_3 | $10^{56}\ 56^{103} \equiv 90$; $6^{21} \equiv 90$ $\Rightarrow$ OK

A_2 | $10^{56}\ 56^{61} \equiv 77$; $6^{20} \equiv 15$ $\Rightarrow$ NO

b) Oscar intercetta i tre messaggi (P_k, A_k). Sulla base delle sole firme verificate valide, calcolare k e a (*attacco del nonce ripetuto*).

$P_1 = 15 \quad A_1 = (56,61)$

$P_2 = 21 \quad A_2 = (56,103)$

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

$$\begin{cases} 61k \equiv 15 - a56 \pmod{108} \\ 103k \equiv 21 - a56 \pmod{108} \end{cases}$$

$42k \equiv 6 \pmod{108} \quad MCD(42,108) = 6 \Rightarrow$ 6 soluzioni

$k_0 \equiv 13 \pmod{18}$

$\Rightarrow k_i \equiv 13, 31, 49, 67, 85, (103) \pmod{108}$

$\Rightarrow \boxed{k = 103}$

Dai dati pubblici:
$r \equiv \alpha^k \pmod{p}$
$6^{103} \equiv 56 \pmod{109}$

$61 \cdot 103 \equiv 15 - a56 \pmod{108}$

$56a \equiv 104 \pmod{108} \quad MCD(56,108) = 4 \Rightarrow$ 4 soluzioni

$14a \equiv 26 \pmod{27}$

$a_0 \equiv 25 \pmod{27}$

$a_i \equiv (25), 52, 79, 106 \pmod{108}$

$\Rightarrow \boxed{a = 25}$

Dai dati pubblici:
$\beta \equiv \alpha^a \pmod{p}$
$6^{25} \equiv 10 \pmod{109}$

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

Matricola:

Domanda 3
(svolgere su questo foglio nello spazio assegnato) (5 punti)

Si consideri l'equazione $\alpha^x \equiv \beta \pmod{p}$ per $p = 251$, $\alpha = 3$, $\beta = 20$.

a) Verificare se esiste certamente una soluzione, indipendentemente dal valore di β. Per quanti valori di $\alpha \in \mathbb{Z}_p^*$ l'equazione ammette soluzione per qualsiasi β?

b) Se l'equazione sopra ammette soluzione, trovarne almeno una applicando l'algoritmo *Baby Step Giant Step*.

a) Test $\alpha^{(p-1)/q_i} \not\equiv 1 \pmod{p} \Rightarrow \alpha$ rad. primitiva di $\mathbb{Z}_p^*$

$p-1 = 250 = 2 \cdot 5^3$

$3^{125} \equiv 1$
$3^{50} \equiv 249$
$\alpha = 3$ NON è rad. prim. di $\mathbb{Z}_{251}^*$

$\Rightarrow \nexists$ soluzione per $\forall \beta$

$\exists$ soluzione per $\forall \beta$ per $\varphi(p-1)$ valori di α (per $\forall$ rad. prim.)

$\varphi(p-1) = \varphi(250) = 100$

b) $N = \lfloor \sqrt{p-1} \rfloor + 1 = 16$ $\quad \alpha^{-1} \equiv 84 \pmod{251}$ (E.E.)

$\alpha^{-N} \equiv 92$ (—) (84^{16})

j	α^j	k	$\beta \alpha^{-Nk} = 20 \cdot 92^k$
0	1	0	20
1	3	1	83
2	9	2	106
3	27	3	214
4	(81)	4	110
5	243	5	80
6	227	6	(81)
7	179	7	~
8	35	8	~

$\alpha^j \equiv \beta \alpha^{-Nk} \pmod{p}$

$\alpha^{j+Nk} \equiv \beta$ (—)

$\Rightarrow x = j + Nk = 4 + 16 \cdot 6 = (100)$

Verifica: $3^{100} \equiv 20 \pmod{251}$

(Anche $x = (225)$)

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

Matricola:

Domanda 4

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

a) Definire la proprietà di *unidirezionalità* di una funzione di *hash*. Specificare per cosa tale definizione si distingue dalla proprietà di *non invertibilità* di una funzione generica.

b) Si consideri una ipotetica funzione di *hash* $h(m) = m^{13} \bmod 1000$. Si dica se tale funzione $h(m)$ è

- invertibile? (spiegare perché)

NO

- unidirezionale? (spiegare perché)

NO

- resistente alle collisioni? (se si risponde NO, fornire un esempio di collisione)

NO

c) Si consideri una versione "potenziata" della funzione di hash del punto b) definita come $h(m) = m^{97} \bmod 10^6$. Un attaccante tenta di ottenere un valore di hash desiderato h_0 calcolando $h(m)$ su variazioni casuali di un messaggio malevolo. Quanti tentativi sono necessari perché l'attacco abbia successo con probabilità almeno 0.5?

$$P(\text{successo in } n \text{ prove}) = 1 - (1-10^{-6})^n$$

$$P = 1/2 \rightarrow (1-10^{-6})^n = 1/2 \qquad n \log(1-10^{-6}) = \log 1/2$$

$$\rightarrow n = \frac{\log 1/2}{\log(1-10^{-6})} = 6{,}9 \cdot 10^5$$

Sicurezza delle Reti
Prof. Stefano Bregni **IV Appello d'Esame 2018-19 – 21 gennaio 2020**

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) Si consideri l'equazione $x^2 \equiv a \pmod{5005}$. Quante soluzioni può avere al massimo questa equazione? Motivare la risposta. *(2 punti)*

$5005 = 5 \cdot 7 \cdot 11 \cdot 13 \rightarrow 16$ soluzioni

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

3) 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. Nel caso di algoritmo di cifratura a chiave pubblica RSA, esiste una terza chiave e_3 tale che la cifratura doppia $C = E_{e_2}(E_{e_1}(P))$ sia equivalente a una cifratura singola $C = E_{e_3}(P)$? Se la risposta è sì, specificarne il valore. Se la risposta è no, spiegare perché è impossibile. *(2 punti)*

4) Si consideri il file di sistema dove sono memorizzate le credenziali degli utenti per l'accesso a un server. *(2 punti)*

- Esiste un modo per decifrare le password degli utenti dal file memorizzato nel sistema?
- Quando un utente inserisce la password di accesso, come avviene la verifica di correttezza?
- Se ipotizzo che la password dell'utente BREGNI appartenga a un vocabolario di 50.000 parole, quanti tentativi sono necessari all'Amministratore per ricavare la sua password dal file? Quanti tentativi sono necessari all'Amministratore, invece, se le password sono salvate nel file con un *salt* di 12 bit?

5) Cos'è il protocollo di Needham-Schroeder? Qual è la sua funzione? Quali sono le sue caratteristiche principali? Descrivere il suo principio di funzionamento. *(4 punti)*