Sicurezza delle Reti

Prof. Stefano Bregni — **II Appello d'Esame 2021-22 – 21 luglio 2022**

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 $p = 131$, $\alpha = 8$, $\beta = \alpha^a \bmod p = 83$, tenendo segreto l'esponente a ($1 < a \leq p\text{-}2$).

Bob estrae il numero casuale segreto k (*nonce*) con MCD(k, p-1) = 1. Usando sempre questo stesso valore di k, Bob calcola le seguenti firme A_1 e A_2 per i rispettivi messaggi P_1 e P_2.

$A_1 = (r_1, s_1) = (10, 85)$ $\quad P_1 = 25$
$A_2 = (r_2, s_2) = (10, 30)$ $\quad P_2 = 30$

Oscar intercetta i due messaggi firmati. Sulla base di essi e delle informazioni pubbliche, calcolare k e a (*attacco del nonce ripetuto*).

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

$\begin{cases} 85k \equiv 25 - a \cdot 10 \pmod{130} \\ 30k \equiv 30 - a \cdot 10 \pmod{130} \end{cases}$

$55k \equiv -5 \pmod{130}$ $\quad MCD(55, 130) = 5 \Rightarrow$ 5 soluzioni

$11k \equiv -1 \pmod{26}$ $\quad 11^{-1} \equiv -7 \pmod{26}$

$k_0 \equiv 7 \pmod{26}$ $\quad k_i \equiv 7, 33, (59), 85, 111 \pmod{130}$

Dai dati pubblici
$r \equiv \alpha^k \pmod{p}$
$10 \equiv 8^k \pmod{131}$

$(k = 59) \Leftarrow$

$30 \cdot 59 \equiv 30 - a \cdot 10 \pmod{130}$

$10a \equiv 80 \pmod{130}$ $\quad MCD(10, 130) = 10 \Rightarrow$ 10 soluzioni

$a_0 \equiv 8 \pmod{13}$

$a_i \equiv 8, 21, 34, (47), 60, 73, 86, 99, 112, 125 \pmod{130}$

$\Rightarrow (a = 47)$

Dai dati pubblici: $\beta \equiv \alpha^a \pmod{p}$

$83 \equiv 8^a \pmod{131}$

Sicurezza delle Reti
Prof. Stefano Bregni — **II Appello d'Esame 2021-22 – 21 luglio 2022**

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (9 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 109$, $\alpha = 4$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 32$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 4$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{5, 6\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Bob estrae il numero casuale segreto (*nonce*) $k = 35$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 25$.

c) Verificare se anche la firma $A' = (r', s') = (11, 39)$ è valida da Bob per lo stesso messaggio $P = 25$.

d) Se è valida, calcolare il valore di k per cui è stata calcolata da Bob, scegliendo il metodo più veloce a disposizione.

a) p primo $1 < \alpha < p-2$ $K \perp p-1$ $p-1 = 108 = 2^2 \cdot 3^3$

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

$\alpha^{\frac{p-1}{2}} \not\equiv 1 \pmod p$

$6^{54} \equiv -1$
$6^{36} \equiv 63$
$\Rightarrow \alpha = 6$ OK ($\alpha = 4,5$ NO)

$\beta \equiv \alpha^a \bmod p = 6^{32} \bmod 109 \equiv 22$

b) $r = \alpha^K \bmod p = 6^{35} \bmod 109 = 65$

$s = K^{-1}(P - ar) \bmod (p-1) = 71(25 - 32 \cdot 65) \bmod 108 = 3$

$K^{-1} \equiv 35^{-1} \equiv 71 \pmod{108}$ $\Rightarrow$ **$A = (65, 3)$**

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

$22^{11} \cdot 11^{39} \equiv 10 \pmod{109}$
$6^{25} \equiv 10$ (—)

$\Rightarrow A' = (11, 39)$ firma valida di $P = 25$

d) Invece di risolvere $6^k \equiv 11 \pmod{109}$, meglio:

$5k \equiv p - 9r \pmod{(p-1)}$

$39k \equiv 25 - 32 \cdot 11 \pmod{108}$

$39k \equiv 105 \pmod{108}$ $\quad MCD(39, 108) = 3 \Rightarrow$ 3 soluzioni

$13k \equiv 35 \pmod{36}$ $\quad 13^{-1} \equiv 25 \pmod{36}$

$k_0 \equiv 35 \cdot 25 \equiv 11 \pmod{36}$

$k_i = 11, 47, 83 \pmod{108}$

$\Rightarrow (k = 83)$

Nei dati pubblici:

$\alpha^k \equiv 1 \pmod{p}$

$6^k \equiv 11 \pmod{109}$

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

Matricola:

Domanda 3

(svolgere su questo foglio nello spazio assegnato) (7 punti)

a) Con che probabilità 2 messaggi casuali, di lunghezza rispettivamente 1024 bit e 2048 bit, hanno lo stesso hash SHA-2 256?

$2^{-256} \approx 0$

b) Spiegare cosa significa affermare che una *generica funzione* $y = y(x)$ è *invertibile*, ma *unidirezionale*.
Spiegare cosa significa affermare che una *funzione di hash* $y = y(x)$ (*non invertibile!)* è *non unidirezionale*.

c) Sappiamo che una certa *funzione di hash* $h = h(x)$ *non è unidirezionale*.
Dato un valore di hash h, potrebbe quindi essere possibile ricavare il messaggio m da cui è stato calcolato? Perché?

d) Si consideri una ipotetica funzione di *hash* $h = h(m) = \alpha^m \bmod p$, dove p è un primo tale per cui il problema del logaritmo discreto sia intrattabile in $\mathbb{Z}_p^*$, α è un elemento generatore di $\mathbb{Z}_p^*$, e m è un intero qualsiasi. Si spieghi perché tale funzione di hash $h = h(m)$ è unidirezionale, ma non debolmente resistente alle collisioni.

Domanda 4

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

a) Ricavare la sequenza binaria pseudo-casuale $\{x_i\}$ generata dall'algoritmo *Blum-Blum-Shab* per $p = 47$, $q = 59$, $x = 60$ e determinarne il periodo P. Il seme iniziale x rispetta le ipotesi del metodo?

i	x_i	b_i	
0	827	1	
1	1771	1	
2	178	0	$P=11$
3	1181	1	
4	2715	1	
5	591	1	
6	2656	0	
7	2597	1	
8	473	1	
9	1889	1	
10	2243	1	
11	827	1	
12			

$m = p \cdot q = 47 \cdot 59 = 2773$

$x_0 \equiv x^2 \pmod{n}$

$x_i \equiv x_{i-1}^2 \pmod{n}$

$47 \equiv 3 \pmod{4}$

$59 \equiv 3 \pmod{4}$

$60 \perp pq$

b) In base alla teoria, quali sono i valori possibili che può assumere il periodo $P = \pi(x_0)$ del generatore precedente, per valori arbitrari del seme $x_0 = x^2 \in \mathbb{Z}_n$?

Si ricorda che $\pi(x_0)$ divide $\lambda(\lambda(n))$, dove $\lambda(n)$ è la Funzione di Charmichael, calcolabile come

$$\lambda(n) = \text{mcm}\left(\left\{\lambda\left(p_i^{a_i}\right)\right\}\right) \qquad \lambda\left(p^k\right) = \begin{cases} \frac{1}{2}\varphi\left(p^k\right) & \text{se } p = 2,\ k \geq 3 \\ \varphi\left(p^k\right) & \text{altrimenti} \end{cases}$$

$\lambda(n) = \text{mcm}(46, 58) = 2 \cdot 23 \cdot 29 = 1334$

$\lambda[\lambda(n)] = \lambda(1334) = \text{mcm}(1, 22, 28) = 308 \quad (= 2^2 \cdot 7 \cdot 11)$

$\Pi(x_0) \in \{1, 2, 4, 7, 11, 14, 22, 28, 44, 77, 154, 308\}$

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) Suggerire come trovare le radici dell'equazione $4 \equiv 3^x \pmod{77}$, se esistono. *(2 punti)*

2) In generale, è più difficile risolvere un *Problema Computazionale di Diffie-Hellman* o un *Problema del Logaritmo Discreto*? Perché? *(2 punti)*

3) A cosa serve il *Protocollo di Needham-Schroeder*? Quali sono gli attori? Viene eseguito allo scopo di produrre o trasferire quale informazione? *(2 punti)*

4) Cos'è l'*ordine* di un elemento $\alpha \in \mathbb{Z}_p^*$? Elencare i valori possibili dell'ordine di un elemento $\alpha \in \mathbb{Z}_{149}^*$. *(2 punti)*

$\{1, 2, 4, 37, 74, 148\}$

5) Sia data una funzione di hash $h = h(m)$ unidirezionale che restituisce valori pseudocasuali di lunghezza fissa 20 bit. Un attaccante tenta di ottenere un valore di hash desiderato H, calcolando la $h(m)$ su variazioni casuali di un messaggio malevolo m. Quanti tentativi sono necessari perché l'attacco abbia successo (si ottenga $h(m) = H$) con probabilità almeno 0.5? *(2 punti)*

$P = \left(1 - \frac{1}{2^{20}}\right)^n \cong (1 - n2^{-20})$

$P = \frac{1}{2} \rightarrow$ / (approssimato) $1 - n2^{-20} = 1/2 \rightarrow n \cong 2^{19} = 524288$

\ (esatto) $(1 - 2^{-20})^n = \frac{1}{2}$ $n \log(1 - 2^{-20}) = \log 1/2$

$\rightarrow n = 726817$

6) Trovare i fattori primi di $n = 22499$ attraverso l'*Algoritmo di Fattorizzazione p−1* di Pollard con base $a = 2$. *(2 punti)*

$b_1 \equiv 2 \pmod{22499}$

$b_2 \equiv 2^2 \equiv 4$ (~)

$b_3 \equiv 4^3 \equiv 64$ (~)

$b_4 \equiv 64^3 \equiv 15461$ (~)

$b_5 \equiv 15461^5 \equiv 2115$ (~)

$MCD(3, n) = 1$

$MCD(63, n) = 1$

$MCD(15460, n) = 1$

$MCD(2114, n) = 151$

$\Rightarrow p = 151$

$q = 149$