Sicurezza delle Reti

Prof. Stefano Bregni — **IV Appello d'Esame 2021-22 – 23 gennaio 2023**

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 $p = 193$, $\alpha = 6$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 65$.

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 un valore valido scelto nell'insieme $\alpha = \{5, 7\}$. 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*) $k = 29$ e spedisce il messaggio $P = 10$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob riceve $C' = (r', t') = (52, 13)$. Calcolare il messaggio decifrato da Bob P'.

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

a) p primo $1 < a < p-2$ $p-1 = 192 = 2^6 \cdot 3$

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

$5^{96} \equiv -1$
$5^{64} \equiv 84$
$\Big\}$ $\alpha = 5$ ($\alpha = 6, 7$ NO) OK

$\beta = \alpha^a \bmod p = 5^{65} \bmod 193 = 34$

b) $r = \alpha^k \bmod p = 5^{29} \bmod 193 = 47$

$t = \beta^k P \bmod p = 34^{29} \cdot 10 \bmod 193 = 1$

$\Rightarrow \boxed{C = (47, 1)}$

c) $P' = t' \cdot r'^{-a} \bmod p = 13 \cdot 52^{-65} \bmod 193 = (21)$

$52^{-1} \equiv 26 \pmod{193}$

d) $5^K \bmod 193 = 52 \Rightarrow (K = 17)$ con BSGS

Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2021-22 – 23 gennaio 2023**

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (6 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 137$, $\alpha = 5$, $\beta = \alpha^a \bmod p = 27$, 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.

$A_1 = (r_1, s_1) = (24, 45)$ $\quad P_1 = 25$
$A_2 = (r_2, s_2) = (24, 63)$ $\quad P_2 = 27$

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

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

$\begin{cases} 45k \equiv 25 - 24a \pmod{136} \\ 63k \equiv 27 - 24a \pmod{136} \end{cases}$

$18k \equiv 2 \pmod{136}$ $\quad MCD(18, 136) = 2 \Rightarrow$ 2 soluzioni

$9k \equiv 1 \pmod{68}$ $\quad 9^{-1} \equiv 53 \pmod{68}$

$k_0 \equiv 53 \pmod{68}$ $\quad k_1 \equiv 53, 121 \pmod{136}$

$K = 53$ ⇐

Dai dati pubblici:
$r \equiv \alpha^k \pmod{p}$
$24 \equiv 5^k \pmod{137}$

$45 \cdot 53 \equiv 25 - 24a \pmod{136}$

$24a \equiv 88 \pmod{136}$ $\quad MCD(24, 136) = 8 \Rightarrow$ 8 soluzioni

$3a \equiv 11 \pmod{17}$ $\quad 3^{-1} \equiv 6 \pmod{17}$

$a_0 \equiv 15 \pmod{17}$ $\quad a_i \equiv 15, 32, 49, 66, 83, 100, 117, 134 \pmod{136}$

$a = 49$ ⇐

Dai dati pubblici: $\beta \equiv \alpha^a \pmod{p}$
$27 \equiv 5^a \pmod{137}$

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

Matricola:

Domanda 3

(svolgere su questo foglio nello spazio assegnato) (8 punti)

a) Spiegare cosa significa affermare che una *generica funzione* $y = y(x)$ è *invertibile*, ma *unidirezionale*.

b) 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?

c) Definire la proprietà di *resistenza forte alle collisioni* di una *funzione di hash* $h = h(x)$.

d) Si consideri una ipotetica funzione di *hash* $h = h(m) = m^e \bmod p$, dove p è primo, $1 < e < p\text{-}1$, n ed e sono pubblici, e m è un intero qualsiasi. Per quali valori di e è banale dimostrare che la funzione $h(m)$ non è unidirezionale?

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 $p = 43$, $q = 59$, $x = 60$ e determinarne il periodo P. Il seme iniziale x rispetta le ipotesi del metodo?

i	x_i	b_i	
0	1063	1	
1	1004	0	
2	827	1	$P=6$
3	1476	0	
4	1830	0	
5	60	0	
6	1063	0	

$n = p \cdot q = 43 \cdot 59 = 2537$

$x_0 \equiv x^2 \pmod n$

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

$47 \equiv 3 \pmod 4$

$59 \equiv 3 \pmod 4$

$60 \perp pq$

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

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

$\lambda(n) = \text{mcm}(42, 58) = 2 \cdot 3 \cdot 7 \cdot 29 = 1218$

$\lambda[\lambda(n)] = \lambda(1218) = \text{mcm}(1, 2, 6, 28) = 84 \ (= 2^2 \cdot 3 \cdot 7)$

$\pi(x_0) \in \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$

Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2021-22 – 23 gennaio 2023**

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

Matricola:

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (11 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) Sia data una funzione di hash $h = h(m)$ che restituisce stringhe pseudocasuali di lunghezza fissa 10 bit. Un attaccante tenta di ottenere un valore di hash desiderato h_0 calcolando la $h(m)$ su variazioni casuali di un messaggio malevolo m. Quanti tentativi sono necessari perché l'attacco abbia successo con probabilità > 0.90? *(3 punti)*

$(1-2^{-10})^n = 0{,}1$

$\rightarrow n \cong 2357$

P(successo in n prove) =

$= 1 - (1 - \frac{1}{2^{10}})^n$

2) L'equazione $x^2 \equiv 3 \pmod{107}$ ha soluzione? Se la risposta è sì, calcolarne le radici.
L'equazione $x^2 \equiv -3 \equiv 104 \pmod{107}$ ha soluzione? Se la risposta è sì, calcolarne le radici. *(2 punti)*

$p = 107$ primo $\rightarrow$ l'eq. ha soluzione se $3^{53} \equiv 1 \pmod{107}$

$3^{53} \equiv 1 \pmod{107} \Rightarrow$ SI

$107 \equiv 3 \pmod 4 \Rightarrow$ l'eq. $x^2 \equiv 3 \pmod{107}$ ha 2 radici

$x^2 \equiv -3 (\text{---})$ non ha soluzione

$x \equiv \pm 3^{27} \equiv \pm 89 \pmod{107}$

$\equiv 18, 89$

3) Cos'è l'*ordine* di un elemento $\alpha \in \mathbb{Z}_p^*$? Elencare i valori possibili dell'ordine di un elemento $\alpha \in \mathbb{Z}_{83}^*$. *(2 punti)*

$\{1, 2, 41, 82\}$

4) Qual è l'unico crittosistema teoricamente inviolabile? Cosa lo rende difficilmente realizzabile in pratica? *(2 punti)*

5) Descrivere lo *Schema di Lamport* per l'autenticazione di un host A da parte di un server B, precisando quali informazioni sono tenute segrete da A e B e quali informazioni sono invece pubbliche o trasferite in chiaro. *(2 punti)*