Sicurezza delle Reti

Prof. Stefano Bregni — **III Appello d'Esame 2025-26 – 31 agosto 2026**

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 di El Gamal* e pubblica $p = 199$, $\alpha = 6$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 128$.

a) Si rende noto che $\alpha = 6$ è una radice primitiva di $\mathbb{Z}_{199}^*$. Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 10$ e spedisce il messaggio $P_1 = 150$ a Bob. Calcolare il messaggio cifrato $C_1 = (r_1, t_1)$.

c) Alice estrae un nuovo numero casuale segreto (*nonce*) k e, usando sempre questo stesso valore, spedisce i messaggi P_2, P_3, P_4. Oscar intercetta i messaggi cifrati $C_2 = (r_2, t_2) = (5, 75)$, $C_3 = (r_3, t_3) = (5, 86)$, $C_4 = (r_4, t_4) = (5, 87)$ e, per altra via, viene a sapere che $P_2 = 110$. Calcolare P_3 e P_4.

a) $\beta = \alpha^a \bmod p = 6^{128} \equiv 122 \pmod{199}$

b) $r_1 = \alpha^k \bmod p = 6^{10} \bmod 199 = 26$

$t_1 = \beta^k \cdot P_1 \bmod p = 122^{10} \cdot 150 \bmod 199 = 55$

$\Rightarrow C_1 = (26, 55)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$

$t_2^{-1} \equiv 75^{-1} \equiv 69 \pmod{199}$ (E.E.)

$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod p \equiv 110 \cdot 86 \cdot 69 \equiv 20$

$P_4 \equiv P_2 \frac{t_4}{t_2} \pmod p \equiv 110 \cdot 87 \cdot 69 \equiv 48$

(C_2, C_3, C_4 calcolati con $k = 42$)

Domanda 2

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

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 223$, $\alpha = 12$, $\beta = \alpha^a \bmod p = 27$, 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.

$A_1 = (r_1, s_1) = (90, 71)$ $\quad P_1 = 11$
$A_2 = (r_2, s_2) = (90, 11)$ $\quad P_2 = 17$

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

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

$\begin{cases} 71k \equiv 11 - a\,90 \pmod{222} \\ 11k \equiv 17 - a\,90 \pmod{222} \end{cases}$

$60k \equiv -6 \pmod{222}$ $\quad MCD(60, 222) = 6 \Rightarrow$ 6 soluzioni

$10k \equiv -1 \pmod{37}$ $\quad 10^{-1} \equiv -11 \pmod{37}$

$\Rightarrow k_0 \equiv 11 \pmod{37}$

$k_i \equiv 11, 48, \underline{85}, 122, 159, 196 \pmod{222}$

$\Rightarrow \boxed{k = 85}$

Dai dati pubblici:
$r = \alpha^k \bmod p$
$90 \equiv 12^k \pmod{222}$

$11 \cdot 85 \equiv 17 - a\,90 \pmod{222}$

$a\,90 \equiv 192 \pmod{222}$ $\quad MCD(90, 222) = 6 \Rightarrow$ 6 soluzioni

$15 \cdot a \equiv 32 \pmod{37}$ $\quad 15^{-1} \equiv 5 \pmod{37}$

$\Rightarrow a_0 \equiv 12 \pmod{37}$

$a_i \equiv 12, 49, 86, \underline{123}, 160, 197 \pmod{222}$

$\Rightarrow \boxed{a = 123}$

Dai dati pubblici:
$\beta \equiv \alpha^a \pmod{p}$
$27 \equiv 12^a \pmod{223}$

Domanda 3

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

a) Ricavare la sequenza binaria pseudo-casuale $\{x_i\}$ generata dall'algoritmo *Blum-Blum-Shab* per $p = 17$, $q = 83$, $x = 82$ e determinarne il periodo P. I primi p, q e il seme iniziale x rispettano le ipotesi del metodo?

i	x_i	b_i
0	1089	0
1	914	0
2	84	0
3	1	1
4	1	1
⋮	⋮	⋮

$n = p \cdot q = 17 \cdot 83 = 1411$

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

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

$17 \equiv 1 \pmod 4 \Rightarrow$ NO

$83 \equiv 3 \pmod 4$

$82 \perp 1411$

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

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

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

$\lambda(n) = \text{mcm}(16, 82) = 2^4 \cdot 41 = 656$

$\lambda[\lambda(n)] = \lambda(656) = \text{mcm}(4, 40) = 40 \qquad \pi(x_0) \mid 40$

$\pi(x_0) \in \{1, 2, 4, 5, 8, 10, 20, 40\}$

Domanda 4

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

a) Definire la proprietà di *unidirezionalità* di una *generica funzione invertibile* $y = y(x)$ e di una *funzione di hash* $y = h(x)$, distinguendo tra i due casi.

b) Se la unidirezionalità di una funzione di hash $h(x)$ è facilmente violabile, è legittimo temere il rischio che qualcuno modifichi in modo fraudolento un mio documento m, di cui ho firmato $h(m)$?

b) Posseggo il file delle password di 1000 utenti di un sistema. La funzione di hash è SHA accorciata agli ultimi 64 bit. Il sale è lungo 16 bit. Quante esecuzioni della funzione $h(x)$ sono necessarie per:

- trovare una password *pw*, che mi consenta di autenticarmi come un certo utente A;

- trovare una password *pw*, che mi consenta di autenticarmi come uno qualsiasi degli utenti;

- trovare una password *pw*, che mi consenta di autenticarmi come un certo utente A, sapendo che la sua password appartiene a un vocabolario di 50000 parole.

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

Matricola:

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (15 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) Definire il *Problema Computazionale di Diffie-Hellman.* Se hai trovato un algoritmo che lo risolve in modo efficiente, come puoi applicare il tuo algoritmo al calcolo di *Logaritmi Discreti?* *(2 punti)*

2) 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)*

3) Si considerino le funzioni di cifratura doppia $C = E_{K_2}(E_{K_1}(P))$ e sua decifratura $P = D_{K_1}(D_{K_2}(C))$, con due chiavi K_1 e K_2 ciascuna di lunghezza 40 bit, $P \in \mathbb{Z}_{128}$, $C \in \mathbb{Z}_{128}$. Si intende svolgere un *attacco testo in chiaro noto* per trovare la coppia di chiavi K_1, K_2. *(3 punti)*

a) Descrivere la procedura di un attacco *Meet-in-the-Middle* per trovare la coppia di chiavi K_1, K_2.

b) Quante esecuzioni degli algoritmi $E_K(X)$ e $D_K(X)$ sono necessarie per l'attacco MiM del punto a)? Qual è l'occupazione totale di memoria necessaria [byte]?

b) $2^{40} \cong 10^{12}$ esecuzioni di $E_K(P)$

$1 \div 2^{40} \cong 10^{12}$ esecuzioni di $D_K(C)$

Occupazione di memoria: $(2^{40}+1) \cdot 16$ byte $= 2^{44}$ byte $= 16$ TB

4) Cos'è l'*ordine* di un elemento $\alpha \in \mathbb{Z}_p^*$? Quanti e quali sono i valori possibili dell'ordine di un elemento $\alpha \in \mathbb{Z}_{107}^*$? *(2 punti)*

$Ord(\alpha) \setminus 106 \Rightarrow$ 4 valori: $\{1, 2, 53, 106\}$

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

Matricola:

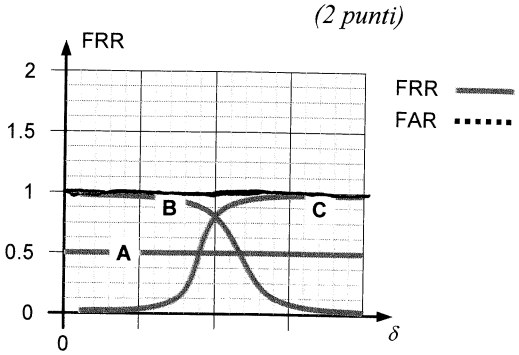
5) Al termine di una negoziazione, la vostra controparte Bob attende che gli inviate il documento concordato da firmare elettronicamente. Descrivete un *attacco del compleanno* con cui tentate di ottenere da Bob una firma valida per un documento fraudolento, se la funzione di hash dell'algoritmo di firma restituisce gli ultimi 12 byte di MD5. Calcolate la quantità di memoria che vi sarà necessaria per completare questo attacco. *(2 punti)*

Per avere successo con prob. > 50%: $2^{49} \cdot 12$ byte = 6 PB

6) Per controllare gli accessi al vostro laboratorio, avete installato un sistema di autenticazione biometrica basato su rilevazione delle impronte digitali dei visitatori, che sembra funzionare discretamente bene. Affidate la misura dell'accuratezza del sistema a uno studente in tirocinio formativo. Al termine dell'attività, lo studente vi consegna le curve FRR(δ) rappresentate in figura, dove δ è la soglia di decisione del discriminatore, segnalando che sono il risultato di tre procedure di misura diverse. *(2 punti)*

a) Quali di queste curve respingete come evidentemente errate? Perché?

A, C



b) Non potendovi fidare, eseguite voi stessi la misura seguendo il procedimento corretto, ma non vi accorgete che il sensore è completamente sporco. Sullo stesso diagramma, disegnate la curva FRR(δ) che ottenete.

7) Trovare i fattori primi di $n = 7739$ attraverso l'*Algoritmo di Fattorizzazione p−1* di Pollard con base $a = 5$. *(2 punti)*

$b_1 \equiv 5 \pmod{7738}$

$b_2 \equiv 5^2 \equiv 25$ (—) $\quad MCD(24, 7739) = 1$

$b_3 \equiv 25^3 \equiv 147$ (—) $\quad MCD(146, 7739) = 1$

$b_4 \equiv 147^4 \equiv 838$ (—) $\quad MCD(837, 7739) = 1$

$b_5 \equiv 838^5 \equiv 1989$ (—) $\quad MCD(1988, 7739) = 71$

$\Rightarrow p = 71$

$q = 109$