Sicurezza delle Reti

Prof. Stefano Bregni — **I Appello d'Esame 2025-26 – 23 giugno 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 $p = 197$, $\alpha = 5$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 195$.

a) Si rende noto che $\alpha = 5$ è una radice primitiva di $\mathbb{Z}_{197}^*$. Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 51$ e spedisce il messaggio $P_1 = 100$ 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 $C_2 = (r_2, t_2) = (85, 14)$, $C_3 = (r_3, t_3) = (85, 137)$, $C_4 = (r_4, t_4) = (85, 47)$ e, per altra via, viene a sapere che $P_2 = 8$. Calcolare P_3 e P_4.

a) $\beta = \alpha^a \bmod p = 5^{195} \equiv 5^{-1} \equiv 79 \pmod{197}$

b) $r_1 = \alpha^k \bmod p = 5^{51} \bmod 197 = 44$

$t_1 = \beta^k \cdot P_1 \bmod p = 79^{51} \cdot 100 \bmod 197 = 56$ $\Rightarrow C_1 = (44, 56)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $\quad t_2^{-1} = 14^{-1} \equiv 183 \pmod{197}$

$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod p \equiv 8 \cdot 137 \cdot 183 \equiv 22 \pmod{197}$

$P_4 \equiv P_2 \frac{t_4}{t_2} \pmod p \equiv 8 \cdot 47 \cdot 183 \equiv 55 \pmod{197}$

(C_2, C_3, C_4 calcolati con $K = 16$)

Domanda 2

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

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 181$, $\alpha = 10$, $\beta = \alpha^a \bmod p = 28$, 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.

$A_1 = (r_1, s_1) = (69, 86)$ $\quad P_1 = 11$
$A_2 = (r_2, s_2) = (69, 151)$ $\quad P_2 = 16$

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

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

$$\begin{cases} 86k \equiv 11 - a\,69 \pmod{180} \\ 151k \equiv 16 - a\,69 \pmod{180} \end{cases}$$

$65k \equiv 5 \pmod{180}$ $\quad mcd(65, 180) = 5 \Rightarrow$ 5 soluzioni

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

$\rightarrow k_0 \equiv 25 \pmod{36}$ $\quad k_i = 25, 61, (97), 133, 169 \pmod{180}$

$\Rightarrow \boxed{k = 97}$

Dai dati pubblici:
$r = \alpha^k \bmod p$
$69 \equiv 10^k \pmod{181}$

$86 \cdot 97 \equiv 11 - a\,69 \pmod{180}$

$69a \equiv 129 \pmod{180}$ $\quad mcd(69, 180) = 3 \Rightarrow$ 3 soluzioni

$23a \equiv 43 \pmod{60}$ $\quad 23^{-1} \equiv 47 \pmod{60}$

$\rightarrow a_0 \equiv 43 \cdot 47 \equiv 41 \pmod{60}$ $\quad a_i \equiv 41, (101), 161 \pmod{180}$

$\Rightarrow \boxed{a = 101}$

Dai dati pubblici:
$\beta \equiv \alpha^a \pmod{p}$
$28 \equiv 10^a \pmod{181}$

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

Matricola:

Domanda 3

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

Si consideri l'equazione $\alpha^x \equiv \beta \pmod{67}$, in cui $p = 67$ è primo.

a) L'elemento $\alpha = 3$ è primitivo in $\mathbb{Z}_{67}^*$? Qual è il suo ordine?

b) Dire se l'equazione $3^x \equiv \beta \pmod{67}$ ammette soluzione per $\forall \beta \in \mathbb{Z}_{67}^*$. Se la risposta è no, determinare per quanti valori di $\beta \in \mathbb{Z}_{67}^*$ l'equazione ammette almeno una soluzione.

c) Per quanti valori di $\alpha \in \mathbb{Z}_{67}^*$ l'equazione $\alpha^x \equiv \beta \pmod{67}$ ammette sicuramente soluzione per $\forall \beta \in \mathbb{Z}_{67}^*$?

d) Trovare tutte le soluzioni di $3^x \equiv 22 \pmod{67}$ (se esistono) applicando l'algoritmo *Baby Step Giant Step*.

a) $p-1 = 66 = 2 \cdot 3 \cdot 11$

$3^{33} \equiv 66$
$3^{22} \equiv 1$
$3^6 \equiv 59$
$\Rightarrow$ $a=3$ non è el. prim. di $\mathbb{Z}_{67}^*$

$\Rightarrow Ord(\alpha=3) = 22$

K	3^K
0	1
1	3
2	9
3	27
4	
5	
6	59
7	
8	
9	
10	
11	66
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	1

Basta calcolare per K|22

b) $\alpha = 3$ non è un elem. primitivo di $\mathbb{Z}_{67}^*$

$\Rightarrow$ l'eq. $3^x \equiv \beta \pmod{67}$ ammette soluzione per $\text{Ord}(\alpha) = 22$ valori di β

c) L'eq. $\alpha^x \equiv \beta \pmod{67}$ ammette soluzione per $\forall \beta$ se α è un elem. primitivo di $\mathbb{Z}_{67}^*$

$\Rightarrow \varphi(66) = 20$ valori di α

d) $3^x \equiv 22 \pmod{67}$

$N = 9$

$\alpha^{-1} \equiv 45 \pmod{67}$

$\alpha^{-N} \equiv 58 \pmod{67}$

j	α^j
0	1
1	(3)
2	9
3	27
4	14
5	42
6	59
7	43
8	62

k	α^{-Nk}	$\beta\alpha^{-Nk}$	
0	1	22	
1	58	(3)	
2	14		
3	⋮	⋮	(42)
4	⋮	⋮	
5	⋮	⋮	
6	⋮	⋮	(1)
7	⋮	⋮	
8	⋮	⋮	(14)

$x \equiv 1 + 9 \cdot 1 \equiv 10 \pmod{22}$

$\Rightarrow x \equiv 10, 32, 54 \pmod{66}$

N.B.: le soluzioni 32, 54 si trovano (anche) con altre corrispondenze nelle tabelle sopra

Domanda 4

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

a) Definire la proprietà di *resistenza debole alle collisioni* di una *funzione di hash* $h = h(m)$.

b) Ci è stata fornita una macchina in grado di trovare una *contro-immagine* dei valori calcolati con la funzione $h = h(m)$ adottata da una Azienda nostra concorrente, che salva i valori degli hash $H_k = h(pw_k)$ calcolati sulle password pw_k degli N utenti (k = 1, …, N) in un file cui abbiamo accesso tramite una backdoor. Siamo in grado di trovare le password degli utenti? Siamo in grado di accedere al sistema al loro posto?

c) Si consideri una ipotetica funzione di hash $h = h(m)$ = BIP(n,l) (*Bit Interleaved Parity*) definita come segue. Sia L la lunghezza del messaggio m. Lo si divida in $l = \lceil L/n \rceil$ blocchi di n bit ciascuno, dove l'ultimo blocco è completato con zeri se L non è un multiplo di n. Si costruiscano la matrice $\mathbf{M} = \{m_{i,j}\}$ (i = 1, 2, ..., l; j = 1, 2, ..., n), dove le l righe sono i blocchi di n bit in cui è stato diviso il messaggio, e il vettore $\mathbf{h} = \{h_1, h_2, \ldots, h_j, \ldots, h_n\}$ (j = 1, 2, ..., n), dove h_j è il bit di parità (somma XOR) calcolato sugli l bit della j-esima colonna di $\mathbf{M}$. Quindi, i bit $\{m_{i,j}\}$ sono i bit del messaggio scritti riga per riga da sinistra a destra, dall'alto verso il basso. Il tutto è rappresentato come sotto a destra:

Si dica se tale funzione $h = h(m)$ è:

- *invertibile*? (spiegare perché SI o perché NO)

$$\begin{array}{cccccc} m_{1,1} & m_{1,2} & \cdots & m_{1,j} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,j} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ m_{i,1} & m_{i,2} & \cdots & m_{i,j} & \cdots & m_{i,n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ m_{l,1} & m_{l,2} & \cdots & m_{l,j} & \cdots & m_{l,n} \\ \hline \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ h_1 & h_2 & \cdots & h_j & \cdots & h_n \end{array}$$

- *unidirezionale*? (spiegare perché SI o perché NO;
se si risponde NO, dire come trovare una contro-immagine)

$$h_j = \left(\sum_{i=1}^{l} m_{i,j} \right)_{\mathrm{mod}\,2}$$

- *resistente alle collisioni*? (spiegare perché SI o perché NO;
se si risponde NO, fornire un esempio di collisione)

Domanda 5

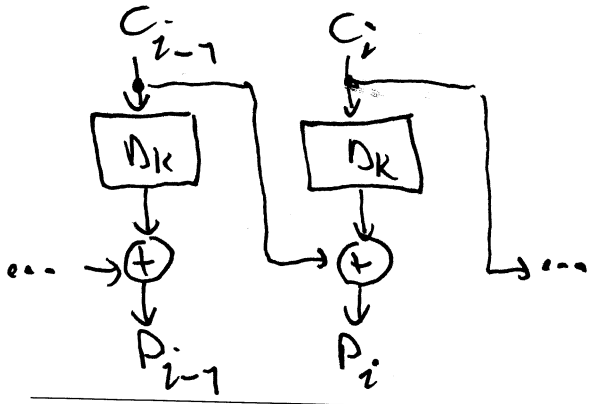
(rispondere su questo foglio negli spazi assegnati) (13 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 281$, $\alpha = 23$, $\beta = \alpha^a \bmod p = 73$, tenendo segreto l'esponente $a = 265$. Decifrare il messaggio $C = (r, t) = (25, 69)$. *(2 punti)*

$P = t \cdot r^{-a} \bmod p =$ (= calcolato per k=36)

$= 69 \cdot 25^{-265} \bmod 281 = 69 \cdot 25^{15} \bmod 281 = 66$

2) Si consideri un cifrario a blocchi concatenato secondo la modalità *Cipher Block Chaining* (CBC), in cui cifratura e decifratura sono svolte rispettivamente come $C_i = E_K(P_i \oplus C_{i-1})$ e $P_i = C_{i-1} \oplus D_K(C_i)$, C_0 è il vettore di inizializzazione, la dimensione dei blocchi P_i e C_i è 64 bit. Disegnare lo schema a blocchi del processo di decifrazione. Il flusso cifrato $\{C_i\}$ subisce errori di trasmissione puramente casuali con tasso ε. Quale sarà il tasso di errore sul flusso decifrato $\{P_i\}$ nei due casi $\varepsilon = 1/20 = 0.05$ e $\varepsilon = 10^{-3}$? *(2 punti)*



$\varepsilon = 0{,}05 \rightarrow E \cong 0{,}5$

NB: Prob(almeno 1 errore in 64 bit) $= 1 - 0{,}95^{64} \cong 96\%$

$\varepsilon = 10^{-3} \rightarrow E \cong 3.3 \cdot 10^{-2}$

3) Dire se le due equazioni $x^2 \equiv +17 \pmod{83}$ e $x^2 \equiv -17 \pmod{83}$ hanno soluzione. Calcolare tutte le soluzioni esistenti delle due equazioni. *(2 punti)*

$p = 83$ primo $\Rightarrow$ l'eq. ha soluzione se $(\pm 17)^{41} \equiv 1 \pmod{83}$

$17^{41} \equiv 1 \pmod{83} \Rightarrow$ SI

$-17^{41} \equiv -1 \pmod{83} \Rightarrow$ NO

$83 \equiv 3 \pmod 4$

$\Rightarrow$ l'eq. $x^2 \equiv 17 \pmod{83}$ ha le 2 radici:

$x_{1,2} \equiv \pm 17^{21} \equiv \pm 10 \pmod{83}$

$\equiv 10, 73 \pmod{83}$

Cognome e nome: *(stampatello)*

(firma leggibile)

Matricola:

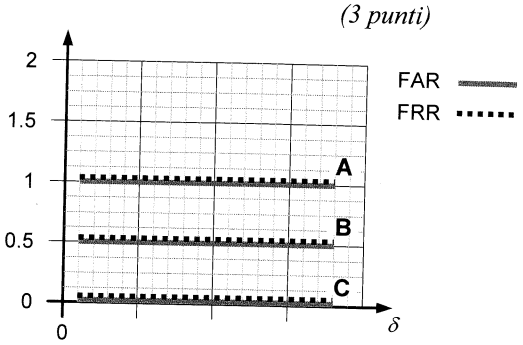
4) Per controllare gli ingressi in un laboratorio, avete comprato un sistema di autenticazione biometrica basato su rilevazione delle impronte digitali dei visitatori. Intendete misurare la curva di FRR del sistema, supervisionando i primi 10000 accessi tramite un funzionario fidato che conosce tutti i dipendenti personalmente, gli unici autorizzati a entrare, e che convalida o corregge ogni decisione da parte del sistema. Che dati raccogliete? Con che formula stimate il valore di FRR sul sistema in prova?

(2 punti)

5) Per controllare gli accessi al vostro laboratorio, state valutando l'acquisto di un sistema di autenticazione biometrica basato su rilevazione delle impronte digitali dei visitatori. Confrontate le curve FAR(δ) e FRR(δ) di tre sistemi concorrenti sul mercato (A, B, C), dove δ è la soglia di decisione del discriminatore. I tre produttori forniscono le curve misurate nell'intervallo tra due valori limite $\delta_1 < \delta < \delta_2$, confrontate nel diagramma sotto riportato. Vi fidate che le curve siano veritiere.

(3 punti)

a) Quale sistema comprate? A, B, o C? Perché?
b) Quale sistema dovrebbe costare meno di tutti, in quanto incorpora l'algoritmo di decisione più elementare? A, B, o C? Perché?
c) Dopo averci pensato meglio, capite che per uno dei tre sistemi le curve FAR(δ) e FRR(δ) sono sicuramente errate. Quale? A, B, o C? Perché?



6) Nel Dark Web, hai trovato un certificato in cui leggi, tra le altre cose: *(2 punti)*

Issuer name: TrueServices.Inc
Period of validity: from 1/1/1990 to 31/12/2199
Subject name: STEFANO.BREGNI@POLIMI.IT
Public Key of the Subject: XXXXX
Signature: YYYYY

a) Che procedura segui per verificare l'autenticità del certificato?
b) Come potresti utilizzarlo, al fine di impersonare Stefano Bregni del Politecnico di Milano?