Sicurezza delle Reti

Prof. Stefano Bregni — **II Appello d'Esame 2025-26 – 14 luglio 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) (6 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 149$, $\alpha = 8$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 81$.

a) Si rende noto che $\alpha = 8$ è una radice primitiva di $\mathbb{Z}_{149}^*$. Calcolare β.

b) Bob estrae il numero casuale segreto (*nonce*) $k = 51$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 30$.

c) Verificare se la firma $A' = (r', s') = (41, 16)$ da Bob è valida per il messaggio $P = 37$.

d) Se è valida, calcolare il valore di k per cui è stata calcolata da Bob risolvendo l'equazione $s \equiv 16 \pmod{p\text{-}1}$ (non *Baby Step Giant Step*).

a) p primo $1 \le a \le p-2$ $K \perp p-1$ $p-1 = 148 = 2^2 \cdot 37$ $\beta = \alpha^a \bmod p = 8^{81} \bmod 149 =$
$= 23$

b) $r = \alpha^k \bmod p = 8^{51} \bmod 149 = 32$

$s = K^{-1}(P - ar) \bmod (p-1) = 119(30 - 81 \cdot 32) \bmod 148 = 2 \Rightarrow A = (32, 2)$

$K^{-1} = 51^{-1} \equiv 119 \pmod{148}$

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

$23^{41} \cdot 41^{16} \equiv 44 \pmod{149}$
$8^{37} \equiv 44 \pmod{149}$
$\Rightarrow A' = (41, 16)$ firma valida di $P = 37$

o1) $K_S \equiv P_{-ar} \pmod{(p-1)}$

$16K \equiv 37 - 31 \cdot 41 \pmod{148}$

$16K \equiv 120 \pmod{148}$ $\quad mcd(16, 148) = 4 \Rightarrow$ 4 soluzioni

$4K \equiv 30 \pmod{37}$ $\quad 4^{-1} \equiv 28 \pmod{37}$

$\rightarrow K_0 \equiv 30 \cdot 28 \equiv 26 \pmod{37}$

$K_i \equiv 26, 63, 100, 137 \pmod{148}$

Dai dati pubblici: $3^K \equiv 41 \pmod{149}$

$\Rightarrow$ $K = 63$

Sicurezza delle Reti
Prof. Stefano Bregni — **II Appello d'Esame 2025-26 – 14 luglio 2026**

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) **5** *punti)*

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 191$, $\alpha = 19$, $\beta = \alpha^a \bmod p = 5$, 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.

$A_1 = (r_1, s_1) = (35, 48)$ $\quad P_1 = 8$
$A_2 = (r_2, s_2) = (35, 128)$ $\quad P_2 = 18$

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

$S \equiv K^{-1}(P - ar) \pmod{(p-1)} \Rightarrow sK \equiv P - ar \pmod{(p-1)}$

$\begin{cases} 48K \equiv 8 - 35a \pmod{190} \\ 128K \equiv 18 - 35a \pmod{190} \end{cases}$

$80K \equiv 10 \pmod{190}$ $\quad MCD(80, 190) = 10 \Rightarrow$ 10 soluzioni

$8K \equiv 1 \pmod{19}$ $\quad 8^{-1} \equiv 12 \pmod{19}$

$\rightarrow K_0 \equiv 12 \pmod{19}$

$K_i = 12, 31, 50, 69, 88, 107, 126, 145, 164, 183 \pmod{190}$

$\Rightarrow (K = 31)$

Dai dati pubblici:
$r = \alpha^K \bmod p$
$35 = 19^K \bmod 191$

$48 \cdot 31 \equiv 8 - 35a \pmod{190}$

$35a \equiv 40 \pmod{190}$ $\quad MCD(35, 190) = 5 \Rightarrow$ 5 soluzioni

$7a \equiv 8 \pmod{38}$ $\quad 7^{-1} \equiv 11 \pmod{38}$

$\rightarrow a_0 \equiv 8 \cdot 11 \equiv 12 \pmod{38}$

$a_i \equiv 12, 50, 88, 126, 164 \pmod{190}$

$\Rightarrow (a = 50)$

Dai dati pubblici:
$\beta = \alpha^a \bmod p$
$5 = 19^a \bmod 191$

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

Matricola:

Domanda 3

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

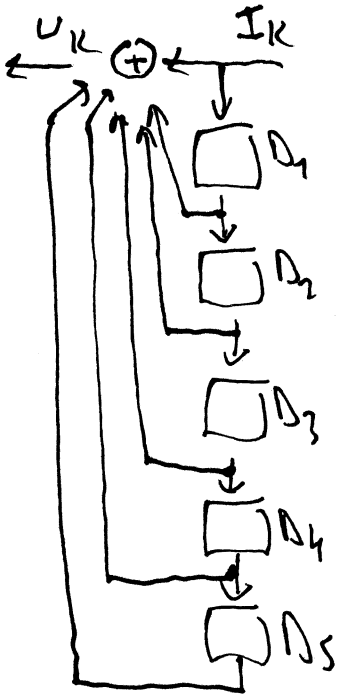
a) Si disegni lo schema di un *descrambler autosincronizzante* basato su registro a scorrimento LFSR con polinomio caratteristico $P(x) = x^5+x^4+x^3+x^2+x+1$. Si indichino la sequenza binaria in ingresso (da decodificare) con $\{I_k\}$ e la sequenza binaria in uscita (decodificata) con $\{U_k\}$.

b) Si inizializzino gli elementi di ritardo D_i ($i = 1, 2, 3, 4, 5$) con $\{1, 1, 1, 1, 1\}$ al passo iniziale $k = 0$. Si alimenti il *descrambler* con la sequenza da decodificare $\{I_k\} = \{0, 1, 0, 1, 0, 0, \ldots\}$ (periodica). Ricavare la sequenza decodificata $\{U_k\}$ all'uscita.

c) Verificare se il polinomio $P(x)$ è irriducibile in $\mathbb{Z}_2[x]$.

d) Volendo utilizzare uno scrambler con periodo della sequenza PRBS lunghissimo, pensiamo di provare con $P(x) = x^{256}+1$. E' una buona idea?

a)



b)

k	I_k	D_1	D_2	D_3	D_4	D_5	U_k
0	0	1	1	1	1	1	1
1	1	0	1	1	1	1	1
2	0	1	0	1	1	1	0
3	1	0	1	0	1	1	0
4	0	1	0	1	0	1	1
5	0	0	1	0	1	0	0
6	0	0	0	1	0	1	0
7	1	0	0	0	1	0	0
8	0	1	0	0	0	1	0

$n = 5$

Nota: La sequenza $\{I_k\}$ è generata dallo scrambler inizializzato con $\{0,0,1,0,1\}$

c)

$$x^5+x^4+x^3+x^2+x+1 \;\big|\; x+1$$

$$x^5+x^4 \qquad\qquad x^4+x^2+1$$

$$x^3+x^2+x+1$$

$$x^3+x^2$$

$$x+1$$

$$x+1$$

$$0$$

$$\Rightarrow P(x) = (x+1)(x^4+x^2+1) = (x+1)(x^2+x+1)^2$$

d) $P(x) = (x+1)^{256}$

Sicurezza delle Reti
Prof. Stefano Bregni **II Appello d'Esame 2025-26 – 14 luglio 2026**

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

Matricola:

Domanda 4
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Si consideri una funzione di hash $h = h(x)$ a 512 bit, robusta, di cui ad oggi non sono mai state violate le proprietà di unidirezionalità e resistenza alle collisioni. Rispondere motivando brevemente la risposta e commentando dove necessario.

- Dati due numeri $m_1 \neq m_2$, allora $h(m_1) \neq h(m_2)$, [redacted] $h = h(x)$ è resistente alle collisioni. Vero o falso?

- Dato un $\overline{h}$ qualsiasi, esiste 1 solo messaggio $\overline{m}$, tale che $h(\overline{m}) = \overline{h}$, praticamente impossibile da trovare se $h(x)$ è davvero unidirezionale. Vero o falso?

- Dati due numeri $m_1 \neq m_2$, qual è la probabilità che $h(m_1) = h(m_2)$?

$2^{-512} = \sim 10^{-155}$

b) Memorizzate i valori di *hash* calcolati con SHA-1 a 160 bit su N file scelti a caso in rete. Quanti file dovete elaborare, affinché la probabilità di trovarne almeno due con lo stesso *hash* sia $P > 0.10$?

$P \cong 1 - e^{-N^2/2^{n+1}}$ (prob. che almeno 2 abbiano lo stesso hash)

$n = 160$ $P > 0,1$

$e^{-N^2/2^{161}} < 0,9$ $N^2 > 2^{161} \cdot \ln \frac{1}{0,9} \cong 5,5 \cdot 10^{23}$

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (14 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

---

1) Cos'è un *residuo quadratico* dell'insieme $\mathbb{Z}_p^*$?

Si calcolino tutti i residui quadratici dell'insieme $\mathbb{Z}_{17}^*$, partendo dalle potenze dell'elemento primitivo $\alpha = 5 \in \mathbb{Z}_{17}^*$. Esaminando i risultati ottenuti, si dica se esistono e quali sono le radici quadrate di 2 e -2 (mod 17). *(2 punti)*

$5^0 \equiv 1 \pmod{17}$

$5^2 \equiv 8$ (- -)

$5^4 \equiv 13$

$5^6 \equiv 2 \longrightarrow \sqrt{2} \equiv \pm 5^2 \equiv \pm 6 \quad \{6, 11\}$

$5^8 \equiv 16$

$5^{10} \equiv 9$

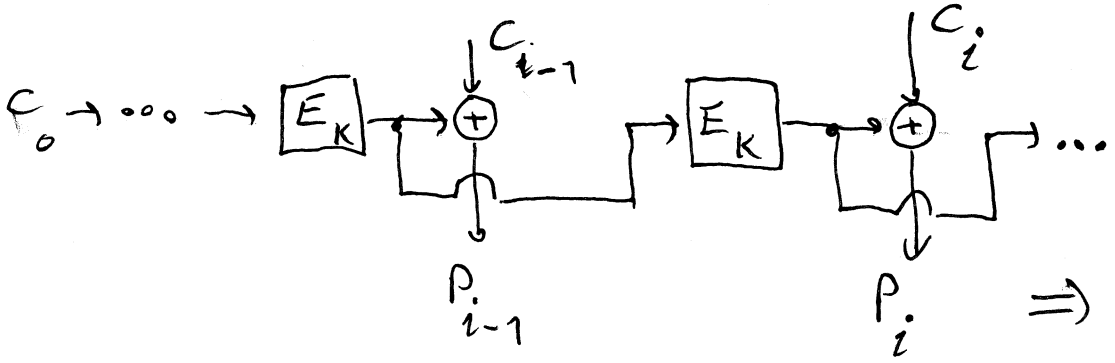
$5^{12} \equiv 4$

$5^{14} \equiv 15 \longrightarrow \sqrt{-2} \equiv \pm 5^7 \equiv \pm 10 \quad \{7, 10\}$

$\alpha_q = \{1, 2, 4, 8, 9, 13, 15, 16\}$

---

2) Si consideri un cifrario a blocchi concatenato secondo la modalità *Output FeedBack Mode* (OFB), in cui cifratura e decifratura sono svolte rispettivamente come $C_i = P_i \oplus E_K^{(i)}(C_0)$, $P_i = C_i \oplus E_K^{(i)}(C_0)$, C_0 è il vettore di inizializzazione, la dimensione dei blocchi P_i e C_i è 16 bit. Disegnare lo schema a blocchi del processo di decifrazione. Il flusso cifrato $\{C_i\}$ viene trasmesso da A a B, ma subisce errori di trasmissione puramente casuali con tasso ε. Quale sarà il tasso di errore sul flusso decifrato $\{P_i\}$ se $\varepsilon = 0.25$? *(2 punti)*



$\Rightarrow \varepsilon_{out} = 0,25$

Sicurezza delle Reti
Prof. Stefano Bregni — **II Appello d'Esame 2025-26 – 14 luglio 2026**

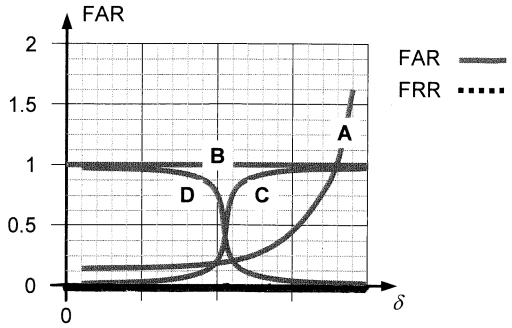
Cognome e nome: *(stampatello)* *(firma leggibile)*

Matricola:

3) 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 FAR(δ) rappresentate in figura, dove δ è la soglia di decisione del discriminatore, segnalando che sono il risultato di quattro procedure di misura diverse. *(2 punti)*

a) Quali di queste curve sono evidentemente errate? Spiegare perché.

A, B, D



b) Eseguite voi stessi la misura, questa volta seguendo il procedimento corretto, ma non vi accorgete che il sensore è completamente sporco. Sullo stesso diagramma, disegnate la curva FAR(δ) che ottenete.

4) Si dice che un giovedì mattina di qualche anno fa, invece del prof. Bregni, si presentò a lezione un tipo che nessuno aveva mai visto, e che si qualificò come un ex studente del corso. Disse che c'era un nuovo libro di testo da studiare, molto più chiaro di quelli consigliati nel programma ufficiale. Promise un nuovo metodo di studio, molto più facile dei libri tradizionali. Distribuì un QR con tutti i dati e l'indirizzo da cui scaricare il PDF. Per doppia sicurezza, però, il testo era stato cifrato due volte con una *Cifratura Affine* (mod 26) con parametri $a = 9$ e $b = 2$. Solo gli studenti esperti di questo metodo di cifratura avrebbero quindi potuto leggere il nuovo testo. Dopodiché, se ne andò e nessuno lo vide mai più. Si racconta che da quel giorno il numero di studenti frequentanti in presenza diminuì drasticamente. Qualcuno continuò a seguire online, ma senza mostrare mai più il viso in webcam.
Voi siete venuti in possesso del PDF. Il nome cifrato dell'autore è: "UBPURTGD". *(2 punti)*

a) Avendo studiato, sapete che non dovete decifrare due volte ma basta una volta sola. Quali sono i parametri della singola cifratura affine equivalente alla doppia sopra definita?

b) Decifrate il nome dell'autore. Decidete di non leggere il testo, cancellate il file sovrascrivendo tutti i byte 256 volte, e distruggete il vostro computer. Come si chiama l'autore?

a) $C_1 \equiv aP+b \pmod{26}$

$C_2 \equiv aC_1+b \pmod{26} \equiv a(aP+b)+b \equiv a^2P+ab+b \pmod{26}$

$\Rightarrow C_2 \equiv \alpha P+\beta \pmod{26}$ $\quad \alpha=3,\ \beta=20$

b) $P \equiv (C_2-\beta)\alpha^{-1} \pmod{26}$ $\quad \alpha^{-1} \equiv 9 \pmod{26}$

$\Rightarrow$ "ALHAZRED"

Alfabeto	
0	a
1	b
2	c
3	d
4	e
5	f
6	g
7	h
8	i
9	j
10	k
11	l
12	m
13	n
14	o
15	p
16	q
17	r
18	s
19	t
20	u
21	v
22	w
23	x
24	y
25	z

5) 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 64 bit, $P \in \mathbb{Z}_{128}$, $C \in \mathbb{Z}_{128}$. *(3 punti)*

a) Quante esecuzioni degli algoritmi $E_K(X)$ e $D_K(X)$ sono necessarie per realizzare un attacco forza bruta che trovi la coppia di chiavi K_1, K_2?

b) Descrivere la procedura di un attacco *Meet-in-the-Middle* per trovare la coppia di chiavi K_1, K_2. Cosa dovete conoscere per eseguire l'attacco?

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

a) 2^{128} esecuzioni di $E_K(x)$

b) P, C

c) 2^{64} esecuzioni di $E_K(P)$
2^{64} esecuzioni di $D_K(C)$

Occupazione memoria: $(2^{64}+1)\,16\ \text{byte} = 2^{68}\ \text{byte} = 256\ \text{EB}$

6) 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 è MD5 a 128 bit. Calcolate la quantità di memoria che vi sarà necessaria per completare questo attacco. *(3 punti)*

Per avere successo con prob > 50%: $(16\ \text{byte}) \cdot 2^{68} = 2^{72}\ \text{byte}$

$= 512\ \text{EB}$