Sicurezza delle Reti

Prof. Stefano Bregni — **V Appello d'Esame 2024-25 – 17 febbraio 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 firma elettronica di El Gamal* e pubblica $p = 139$, $\alpha = 12$, $\beta = \alpha^a \bmod p = 79$, 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.

$A_1 = (r_1, s_1) = (126, 84)$ $\quad P_1 = 12$
$A_2 = (r_2, s_2) = (126, 3)$ $\quad P_2 = 15$

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

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

$$\begin{cases} 84k \equiv 12 - a \cdot 126 \pmod{138} \\ 3k \equiv 15 - a\,126 \pmod{138} \end{cases}$$

$84k \equiv -3 \pmod{138}$ $\quad MCD(84, 138) = 3 \Rightarrow$ 3 soluzioni

$28k \equiv -1 \pmod{46}$ $\quad 28^{-1} \equiv 29 \pmod{46}$

$\rightarrow k_0 \equiv 17 \pmod{46}$ $\quad k_i \equiv 17, 63, 109 \pmod{138}$

$\Rightarrow$ **$k = 109$**

Dai dati pubblici:
$r \equiv \alpha^k \pmod{p}$ $\quad 126 \equiv 12^k \pmod{13}$

$3 \cdot 109 \equiv 15 - a\,126 \pmod{138}$

$126a \equiv 102 \pmod{138}$ $\quad MCD(126, 138) = 6 \Rightarrow$ 6 soluzioni

$21a \equiv 17 \pmod{23}$ $\quad 21^{-1} \equiv 11 \pmod{23}$

$\rightarrow a_0 \equiv 11 \cdot 17 \equiv 3 \pmod{23}$ $\quad a_i \equiv 3, 26, 49, 72, 95, 118 \pmod{138}$

$\Rightarrow$ **$a = 72$**

Dai dati pubblici:
$\beta \equiv \alpha^a \pmod{p}$ $\quad 79 \equiv 12^a \pmod{139}$

Sicurezza delle Reti
Prof. Stefano Bregni — **V Appello d'Esame 2024-25 – 17 febbraio 2026**

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

Matricola:

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

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 103$, $\alpha = 11$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 99$.

a) Si rende noto che $\alpha = 11$ è una radice primitiva di $\mathbb{Z}_{103}^*$. Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 106$ e spedisce il messaggio $P = 49$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob riceve $C' = (r', t') = (16, 29)$. Calcolare il messaggio decifrato da Bob P'.

a) p primo $1 < q \le p-2$ $p-1 = 102 = 2 \cdot 3 \cdot 17$ Tot ne α elem. prim. $\in \mathbb{Z}_p^*$

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

$11^{51} \equiv 102$
$11^{34} \equiv 56$
$11^{6} \equiv 64$
$\Rightarrow \alpha = 11$ OK

$\beta = \alpha^a \bmod p = 11^{99} \bmod 103 = 90$

b) $r = \alpha^k \bmod p = 11^{106} \bmod 103 = 11^4 \bmod 103 = 15$

$t = \beta^k \cdot P \bmod p = 90^4 \cdot 49 \bmod 103 = 28$

$\Rightarrow C = (15, 28)$

c) $P' = t' \cdot r'^{-a} \bmod p = 29 \cdot 16^{-99} \bmod 103 = 29 \cdot 16^3 \bmod 103 = 25$

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

Matricola:

Domanda 3

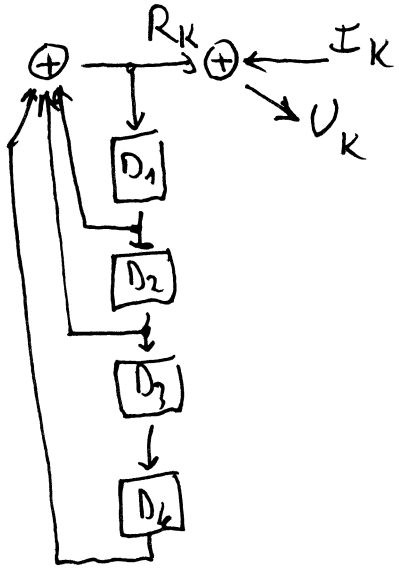
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Si disegni lo schema di uno *scrambler additivo* basato su registro a scorrimento LFSR con polinomio caratteristico $P(x) = x^4+x^2+x+1$. Si indichino la sequenza binaria in ingresso con $\{I_k\}$, la sequenza binaria in uscita con $\{U_k\}$, e la sequenza binaria pseudocasuale generata dallo scrambler con $\{R_k\}$.

b) Si inizializzino gli elementi di ritardo D_i ($i = 1, 2, 3, 4$) con {1, 0, 0, 1} al passo iniziale $k = 0$. Si alimenti lo *scrambler* con la sequenza $\{I_k\} = \{1, 1, 1, \ldots\}$ (tutti "1"). Ricavare la sequenza restituita all'uscita $\{U_k\}$, evidenziando la sua periodicità. Qual è il periodo P della sequenza?

c) Verificare se il polinomio $P(x)$ è irriducibile.

a)



b)

K	I_K	D_{1K}	D_{2K}	D_{3K}	D_{4K}	R_K	U_K
0	1	1	0	0	1	0	1
1	1	0	1	0	0	1	0
2	1	1	0	1	0	1	0
3	1	1	1	0	1	1	0
4	1	1	1	1	0	0	1
5	1	0	1	1	1	0	1
6	1	0	0	1	1	1	0
7	1	1	0	0	1	0	1

$T = 7$

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

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

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

$x^3 + x^2$

$x + 1$

$x + 1$

0

$\Rightarrow P(x)$ irriducibile

$P(x) = (x+1)(x^3+x^2+1)$

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

Matricola:

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* $y = h(x)$.

b) Memorizzate i valori di *hash* calcolati con MD5 a 128 bit su N file scelti a caso in rete. Per quale N la probabilità che tra di essi non vi siano nemmeno due file che abbiano lo stesso *hash* risulta $P < 0.01$?

$P \cong 1 - e^{-N^2/2^{n+1}}$

$n = 128$

$e^{-N^2/2^{129}} < 0{,}01$

$-N^2/2^{129} < \ln 0{,}01$

$N^2 > 2^{129} \cdot \ln 100 \Rightarrow N > 5{,}6 \cdot 10^{19}$

c) Si consideri la funzione di hash standard SHA-2 a 256 bit, denominata per brevità $h = h(x)$. Rispondere e motivare brevemente le risposte alle seguenti domande.

- Dati due valori m_1 e m_2, se $h(m_1) \neq h(m_2)$, allora $m_1 \neq m_2$, perché SHA è fortemente resistente alle collisioni. VERO o FALSO?

- Dati due valori m_1 e m_2, se $h(m_1) = h(m_2)$, allora $m_1 = m_2$. VERO o FALSO?

- Dati due valori m_1 e m_2 casuali, è più probabile che h_1 e h_2 differiscano per un numero maggiore di bit se $h_1 = h(m_1)$ e $h_2 = h(m_2)$, oppure se $h_1 = h(m_1)$ e $h_2 = h(m_1+1)$?

Sicurezza delle Reti
Prof. Stefano Bregni — **V Appello d'Esame 2024-25 – 17 febbraio 2026**

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

Matricola:

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) Si consideri ancora il problema assegnato nella Domanda 2. Calcolare il valore di k per il quale Alice ha calcolato $C' = (16, 29)$ del punto c), applicando l'algoritmo *Baby Step Giant Step* per risolvere l'equazione esponenziale discreta (bastano le prime 6 righe della tabella). *(2 punti)*

$11^K \bmod 103 = 16$

$N = \lceil \sqrt{p-1} \rceil = 11$

$\alpha^{-1} = 11^{-1} \equiv 75 \pmod{103}$

$\alpha^{-N} \equiv 21 \pmod{103}$

$K \equiv 5 + 11 \cdot 3 \equiv 38 \pmod{102}$

j	α^j	K	α^{-NK}	$\beta\alpha^{-NK}$
0	1	0	1	16
1	11	1	21	27
2	18	2	29	52
3	95	⇒3	94	(62)
4	15	4	17	
⇒5	(62)	5	48	

2) Vi siete persi girando in auto tra le montagne del Massachusetts. Arrivate in una cittadina quando ormai è notte. Chiedete all'unica persona che trovate per strada dove vi trovate. Il tizio non risponde, ma vi indica un cartello isolato che dice "CRUFLVE(7,7)" e rimane a fissarvi. Non sapendo cosa fare di meglio, provate a decifrare supponendo che sia una *Cifratura Affine* (mod 26) con chiave $a = 7$, $b = 7$. Rinunciate a cercare un motel e ripartite sgommando in derapata. Come si chiama la cittadina? *(2 punti)*

$C = E_K(P) = aP + b \bmod 26$

$P = D_K(C) = (C-b)a^{-1} \bmod 26$

$a^{-1} = 7^{-1} \equiv 15 \pmod{26}$

⇒ DUNWICH

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

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

Matricola:

3) Si consideri un generatore di password consistenti di 8 simboli casuali scelti nell'alfabeto Fremen, che comprende in tutto 27 caratteri (lettere), 3 forme mediali e 9 cifre (non c'è lo zero). Qual è la quantità di informazione [bit] delle password, se i simboli sono scelti indipendentemente uno dall'altro, la probabilità che un simbolo sia una lettera è 80%, che sia una forma mediale è 5%, che sia una cifra è 15%? *(2 punti)*

$$H(X) = -\left(0{,}80 \log_2 \frac{0{,}80}{27} + 0{,}05 \log_2 \frac{0{,}05}{3} + 0{,}15 \log_2 \frac{0{,}15}{9}\right) =$$

$$= 4{,}061 + 0{,}295 + 0{,}886 = 5{,}243 \text{ bit/simbolo}$$

$$H(8 \text{ simboli}) = 41{,}9 \text{ bit}$$

4) L'equazione $x^2 \equiv 26 \pmod{211}$ ha soluzione? Se la risposta è sì, calcolarne le radici, altrimenti risolvere $x^2 \equiv -26 \equiv 185 \pmod{211}$. *(2 punti)*

$p = 211$ primo $\Rightarrow$ l'eq. ha soluzione se $26^{105} \equiv 1 \pmod{211}$

$26^{105} \equiv -1 \pmod{211} \Rightarrow$ NO

$211 \equiv 3 \pmod 4 \Rightarrow$ l'eq. $x^2 \equiv 26 \pmod{211}$ non ha soluzione

l'eq. $x^2 \equiv -26 \pmod{211}$ ha 2 radici:

$$x_{1,2} \equiv \pm 26^{53} \equiv \pm 94 \pmod{211}$$

$$\equiv 94, 117 \pmod{211}$$

5) Dopo laboriose ricerche, su Astalavista hai trovato uno che vende certificati garantiti autentici emessi da TheTruth.Org per SUBJECT: <www.whitehouse.gov>. Ne compri uno. Che procedura segui per verificare l'autenticità del certificato? *(2 punti)*

6) Descrivere un *attacco del compleanno* che miri a ottenere una firma valida di un documento fraudolento, utilizzando una funzione di hash di lunghezza N bit. *(2 punti)*

7) Per un aeroporto, avete appena comprato un sistema di autenticazione biometrica basato su ripresa di immagini del viso dei passeggeri. Intendete misurare empiricamente FAR e FRR nella prima settimana di utilizzo. Che dati raccogliete? Con che formule stimate i valori di FAR e FRR del vostro sistema? *(2 punti)*