Sicurezza delle Reti

Prof. Stefano Bregni — **III Appello d'Esame 2024-25 – 11 settembre 2025**

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 $p = 163$, $\alpha = 7$, $\beta = \alpha^a \bmod p = 31$, 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.

$A_1 = (r_1, s_1) = (75, 14)$ $\quad P_1 = 25$
$A_2 = (r_2, s_2) = (75, 26)$ $\quad P_2 = 31$

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

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

$$\begin{cases} 14k \equiv 25 - 75a \pmod{162} \\ 26k \equiv 31 - 75a \pmod{162} \end{cases}$$

$12k \equiv 6 \pmod{162}$ $\quad MCD(12, 162) = 6 \Rightarrow$ 6 soluzioni

$2k \equiv 1 \pmod{27}$ $\quad 2^{-1} \equiv 14 \pmod{27}$

$\rightarrow k_0 \equiv 14 \pmod{27}$ $\quad k_i \equiv 14, 41, 68, (95), 122, 149 \pmod{162}$

$\Rightarrow \boxed{k = 95}$

Dai dati pubblici:
$r \equiv \alpha^k \pmod{p}$
$75 \equiv 7^k \pmod{163}$

$14 \cdot 95 \equiv 25 - 75a \pmod{162}$

$75a \equiv 153 \pmod{162}$ $\quad MCD(75, 162) = 3 \Rightarrow$ 3 soluzioni

$25a \equiv 51 \pmod{54}$ $\quad 25^{-1} \equiv 13 \pmod{54}$

$\rightarrow a_0 \equiv 51 \cdot 13 \equiv 15 \pmod{54}$ $\quad a_i \equiv 15, 69, (123) \pmod{162}$

$\Rightarrow \boxed{a = 123}$

Dai dati pubblici:
$\beta \equiv \alpha^a \pmod{p}$
$31 \equiv 7^a \pmod{163}$

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2024-25 – 11 settembre 2025**

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

Matricola:

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

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 257$, $\alpha = 18$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 200$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 18$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{19, 21\}$. 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*) $k = 12$ e spedisce il messaggio $P_1 = 60$. 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 $C_2 = (r_2, t_2) = (53, 91)$, $C_3 = (r_3, t_3) = (53, 65)$, $C_4 = (r_4, t_4) = (53, 111)$ e, per altra via, viene a sapere che $P_2 = 5$. Calcolare P_3 e P_4.

a) p primo $1 < a < p-2$ $p-1 = 256 = 2^8$ Tutti gli α el. prim. $\in \mathbb{Z}_p^*$

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

$19^{128} \equiv -1 \Rightarrow \alpha = 19$ OK ($\alpha = 18, 21$ NO) $\beta = \alpha^a \bmod p = 19^{200} \bmod 257 = 34$

b) $r_1 = \alpha^k \bmod p = 19^{12} \bmod 257 = 111$

$t_1 = \beta^k \cdot P_1 \bmod p = 34^{12} \cdot 60 \bmod 257 = 17 \Rightarrow C_1 = (111, 17)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $t_2^{-1} = 91^{-1} \equiv 209 \pmod{257}$

$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod p \equiv 5 \cdot 65 \cdot 209 \equiv 77 \pmod{257}$

$P_4 \equiv P_2 \frac{t_4}{t_2} \pmod p \equiv 5 \cdot 111 \cdot 209 \equiv 88 \pmod{257}$

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2024-25 – 11 settembre 2025**

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

Matricola:

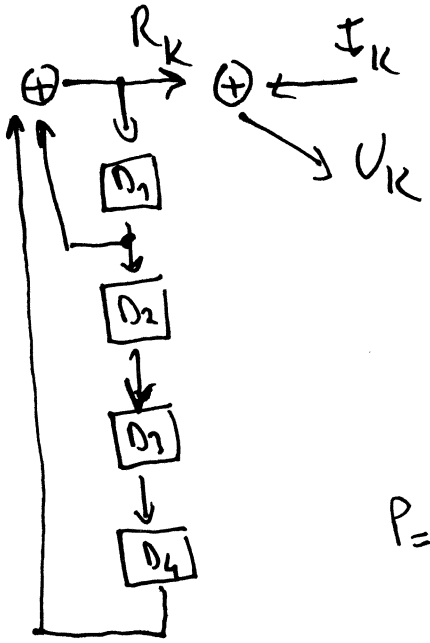
Domanda 3
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Si disegni lo schema di uno *scrambler additivo* basato su registro a scorrimento LFSR con polinomio caratteristico $P(x) = 1+x+x^4$. 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 $\{1, 0, 0, 0\}$ 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	0	1	0
1	1	1	1	0	0	1	0
2	1	1	1	1	0	1	0
3	1	1	1	1	1	0	1
4	1	0	1	1	1	1	0
5	1	1	0	1	1	0	1
6	1	0	1	0	1	1	0
7	1	1	0	1	0	1	0
8	1	1	1	0	1	0	1
9	1	0	1	1	0	0	1
10	1	0	0	1	1	1	0
11	1	1	0	0	1	0	1
12	1	0	1	0	0	0	1
13	1	0	0	1	0	0	1
14	1	0	0	0	1	1	0
15	1	1	0	0	0		
16	1						

$P = 15$

c)

$$\begin{array}{r|l} x^4+x+1 & x+1 \\ \hline x^4+x^3 & x^3+x^2+x \\ \hline x^3+x+1 & \\ x^3+x^2 & \\ \hline x^2+x+1 & \\ x^2+x & \\ \hline 1 & \end{array}$$

$$\begin{array}{r|l} x^4+x+1 & x^2+x+1 \\ \hline x^4+x^3+x^2 & x^2+x \\ \hline x^3+x^2+x+1 & \\ x^3+x^2+x & \\ \hline 1 & \end{array}$$

$\Rightarrow P(x)$ irriducibile

Domanda 4

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

a) Spiegare cosa significa affermare che una *funzione di hash* $h = h(x)$, necessariamente *non invertibile*, è *unidirezionale*.

b) Si consideri la funzione di hash standard SHA-2 a 256 bit, denominata per brevità $h = h(x)$. Per ognuna delle seguenti affermazioni, dire se è VERA o FALSA, motivando brevemente la risposta.

- Dato un $\overline{h}$ qualsiasi, esiste 1 solo numero $\overline{m}$, tale che $h(\overline{m}) = \overline{h}$, ma non posso calcolarlo perché SHA-2 è unidirezionale.

- 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.

- Per quanti bit differiscono le stringhe h_1 e h_2, dove $h_1 = h(m)$ e $h_2 = h(m+1)$, dato un m generico?

c) Si consideri una ipotetica funzione di *hash* $h = h(m) = m^{19} \bmod n$, dove $n = p \cdot q$, p e q sono due primi molto grandi noti, e m è un intero qualsiasi. Tale funzione di hash $h = h(m)$ è unidirezionale? E' resistente alle collisioni? Giustificare la risposta.

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 $p = 103$, $\alpha = 62$, $\beta = \alpha^a \bmod p = 25$, tenendo segreto l'esponente $a = 100$. Decifrare il messaggio $C = (r, t) = (24, 5)$. *(2 punti)*

$$P = t \cdot r^{-a} = 5 \cdot 24^{-100} \bmod 103 =$$
$$= 5 \cdot 24^{2} \bmod 103 = 99$$

2) Risolvere l'equazione $\alpha^x \equiv \beta \pmod p$ per $p = 61$, $\alpha = 6$, $\beta = 28$, applicando l'algoritmo *Baby Step Giant Step*. Per quanti valori di $\alpha \in \mathbb{Z}_p^*$ l'equazione ammette sicuramente soluzione, per qualsiasi valore di $\beta \in \mathbb{Z}_p^*$? *(3 punti)*

$6^x \equiv 28 \pmod{61}$

$N = 8$

$\alpha^{-1} = 51 \pmod{61}$

$\alpha^{-N} = 16 \pmod{61}$

$x \equiv 1 + 8 \cdot k \equiv 33 \pmod{61}$

j	α^j	k	α^{-Nk}	$\beta\alpha^{-Nk}$
0	1	0	1	28
(1)	(6)	1	16	21
2	36	2	12	31
3	33	3	9	8
4	15	(4)	22	(6)
5	29	5	47	35
6	52	6	20	11
7	7	7	15	54

$\Rightarrow x \equiv 33 \pmod{60}$

$\varphi(p-1) = 16$

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

Matricola:

3) Su Astalavista, 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: XXXXXXXXXXXXXXXXXXXX
Signature: YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY.

Sostituisci i tre parametri *Subject name / Public Key of the Subject / Signature* rispettivamente con: il tuo nome, la tua P.K., la tua firma. Il certificato è formalmente valido? Se no, cosa devi fare per renderlo formalmente valido?

4) 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 n bit, $P \in \mathbb{Z}_{256}^*$, $C \in \mathbb{Z}_{256}^*$. Descrivere la procedura di un attacco *Meet-in-the-Middle* per trovare la coppia di chiavi K_1, K_2. L'attacco si basa sulla conoscenza di quali informazioni? Quanti calcoli sono necessari? Quale occupazione di memoria [byte] è necessaria? *(3 punti)*

5) 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. *(3 punti)*