Sicurezza delle Reti

Prof. Stefano Bregni — **III Appello d'Esame 2022-23 – 5 settembre 2023**

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 $p = 109$, $\alpha = 6$ $\beta = \alpha^a \bmod p = 102$, 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.

$A_1 = (r_1, s_1) = (57, 26)$ $\quad P_1 = 20$
$A_2 = (r_2, s_2) = (57, 83)$ $\quad P_2 = 23$

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

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

$$\begin{cases} 26k \equiv 20 - 57a \pmod{108} \\ 83k \equiv 23 - 57a \pmod{108} \end{cases}$$

$57k \equiv 3 \pmod{108}$ $\quad MCD(57, 108) = 3 \Rightarrow$ 3 soluzioni

$19k \equiv 1 \pmod{36}$ $\quad 19^{-1} \equiv 19 \pmod{36}$

$k_0 \equiv 19 \pmod{36}$ $\quad k_i \equiv 19, 55, 91 \pmod{108}$

$\Rightarrow \boxed{k = 19}$

Dai dati pubblici:
$r \equiv \alpha^k \pmod{p}$
$57 \equiv 6^k \pmod{109}$

$26 \cdot 19 \equiv 20 - 57a \pmod{109}$

$57a \equiv 66 \pmod{109}$ $\quad MCD(57, 108) = 3 \Rightarrow$ 3 soluzioni

$19a \equiv 22 \pmod{36}$ $\quad 19^{-1} \equiv 19 \pmod{36}$

$a_0 \equiv 22 \pmod{36}$ $\quad a_i \equiv 22, 58, 94 \pmod{109}$

$\Rightarrow \boxed{a = 94}$

Dai dati pubblici:
$\beta \equiv \alpha^a \pmod{p}$
$102 \equiv 6^a \pmod{109}$

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2022-23 – 5 settembre 2023**

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 $p = 197$, $\alpha = 2$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 10$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 2$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{4, 6\}$. 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*) $k = 33$ e spedisce il messaggio $P_1 = 111$. 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 $C_2 = (r_2, t_2) = (89, 31)$, $C_3 = (r_3, t_3) = (89, 116)$, $C_4 = (r_4, t_4) = (89, 93)$ e, per altra via, viene a sapere che $P_2 = 50$. Calcolare P_3 e P_4.

a) p primo $1 < a < p-2$ $p-1 = 196 = 2^2 \cdot 7^2$ Tutte a elem. prim. di $\mathbb{Z}_p^*$

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

$2^{98} \equiv -1$, $2^{196} \equiv 1$ $\Rightarrow$ $\alpha = 2$ OK ($\alpha = 4, 6$ NO)

$\beta = \alpha^a \bmod p = 2^{10} \bmod 197 = 39$

b) $r_1 = \alpha^k \bmod p = 2^{33} \bmod 197 = 176$

$t_1 = \beta^k P_1 \bmod p = 39^{33} \cdot 111 = 130$

$\Rightarrow C_1 = (176, 130)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $\quad t_2^{-1} \equiv 31^{-1} \equiv 89 \pmod{197}$

$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod p$ $\quad P_3 \equiv 50 \cdot 116 \cdot 89 \equiv 60 \pmod{197}$

$P_4 \equiv P_2 \frac{t_4}{t_2} \pmod p$ $\quad P_4 \equiv 50 \cdot 93 \cdot 89 \equiv 150 \pmod{197}$

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2022-23 – 5 settembre 2023**

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

Matricola:

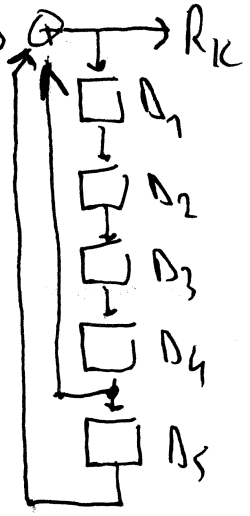
Domanda 3
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Si disegni lo schema di un generatore di sequenza PRBS basato su registro a scorrimento LFSR, realizzato come *scrambler autosincronizzante* con polinomio caratteristico $P(x) = x^5+x^4+1$ alimentato con tutti "0". Si indichino la sequenza binaria in ingresso con $\{I_k\} \equiv \{0\}$ e la sequenza binaria in uscita con $\{R_k\}$.

b) Si inizializzino gli elementi di ritardo D_i ($i = 1, 2, 3, 4, 5$) con $\{1, 0, 0, 0, 0\}$ al passo iniziale $k = 0$. Ricavare la sequenza PRBS $\{R_k\}$ generata all'uscita, evidenziando la sua periodicità. Qual è il periodo Π della sequenza?

c) Verificare se il polinomio $P(x)$ è irriducibile. Se non lo è, scomporlo in fattori (polinomi irriducibili). Il periodo Π riscontrato al passo b) è uno dei valori previsti dalla teoria nel caso in cui $P(x)$ sia irriducibile?

a)



b)

k	I_k	D_{1k}	D_{2k}	D_{3k}	D_{4k}	D_{5k}	R_k
0	0	1	0	0	0	0	0
1	0	0	1	0	0	0	0
2	0	0	0	1	0	0	0
3	0	0	0	0	1	0	1
4	0	1	0	0	0	1	1
5	0	1	1	0	0	0	0
6	0	0	1	1	0	0	0
7	0	0	0	1	1	0	1
8	0	1	0	0	1	1	0
9	0	0	1	0	0	1	1
10	0	1	0	1	0	0	0
11	0	0	1	0	1	0	1
12	0	1	0	1	0	1	1
13	0	1	1	0	1	0	1
14	0	1	1	1	0	1	1
15	0	1	1	1	1	0	1
16	0	1	1	1	1	1	0
17	0	0	1	1	1	1	0
18	0	0	0	1	1	1	0
19	0	0	0	0	1	1	0
20	0	0	0	0	0	1	1
21	0	1	0	0	0	0	0

$\Pi = 21$

c) $\Pi \notin \{1, 31\}$

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

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

$x^3 + 1$

$x^3 + x^2 + x$

$x^2 + x + 1$

$x^2 + x + 1$

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

Domanda 4

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

a) Si consideri una ipotetica funzione di hash basata su SHA, ma semplificata perché troncata ai primi 32 bit generati da SHA-2 256. Come procederesti per tentare di violarne la *unidirezionalità*? Ci riuscirai?

b) Si consideri una ipotetica funzione di hash basata su SHA, ma semplificata perché troncata ai primi 32 bit generati da SHA-2 256. Come procederesti per tentare di dimostrare che non è *fortemente resistente alle collisioni*? Ci riuscirai?

c) Si consideri una ipotetica funzione di *hash* $h = h(m) = m^3 \bmod n$, dove $n = p \cdot q$, p e q sono due primi molto grandi e m è un intero qualsiasi. Si spieghi perché tale funzione di hash $h = h(m)$ è unidirezionale, ma non resistente alle collisioni (neanche debolmente).

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2022-23 – 5 settembre 2023**

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 un generatore di password consistenti di 8 simboli casuali scelti nell'alfabeto greco, che comprende 17 consonanti e 7 vocali. Qual è la quantità di informazione [bit] delle password, se i simboli sono scelti indipendentemente una dall'altro, la vocale è sempre una α, e la probabilità che i simboli siano una consonante o una vocale α vale rispettivamente 50% e 50%? *(2 punti)*

$H(x) = -\left(0{,}50 \log_2 \frac{0{,}50}{17} + 0{,}50 \log_2 0{,}50\right) = 3{,}544 + 0{,}5 = 3{,}044$ bit/simbolo

$H(8 \text{ simboli}) = 24{,}35$ bit

2) Quali sono i valori che può assumere il periodo $\Pi = \pi(x_0)$ delle sequenze PRBS generate dall'Algoritmo *Blum-Blum-Shab* per $p = 17$, $q = 89$ e valori arbitrari del seme $x_0 = x^2 \in \mathbb{Z}_n$? *(2 punti)*

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

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

$\lambda(n) = \text{mcm}(16, 88) = 2^4 \cdot 11 = 176$

$\lambda[\lambda(n)] = \lambda(176) = \text{mcm}(\lambda(2^4), \lambda(11)) = \text{mcm}(4, 10) = 20$

$\Pi \mid 20 \Rightarrow \Pi \in \{1, 2, 4, 5, 10, 20\}$

3) Cos'è l'*ordine* di un elemento $\alpha \in \mathbb{Z}_p^*$? Quanti sono i valori possibili dell'ordine di un elemento $\alpha \in \mathbb{Z}_{89}^*$? *(2 punti)*

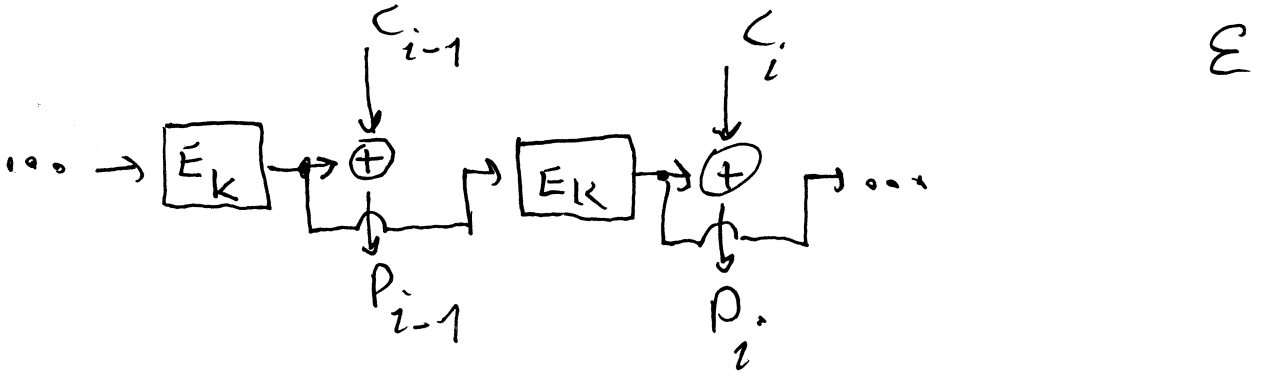
$(\text{ord}(\alpha) \mid 88)$ 8

4) Trovare i parametri (*a, b*) del *Cifrario Affine* (mod 26) che cifra "nyarlathotep" in "xkkxxkxxkxkx". Esiste una sola risposta alla domanda posta? *(2 punti)*

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

- $E_K(x) = ax + b \bmod 26$
- "a" → "k": $a \cdot 0 + b \equiv 10 \pmod{26} \Rightarrow b = 10$
- "y" → "x": $a \cdot 17 + 10 \equiv 23 \pmod{26}$
(scelgo "y" perché $17 \nmid 26$)
$17a \equiv 13 \pmod{26}$
$a \equiv 23 \cdot 13 \equiv 13 \pmod{26} \Rightarrow a = 13$
- Sì

5) Si consideri un cifrario a blocchi concatenato secondo la modalità *Output FeedBack Mode* (CFB), 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 1024 bit. Se il flusso cifrato $\{C_i\}$ subisce errori di trasmissione puramente casuali con tasso ε molto piccolo (ossia, gli errori sono rari ed isolati), quale sarà il tasso di errore sul flusso decifrato $\{P_i\}$? Per rispondere, può essere utile disegnare lo schema a blocchi del processo di decifrazione. *(2 punti)*



ε

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

Matricola:

6) Menzionare un vantaggio e uno svantaggio di utilizzare a) una sequenza di bit puramente casuale piuttosto che b) una pseudo casuale generata con un certo algoritmo, per cifrare un flusso di dati tramite somma binaria XOR. *(2 punti)*

7) Descrivere il *Test di Primalità di Fermat*. Cos'è un *Numero di Carmichael*? *(2 punti)*