Sicurezza delle Reti

Prof. Stefano Bregni — **II Appello d'Esame 2024-25 – 25 luglio 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) (6 punti)

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 251$, $\alpha = 6$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 24$.

a) Si rende noto che $\alpha = 6$ è una radice primitiva di $\mathbb{Z}_{251}^*$. Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 32$ e spedisce il messaggio $P_1 = 200$. 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 $C_2 = (r_2, t_2) = (127, 83)$, $C_3 = (r_3, t_3) = (127, 48)$, $C_4 = (r_4, t_4) = (127, 72)$ e, per altra via, viene a sapere che $P_2 = 20$. Calcolare P_3 e P_4.

$(k=31)$

a) $\beta = \alpha^a \bmod p = 6^{24} \bmod 251 = 23$

b) $r_1 = \alpha^k \bmod p = 6^{32} \bmod 251 = 9$

$t_1 = \beta^k \cdot P_1 \bmod p = 23^{32} \cdot 200 \bmod 251 = 14$ $\Rightarrow C_1 = (9, 14)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $\qquad t_2^{-1} = \beta^{-1} \equiv 124 \pmod{251}$

$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod p \equiv 20 \cdot 48 \cdot 124 \equiv 66 \pmod{251}$

$P_4 \equiv P_2 \frac{t_4}{t_2} \pmod p \equiv 20 \cdot 72 \cdot 124 \equiv 99 \pmod{251}$

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 $p = 127$, $\alpha = 7$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 97$.

a) Si rende noto che $\alpha = 7$ è una radice primitiva di $\mathbb{Z}_{127}^*$. Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 12$ e spedisce il messaggio $P = 99$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob riceve $C' = (r', t') = (30, 85)$. Calcolare il messaggio decifrato da Bob P'.

a) p primo $1 < a \leq p-2$ $p-1 = 126 = 2 \cdot 3^2 \cdot 7$

$\beta = \alpha^a \bmod p = 7^{97} \bmod 127 = 46$

b) $r = \alpha^k \bmod p = 7^{12} \bmod 127 = 50$

$t = \beta^k P \bmod p = 46^{12} \cdot 99 \bmod 127 = 62 \Rightarrow C = (50, 62)$

c) $P' = t' \cdot r'^{-a} = 85 \cdot 30^{-97} \bmod 127 \equiv 85 \cdot 30^{29} \equiv 101$

Domanda 3

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

a) Ricavare la sequenza binaria pseudo-casuale $\{x_i\}$ generata dall'algoritmo *Blum-Blum-Shab* per $p = 31$, $q = 59$, $x = 60$ e determinarne il periodo P. I primi p,q e il seme iniziale x rispettano le ipotesi del metodo?

i	x_i	b_i
0	1771	1
1	1535	1
2	573	1
3	591	1
4	1771	1
⋮	⋮	⋮

$\pi = 4$

$n = p \cdot q = 31 \cdot 59 = 1829$

$x_0 \equiv x^2 \pmod n$

$x_i \equiv x_{i-1}^2 \pmod n$

$31 \equiv 3 \pmod 4$
$59 \equiv 3 \pmod 4$
$60 \perp 1829$
$\Rightarrow$ OK

b) In base alla teoria, quali sono i valori possibili che può assumere il periodo $P = \pi(x_0)$ del generatore precedente, per valori arbitrari del seme $x_0 = x^2 \in \mathbb{Z}_n$?

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

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

$\lambda(n) = \operatorname{mcm}(30, 58) = 2 \cdot 3 \cdot 5 \cdot 29 = 870$

$\lambda[\lambda(n)] = \lambda(870) = \operatorname{mcm}(2, 4, 28) = 28$

$\pi(x_0) \in \{1, 2, 4, 7, 14, 28\}$

Domanda 4

(svolgere su questo foglio nello spazio assegnato) (8 punti)

a) Definire la proprietà di *resistenza forte alle collisioni* di una *funzione di hash* $y = h(x)$.

b) Si consideri una *funzione di hash* $y = h(x)$, *ovviamente* non invertibile, ma che tutti ben sanno non unidirezionale.

- Perché "*ovviamente*"?

- Se la unidirezionalità di $h(x)$ è facilmente violabile, è legittimo temere il rischio che qualcuno ricavi la nostra password pw, se pubblichiamo il suo valore di hash $y = h(pw)$?

c) Memorizzate i valori di *hash* calcolati con SHA2-160 su N file scelti a caso in rete. Per quale N la probabilità che almeno due file abbiano lo stesso *hash* risulta $P > 0.9$?

$P \cong 1 - e^{-N^2/2^{n+1}}$ $\quad e^{-N^2/2^{161}} < 0,1$

$n = 160$ $\quad -N^2/2^{161} < \ln 0,1$

$N^2 > 2^{161} \cdot \ln 10 \Rightarrow N > N 2,6 \cdot 10^{24}$

d) Si consideri una ipotetica funzione di hash $h = h(m) = m^e \bmod n$, con $e = 8$, $n = p \cdot q$, con p e q primi di 200 cifre utilizzati per calcolare n e poi dimenticati (ossia, una cifratura RSA del messaggio m con chiave pubblica (e, n)).

- La funzione $h(m)$ è unidirezionale o no? Perché?

- Provare che $h(m)$ non è resistente alle collisioni, fornendo un esempio di collisione.

Sicurezza delle Reti
Prof. Stefano Bregni — **II Appello d'Esame 2024-25 – 25 luglio 2025**

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

Matricola:

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (11 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 per quale valore di k Alice ha calcolato $C' = (30, 85)$ del punto c), applicando l'algoritmo *Baby Step Giant Step* per risolvere l'equazione esponenziale discreta. *(3 punti)*

$7^k \equiv 30 \pmod{127}$

$N = \lceil p-1 \rceil = 12$

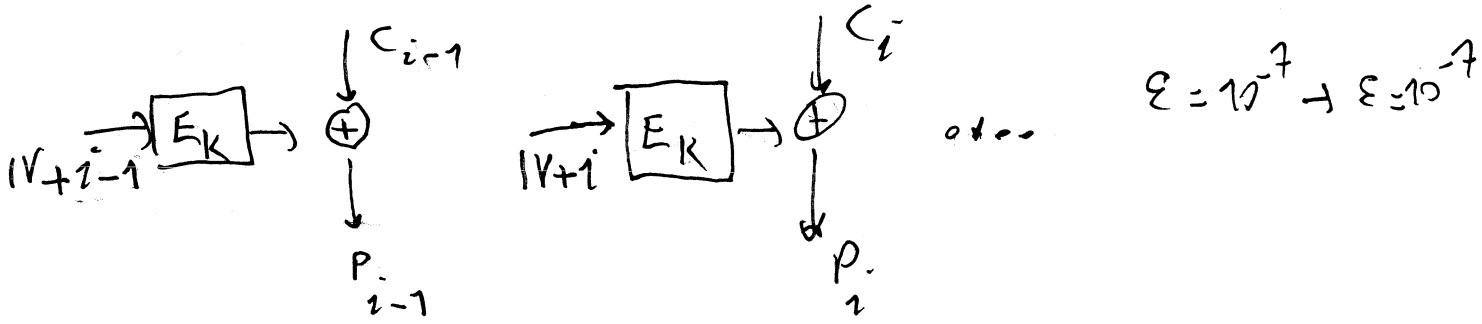
$\alpha^{-1} \equiv 7^{-1} \equiv -18 \equiv 109 \pmod{127}$

$\alpha^{-N} \equiv 94 \pmod{127}$

$\Rightarrow K = 4 + 12 \cdot 8 = (100) \pmod{126}$

j	α^j	k	α^{-Nk}	$\beta\alpha^{-Nk}$
0	1	0	1	30
1	7	1	94	26
2	49	2	73	31
3	89	3	4	120
→ 4	(115)	4	122	104
5	43	5	38	124
6	47	6	16	99
7	75	7	107	35
8	17	→ 8	25	(115)
9	119	9	64	
10	71	10	47	
11	116	11	100	

2) Si consideri un cifrario a blocchi concatenato secondo la modalità *Counter Mode* (CTR), in cui cifratura e decifratura sono svolte rispettivamente come $C_i = P_i \oplus E_K(IV^{(i)})$, $P_i = C_i \oplus E_K(IV^{(i)})$, $IV^{(i)} = IV+i$, IV è il vettore di inizializzazione, la dimensione dei blocchi P_i e C_i è 512 bit. Disegnare lo schema a blocchi del processo di decifrazione. Se il flusso cifrato $\{C_i\}$ subisce errori di trasmissione puramente casuali con tasso $\varepsilon = 10^{-7}$, quale sarà il tasso di errore sul flusso decifrato $\{P_i\}$? *(2 punti)*



3) Trovare i parametri (*a, b*) del *Cifrario Affine* (mod 26) che decifra "DMQLZQPRSPYH" in "NYARLATHOTEP". *(2 punti)*

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

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

"Q" $\xrightarrow{D_K}$ "A" $\Rightarrow 0 \equiv (16-b)a^{-1} \pmod{26} \Rightarrow \boxed{b=16}$

"L" $\xrightarrow{D_K}$ "R" $\Rightarrow 17 \equiv (11-b)a^{-1} \pmod{26}$

$17 \equiv -5a^{-1} \pmod{26} \quad 17 \equiv 21a^{-1} \pmod{26}$

$a^{-1} \equiv 17 \cdot 5 \equiv 7$

$a \equiv 7^{-1} \equiv 15 \Rightarrow \boxed{a=15}$

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

4) Avete appena messo all'opera un nuovo sistema di autenticazione biometrica basato su ripresa di immagini del viso degli utenti. Intendete misurare empiricamente il FRR nella prima settimana di utilizzo. Che dati raccogliete? Come stimate il valore di FRR del vostro sistema? *(2 punti)*

5) Dopo laboriose ricerche, su Astalavista hai trovato uno che vende certificati garantiti autentici emessi da TheTruthOrg per SUBJECT: <www.whitehouse.gov>. Ne compri uno. *(2 punti)*

a) Che procedura segui per verificare l'autenticità del certificato?

b) Dopo la verifica a), il certificato risulta valido. Tuttavia, la Casa Bianca contattata in proposito dichiara di non avere nulla a che fare con questo certificato. Quale segreto deve avere violato l'impostore, per poter creare il certificato?