

Sicurezza delle Reti

Prof. Stefano Bregni

V Appello d'Esame 2023-24 – 29 gennaio 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) (7 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 $a = 103$.

- Si rende noto che $\alpha = 7$ è una radice primitiva di \mathbb{Z}_{127}^* . Calcolare β .
- Alice estrae il numero casuale segreto (nonce) $k = 128$ e spedisce il messaggio $P = 100$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.
- Bob riceve $C' = (r', t') = (31, 20)$. Calcolare il messaggio decifrato da Bob P' .
- Calcolare il valore di k per cui Alice ha calcolato $C' = E[P]$ applicando l'algoritmo Baby Step Giant Step (bastano le prime 7 righe della tabella).

a) p primo $1 < a \leq p-2$ $p-1 = 126 = 2 \cdot 3^2 \cdot 7$ Teste elem. primitivo $\in \mathbb{Z}_p^*$
 $7^{63} \equiv 126$
 $7^{42} \equiv 127$
 $7^{18} \equiv 64$ $\Rightarrow \alpha = 7$ OK $\beta = \alpha^a \bmod p = 7^{103} \bmod 127 = 3$
 $\alpha^{p-1} \not\equiv 1 \pmod{p}$

b) $r = \alpha^k \bmod p = 7^{128} \bmod 127 \equiv 7^2 \equiv 49$
 $t = \beta^k P \bmod p = 3^2 \cdot 100 \bmod 127 = 11$

$\Rightarrow C = (49, 11)$

c) $P' = t' \cdot r'^{-a} \bmod p = 20 \cdot 31^{-103} \bmod 127 \equiv 20 \cdot 31^{23} \bmod 127 = 55$

d) $7^k \bmod 127 = 31$

$N = [p-1] = 12$

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

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

$k \equiv 4 + 12 \cdot 6 \equiv 76 \pmod{126}$

(mod p)	i	α^i	k	α^{-Nk}	$\beta \alpha^{-Nk}$
0	1	0	1	31	
1	7	1	94	120	
2	49	2	73	104	
3	89	3	4	124	
4	115	4	122	99	
5	43	5	38	35	
6	47	6	16	115	

Domanda 2

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

Bob adotta il sistema di firma elettronica di El Gamal e pubblica $p = 181$, $\alpha = 10$, $\beta = \alpha^a \bmod p = 22$, tenendo segreto l'esponente a ($1 < a \leq p-2$).

Bob estrae il numero casuale segreto k (nonce) con $\text{MCD}(k, p-1) = 1$. 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 .

$$A_1 = (r_1, s_1) = (78, 11) \quad P_1 = 25$$

$$A_2 = (r_2, s_2) = (78, 96) \quad P_2 = 30$$

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

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

$$\begin{cases} 11 \cdot k \equiv 25 - 78a \pmod{180} \\ 96 \cdot k \equiv 30 - 78a \pmod{180} \end{cases}$$

$$\begin{aligned} 15k &\equiv 5 \pmod{180} & \text{MCD}(15, 180) = 15 \Rightarrow 12 \text{ soluzioni} \\ 17k &\equiv 1 \pmod{36} & 17^{-1} \equiv 17 \pmod{36} \end{aligned}$$

$$k_0 \equiv 17 \pmod{36}$$

$$k_i \equiv 17, 53, 89, 125, 161 \Rightarrow \boxed{k = 53}$$

Nei dati pubblici:

$$r \equiv \alpha^k \pmod{p}$$

$$10^{53} \equiv 78 \pmod{181}$$

$$11 \cdot 53 \equiv 25 - 78a \pmod{180}$$

$$78a \equiv 162 \pmod{180}$$

$$\text{MCD}(78, 180) = 6 \Rightarrow 6 \text{ soluzioni}$$

$$13a \equiv 27 \pmod{30}$$

$$13^{-1} \equiv 7 \pmod{30}$$

$$a_0 \equiv 7 \cdot 27 \equiv 9 \pmod{30}$$

$$a_i \equiv 9, 39, 69, 99, 129, 159 \pmod{180}$$

$$\Rightarrow \boxed{a = 99}$$

Nei dati pubblici

$$\beta \equiv \alpha^a \pmod{p}$$

$$10^{99} \equiv 22 \pmod{181}$$

Domanda 3

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

Alice e Bob adottano un sistema di firma cieca RSA. Alice pubblica il modulo $n = 589$ e l'esponente di cifratura $e = 23$. Bob estrae il numero casuale segreto (nonce) $k = 82$ e chiede ad Alice di firmare ciecamente il messaggio $P = 500$.

a) Verificare la correttezza dei dati forniti secondo le ipotesi del metodo di firma cieca RSA.

$$(k = -7)$$

b) Calcolare i messaggi scambiati da Alice e Bob e la firma A del messaggio P .

$$a) m = 589 = 19 \cdot 31 \quad \phi(m) = 540 = 2^2 \cdot 3^3 \cdot 5 \quad \phi[\phi(m)] = 144$$

$$b) d = e^{-1} \bmod \phi(m) = 23^{-1} \bmod 540 = 47 \quad (\text{meglio con E.E.})$$

$$A \leftarrow B \quad t = k^e P \bmod n = (-7)^{23} \cdot 500 \bmod 589 = -9 \equiv 580$$

$$A \rightarrow B \quad s = t^d \bmod n = (-9)^{47} \bmod 589 = -81 \equiv 508$$

$$\text{Bob calcola le firme: } A = s/k \bmod n = (-81) \cdot (-580) \bmod 589$$

$$k^{-1} \bmod n = -580 = 89 \quad (\text{E.E.}) \quad (= 264)$$

$$\text{Verifica: } A = P^d \bmod n = 500^{47} \bmod 589 = 264$$

Domanda 4

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

a) Definire la proprietà di *resistenza forte alle collisioni* di una funzione di hash $y = h(x)$.b) I valori di *hash* di $N = 1000$ file sono calcolati con SHA-3 e quindi troncati agli ultimi n bit per risparmiare memoria. Quanto dovrebbe valere n , affinché la probabilità P che almeno due file abbiano lo stesso *hash* sia $< 10^{-4}$?

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

$$N = 1000$$

$$P < 10^{-4}$$

$$e^{-N^2/2^{n+1}} > 0,9999$$

$$2^{n+1} > \frac{10^6}{-\ln 0,9999} \Rightarrow n \geq 33$$

c) Hai proposto alla tua Azienda di adottare la funzione di hash $h(m) = E_K("00...0")$, definita come la cifratura AES di un blocco di 128 zeri "00...0" con chiave K uguale agli ultimi 128 bit (i 128 bit meno significativi) del messaggio m . Per verificarne la robustezza, l'Azienda mette a disposizione un premio di €100.000 per il primo che riesca a vincere una delle seguenti sfide pubbliche a tua scelta:

- 1) provare entro 1 ora dalla pubblicazione che $h(m)$ non è unidirezionale;
- 2) provare entro 1 ora dalla pubblicazione che $h(m)$ non è fortemente resistente alle collisioni;

Se nessuno vince la sfida da te scelta, il premio va a te.

Quale delle due sfide scegli di bandire? Perché?

Cognome e nome:

(stampatello)

(firma leggibile)

Matricola:

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) La biblioteca della Miskatonic University riceve da un anonimo mecenate un pacco contenente un antico volume. Sull'involucro, una sola parola: "RUMHIRIAKMIR". Viene interpellato il Dott. Henry Armitage, il quale, ricordando gli accadimenti del 9 luglio, riconosce una *Cifratura Affine* (mod 26) e decifra la parola in "NECRONOMICON". Quali sono i parametri a e b di quella cifratura così decodificata? (3 punti)

$$C = E_K(P) = aP + b \pmod{26}$$

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

$$\begin{aligned} "A" \xrightarrow{D_K} "M" &\Rightarrow (C - b)a^{-1} \equiv 12 \pmod{26} \\ b &\equiv 14a \pmod{26} \end{aligned}$$

$$\Rightarrow \begin{cases} a = 17 \\ b = 4 \end{cases}$$

$$\begin{aligned} "N" \xrightarrow{D_K} "R" &\Rightarrow (17 - b)a^{-1} \equiv 13 \pmod{26} \\ 13a + b &\equiv 17 \pmod{26} \\ a &\equiv 17 \cdot 1 \equiv 17 \end{aligned}$$

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

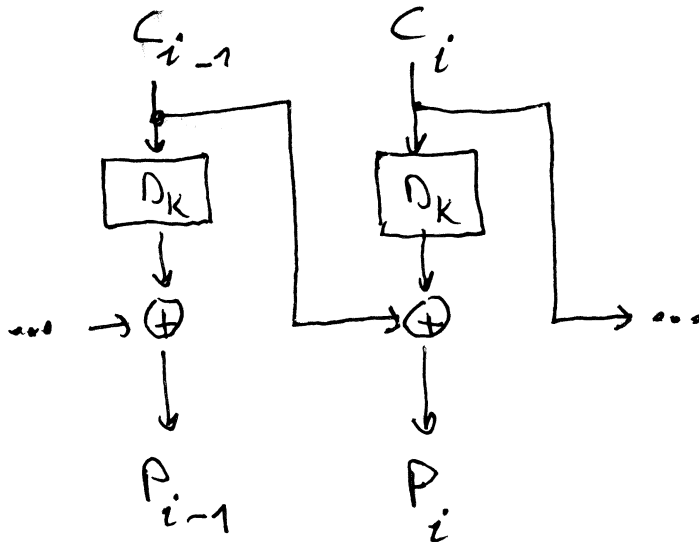
- 2) Cos'è un residuo quadratico dell'insieme \mathbb{Z}_p^* ? Quanti sono i residui quadratici in \mathbb{Z}_{1009}^* ?

(2 punti)

- 3) Nel protocollo di *Diffie-Hellman* per l'instaurazione di una chiave simmetrica K_{AB} , cosa succede se α non è una radice primitiva di \mathbb{Z}_p^* ? Il metodo funziona lo stesso o no?

(2 punti)

- 4) Si consideri un cifrario a blocchi concatenato secondo la modalità *Cipher Block Chaining* (CBC), in cui cifratura e decifratura sono svolte rispettivamente come $C_i = E_K(P_i \oplus C_{i-1})$ e $P_i = C_{i-1} \oplus D_K(C_i)$, C_0 è il vettore di inizializzazione, la dimensione dei blocchi P_i e C_i è 2048 bit. Disegnare lo schema a blocchi del processo di decifrazione. Se il flusso cifrato $\{C_i\}$ viene trasmesso da A a B, ma subisce errori di trasmissione puramente casuali con tasso $\varepsilon = 10^{-9}$, quale sarà il tasso di errore sul flusso decifrato $\{P_i\}$? (2 punti)



$$\varepsilon \cong 10^{-6}$$

- 5) State considerando l'acquisto di un sistema di autenticazione di utenti basato su biometria. Dalle statistiche di utilizzo, il Fornitore mette in evidenza il dato empirico $FRR = 10^{-9}$. Siete soddisfatti? (2 punti)

- 6) Avete comprato una macchina in grado di violare la unidirezionalità di SHA-2 a 256 bit in pochi minuti. Un server memorizza gli hash SHA-2 256 delle password degli utenti in un file pubblico. Perché è impossibile che ricaviate le password degli utenti, nonostante la vostra macchina? Il server ha ugualmente qualcosa da temere da voi? (2 punti)