

Sicurezza delle Reti

Prof. Stefano Bregni

I Appello d'Esame 2023-24 – 1 luglio 2024

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 firma elettronica di El Gamal e pubblica $p = 139$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 27$.

- Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 3$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{4, 5\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β .
- Bob estrae il numero casuale segreto (*nonce*) $k = 83$. Per questo valore di k , calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 25$.
- Verificare se la firma $A' = (r', s') = (17, 12)$ è valida da Bob per il messaggio $P = 9$.
- Se è valida, calcolare il valore di k per cui è stata calcolata da Bob risolvendo l'equazione che restituisce $s = 12$ (non Baby Step Giant Step).

a) primo $1 \leq \alpha \leq p-2$ $k \perp p-1$ $p-1 = 138 = 2 \cdot 3 \cdot 23$

127 e α el. prim. $\neq 1 \pmod{p}$
 $\alpha^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$

$$\left. \begin{array}{l} 3^{69} \equiv -1 \\ 3^{46} \equiv 42 \\ 3^6 \equiv 34 \end{array} \right\} \Rightarrow \alpha = 3 \text{ (OK)} \quad (\alpha = 4, 5 \text{ NO}) \quad \beta = \alpha^a \bmod p = 3^{27} \bmod 139 = 8$$

b) $r = \alpha^k \bmod p = 3^{83} \bmod 139 = 21$

$$s = k^{-1}(P - ar) \pmod{p-1} = 5 \cdot (25 - 27 \cdot 21) \bmod 138 = 50 \Rightarrow A = (21, 50)$$

$$k^{-1} = 83^{-1} \equiv 5 \pmod{138}$$

c) $\beta^r \cdot r^s \equiv \alpha^P \pmod{p}$

$$8^{17} \cdot 17^{12} \equiv 84 \pmod{139}$$

$$3^9 \equiv 84 \pmod{139}$$

$$\left. \begin{array}{l} 8^{17} \cdot 17^{12} \equiv 84 \pmod{139} \\ 3^9 \equiv 84 \pmod{139} \end{array} \right\} \Rightarrow A' = (17, 12) \text{ firma valida di } P = 9$$

$$d) \quad Ks \equiv P - ar \pmod{p-1}$$

$$12 \cdot K \equiv 9 - 27 \cdot 17 \pmod{139}$$

$$12 \cdot K \equiv 102 \pmod{139} \quad \text{m.c.d.}(12, 139) = 1 \Rightarrow 6 \text{ soluzioni}$$

$$\rightarrow 2K \equiv 17 \pmod{23} \quad 2^{-1} \equiv 12 \pmod{23}$$

$$\Rightarrow K_0 \equiv 20 \pmod{23}$$

$$K_i \equiv 20, 43, 66, 89, 112, 135 \pmod{139}$$

$$\text{Dai dati pubblici: } 3^K \equiv 17 \pmod{139}$$

$$\Rightarrow K = 43$$

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 $p = 263$, $\alpha = 5$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 125$.

- a) Si rende noto che $\alpha = 5$ è una radice primitiva di \mathbb{Z}_{263}^* . Calcolare β .
- b) Alice estrae il numero casuale segreto (nonce) $k = 7$ 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 $C_2 = (r_2, t_2) = (232, 58)$, $C_3 = (r_3, t_3) = (232, 29)$, $C_4 = (r_4, t_4) = (232, 146)$ e, per altra via, viene a sapere che $P_2 = 200$. Calcolare P_3 e P_4 .
- d) Calcolare per quale valore di k Alice ha calcolato i messaggi C_2, C_3, C_4 del punto c), applicando l'algoritmo Baby Step Giant Step (NB: bastano le prime 6 righe della tabella).

$$a) \beta = \alpha^a \bmod p = 5^{125} \bmod 263 = 56$$

$$b) r_1 = \alpha^k \bmod p = 5^7 \bmod 263 = 14$$

$$t_1 = \beta^k \cdot P_1 \bmod p = 56^7 \cdot 200 = 155$$

$$\Rightarrow C_1 = (14, 155)$$

$$c) \frac{t_2}{P_2} = \frac{t_3}{P_3} = \frac{t_4}{P_4} = \beta^k \bmod p \quad t_2^{-1} = 58^{-1} = 195 \bmod 263$$

$$P_3 \equiv \frac{P_2 t_3}{t_2} \bmod p \equiv 200 \cdot 29 \cdot 195 \equiv 100 \bmod 263$$

$$P_4 \equiv \frac{P_2 t_4}{t_2} \bmod p \equiv 200 \cdot 146 \cdot 195 \equiv 50 \bmod 263$$

$$d) 5^k \bmod 263 = 232$$

$$N = 17$$

$$\alpha^{-1} \equiv 150 \bmod 263$$

$$\alpha^{-N} \equiv 77 \bmod 263$$

$$\Rightarrow k = 5$$

j	α^j	k	α^{-Nk}	$\beta \alpha^{-Nk}$
0	1	0	1	232
1	5	{	{	{
2	25			
3	125			
4	99			
5	232			

Domanda 3

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

Bob adotta il sistema di cifratura a chiave pubblica RSA. pubblica il modulo $n = 26219$ e un esponente di cifratura scelto tra $e_1 = 363$, $e_2 = 1016$, $e_3 = 1363$.

- a) Fattorizzare n con il metodo di Fermat. Verificare la correttezza dei dati forniti in base alle ipotesi del metodo RSA. Scegliere il valore corretto tra i tre esponenti e_1 , e_2 , e_3 .
- b) Alice trasmette a Bob il messaggio cifrato $C = 22$, calcolato utilizzando il valore corretto dell'esponente e . Decifrarlo e calcolare il corrispondente messaggio in chiaro P .

$$a) n = 26219 = 157 \cdot 167 \text{ (p, q primi)}$$

$$\phi(n) = 156 \cdot 166 = 25896 = 2^3 \cdot 3 \cdot 13 \cdot 83$$

$$\text{MCD}(363, 25896) = 3$$

$$\text{MCD}(1016, \text{---}) = 8$$

$$\text{MCD}(1363, \text{---}) = 1 \Rightarrow e = 1363$$

i	$n + i^2$
1	26220
2	26233
3	26249
4	26276
5	26319 = 162^2

$$\Rightarrow n = (162-5)(162+5)$$

$$e \perp \phi(n)$$

$$b) d \equiv e^{-1} \pmod{\phi(n)}$$

con Euclide Esteso: $d = 19$

$$25896 = 18 \cdot 1363 + 1362$$

$$1363 = 1 \cdot 1362 + 1$$

$$x_0 = 0 \quad x_1 = 1$$

$$x_2 = (-1)(1) + 0 = -1$$

$$x_3 = (-1)(-1) + 1 = 19$$

$$P = C^d \pmod{n} =$$

$$= 22^{19} \pmod{26219} =$$

$$= 3903$$

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 *generica funzione* $y = y(x)$, invertibile, e non unidirezionale. Si consideri una *funzione di hash* $y = h(x)$, non invertibile, e non unidirezionale. Spiegare quale differenza sussiste tra le proprietà di non unidirezionalità delle due funzioni.
- c) Si consideri una ipotetica funzione di hash $h = h(m) = \text{AES}_m("00...0")$, definita come la cifratura AES di un blocco di 128 zeri con chiave pari agli ultimi 128 bit (i 128 bit meno significativi) del messaggio m .
Si dica se tale funzione $h = h(m)$ è:
- invertibile? (spiegare perché SI o perché NO)
no
 - unidirezionale? (spiegare perché SI o perché NO)
si
 - resistente alle collisioni? (spiegare perché SI o perché NO; se si risponde NO, fornire un esempio di collisione)
no
- d) Una Fondazione, per celebrare il cinquantenario della sua istituzione, offre un premio di \$1.000.000 al primo crittografo che, a partire dal bando, riesca a ideare una funzione di hash che restituisca valori di tipo unsigned long long (64 bit) e che *si dimostri unidirezionale e fortemente resistente alle collisioni per almeno 1 anno* dalla pubblicazione dell'algoritmo (cioè, il premio è assegnato all'ideatore se per almeno 1 anno dalla pubblicazione del suo algoritmo nessuno sfidante riesce a violare alcuna delle due proprietà). Entro quanto tempo pensate che sarà assegnato il premio? In 1 giorno? In 1 anno? Mai?

Mai

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (10 punti)

(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

- 1) Alice e Bob adottano il protocollo di Diffie-Hellman per l'instaurazione della loro chiave simmetrica K_{AB} e pubblicano $p = 67$, $\alpha = 3$. Alice sceglie $1 \leq x \leq p-2$ (segreto). Bob sceglie $1 \leq y \leq p-2$ (segreto). Oscar osserva che sul canale pubblico Alice e Bob scambiano lo stesso valore $\alpha^x \equiv \alpha^y \equiv 5 \pmod{p}$ nelle due direzioni. E' corretto dedurre quindi che $x \equiv y \pmod{p-1}$? Calcolare K_{AB} . (3 punti)

$\alpha = 3$ è un elem. primitivo di \mathbb{Z}_{67}^* se $\alpha^{p-1} \not\equiv 1 \pmod{p}$

$$p-1 = 66 = 2 \cdot 3 \cdot 11 \quad \left. \begin{array}{l} 3^{33} \equiv 66 \\ 3^{22} \equiv 1 \\ 3^6 \equiv 59 \end{array} \right\} \Rightarrow \text{NO} \Rightarrow \text{anche } x \not\equiv y \pmod{p-1}$$

Can RSCS: $x_i = 19, 41, 63 \pmod{66}$
($N=9$)

(basta prendere 1 pa
calcolare K_{AB})

$$x \equiv y \pmod{22}$$

$$\text{Ord}(3) = 22 \text{ in } \mathbb{Z}_{67}^*$$

$$K_{AB} = \alpha^{xy} \equiv 5^{19} \equiv 52$$

- 2) La mattina del 9 luglio, sul portone delle biblioteca della Miskatonic University viene trovata la misteriosa scritta "ZWSFCSF". Il Dott. Armitage apprende in sogno che la scritta è una *Cifratura Affine* (mod 26) e intuisce che la sua chiave è rappresentata dalla data: $a=9$, $b=7$. Decifrare la scritta e ricavare lo spaventoso messaggio. (3 punti)

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

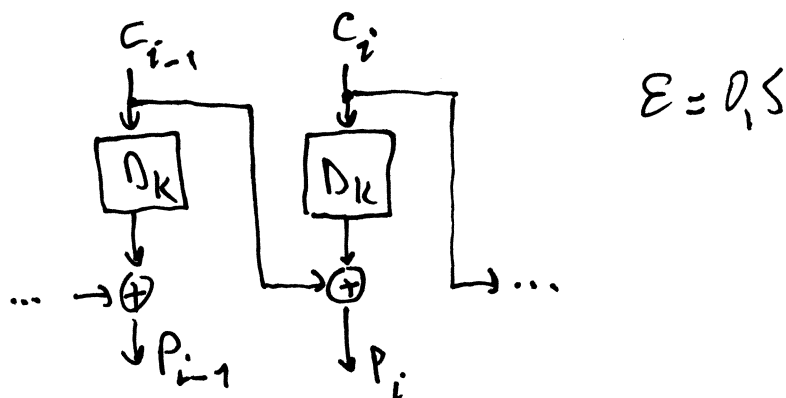
$$P = D_K(C) = (C - b)a^{-1} \pmod{26}$$

$$a^{-1} = 9^{-1} \equiv 3 \pmod{26}$$

$$\Rightarrow \text{"CTHULHU"}$$

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

- 3) 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 512 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 $\varepsilon=0.5$, quale sarà il tasso di errore sul flusso decifrato $\{P_i\}$? (2 punti)



- 4) Se dal PC in ufficio accedo a un sito [www](https://www.*.com) con URL https://www.*.com, chi fornisce le chiavi con cui è cifrata la comunicazione tra il mio browser e il server [www](https://www.*.com)? L'admin della mia azienda è a conoscenza o no del fatto che ho visitato il sito? Se il sito mi chiede una password per accedere ai contenuti, questa sarà leggibile dall'admin? (2 punti)