

# Sicurezza delle Reti

Prof. Stefano Bregni

III Appello d'Esame 2023-24 – 31 agosto 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) (6 punti)

Bob adotta il sistema di cifratura a chiave pubblica di El Gamal e pubblica  $p = 199$ ,  $\alpha = 2$ ,  $\beta = \alpha^a \bmod p$ , tenendo segreto l'esponente  $a = 70$ .

- 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  $\alpha = \{3, 4\}$ . Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare  $\beta$ .
- Alice estrae il numero casuale segreto (*nonce*)  $k = 76$  e spedisce il messaggio  $P_1 = 98$ . Calcolare il messaggio cifrato  $C_1 = (r_1, t_1)$ .
- 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  $C_2 = (r_2, t_2) = (10, 63)$ ,  $C_3 = (r_3, t_3) = (10, 10)$ ,  $C_4 = (r_4, t_4) = (10, 56)$  e, per altra via, viene a sapere che  $P_2 = 100$ . Calcolare  $P_3$  e  $P_4$ .

a)  $p$  primo  $1 < \alpha < p-2$   $p-1 = 198 = 2 \cdot 3^2 \cdot 11$   $\alpha$  è elem. prim. di  $\mathbb{Z}_p^*$ :  
 $\alpha^{q_i} \not\equiv 1 \pmod{p}$

$$\left. \begin{array}{l} 3^{99} \equiv -1 \\ 3^{66} \equiv 106 \\ 3^{18} \equiv 125 \end{array} \right\} \Rightarrow \alpha = 3 \quad (\alpha = 2, 4 \text{ no}) \quad \beta = \alpha^a \bmod p = 3^{70} \bmod 199 = 29$$

b)  $r_1 = \alpha^k \bmod p = 3^{76} \bmod 199 = 47$

$t_1 = \beta^k P \bmod p = 29^{76} \cdot 98 \bmod 199 = 80 \Rightarrow C_1 = (47, 80)$

c)  $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod{p}$   $t_2^{-1} \equiv 63^{-1} \equiv 139 \pmod{199}$

$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod{p}$   $P_3 \equiv 100 \cdot 10 \cdot 139 \equiv 98 \pmod{199}$

$P_4 \equiv P_2 \frac{t_4}{t_2} \pmod{p}$   $P_4 \equiv 100 \cdot 56 \cdot 139 \equiv 711 \pmod{199}$



Cognome e nome:

(stampatello)

(firma leggibile)

Matricola:

## Domanda 2

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

Bob adotta il sistema di firma elettronica di El Gamal e pubblica  $p = 109$ ,  $\alpha = 10$ ,  $\beta = \alpha^a \bmod p = 15$ , 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  $P_2$ .

$$A_1 = (r_1, s_1) = (30, 41) \quad P_1 = 25$$

$$A_2 = (r_2, s_2) = (30, 56) \quad P_2 = 28$$

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

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

$$\begin{cases} 41k \equiv 25 - a30 \pmod{108} \\ 56k \equiv 28 - a30 \pmod{108} \end{cases}$$

$$15k \equiv 3 \pmod{108}$$

$$\text{MCD}(15, 108) = 3 \Rightarrow 3 \text{ soluzioni}$$

$$5k \equiv 1 \pmod{36}$$

$$5^{-1} \equiv 29 \pmod{36}$$

$$k_0 \equiv 29 \pmod{36}$$

$$k_i \equiv 29, 65, 101 \pmod{108}$$

$$\Rightarrow \boxed{k = 29}$$

Dai dati pubblici:

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

$$10^{29} \equiv 30 \pmod{109}$$

$$41 \cdot 29 \equiv 25 - a30 \pmod{108}$$

$$30a \equiv 24 \pmod{108}$$

$$\text{MCD}(30, 108) = 6 \Rightarrow 6 \text{ soluzioni}$$

$$5a \equiv 4 \pmod{18}$$

$$5^{-1} \equiv 11 \pmod{18}$$

$$a_0 \equiv 4 \cdot 11 \equiv 8 \pmod{18}$$

Dai dati pubblici:

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

$$3^{44} \equiv 15$$

$$a_i \equiv 8, 26, \underline{44}, 62, 80, 98 \pmod{108}$$

$$\Rightarrow \boxed{a = 44}$$



Cognome e nome:

(stampatello)

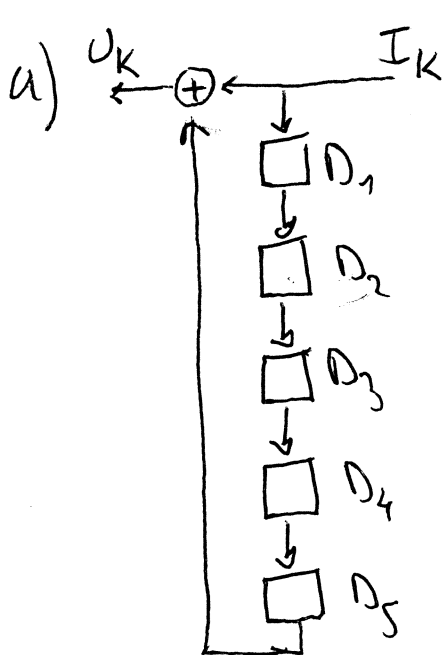
(firma leggibile)

Matricola:

## Domanda 3

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

- a) Si disegni lo schema di un *descrambler autosincronizzante* basato su registro a scorrimento LFSR con polinomio caratteristico  $P(x) = x^5 + 1$ . Si indichino la sequenza binaria in ingresso (da decodificare) con  $\{I_k\}$  e la sequenza binaria in uscita (decodificata) con  $\{U_k\}$ .
- b) Si inizializzino gli elementi di ritardo  $D_i$  ( $i = 1, 2, 3, 4$ ) con  $\{0, 0, 1, 0, 0\}$  al passo iniziale  $k = 0$ . Si alimenti il *descrambler* con la sequenza da decodificare  $\{I_k\} = \{0, 0, 1, 0, 0, 1, 1, 0, 1, 1, \dots\}$  (periodica). Ricavare la sequenza decodificata  $\{U_k\}$  all'uscita.
- c) Cosa cambierebbe nella risposta alla domanda b), se gli elementi di ritardo fossero inizializzati diversamente?



b)

$k$	$I_k$	$D_{1k}$	$D_{2k}$	$D_{3k}$	$D_{4k}$	$D_{5k}$	$U_k$
0	0	0	0	1	0	0	0
1	0	0	0	0	1	0	0
2	1	0	0	0	0	1	0
3	0	1	0	0	0	0	0
4	0	0	1	0	0	0	0
5	1	0	0	1	0	0	1
6	1	1	0	0	1	0	1
7	0	1	1	0	0	1	1
8	1	0	1	1	0	0	1
9	1	1	0	1	1	0	1
10	0	1	1	0	1	1	1
11	0	0	1	1	0	1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

**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) La vostra organizzazione impiega una funzione di hash  $h = h(m)$  reputata sicura (unidirezionale e resistente alle collisioni). I contratti sono firmati apponendo una firma DSA (El Gamal) dell'hash  $h = h(m)$  del loro testo  $m$ . Oggi leggete in rete che, essendo la lunghezza del messaggio  $m$  arbitraria, mentre la lunghezza dell'hash  $h$  è fissa, allora esistono infiniti messaggi che producono ogni singolo valore di hash  $h$ , comunque assegnato. Quindi, esistono infiniti contratti per cui la stessa firma è valida. Rischiate di essere truffati? Come?

- c) Per il file che raccoglie gli hash delle password degli utenti registrati, hai proposto alla tua Azienda di adottare la funzione di hash  $h = h(m) = \text{DES}_K(m)$ , definita come la cifratura DES della password  $m$  con chiave  $K$  fissa e segreta (un stringa di 56 bit, uguale per tutte le password registrate nel file, scelta in modo casuale all'installazione del sistema e non conoscibile da nessuno, neanche esaminando il codice). Le password hanno lunghezza massima 64 bit. Se la password ha lunghezza inferiore, la stringa viene portata a 64 bit aggiungendo degli "0" in fondo (*0-padding*). In conclusione: le stringhe  $h$  e  $m$  hanno lunghezza fissa 64 bit.

Si dica e si argomenti se tale funzione di hash  $h = h(m)$ :

- è invertibile?
  
  
  
  
  
  
  
  
  
  
- è unidirezionale?
  
  
  
  
  
  
  
  
  
  
- è resistente alle collisioni?

## 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 ancora il problema assegnato nella Domanda 1. 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* per risolvere l'equazione esponenziale discreta (NB: bastano le prime 5 righe della tabella). (2 punti)

$$3^x \equiv 10 \pmod{199}$$

$$N=15 \quad \alpha=3 \quad \beta=10$$

$$\alpha^{-1} \equiv 133 \pmod{199}$$

$$\alpha^{-N} \equiv 83 \pmod{199}$$

$$\Rightarrow \boxed{k=46}$$

$j$	$\alpha^j$	$k$	$\alpha^{-Nk}$	$\beta \alpha^{-Nk}$	$\pmod{199}$
0	1	0	1	10	
1	3	1	83	34	
2	9	2	123	36	
3	27	3	65	3	
4	81	4	5	50	
5	44	5	17	170	

$$\Rightarrow x \equiv 1 + 15 \cdot 3 \equiv 46 \pmod{199}$$

- 2) Decifrare il messaggio "QDSKGUGRUCGMGW" codificato attraverso il *Cifrario di Vigenère* (mod 26) con chiave  $K = (2, 4, 1)$ . (2 punti)

"OZRICTENTALES"

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 calcolino tutti i residui quadratici dell'insieme  $\mathbb{Z}_{13}^*$  applicando un metodo a scelta. Esaminando i risultati ottenuti, si dica quali sono le radici quadrate di -1 (mod 13). (2 punti)

$$(\pm 1)^2 \equiv 1 \pmod{13}$$

$$(\pm 2)^2 \equiv 4$$

$$(\pm 3)^2 \equiv 9$$

$$(\pm 4)^2 \equiv 3$$

$$(\pm 5)^2 \equiv 12$$

$$(\pm 6)^2 \equiv 10$$

$$\alpha_9 \equiv \{1, 3, 4, 9, 10, 12\}$$

$$\sqrt{-1} \equiv \sqrt{12} \equiv \pm 5 \equiv \{5, 8\}$$

- 4) Descrivere la proprietà di *confusione*, che secondo Claude Shannon un buon crittosistema dovrebbe avere per ostacolarne l'analisi. (2 punti)

- 5) Su AliExpress, ho comperato una macchina che risolve in modo efficiente il *Problema Computazionale di Diffie-Hellman*. Posso utilizzarla per calcolare *Logaritmi Discreti*? Come? (2 punti)



Cognome e nome:

(stampatello)

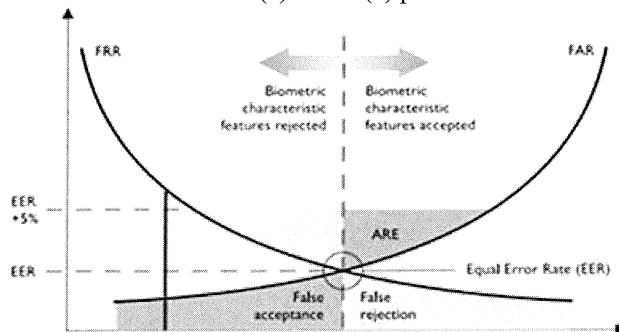
(firma leggibile)

Matricola:

6) Si spieghi il significato del grafico sotto riportato. In particolare, specificare:

(2 punti)

- qual è la grandezza in ascissa?
- come sono definite le grandezze FAR e FRR, rappresentate dalle curve in figura?
- a quali valori tendono  $FAR(x)$  e  $FRR(x)$  per  $x \rightarrow 0$  e  $x \rightarrow \infty$ ?



7) Descrivere lo *Schema di Lamport* per l'autenticazione di un host A da parte di un server B, precisando quali informazioni sono tenute segrete da A e B e quali informazioni sono invece pubbliche o trasferite in chiaro. (2 punti)