

# Sicurezza delle Reti

Prof. Stefano Bregni

IV Appello d'Esame 2023-24 – 9 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 firma elettronica di El Gamal e pubblica  $p = 127$ ,  $\alpha = 6$ ,  $\beta = \alpha^a \bmod p$ , tenendo segreto l'esponente  $a = 13$ .

- Si rende noto che  $\alpha = 6$  è una radice primitiva di  $\mathbb{Z}_{127}^*$ . Calcolare  $\beta$ .
- Bob estrae il numero casuale segreto (nonce)  $k = 11$ . Per questo valore di  $k$ , calcolare la firma di Bob  $A = (r, s)$  del messaggio  $P = 4$ .
- Verificare se la firma  $A' = (r', s') = (3, 38)$  è valida da Bob per il messaggio  $P = 5$ .
- Se è valida, calcolare il valore di  $k$  per cui è stata calcolata da Bob risolvendo l'equazione  $s \equiv k^{-1}(P - ar) \equiv 38 \pmod{p-1}$  (non Baby Step Giant Step).

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

$$\left. \begin{array}{l} 6^3 \equiv -1 \\ 6^{42} \equiv 127 \\ 6^{18} \equiv 64 \end{array} \right\} \Rightarrow \alpha = 6 \quad \beta = \alpha^a \bmod p = 6^{13} \bmod 127 = 46$$

Test se  $\alpha$  è prim. in  $\mathbb{Z}_p^*$   
 $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}$

b)  $r = \alpha^k \bmod p = 6^{11} \bmod 127 = 93$

$$s = k^{-1}(P - ar) \bmod (p-1) = 23(4 - 93 \cdot 13) \bmod 126 = 5$$

$$k^{-1} = 11^{-1} \bmod 126 = 23$$

$$\Rightarrow A = (93, 5)$$

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

$$46^3 \cdot 3^{38} \equiv 29 \pmod{127}$$

$$6^5 \equiv 29 \pmod{127}$$

$$\left. \begin{array}{l} 46^3 \cdot 3^{38} \equiv 29 \pmod{127} \\ 6^5 \equiv 29 \pmod{127} \end{array} \right\} \Rightarrow A' = (3, 38) \text{ firma valida di } P = 5$$

$$d) K_S \equiv P \cdot a \cdot r \pmod{p-1}$$

$$38 \cdot K \equiv 5 - 13 \cdot 3 \pmod{126}$$

$$38 \cdot K \equiv 92 \pmod{126} \quad \text{MCD}(38, 126) = 2 \text{ soluzioni}$$

$$\rightarrow 19K \equiv 46 \pmod{63} \quad 19^{-1} \equiv 10 \pmod{63}$$

$$\rightarrow K_0 \equiv 19 \pmod{63}$$

$$K_i \equiv 19, 82 \pmod{126}$$

Da dati pubblici:  $6^K \equiv 3 \pmod{127}$

$$\Rightarrow K = 19$$

## 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  $p = 277$ ,  $\alpha = 2$ ,  $\beta = \alpha^a \bmod p$ , tenendo segreto l'esponente  $a = 7$ .

- 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  $\alpha = \{5, 7\}$ . Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare  $\beta$ .
- b) Alice estrae il numero casuale segreto (*nonce*)  $k = 18$  e spedisce il messaggio  $P_1 = 7$ . 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  $C_2 = (r_2, t_2) = (34, 38)$ ,  $C_3 = (r_3, t_3) = (34, 90)$ ,  $C_4 = (r_4, t_4) = (34, 73)$  e, per altra via, viene a sapere che  $P_2 = 77$ . Calcolare  $P_3$  e  $P_4$ .

a)  $p$  primo  $1 < a < p-2$   $p-1 = 276 = 2^2 \cdot 3 \cdot 23$  Test se  $\alpha$  el. prim.  $\in \mathbb{Z}_p^*$   
 $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}$

$$\left. \begin{array}{l} 5^{738} \equiv -1 \\ 5^{92} \equiv 116 \\ 5^{12} \equiv 27 \end{array} \right\} \Rightarrow \alpha = 5$$

$$\alpha = 5$$

$$OK \quad (\alpha = 2, 7 \text{ NO})$$

$$\beta = \alpha^a \bmod p = 5^7 \bmod 277 = 11$$

b)  $r_1 = \alpha^k \bmod p = 5^{18} \bmod 277 = 4$

$$t_1 = \beta^k P \bmod p = 11^{18} \cdot 7 \bmod 277 = 10$$

$$\Rightarrow C_1 = (4, 10)$$

c)  $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod{p}$   $t_2^{-1} = 38^{-1} \equiv (-51) \pmod{277}$

$$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod{p} \quad P_3 \equiv 77 \cdot 90 \cdot (-51) \equiv 22 \pmod{277}$$

$$P_4 \equiv P_2 \frac{t_4}{t_2} \pmod{p} \quad P_4 \equiv 77 \cdot 73 \cdot (-51) \equiv 24 \pmod{277}$$



## Domanda 3

(svolgere su questo foglio nello spazio assegnato) (4 punti)

- a) Ricavare la sequenza binaria pseudo-casuale  $\{x_i\}$  generata dall'algoritmo Blum-Blum-Shab per  $p = 19$ ,  $q = 59$ ,  $x = 60$  e determinarne il periodo  $P$ . Il seme iniziale  $x$  rispetta le ipotesi del metodo?

| $i$ | $x_i$ | $b_i$ |
|-----|-------|-------|
| 0   | 237   | 1     |
| 1   | 119   | 1     |
| 2   | 709   | 1     |
| 3   | 473   | 1     |
| 4   | 650   | 0     |
| 5   | 1004  | 0     |
| 6   | 237   | 1     |

$P = 6$

$$m = p \cdot q = 19 \cdot 59 = 1121$$

$$x_0 = x^2 \pmod{m}$$

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

$$19 \equiv 3 \pmod{4}$$

$$59 \equiv 3 \pmod{4}$$

$$60 \perp 1121$$

- 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  $x_0 = x^2 \in \mathbb{Z}_m$ ?

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

$$\lambda(n) = \text{lcm}(\{\lambda(p_i^{a_i})\}) \quad \lambda(p^k) = \begin{cases} \frac{1}{2}\phi(p^k) & \text{se } p = 2, k \geq 3 \\ \phi(p^k) & \text{altrimenti} \end{cases}$$

$$\lambda(n) = \text{lcm}(18, 58) = 2 \cdot 3^2 \cdot 29 = 522$$

$$\lambda[\lambda(n)] = \lambda(522) = \text{lcm}(1, 6, 28) = 84$$

$$\pi(x_0) \in \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$$

**Domanda 4**

*(svolgere su questo foglio nello spazio assegnato) (7 punti)*

- a) Definire la proprietà di *resistenza forte alle collisioni* di una *funzione di hash*  $y = h(x)$ .
- b) La CIA, grazie a un supercomputer quantistico sperimentale, è in grado di violare la unidirezionalità di SHA-2 a 256 bit in pochi minuti. Un Forum privato "attenzionato" dalla CIA memorizza gli hash SHA-2 256 delle password degli utenti in un database, reputato sicuro ma che la CIA è in grado di leggere liberamente. La CIA può quindi ricavare le password degli utenti? Quali altre operazioni ostili al Forum e ai suoi utenti sono possibili per la CIA?

- c) Si consideri una ipotetica funzione di hash  $h = h(m) = m^e \bmod n$ , con  $e = 17$ ,  $n = p \cdot q$ , con  $p$  e  $q$  primi di 160 cifre utilizzati per calcolare  $n$  e poi dimenticati (ossia, una cifratura RSA del messaggio  $m$ ).

Si dica se tale funzione  $h = h(m)$  è:

- invertibile? (spiegare perché SI o perché NO e sotto quali condizioni)

NO (SI se  $m < n$ )

- 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  $m_1 \equiv m_2 \pmod{n}$

Cognome e nome:

(stampatello)

(firma leggibile)

Matricola:

## Domanda 5

(rispondere su questo foglio negli spazi assegnati) (12 punti)

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

- 1) Decifrare il messaggio "EGAELVTS" codificato attraverso il *Cifrario di Vigenère* (mod 26) con chiave  $K = (4, 7, 0, 11)$ . (2 punti)

 $\Rightarrow$  AZATHOTH

| 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) In che modo un algoritmo che risolva in modo efficiente il *Problema Computazionale di Diffie-Hellman* può aiutarmi a calcolare *Logaritmi Discreti*? (2 punti)

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

288

- 5) Si consideri un generatore di password consistenti di 20 simboli casuali scelti nell'alfabeto Fremen, che comprende in tutto 27 caratteri (lettere) e 9 cifre (non c'è lo zero). Qual è la quantità di informazione [bit] delle password, se i simboli sono scelti indipendentemente una dall'altro e la probabilità che un simbolo sia un carattere o una cifra è la stessa? (2 punti)

La domanda non è precisa. Due risposte:

1)  $H(X) = -\log_2 \frac{1}{36} = 5,17 \text{ bit/symbol}$   
 $H(20 \text{ symbols}) = 103,4 \text{ bit}$

2)  $H(X) = -\left(0,5 \log_2 \frac{0,5}{27} + 0,5 \log_2 \frac{0,5}{9}\right) =$   
 $= 4,96 \text{ bit/symbol}$   
 $H(60 \text{ symbols}) = 99,25 \text{ bit}$

- 6) Su Astalavista, hai trovato un certificato in cui leggi, tra le altre cose: (2 punti)

[illegible]

Sostituisci i parametri *Subject name* / *Public Key* / *Signature* rispettivamente con: il tuo nome, la tua P.K., la tua firma. Il certificato è formalmente valido? Se no, cosa devi fare per renderlo formalmente valido?