

Sicurezza delle Reti

Prof. Stefano Bregni

II Appello d'Esame 2017-18 – 27 luglio 2018

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 firma elettronica di El Gamal e pubblica $p = 157$, $\alpha = 5$, $\beta = \alpha^a \bmod p = 109$, tenendo segreto l'esponente a ($1 < a \leq p-2$).

a) Bob estrae il numero casuale segreto k (nonce) ($k \perp p-1$). Usando sempre questo stesso valore di k , Bob calcola le seguenti firme A_k per i rispettivi messaggi P_k :

$$A_1 = (r_1, s_1) = (26, 34) \quad P_1 = 10$$

$$A_2 = (r_2, s_2) = (26, 2) \quad P_2 = 11$$

$$A_3 = (r_3, s_3) = (26, 20) \quad P_3 = 12$$

Verificare che le tre firme siano valide.

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

$$A_1 \left| \begin{array}{l} 109^{26} \cdot 26^{34} \equiv 68 \\ 5^{10} \equiv 68 \end{array} \right\} \Rightarrow \text{OK}$$

$$A_2 \left| \begin{array}{l} 109^{26} \cdot 26^2 \equiv 4 \\ 5^{11} \equiv 26 \end{array} \right\} \Rightarrow \text{NO}$$

$$A_3 \left| \begin{array}{l} 109^{26} \cdot 26^{20} \equiv 130 \\ 5^{12} \equiv 130 \end{array} \right\} \Rightarrow \text{OK}$$

- b) Oscar intercetta i tre messaggi (P_k, A_k) . Sulla base delle sole firme verificate valide, calcolare k e a (attacco del nonce ripetuto).

$$P_1 = 10 \quad A_1 = (26, 34)$$

$$P_2 = 12 \quad A_2 = (26, 20)$$

$$S \equiv K^{-1} (P - ar) \pmod{p-1} \rightarrow SK \equiv P - ar \pmod{p-1}$$

$$\begin{cases} 34K \equiv 10 - a \cdot 26 \pmod{156} \\ 20K \equiv 12 - a \cdot 26 \pmod{156} \end{cases}$$

$$\begin{cases} 34K \equiv 10 - a \cdot 26 \pmod{156} \\ 20K \equiv 12 - a \cdot 26 \pmod{156} \end{cases}$$

$$14K \equiv -2 \pmod{156}$$

$$\gcd(14, 156) = 2 \Rightarrow 2 \text{ soluzioni}$$

$$7K \equiv -1 \pmod{78}$$

$$7^{-1} \equiv -11 \pmod{78} \quad (E.E.)$$

$$\Rightarrow K_0 \equiv 11 \pmod{78}$$

$$K_i \equiv 11, 89 \pmod{156}$$

$$\Rightarrow \boxed{K = 11}$$

Dei dati pubblici:

$$r = \alpha^K \pmod{p}$$

$$S^{11} \pmod{157} = 26 \quad \text{OK}$$

$$34 \cdot 11 \equiv 10 - a \cdot 26 \pmod{156}$$

$$26 \cdot a \equiv 104 \pmod{156}$$

$$\gcd(26, 156) = 26 \Rightarrow 26 \text{ soluzioni}$$

$$a_0 \equiv 4 \pmod{6}$$

$$a_i \equiv 4, 10, 16, 22, 28, 34, 40, 46, 52, 58, 64, 70, 76, 82, 88, 94, 100, 106, 112, 118, 124, 130, 136, 142, 148, 154$$

Dei dati pubblici: $\beta \equiv \alpha^a \pmod{p}$

$$S^{100} \equiv 109 \pmod{157}$$

$$\Rightarrow (a = 100)$$

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 $p = 89$, $\alpha = 7$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 71$.

- a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 7$ non risultasse una scelta valida, Bob userà invece $\alpha = 8$, oppure ancora $\alpha = 9$ (da verificare). Se anche queste scelte non risultassero valide, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β .
- b) Alice estrae il numero casuale segreto (*nonce*) $k = 26$ e spedisce il messaggio $P = 50$. Calcolare il messaggio cifrato $C = (r, t)$.
- c) Bob, per un errore di trasmissione, riceve $C' = (r', t') = (21, 22)$. Calcolare il messaggio decifrato da Bob P' .

4) p primo $1 < a \leq p-2$ Tht α elem. prim. di \mathbb{Z}_p^* :

$$\left. \begin{array}{l} 7^{44} \equiv 88 \\ 7^8 \equiv 4 \end{array} \right\} \Rightarrow \alpha = 7 \text{ OK}$$

$$\beta = \alpha^a \bmod p = 7^{71} \bmod 89 = 31$$

$$\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}$$

$$p-1 = 88 = 2^3 \cdot 11$$

$$b) r = \alpha^k \bmod p = 7^{26} \bmod 89 = 21$$

$$t = \beta^k \cdot P \bmod p = 31^{26} \cdot 50 \bmod 89 = 21$$

$$\Rightarrow C = (21, 21)$$

$$c) C' = (r', t') = (21, 21)$$

$$P' = t' \cdot r'^{-a} \bmod p = 21 \cdot 21^{-71} \bmod 89 = 10$$

Sicurezza delle Reti

Prof. Stefano Bregni

II Appello d'Esame 2017-18 – 27 luglio 2018

Cognome e nome:

(stampatello)

(firma leggibile)

Matricola:

Domanda 3

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

Alice e Bob adottano il protocollo di Diffie-Hellman per l'instaurazione della loro chiave simmetrica K_{AB} . Alice pubblica $p = 199$ e inizialmente $\alpha = 3$. Alice sceglie $1 \leq x \leq p-2$ (segreto). Bob sceglie $1 \leq y \leq p-2$ (segreto).

- a) Alice verifica la correttezza dei dati secondo le ipotesi di Diffie-Hellman. Nel caso $\alpha = 3$ non risulti una scelta valida, Alice si corregge e pubblica invece un valore valido scelto nell'insieme $\alpha = \{3, 4, 5\}$. Se nessuna di queste scelte risultasse valida, Alice e Bob rinunceranno a proseguire (e l'esercizio termina qui).

$$\begin{aligned} \text{Test } \alpha^{\frac{p-1}{q_i}} &\not\equiv 1 \pmod{p} & p-1 = 198 = 2 \cdot 3^2 \cdot 11 \\ \left. \begin{aligned} 3^{99} &\equiv 198 \\ 3^{66} &\equiv 106 \\ 3^{18} &\equiv 125 \end{aligned} \right\} &\Rightarrow \alpha = 3 \quad (\text{unico elem. prim. dell'insieme}) \\ && \text{OK} \end{aligned}$$

- b) Oscar osserva i numeri scambiati da Alice e Bob:

$$\text{Alice} \rightarrow \text{Bob}: \quad \alpha^x \equiv 106 \pmod{p}$$

$$\text{Alice} \leftarrow \text{Bob}: \quad \alpha^y \equiv 14 \pmod{p}$$

Sulla base delle informazioni conosciute da Oscar, calcolare gli esponenti segreti x e y e la chiave K_{AB} .

$$\begin{aligned} x &\equiv 66 \pmod{198} & \text{Per tentativi, o BSGS,} \\ y &\equiv 50 \pmod{\quad} & \text{e dal punto a)} \end{aligned}$$

$$K_{AB} = \alpha^{xy} \pmod{p} = 3^{66 \cdot 50} = 92 \pmod{199}$$

Sicurezza delle Reti

Prof. Stefano Bregni

II Appello d'Esame 2017-18 – 27 luglio 2018

Cognome e nome:

(stampatello)

(firma leggibile)

Matricola:

Domanda 4

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

- a) Cos'è una funzione di *hash* $y = h(x)$?
- b) Definire la proprietà di *unidirezionalità* di una funzione di *hash*, distinguendola dalla proprietà di *non invertibilità*. Fare un esempio di funzione di hash non invertibile ma non unidirezionale.
- c) Si consideri una funzione $h(x)$ che produce *hash* lunghi 32 bit. Dato un hash h_1 , qual è l'ordine di grandezza (cioè: 10 elevato a...?) del numero di messaggi m di lunghezza minore o uguale a 400 bit, tali per cui $h(m) = h_1$?

$$\begin{aligned} |h| &= 2^{32} \\ |m| &= 2^{400} \rightarrow 2^{369} \approx 10^{111} \end{aligned}$$

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (15 punti)

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

1) Si consideri un generatore di password composte da 8 caratteri casuali X scelti nell'alfabeto di 16 $\{A, B, \dots, P\}$. (3 punti)

a) Qual è la quantità di informazione [bit] delle password, se i 16 caratteri sono equiprobabili?

b) Qual è la quantità di informazione delle password, se invece la probabilità che $X=A$ è 0.80, mentre gli altri 15 caratteri sono equiprobabili?

$$a) P(X=x_i) = \frac{1}{16}$$

$$H(X) = - \sum_{i=1}^{16} \frac{1}{16} \log_2 \frac{1}{16} = 4 \text{ bit/carattere (caso ovvio)}$$

$$\Rightarrow H(8 \text{ caratteri}) = 32 \text{ bit}$$

$$b) P(X="A") = 0,80 \quad P(X="B") = P(X="C") = \dots = \frac{0,20}{15}$$

$$H(X) = - \left[0,80 \log_2 0,80 + \sum_{i=1}^{15} \frac{0,20}{15} \log_2 \frac{0,20}{15} \right] \approx 0,2575 + 1,2450 =$$

$$\Rightarrow H(8 \text{ caratteri}) \approx 12,03 \text{ bit} \quad \approx 1,503 \text{ bit/carattere}$$

2) Nella suite di protocolli *Transport Level Security (TLS)*:

(3 punti)

a) quali servizi di trasporto sicuro fornisce il *TLS Record Protocol*? quali altri protocolli li utilizzano?b) quali funzioni svolge *Handshake Protocol*? a chi fornisce i suoi servizi? che protocollo trasporta i suoi messaggi?

3) Qual è la funzione del comando STARTTLS in SMTP? Qual è il suo effetto? E in IMAP e POP3? (3 punti)

4) Quali sono i ruoli dell'*Authentication Server* e del *Ticket-Granting Server* in Kerberos? Cosa significa se il primo autorizza un client ma il secondo no? Citare un miglioramento o estensione introdotto in Kv5 rispetto a Kv4. (3 punti)

5) Che differenza c'è tra i protocolli di *symmetric key agreement* e *symmetric key distribution*? In cosa consiste un *replay attack* ai protocolli di distribuzione delle chiavi? Come possono essere impediti? Fare almeno un esempio. (3 punti)