

Sicurezza delle Reti

Prof. Stefano Bregni

IV Appello d'Esame 2017-18 – 23 gennaio 2019

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 $p = 113$, $\alpha = 6$, $\beta = \alpha^a \bmod p = 16$, 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 :

$$A_1 = (r_1, s_1) = (94, 13) \quad P_1 = 11$$

$$A_2 = (r_2, s_2) = (94, 10) \quad P_2 = 13$$

$$A_3 = (r_3, s_3) = (94, 9) \quad P_3 = 15$$

Verificare che le tre firme siano valide.

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

$$A_1 \left| \begin{array}{l} 16^{94} \cdot 94^{13} \equiv 47 \\ 6^{11} \equiv 47 \end{array} \right\} \Rightarrow \text{OK}$$

$$A_2 \left| \begin{array}{l} 16^{94} \cdot 94^{10} \equiv 18 \\ 6^{13} \equiv 110 \end{array} \right\} \Rightarrow \text{NO}$$

$$A_3 \left| \begin{array}{l} 16^{94} \cdot 94^9 \equiv 5 \\ 6^{15} \equiv 5 \end{array} \right\} \Rightarrow \text{OK}$$

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).

$$P_1 = 11 \quad A_1 = (94, 13)$$

$$P_3 = 15 \quad A_3 = (94, 9)$$

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

$$\begin{cases} 13k \equiv 11 - a94 \pmod{112} \\ 9k \equiv 15 - a94 \pmod{112} \end{cases}$$

$$\begin{cases} 13k \equiv 11 - a94 \pmod{112} \\ 9k \equiv 15 - a94 \pmod{112} \end{cases}$$

$$4k \equiv -4 \pmod{112}$$

$$\text{MCD}(4, 112) = 4 \rightarrow 4 \text{ soluzioni}$$

$$k \equiv -1 \pmod{28}$$

$$\Rightarrow k_i \equiv -1, 27, 55, 83 \pmod{112}$$

$$\Rightarrow \boxed{k \equiv 55}$$

Dai dati pubblici:

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

$$6^{55} \equiv 94 \text{ OK}$$

$$13 \cdot 55 \equiv 11 - a94 \pmod{112}$$

$$a94 \equiv 80 \pmod{112}$$

$$\text{MCD}(94, 112) = 2 \Rightarrow 2 \text{ soluzioni}$$

$$a47 \equiv 40 \pmod{56}$$

$$47^{-1} \equiv 31 \pmod{56}$$

$$a_0 \equiv 8 \pmod{56}$$

$$a_0 \equiv 8, 64 \pmod{112}$$

$$\Rightarrow \boxed{a = 64}$$

Dai dati pubblici:

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

$$6^{64} \equiv 16 \pmod{113}$$

Sicurezza delle Reti

Prof. Stefano Bregni

IV Appello d'Esame 2017-18 – 23 gennaio 2019

Cognome e nome:

(stamatello)

(firma leggibile)

Matricola:

Domanda 2

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

Bob adotta il sistema di firma elettronica di El Gamal e pubblica $p = 137$, $\alpha = 2$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 129$.

- 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 β .
- Bob estrae il numero casuale segreto (nonce) $k = 21$. Per questo valore di k , calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 100$.
- Verificare se anche la firma $A' = (r', s') = (48, 4)$ è valida per lo stesso messaggio $P = 100$. Se è valida, calcolare il valore di k per cui è stata calcolata da Bob.

a) p primo $1 < \alpha < p-2$ $K \perp p-1$ α elem. prim. di \mathbb{Z}_p^*
 Test se α elem. primitivo di \mathbb{Z}_{137}^* : $\alpha^{(p-1)/q_i} \neq 1 \pmod{p}$
 $\left. \begin{array}{l} 2^{68} \equiv 1 \\ 2^8 \equiv 1 \end{array} \right\} \Rightarrow \alpha=2 \text{ NO}$ $\left. \begin{array}{l} 3^{68} \equiv 136 \\ 3^8 \equiv 122 \end{array} \right\} \Rightarrow \alpha=3$ $p-1=136=2^3 \cdot 17$
 $\Rightarrow \alpha=3$

$$\beta = \alpha^a \bmod p = 3^{129} \bmod 137 = 82$$

$$b) r = \alpha^k \bmod p = 3^{21} \bmod 137 = (12)$$

$$s = k^{-1} (P - ar) \bmod (p-1) = 13(100 - 129 \cdot 12) \bmod 136 = (80)$$

$$k^{-1} \bmod (p-1) = 21^{-1} \bmod 136 = 13$$

$$\Rightarrow A = (12, 80)$$

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

$$\left. \begin{array}{l} 82^{48} 48^{80} \equiv 65 \\ 3^{100} \equiv 65 \end{array} \right\} \Rightarrow A' = (48, 4) \text{ firma valida di } P=100$$

$$sK \equiv P - ar \pmod{136}$$

$$4K \equiv 100 - 129 \cdot 48 \pmod{136}$$

$$4K \equiv 28 \pmod{136} \quad \gcd(4, 136) = 4 \rightarrow 4 \text{ soluzioni}$$

$$K_1 \equiv 7 \pmod{34}$$

$$K_i \equiv 7, 41, 75, 109 \pmod{136}$$

$$\text{Dai dati pubblici: } r = \alpha^k \bmod p \quad 48 \equiv 3^{41} \pmod{137}$$

$$\Rightarrow (K = 41)$$

Domanda 3

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

La Trusted Authority TA adotta lo Schema di Blom per distribuire chiavi simmetriche di sessione $K_{ij} = K_{ji}$ a 100 utenti U_k ($k = 1, \dots, N$) per la comunicazione tra gli stessi. TA sceglie e tiene segreti a, b, c , e pubblica p . Un provider fornisce canali sicuri da TA verso ogni utente, ma a pagamento.

- a) Quanti numeri devono essere inviati in tutto da TA, adottando appunto lo schema di Blom?

200

- b) Se invece TA generasse centralmente tutte le possibili chiavi di sessione e le inviasse ai rispettivi utenti, quanti numeri dovrebbe inviare in tutto?

4950

- c) Si consideri il caso di tre soli utenti A, B e C, con identificativi pubblici rispettivamente uguali a $r_A = 10$, $r_B = 20$, $r_C = 30$. TA sceglie e tiene segreti a, b, c , e pubblica $p = 1009$. Gli utenti A e B però si accordano e si scambiano le informazioni $a_A = 591$, $b_A = 132$, $a_B = 73$, $b_B = 114$.

- Calcolare i parametri segreti a, b, c .
- Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC} .

$$\begin{aligned} a_A &= \begin{cases} a + b \cdot 10 \equiv 591 \pmod{1009} \\ a + b \cdot 20 \equiv 73 \pmod{1009} \end{cases} \\ b_A &= \begin{cases} b + c \cdot 10 \equiv 132 \pmod{1009} \end{cases} \end{aligned}$$

$$\begin{aligned} b \cdot 10 &\equiv 491 \pmod{1009} & 10^{-1} &\equiv 101 \pmod{1009} \\ b &\equiv 150 \pmod{1009} \end{aligned}$$

$$a \equiv 591 - 10 \cdot 150 \equiv 102 \pmod{1009}$$

$$c \equiv (132 - 150) \cdot 101 \equiv 200 \pmod{1009}$$

$$\begin{aligned} K_{AB} &= 204 \\ K_{AC} &= 515 \\ K_{CB} &= 466 \end{aligned}$$

Domanda 4*(svolgere su questo foglio nello spazio assegnato) (6 punti)*

- a) Definire la proprietà di *unidirezionalità* di una funzione di *hash*, distinguendola dalla proprietà di *non invertibilità* di una funzione generica. E' possibile definire una funzione di hash invertibile? In che caso? Fare un esempio di funzione di hash non invertibile ma non unidirezionale.
- b) Definire e distinguere le proprietà desiderate per una buona funzione di hash "*debolmente resistente alle collisioni*" e "*fortemente resistente alle collisioni*". Data una funzione candidata $h = h(m)$, quale delle due proprietà vi sarebbe più facile tentare di violare? Perché?
- c) Si consideri una funzione $h(x)$ che produce *hash* di lunghezza $n = 32$ bit. Dato un hash desiderato \bar{h} , si tenti di ottenere quel valore applicando la funzione $h(x)$ a messaggi totalmente casuali di lunghezza qualsiasi. Qual è la probabilità di ottenere lo hash desiderato in un solo tentativo? E in 10^9 tentativi?

$$P_1 = 2^{-32} \approx 23 \cdot 10^{-10}$$

$$P_2 = 1 - (1 - 2^{-32})^{10^9} \approx 0,20$$

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) Cos'è un *elemento primitivo* $\alpha \in \mathbb{Z}_p^*$? Quanti sono gli elementi primitivi di \mathbb{Z}_{947}^* ?

(2 punti)

$$\phi(946) = 420$$

-
- 2) Qual è la funzione del comando STARTTLS in IMAP e POP3? Qual è il suo effetto?

(2 punti)

-
- 3) Descrivere in sintesi il principio del protocollo HTTPS. Rispetto al protocollo base HTTP, quali informazioni trasmesse dall'utente che si connette a un server *www* vengono cifrate? Quali protocolli stabiliscono una connessione end-to-end tra i *peer* su *client* e *server*? (percorrere la pila dall'alto al basso)

(3 punti)

Cognome e nome:*(stampatello)**(firma leggibile)***Matricola:**

- 4) Descrivere lo *Schema di Lamport* per l'autenticazione di un host Alice da parte di un server Bob, precisando quali informazioni sono conosciute segretamente da A e B, e quali informazioni sono invece pubbliche o trasferite in chiaro da A o B. (3 punti)

- 5) Si consideri un certificato di Alice emesso da un'Autorità TA: $C_A = \{ A, K_A, \{h(A, K_A)\}_{K^{-1}_{TA}} \}$. Chi possiede K_{TA} ? A cosa serve K_{TA} ? Che informazione serve a chi firma il certificato C_A ? Se verifico che la firma del Certificato C_A è valida, posso fidarmi che chi mi ha passato il certificato sia veramente Alice? A cosa serve la *Revocation List*? (3 punti)