Sicurezza delle Reti

Prof. Stefano Bregni — **III Appello d'Esame 2020-21 – 31 agosto 2021**

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 cifratura a chiave pubblica di El Gamal* e pubblica $p = 107$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 23$.

a) 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.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 79$ e spedisce il messaggio $P = 55$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob riceve $C' = (r', t') = (23, 8)$. Calcolare il messaggio decifrato da Bob P'.

d) Calcolare per quale valore di k Alice ha calcolato $C' = E[P']$.

a) p primo $1 < q < p-2$ $p-1 = 106 = 2 \cdot 53$

$5^{53} \equiv 106$, $5^2 \equiv 25$ $\Rightarrow$ $\alpha = 5$ ok ($\alpha = 3, 4$ NO)

Test se α elem. prim. di $\mathbb{Z}_p^*$:
$\alpha^{(p-1)/q_i} \not\equiv 1 \pmod p$

$\beta = \alpha^a \bmod p = 5^{23} \bmod 107 = 59$

b) $r = \alpha^k \bmod p = 5^{79} \bmod 107 = 8$

$t = \beta^k P \bmod p = 59^{79} \cdot 55 \bmod 107 = 29$ $\Rightarrow$ $C = (8, 29)$

c) $P' = t' \cdot r'^{-a} \bmod p = 8 \cdot 23^{-23} \bmod 107 = 65$

$23^{-23} \equiv 23^{83} \equiv (74)^{23} \pmod{107}$

d) $5^k \bmod 107 = 23$

$\rightarrow$ $k = 79$ (B565)

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2020-21 – 31 agosto 2021**

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (5 punti)

Alice e Bob adottano un *sistema di firma cieca RSA.* Alice pubblica il modulo $n = 667$ e l'esponente di cifratura $e = 29$. Bob estrae il numero casuale segreto (*nonce*) $k = 2$ e chiede ad Alice di firmare ciecamente il messaggio $P = 500$.

a) Verificare la correttezza dei dati forniti secondo le ipotesi del metodo di firma cieca RSA.

b) Calcolare i messaggi scambiati da Alice e Bob e la firma A del messaggio P.

a) $n = 667 = 23 \cdot 29$ $\varphi(n) = 616 = 2^3 \cdot 7 \cdot 11$ $\varphi[\varphi(n)] = 240$

b) $d = e^{-1} \bmod \varphi(n) = 29^{239} \bmod 616 = 85$ (meglio con E.E.)

$A \leftarrow B$ $t = k^e P \bmod n = 2^{29} \cdot 500 \bmod 667 = 14$

$A \rightarrow B$ $s = t^d \bmod n = 14^{85} \bmod 667 = 217$

Bob calcola la firma: $A = s/k \bmod n = 217 \cdot 334 \bmod 667$

dove $k^{-1} \bmod n = 334$ (E.E.) $= 442$

Verifica: $A = P^d \bmod n = 500^{85} \bmod 667 = 442$

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

Matricola:

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 500 utenti U_k ($k = 1, \ldots, N$) 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 agli utenti adottando lo schema di Blom?

1000

b) Se invece TA generasse centralmente tutte le possibili chiavi di sessione $K_{ij} = K_{ji}$ e le inviasse ai rispettivi utenti, quanti numeri dovrebbe inviare in tutto?

249500

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 $p = 1013$. Gli utenti A e B però si accordano e si scambiano le informazioni $a_A = 305$, $b_A = 513$, $a_B = 499$, $b_B = 804$.
   - Calcolare i parametri segreti a, b, c.
   - Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$$a_A = \begin{cases} a + b10 \equiv 305 \pmod{1013} \\ a + b20 \equiv 499 \pmod{} \\ b + c10 \equiv 513 \pmod{} \end{cases}$$

$$a_B =$$

$$b_A =$$

$b \cdot 10 \equiv 194 \pmod{1013}$ $\quad 10^{-1} \equiv 304 \pmod{1013}$

$b \equiv 194 \cdot 304 \equiv 222$ $\pmod{}$

$a \equiv 305 - 222 \cdot 10 \equiv 111$ $\pmod{}$

$c \equiv (513 - 222)\,304 \equiv 333$ $\pmod{}$

$K_{AB} = 435$

$K_{AC} = 500$

$K_{CB} = 307$

Domanda 4

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

a) Definire la proprietà di *unidirezionalità* di una funzione di *hash* $h = h(x)$. Perché una funzione di hash non può essere invertibile?

b) Definire la proprietà di *resistenza debole alle collisioni* di una funzione di *hash* $h = h(x)$. Specificare per cosa tale definizione si distingue dalla proprietà di *resistenza forte alle collisioni*. Spiegare perché è più facile provare che una funzione di *hash* non è fortemente resistente alle collisioni, piuttosto che non è debolmente resistente.

c) Si consideri una ipotetica funzione di *hash* $h(m) = \log^{D}_{11}(m) \pmod p$, dove p è un primo di 300 cifre, 11 è un elemento primitivo di $\mathbb{Z}_p^*$, e $0 < m < p$. Si dica se tale funzione $h(m)$ è

- invertibile? (spiegare perché SI o perché NO)

- unidirezionale? (spiegare perché SI o perché NO)

- Spiegare perché tale funzione $h(m)$ non può essere adottata come funzione di hash, pur con il vincolo $0 < m < p$.

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) Un sedicente Stefano Bregni ti contatta, presentando il certificato "SUBJECT: Stefano Bregni" emesso da Verisign. Che procedura segui per sincerarti dell'autenticità del certificato? Se la validazione del certificato va a buon fine, procedi dando per assodato di essere stato contattato da Stefano Bregni, oppure devi fare altro per esserne certo?*(2 punti)*

2) Se utilizzo HTTPS con un browser web, l'Amministratore della rete attraverso cui mi collego a Internet conosce l'indirizzo IP del server a cui mi collego? Conosce i titoli delle pagine che visito? *(2 punti)*

3) L'Amministratore esamina il file di sistema dove sono memorizzate le credenziali degli utenti per l'accesso a un server. Se ipotizzo che la password dell'utente BREGNI appartenga a un vocabolario di 50.000 parole, cosa deve fare l'Amministratore per ricavare la sua password dal file? Di quanto aumenta il tempo necessario all'Amministratore, se le password sono salvate nel file con un *salt* di 16 bit? *(2 punti)*

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

Matricola:

4) Supponiamo di adottare come *password* parole in Inglese, o Francese, o Tedesco, o Italiano, utilizzando lo stesso alfabeto di 26 caratteri per tutte le lingue. Vorrei sapere in quale di queste lingue l'entropia delle *password* è massima. Cosa posso fare per scoprirlo? *(2 punti)*

5) In Kerberos, cos'è un *Ticket Granting Ticket*? Cos'è un *Service Ticket*? Che differenza c'è? *(2 punti)*

6) Si calcolino tutti i residui quadratici dell'insieme $\mathbb{Z}_{13}^*$, partendo dalle potenze dell'elemento primitivo più piccolo di $\mathbb{Z}_{13}^*$. Esaminando i risultati ottenuti, si dica quali sono le radici quadrate di -2 (mod 13). *(2 punti)*

$\begin{cases} 2^6 \equiv 12 \\ 2^4 \equiv 3 \end{cases} \pmod{13} \Rightarrow \alpha = 2$ OK

$2^0 \equiv 1 \pmod{13}$
$2^2 \equiv 4$
$2^4 \equiv 3$
$2^6 \equiv 12$
$2^8 \equiv 9$
$2^{10} \equiv 10$

$\alpha_q = \{1, 3, 4, 9, 10, 12\}$

$\Rightarrow \nexists \sqrt{-2} \pmod{13}$