Sicurezza delle Reti

Prof. Stefano Bregni — **II Appello d'Esame 2018-19 – 26 luglio 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 $p = 131$, $\alpha = 6$, $\beta = \alpha^a \bmod p = 2$, tenendo segreto l'esponente a ($1 < a \leq p\text{-}2$).

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

$A_1 = (r_1, s_1) = (30, 90)$ $\quad P_1 = 10$
$A_2 = (r_2, s_2) = (30, 45)$ $\quad P_2 = 15$
$A_3 = (r_3, s_3) = (30, 1)$ $\quad P_3 = 20$

Verificare che le tre firme siano valide.

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

A_1 | $2^{30}\ 30^{90} \equiv 113$; $6^{10} \equiv 113$ } $\Rightarrow$ OK

A_2 | $2^{30}\ 30^{45} \equiv 71$; $6^{15} \equiv 71$ } $\Rightarrow$ OK

A_3 | $2^{30}\ 30^{1} \equiv 26$; $6^{20} \equiv 62$ } $\Rightarrow$ NO

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*).

$P_1 = 10 \quad A_1 = (30, 90)$

$P_2 = 15 \quad A_2 = (30, 45)$

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

$$\begin{cases} 90k \equiv 10 - a30 \pmod{130} \\ 45k \equiv 15 - a30 \pmod{130} \end{cases}$$

$45k \equiv -5 \pmod{130} \quad MCD(45, 130) = 5 \rightarrow$ 5 soluzioni

$9k_0 \equiv -1 \pmod{26} \quad 9^{-1} \equiv 3 \pmod{26}$

$\rightarrow k_0 \equiv -3 \pmod{26}$

$k_i \equiv -3, (23), 49, 75, 101 \pmod{130}$ Dai dati pubblici:

$\Rightarrow (k = 23)$ $r = \alpha^k \bmod p$

$6^{23} \equiv 30 \bmod 131$

$30 \cdot 23 \equiv 10 - a30 \pmod{130}$

$a30 \equiv 20 \pmod{130} \quad MCD(30, 130) = 10 \rightarrow$ 10 soluzioni

$3a_0 \equiv 2 \pmod{13} \quad 3^{-1} \equiv 9 \pmod{13}$

$\rightarrow a_0 = 5 \pmod{13}$

$a_i = 5, 18, 31, 44, (57), 70, 83, 96, 109, 122 \pmod{130}$

$\Rightarrow (a = 57)$ Dai dati pubblici:

$\beta \equiv \alpha^a \pmod{p} \quad 6^{57} \equiv 2 \pmod{131}$

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

Matricola:

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 $p = 127$, $\alpha = 5$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 64$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 5$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{6, 8\}$. 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*) $k = 11$ e spedisce il messaggio $P = 10$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob riceve $C' = (r', t') = (89, 117)$. Calcolare il messaggio decifrato da Bob P'.
Per quale valore di k Alice ha calcolato $C' = E(P')$?

a) p prima $1 < q \leq p-2$ $p-1 = 126 = 2 \cdot 3^2 \cdot 7$ Tutti gli elem. prim. di $\mathbb{Z}_p^*$

$\alpha^{(p-1)/q_i} \not\equiv 1 \pmod p$

$5^{63} \equiv 126$, $5^{42} \equiv 1$, $5^{18} \equiv 64$ $\Rightarrow$ $\alpha = 5$ NO

$6^{63} \equiv 126$, $6^{42} \equiv 107$, $6^{18} \equiv 64$ $\Rightarrow$ $\alpha = 6$ OK

$\beta = \alpha^a \bmod p = 6^{64} \bmod 127 = 121$

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

$t = \beta^k \cdot P \bmod p = 121^{11} \cdot 10 \bmod 127 = 86$

$\Rightarrow C = (93, 86)$

c) $C' = (r', t') = (89, 117)$

$P' = t' \cdot r'^{-a} \bmod p = 117 \cdot 89^{62} \bmod 127 = 100$

$6^3 \bmod 127 = 89 \Rightarrow K = 3$ (plaintekini + B65)

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

Matricola:

Domanda 3

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

Bob adotta il *sistema di cifratura a chiave pubblica RSA.* Pubblica il modulo $n = 9797$ e due esponenti di cifratura $e_1 = 2087$, $e_2 = 2097$.

a) Verificare la correttezza dei dati forniti in base alle ipotesi del metodo RSA. Scegliere il valore corretto tra i due esponenti e_1 , e_2.

b) Oscar vuole firmare messaggi impersonando Bob sulla base dei dati pubblici. Calcolare quindi la firma di Bob $A(m)$ per il messaggio di Oscar $m = 111$ per il valore corretto dell'esponente e.

a) $n = 9797 = 97 \cdot 101$ (per tentativi)

$\varphi(n) = 96 \cdot 100 = 9600 = 2^7 \cdot 3 \cdot 5^2$

$\varphi[\varphi(n)] = 2560$

$\left.\begin{array}{l} MCD(2087, 9600) = 1 \\ MCD(2097, 9600) = 3 \end{array}\right\} \Rightarrow \boxed{e = 2087}$ $(e \perp \varphi(n))$

b) $d \equiv e^{-1} \pmod{\varphi(n)}$

Con Euclide Esteso: $\boxed{d \equiv 23} \pmod{9600}$

$A = m^d \bmod n = 111^{23} \bmod 9797 = \boxed{4131}$

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

Matricola:

Domanda 4

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

a) Un tizio propone una versione modificata dell'algoritmo SHA che restituisce parole di 3 byte (SHA-24), con l'intenzione di velocizzarne l'esecuzione e ridurre l'occupazione di memoria per gli hash. Con il calcolatore a disposizione, il tempo di esecuzione di SHA-24 sia dell'ordine di 1 μs.

Un attaccante tenta di ottenere un valore di hash desiderato provando SHA-24 su messaggi casuali (si assuma il tempo di generazione trascurabile). In quanto tempo l'attacco ha successo con probabilità almeno 0.5? Limitarsi a fornire l'ordine di grandezza 10^x del numero di secondi necessario.

$P = 1 - (1-2^{-24})^m \cong 1 - (1 - m2^{-24}) = m2^{-24} \rightarrow P = \frac{1}{2}$ per $m = 2^{23} \cong 10^7$

Valore esatto: $(1-2^{-24})^m = \frac{1}{2} \rightarrow m \cong 1{,}16 \cdot 10^7$

$\Rightarrow T \cong 10$ sec

b) Per ognuna delle seguenti funzioni $h(x)$, dire se e per quali condizioni $h(x)$ è *i) invertibile, ii) unidirezionale, iii) resistente alle collisioni*, motivando le risposte e fornendo un esempio di collisione se si risponde NO alla iii).

- $h(x) = x^2 \bmod p$ *invertibile* *unidirezionale* *resistente alle collisioni*

  NO NO NO

- $h(x) = \alpha^x \bmod p$ *invertibile* *unidirezionale* *resistente alle collisioni*

  NO SI (se p grande) NO

- $h(x) = \mathrm{DES}_K(x)$ (ultimo blocco di cifratura CBC-DES del messaggio x con chiave K e IV assegnati)
  invertibile *unidirezionale* *resistente alle collisioni*

  NO SI SI

Sicurezza delle Reti
Prof. Stefano Bregni **II Appello d'Esame 2018-19 – 26 luglio 2019**

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

Matricola:

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) Trovare i fattori primi di $n = 1\,734\,389$ attraverso il *Metodo di Fattorizzazione di Fermat.* *(2 punti)*

$n+1^2 = \dots$
$n+2^2 = \dots$
$n+3^2 = \dots$
$\vdots$
$n+10^2 = 1736489 = 1317^2$

$\Rightarrow n = 1317^2 - 10^2 =$
$(1317-10)(1317+10) =$
$= 1307 \cdot 1327$

2) Nello *Schema di Lamport* per l'autenticazione di un host Alice da parte di un server Bob, descrivere lo *Small*-n *Attack* portato da Oscar a Bob e Alice. *(3 punti)*

3) Descrivere brevemente l'attacco *Man-in-the-Middle* al Protocollo di Instaurazione della Chiave di Diffie-Hellman. Come è possibile ostacolarlo? *(3 punti)*

4) Si consideri un pacchetto IP trasportato via *Transport Mode* o *Tunnel Mode* nell'opzione *Encapsulating Security Payload* (ESP) di IPsec. Quali parti del pacchetto vengono cifrate e autenticate nelle due modalità? Il percorso del pacchetto nella rete cambia a seconda della modalità? *(2 punti)*

5) Quali sono i ruoli dell'*Autentication Server* e del *Ticket-Granting Server* in Kerberos? Cosa significa se il primo autorizza un client ma il secondo no? Cosa è un *ticket*? *(3 punti)*