Sicurezza delle Reti

Prof. Stefano Bregni — **V Appello d'Esame 2018-19 – 11 febbraio 2020**

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 $p = 271$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 15$.

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 $\alpha = \{6, 7\}$. 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*) $k = 17$ e spedisce il messaggio $P_1 = 150$. 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 $C_2 = (r_2, t_2) = (12, 161)$, $C_3 = (r_3, t_3) = (12, 53)$, $C_4 = (r_4, t_4) = (12, 183)$ e, per altra via, viene a sapere che $P_2 = 200$. Calcolare P_3 e P_4.

d) Calcolare per quale valore di k Alice ha calcolato i messaggi C_2, C_3, C_4 del punto c).

a) p primo $1 < a < p-2$ $p-1 = 270 = 2 \cdot 3^3 \cdot 5$ Tst se α elem. prim. di $\mathbb{Z}_p^*$: $\alpha^{(p-1)/q_i} \not\equiv 1 \pmod p$

$6^{135} \equiv 270$, $6^{90} \equiv 242$, $6^{54} \equiv 10$ $\Rightarrow$ $\alpha = 6$ OK ($\alpha = 3, 7$ NO)

$\beta = \alpha^a \bmod p = 6^{15} \bmod 271 = 23$

b) $r_1 = \alpha^k \bmod p = 6^{17} \bmod 271 = 15$

$t_1 = \beta^k P_1 \bmod p = 23^{17} \cdot 150 \bmod 271 = 89$

$\Rightarrow$ $C_1 = (15, 89)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $t_2^{-1} \equiv 161^{-1} \equiv 101 \pmod{271}$ (E. E.)

$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod p \equiv 200 \cdot 53 \cdot 101 \equiv 150$

$P_4 \equiv P_2 \frac{t_4}{t_2} (\dots) \equiv 200 \cdot 183 \cdot 101 \equiv 160$

d) $3^k \bmod 271 = 12$ $\Rightarrow$ $K = 155$ (BSGS)

Sicurezza delle Reti
Prof. Stefano Bregni — **V Appello d'Esame 2018-19 – 11 febbraio 2020**

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

Matricola:

Domanda 2

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

Bob adotta il *sistema di cifratura a chiave pubblica RSA.* Pubblica il modulo $n = 11227$ e un esponente di cifratura scelto tra i due $e_1 = 3961$, $e_2 = 3973$.

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) Alice trasmette a Bob il messaggio cifrato $C = 69$, calcolato utilizzando il valore corretto dell'esponente e. Decifrarlo e calcolare il corrispondente messaggio in chiaro P.

a) $n = 11227 = 103 \cdot 109$ (per tentativi)

$\varphi(n) = 102 \cdot 108 = 11016 = 2^3 \cdot 3^4 \cdot 17$

$\varphi[\varphi(n)] = 3456$

$\left.\begin{array}{l} MCD(3961, 11016) = 17 \\ MCD(3973, 11016) = 1 \end{array}\right\} \Rightarrow \boxed{e = 3973}$ $(e \perp \varphi(n))$

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

Con Euclide Esteso: $d \equiv 61 \pmod{11016}$

Verifica: $3973 \cdot 61 \bmod 11016 = 1$

$P = C^d \bmod n = 69^{61} \bmod 11227 = (333)$

Sicurezza delle Reti
Prof. Stefano Bregni — **V Appello d'Esame 2018-19 – 11 febbraio 2020**

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

Matricola:

Domanda 3
(svolgere su questo foglio nello spazio assegnato) (6 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 163$, $\alpha = 5$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 33$.

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 $\alpha = \{6, 7\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Bob estrae il numero casuale segreto (*nonce*) $k = 17$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 150$.

c) Verificare se anche la firma $A' = (r', s') = (12, 60)$ è valida per lo stesso messaggio $P = 150$. 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. primitivo di $\mathbb{Z}_p^*$

Test se α elem primitivo: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $p-1 = 162 = 2 \cdot 3^4$

$7^{81} \equiv 162$
$7^{54} \equiv 154$ $\Rightarrow \alpha = 7$ ($\alpha = 5, 6$ NO)
OK

$\beta = \alpha^a \bmod p = 7^{33} \bmod 163 = 27$

b) $r = \alpha^k \bmod p = 7^{17} \bmod 139 = 29$

$s = k^{-1}(P - ar) \bmod (p-1) = 143 (150 - 33 \cdot 29) \bmod 163 = 105$ $\Rightarrow A = (29, 105)$

$k^{-1} \bmod (p-1) = 17^{-1} \bmod 162 = 143$ (E.E.)

Verifica: $17 \cdot 143 \equiv 1 \pmod{162}$

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

$27^{12} 12^{60} \equiv 158 \pmod{163}$
$7^{150} \equiv 158$ (—) $\Rightarrow A' = (12, 60)$ firma valida di $P = 150$

$s K \equiv P - q r \pmod{(p-1)}$

$60 K \equiv 150 - 12 \cdot 33 \pmod{162}$

$60 K \equiv 78 \pmod{162}$ $\quad MCD(60, 162) = 6 \rightarrow$ 6 soluzioni

$10 K \equiv 13 \pmod{27}$ $\quad 10^{-1} \equiv 19 \pmod{27}$

$\rightarrow K_0 \equiv 4 \pmod{27}$

$K_i \equiv 4, 31, 58, 85, 112, (139) \pmod{162}$

Dai dati pubblici: $r = \alpha^K \bmod p \quad 7^K \equiv 12 \pmod{163}$

$\Rightarrow (K = 139)$

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*. Specificare per cosa tale definizione si distingue dalla proprietà di *resistenza debole alle collisioni*. Perché la resistenza forte è più difficile da garantire di quella debole?

b) Si consideri la funzione $h(x) = \mathrm{LSB}_{32}(x^4)$, che restituisce i 16 bit meno significativi di x^4, con x intero. Provare che $h(x)$ non è fortemente resistente alle collisioni.

c) Una tabella raccoglie i valori di *hash*, di lunghezza $L = 24$ bit, calcolati su 20.000.000 di file MP4 diversi.

- Qual è la probabilità che almeno due file abbiano lo stesso hash in tabella?

$N = 2^{24} \cong 1{,}678 \cdot 10^{-7}$ $\quad r = 2 \cdot 10^7$ $\quad P \cong 1 - e^{-r^2/2N} \cong 1 - e^{-10^7} = 1$

- Quanto vale questa probabilità, se i file sono solo 5000?

$r = 5000$ $\quad P \cong 1 - e^{-25/(2 \cdot 1{,}678)} \cong 0{,}525$

- Qual è la lunghezza minima degli *hash*, perché detta probabilità sia <50% ancora su 20.000.000 di file diversi?

$e^{-r^2/2N} > 1/2$ $\quad r^2/2N < \ln 2$ $\quad N > \dfrac{r^2}{2 \ln 2} = 2{,}9 \cdot 10^{14} \cong 2^{48}$

$\Rightarrow$ 48 bit

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (11 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) Si considerino le funzioni di cifratura doppia $C = E_{K_2}(E_{K_1}(P))$ e sua decifratura $P = D_{K_1}(D_{K_2}(C))$, con due chiavi K_1 e K_2 ciascuna di lunghezza $n = 48$ bit, parole in chiaro e cifrate di lunghezza 8 bit ($P \in \mathbb{Z}_{256}^*$, $C \in \mathbb{Z}_{256}^*$), algoritmo di cifratura non precisato. Si tenta un attacco *Meet-in-the-Middle* per trovare la coppia di chiavi K_1, K_2. *(4 punti)*

- Descrivere il procedimento. Quali informazioni è necessario conoscere? L'attacco ha sempre successo?
- Si indichi con E il peso computazionale di una operazione di cifratura semplice $E_K(X)$, uguale al peso di una decifratura $D_K(X)$. Quanti calcoli sono necessari (in unità E) per completare l'attacco con successo?
- Quale occupazione di memoria [byte] è necessaria per completare l'attacco con successo?

Numero operazioni: $2^{48} \cdot E \div 2^{49} \cdot E$ $(\sim 10^{14} E)$

Occupazione memoria:

256 TB

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

Matricola:

2) Descrivere i ruoli dell'*Autentication Server* e del *Ticket-Granting Server* in Kerberos. Cosa sta succedendo, se un client riceve un ticket valido dal primo ma non dal secondo? *(2 punti)*

3) Illustrare il principio di funzionamento di HTTPS. Cosa succede quando un client invia una richiesta di connessione HTTPS al server? Quali informazioni inviate dal client HTTPS durante la connessione sono cifrate? Quali protocolli sono utilizzati ai livelli inferiori? *(2 punti)*

4) Si spieghi il significato del grafico sotto riportato. In particolare, specificare: *(3 punti)*

- qual è la grandezza in ascissa? qual è la grandezza in ordinata? cosa rappresentano le due curve FAR(x) e FRR(x)?
- quali sono i valori limite di FAR(x) per $x \to 0$ e $x \to \infty$?
- perché si considera "ottimale" il valore di x per cui le due curve si intersecano? cioè, quale grandezza è minimizzata o massimizzata?