Sicurezza delle Reti

Prof. Stefano Bregni — **IV Appello d'Esame 2016-17 – 23 gennaio 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 $p = 139$, $\alpha = 11$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 128$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 11$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{10, 11, 12\}$. 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*) $k = 13$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 50$.

c) Verificare se anche la firma $A' = (r', s') = (3, 94)$ è valida per lo stesso messaggio $P = 50$. Se è valida, calcolare il valore di k per cui è stata calcolata da Bob.

a) p primo $1 < a < p-2$ $K \perp p-1$ α elem. primitivo di $\mathbb{Z}_p^*$

Test α elem. primitivo $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $\quad p-1 = 138 = 2 \cdot 3 \cdot 23$

$11^{69} \equiv 1$ — — $\pmod{139}$ $\Rightarrow$ NO

$12^{69} \equiv 138$
$12^{46} \equiv 96$
$12^{6} \equiv 125$
$\Rightarrow \alpha = 12$ elem. primitivo di $\mathbb{Z}_{139}^*$

$\beta = \alpha^a \bmod p = 12^{128} \bmod 139 = 83$

b) $r = \alpha^K \bmod p = 12^{73} \bmod 139 = 128$

$s \equiv K^{-1}(P - ar) \bmod (p-1) \equiv 95\,(50 - 128 \cdot 128) \bmod 138 \equiv 28$

$K^{-1} \bmod (p-1) = 73^{-1} \bmod 138 = 95$ (con Euclide Esteso)

Verifica: $73 \cdot 95 \equiv 1 \pmod{138}$

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

$3^3 \cdot 3^{94} \bmod 139 \equiv 37$
$12^{50} \bmod 139 \equiv 37$
$\Rightarrow$ OK

$A = (3, 94)$
firma valida di $P = 50$

$sK \equiv P - ar \pmod{138}$

$94K \equiv 50 - 128 \cdot 3 \pmod{138}$

$94K \equiv 80 \pmod{138}$ $\quad \gcd(94, 80) = 2 \rightarrow$ 2 soluzioni

$47K \equiv 40 \pmod{69}$ $\quad 47^{-1} \equiv 47 \pmod{69}$ (E.E.)

$\rightarrow K_0 \equiv 40 \cdot 47 \equiv 17 \pmod{69}$

$K_1 \equiv 17, 86 \pmod{138}$

Dai dati pubblici:

$r = \alpha^K \bmod p$

$\Rightarrow K = 17$

Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2016-17 – 23 gennaio 2018**

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 $p = 239$, $\alpha = 7$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 65$.

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 $\alpha = 6$. 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*) $k = 24$ e spedisce il messaggio $P_1 = 100$. 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 $C_2 = (r_2, t_2) = (56, 43)$, $C_3 = (r_3, t_3) = (56, 86)$, $C_4 = (r_4, t_4) = (56, 237)$ e, per altra via, viene a sapere che $P_2 = 100$. Calcolare P_3 e P_4.

a) p primo $1 < \alpha < p-2$ $p-1 = 238 = 2 \cdot 7 \cdot 17$

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

$7^{119} \equiv 238 \pmod{239}$
$7^{34} \equiv 24$
$7^{14} \equiv 211$

$\Rightarrow$ OK $\alpha = 7$ elem. primitivo di $\mathbb{Z}_{239}^*$ ($\alpha = 6$ no)

$\beta = \alpha^a \bmod p = 7^{65} \bmod 239 = 171$

b) $r_1 = \alpha^k \bmod p = 7^{24} \bmod 239 = 93$

$t_1 = \beta^k P \bmod p = 171^{24} \cdot 100 \bmod 239 = 161$

$\Rightarrow C_1 = (93, 161)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $\quad t_2^{-1} = 43^{-1} \equiv 189 \pmod{239}$ (con E.E.)

$P_3 = P_2 \frac{t_3}{t_2} \bmod p = 100 \cdot 86 \cdot 189 \bmod 239 = 200$

$P_4 = P_2 \frac{t_4}{t_2} \bmod p = 100 \cdot 237 \cdot 189 \bmod 239 = 201$

Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2016-17 – 23 gennaio 2018**

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

Matricola:

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

Alice e Bob adottano il protocollo di *Diffie-Hellman* per l'instaurazione della loro chiave simmetrica K_{AB}. Alice pubblica $p = 97$ e inizialmente $\alpha = 5$. Alice sceglie $1 \le x \le p-2$ (segreto). Bob sceglie $1 \le y \le p-2$ (segreto).

a) Alice verifica la correttezza dei dati secondo le ipotesi di Diffie-Hellman. Nel caso $\alpha = 5$ non risulti una scelta valida, Alice si corregge e pubblica invece un valore valido scelto nell'insieme $\alpha = \{2, 3, 4, 5\}$. Se nessuna di queste scelte risultasse valida, Alice e Bob rinunceranno a proseguire (e l'esercizio termina qui).

Test se α elem. prim. di $\mathbb{Z}_p^*$: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $\quad p-1 = 96 = 2^5 \cdot 3$

$5^{48} \equiv 96$
$5^{32} \equiv 35$
$\Rightarrow$ OK $(\alpha = 5)$ (unico elem. primitivo dell'insieme)

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

Alice ➔ Bob: $\alpha^x \equiv 30 \pmod p$

Alice ➔ Bob: $\alpha^y \equiv 85 \pmod p$

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

$x \equiv 9 \pmod{97}$ (per tentativi 5^65)

$y \equiv 90 \pmod{97}$

$K_{AB} = \alpha^{xy} \bmod p = 5^{9 \cdot 90} \bmod 97 \equiv 12 \pmod{97}$

Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2016-17 – 23 gennaio 2018**

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

Matricola:

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

a) Ricavare la sequenza binaria pseudo-casuale $\{x_i\}$ generata dall'algoritmo *Blum-Blum-Shab* per $p = 11$, $q = 43$, $x = 10$ e determinarne il periodo P.

i	x_i	b_i	
0	100	0	
1	67	1	
2	232	0	$P=6$
3	375	1	
4	144	0	
5	397	1	
6	100	0	
7	⋮		
8	⋮		
9	!		
10			
11			

$M = p \cdot q = 11 \cdot 43 = 473$

$x_0 \equiv x^2 \pmod{n}$

$x_i \equiv x_{i-1}^2 \pmod{n}$

b) In base alla teoria, quali sono i valori possibili che può assumere il periodo $P = \pi(x_0)$ del generatore precedente, per valori arbitrari del seme $x_0 = x^2 \in \mathbb{Z}_n$?

Si ricorda che $\pi(x_0)$ divide $\lambda(\lambda(n))$, dove $\lambda(n) := \text{mcm}\left(\left\{\varphi\left(p_i^{a_i}\right)\right\}\right)$ è la Funzione di Charmichael.

$\lambda(n) = \text{mcm}(10, 42) = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

$10 = 2 \cdot 5$

$42 = 2 \cdot 3 \cdot 7$

$\lambda(\lambda(n)) = \lambda(210) = \text{mcm}(1, 2, 4, 6) = 24$

$\pi(x_0) \in \{1, 2, 3, 4, 6, 8, 12\}$ $\qquad \pi_{MAX} = 12$

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (14 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) Descrivere lo *Schema di Lamport* per l'autenticazione di un host A da parte di un server B, precisando quali informazioni sono pubbliche o trasferite in chiaro, e quali altre sono private e memorizzate in A o B. *(3 punti)*

2) Che differenza c'è tra i protocolli di *symmetric key agreement* e *symmetric key distribution*? In cosa consiste un *replay attack* ai protocolli precedenti? Come possono essere impediti i *replay attack*? *(3 punti)*

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

Matricola:

3) Perché l'Amministratore di un sistema non può ricavare le password di accesso degli utenti dal database? Come avviene la verifica di correttezza della password inserita da un utente? Se ipotizzo che la password di un utente appartenga a un vocabolario di 100.000 parole, quanti tentativi sono necessari all'Amministratore per ricavare la password dal database? Quanti tentativi sono necessari all'Amministratore, invece, se l'informazione è salvata con *salt* di 32 bit? *(3 punti)*

4) Cosa garantisce un *certificato di identità* emesso da una CA in una PKI? Quale procedura segue un utente per verificare l'autenticità di quel certificato? *(2 punti)*

5) Trovare i fattori primi di $n = 8213$ attraverso l'*Algoritmo di Fattorizzazione p−1* di Pollard con base $a = 2$. *(3 punti)*

$b_1 \equiv 2 \pmod{8213}$

$b_2 \equiv 2^2 \equiv 4$ $\quad \text{MCD}(3, n) = 1$

$b_3 \equiv 4^3 \equiv 64$ $\quad \text{MCD}(63, n) = 1$

$b_4 \equiv 64^4 \equiv 6270$ $\quad \text{MCD}(6269, n) = 1$

$b_5 \equiv 6270^5 \equiv 4900$ $\quad \text{MCD}(4899, n) = 1$

$b_6 \equiv 4900^6 \equiv 5310$ $\quad \text{MCD}(5309, n) = 1$

$b_7 \equiv 5310^7 \equiv 4043$ $\quad \text{MCD}(4042, n) = 43$

$\Rightarrow p = 43$

$q = n/p = 191$