Sicurezza delle Reti

Prof. Stefano Bregni — **III Appello d'Esame 2018-19 – 31 agosto 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 $p = 127$, $\alpha = 4$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 57$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 4$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{5, 6\}$. 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*) $k = 25$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 15$.

c) Verificare se anche la firma $A' = (r', s') = (12, 69)$ è valida per lo stesso messaggio $P = 15$. 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 per α elem. primitivo: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $\quad p-1 = 126 = 2 \cdot 3^2 \cdot 7$

$4^{63} \equiv 1$, $4^{42} \not\equiv 1$, $4^{18} \equiv$ $\Rightarrow$ NO

$5^{63} \equiv$, $5^{42} \equiv 1$, $5^{18} \equiv$ $\Rightarrow$ NO

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

$\beta = \alpha^a \bmod p = 6^{57} \bmod 127 = 27$

b) $r = \alpha^k \bmod p = 6^{25} \bmod 127 = 14$

$s = k^{-1}(P - ar) \bmod (p-1) = 121\,(15 - 57 \cdot 14) \bmod 126 = 9$ $\Rightarrow A = (14, 9)$

$k^{-1} \bmod (p-1) = 25^{-1} \bmod 126 = 121$ (con E.E.)

Verifica: $25 \cdot 121 \equiv 1 \pmod{126}$

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

$27^{12} 12^{69} \equiv 5 \pmod{127}$
$6^{15} \equiv 5 \pmod{127}$
$\Rightarrow$ $A^1 = (12, 69)$ firma valida di $P_{=15}$

$5K \equiv P - ar \pmod{p-1}$

$69K \equiv 15 - 57 \cdot 12 \pmod{126}$

$69K \equiv 87 \pmod{126}$ $\quad mcd(69, 126) = 3 \rightarrow$ 3 soluzioni

$23K \equiv 29 \pmod{42}$ $\quad 23^{-1} \equiv 11 \pmod{42}$

$\rightarrow K_0 \equiv 25 \pmod{42}$

$K_i \equiv 25, 67, 109 \pmod{126}$

Dai dati pubblici: $r = \alpha^K \bmod p$ $\quad 6^K \equiv 12 \pmod{127}$

$\Rightarrow$ $K = 109$

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2018-19 – 31 agosto 2019**

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 di El Gamal* e pubblica $p = 233$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 70$.

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 $\alpha = \{4, 7\}$. 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*) $k = 15$ e spedisce il messaggio $P_1 = 230$. 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 $C_2 = (r_2, t_2) = (27, 83)$, $C_3 = (r_3, t_3) = (27, 91)$, $C_4 = (r_4, t_4) = (27, 200)$ e, per altra via, viene a sapere che $P_2 = 20$. Calcolare P_3 e P_4.

a) p primo $1 < \alpha < p-2$ $p-1 = 232 = 2^3 \cdot 29$

Test se α elem primitivo di $\mathbb{Z}_p^*$: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$

$3^{116} \equiv 232 \pmod{233}$
$3^8 \equiv 37$
$\Rightarrow \alpha = 3$ ok ($\alpha = 4, 7$ no)

$\beta = \alpha^a \bmod p = 3^{70} \bmod 233 = 52$

b) $r_1 = \alpha^k \bmod p = 3^{15} \bmod 233 = 64$

$t_1 = \beta^k P \bmod p = 52^{15} \cdot 230 \bmod 233 = 90$

$\Rightarrow C_1 = (64, 90)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$

$t_2^{-1} = \beta^{-3} \equiv 73 \pmod{233}$

$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod{233} \equiv 20 \cdot 91 \cdot 73 \equiv 50$

$P_4 \equiv P_2 \frac{t_4}{t_2} \pmod{233} \equiv 20 \cdot 200 \cdot 73 \equiv 51$

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 1000 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 adottando lo schema di Blom sopra descritto?

$2N = 2000$

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

$N(N-1) = 999000$

c) Si consideri il caso di tre soli utenti A, B e C, con identificativi pubblici rispettivamente uguali a $r_A = 100$, $r_B = 200$, $r_C = 300$. TA sceglie e tiene segreti a, b, c, e pubblica $p = 1013$. Gli utenti A e B però si accordano e si scambiano le rispettive informazioni $a_A = 929$, $b_A = 173$ e $a_B = 838$, $b_B = 276$.
   - Calcolare i tre parametri segreti a, b, c.
   - Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$$\begin{cases} a_A = a + b100 \equiv 929 \pmod{1013} \\ a_B = a + b200 \equiv 838 \pmod{1013} \\ b_A = b + c100 \equiv 173 \pmod{1013} \end{cases}$$

$b100 \equiv 922 \pmod{1013}$ $\qquad 100^{-1} \equiv 233 \pmod{1013}$

$b \equiv 70 \pmod{1013}$

$a \equiv 929 - 100 \cdot 70 \equiv 7 \pmod{1013}$

$c \equiv (173 - 70)\,233 \equiv 700 \pmod{1013}$

$$\begin{cases} K_{AB} = 74 \\ K_{AC} = 153 \\ K_{BC} = 572 \end{cases}$$

Domanda 4

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

a) Definire la proprietà di *unidirezionalità* di una funzione di *hash*. Specificare per cosa tale definizione si distingue dalla proprietà di *non invertibilità* di una funzione generica.

b) La funzione $h(x) = \alpha^x \bmod p$ (p primo di 400 cifre decimali) è invertibile? E' unidirezionale? Potrebbe essere usata come funzione di hash? Perché SI o perché NO? Spiegare.

c) Si consideri una ipotetica funzione di hash $h(m)$ che restituisce valori di 32 bit, rispettivamente calcolati come parità dei bit del messaggio m in posizione (0, 32, 64, ...); (1, 33, 65, ...); ecc. Ossia, il bit i ($i = 0, 1, \ldots, 31$) di $h(m)$ è la parità dei bit i, i+32, i+64, ... del messaggio m fino al termine dei bit di quest'ultimo. Si dica se tale funzione $h(m)$ è

- invertibile?

- unidirezionale (se si risponde NO, fornire un esempio)?

- resistente alle collisioni (se si risponde NO, fornire un esempio di collisione)?

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

Matricola:

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) L'equazione $x^2 \equiv 11 \pmod{359}$ ha soluzione? Se la risposta è sì, calcolarne le radici, altrimenti risolvere $x^2 \equiv -11 \equiv 348 \pmod{359}$. *(2 punti)*

359 primo → l'eq. ha soluzione se $11^{179} \equiv 1 \pmod{359}$

$11^{179} \equiv 1 \pmod{359} \Rightarrow$ sì

$359 \equiv 3 \pmod 4 \Rightarrow$ l'eq $x^2 \equiv 11 \pmod{359}$ ha 2 radici

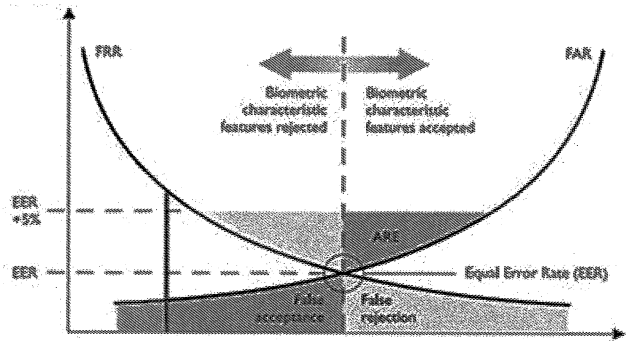
$x \equiv \pm 11^{90} \equiv \pm 27 \pmod{359}$

$\Rightarrow x_{1,2} \equiv 27, 332 \pmod{359}$

2) Perché l'Amministratore non può ricavare le password di accesso degli utenti dal database del sistema? Come avviene la verifica di correttezza della password inserita da un utente?
Se ipotizzo che la password dell'utente BREGNI appartenga a un vocabolario di 100.000 parole, quanti tentativi sono necessari all'Amministratore per ricavare la sua password dal database del sistema? Quanti tentativi sono necessari all'Amministratore, invece, se la password di BREGNI è salvata nel database con un *salt* di 24 bit? *(2 punti)*

3) 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)?
- perché si considera "ottimale" il valore di x per cui le due curve hanno lo stesso valore? cioè, cosa è minimizzato o massimizzato?



4) Esprimere il *Problema Decisionale di Diffie-Hellman*. Questo problema è più o meno difficile del *Problema Computazionale di Diffie-Hellman*? Saper risolvere il primo può aiutare a risolvere il secondo? *(2 punti)*

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

Matricola:

5) Si consideri una modalità di cifratura AES-128 a blocchi con concatenazione (CBC, CFB…). Alice tiene segreta la chiave, ma pubblica il vettore di inizializzazione. Ci sono comunque dei vantaggi rispetto alla modalità semplice non concatenata ECB, anche se la lunghezza della chiave segreta non è stata raddoppiata? *(2 punti)*

6) Trovare i fattori primi di $n = 19549$ attraverso l'*Algoritmo di Fattorizzazione p−1* di Pollard con base $a = 2$. *(3 punti)*

$b_1 \equiv 2 \pmod{19549}$

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

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

$b_4 \equiv 64^4 \equiv 4174$ $\quad MCD(4173, n) = 1$

$b_5 \equiv 4174^5 \equiv 14494$ $\quad MCD(14494, n) = 1$

$b_6 \equiv 14494^6 \equiv 6151$ $\quad MCD(6150, n) = 1$

$b_7 \equiv 6151^7 \equiv 2035$ $\quad MCD(2034, n) = 113$

$\Rightarrow p = 113$

$q = 173$