Sicurezza delle Reti

Prof. Stefano Bregni — **III Appello d'Esame 2016-17 – 28 agosto 2017**

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 cifratura a chiave pubblica di El Gamal* e pubblica $p = 191$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 32$.

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 $\alpha = \{$[illegible], 16, 17, 18, 19, 20$\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Alice estrae un numero casuale segreto (*nonce*) k e spedisce il messaggio cifrato $C_1 = (75,33)$. Calcolare il messaggio P_1 decifrato da Bob.

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 $C_2 = (r_2, t_2) = (25, 109)$, $C_3 = (r_3, t_3) = (25, 126)$, $C_4 = (r_4, t_4) = (25, 12)$ e, per altra via, viene a sapere che $P_2 = 50$. Calcolare P_3 e P_4.

a) p primo $1 < \alpha < p-2$ $p-1 = 190 = 2 \cdot 5 \cdot 19$

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

Solo $\alpha = 19$ elem primitivo di $\mathbb{Z}_p^*$

$\beta = \alpha^a \bmod p = 19^{32} \bmod 191 = 92$

$19^{95} \equiv 190$ OK

$19^{38} \equiv 39$

$19^{10} \equiv 52$

b) $P \equiv t r^{-a} \pmod p$

$\equiv 35 \cdot 75^{-32} \equiv 33 (-28)^{32} \equiv 22$

$75^{-1} \equiv -28 \pmod{191}$

(Euclide Esteso)

c) $\frac{t_2}{p_2} \equiv \frac{t_3}{p_3} \equiv \frac{t_4}{p_4} \equiv \beta^k \pmod p$

$t_2^{-1} = 109^{-1} \equiv 184 \pmod{191}$

$P_3 = P_2 \frac{t_3}{t_2} \bmod p = 50 \cdot 126 \cdot 184 \bmod 191 = 21$

$P_4 = P_2 \frac{t_4}{t_2} \bmod p = 50 \cdot 12 \cdot 184 \bmod 191 = 2$

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2016-17 – 28 agosto 2017**

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (6 punti)

Alice e Bob adottano un *sistema di firma cieca RSA*. Alice pubblica il modulo $n = 1457$ e l'esponente di cifratura $e = 41$. Bob estrae il numero casuale segreto (*nonce*) $k = 50$ 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) $n = 1457 = 31 \cdot 47$ $\varphi(n) = 1380 = 2^2 \cdot 3 \cdot 23 \cdot 5$ $\varphi[\varphi(n)] = 352$

$K \perp n$ OK $e \perp \varphi(n)$ OK

b) $d \equiv e^{-1} \pmod{\varphi(n)}$ $d \equiv 41^{352} \bmod 1380 = 101$ (meglio E.E.)

$B \to A$: $t = K^e P \bmod n = 50^{41} \cdot 500 \bmod 1457 = 133$

$A \to B$: $s = t^d \bmod n = 133^{101} \bmod 1457 = 1347$

Bob calcola la firma: $A = s/K \bmod n = 1347 \cdot 204 \bmod 1457$

$= 872$

dove $K^{-1} \bmod n \equiv 204$ (E.E.)

Verifica: $A = P^d \bmod n = 500^{101} \bmod 1457 = 872$ (come sopra)

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2016-17 – 28 agosto 2017**

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

Matricola:

Domanda 3
(svolgere su questo foglio nello spazio assegnato) (5 punti)

Si consideri il campo GF(2^8) = $\mathbb{Z}_2(x)$ mod ($x^8+x^4+x^3+x+1$).

Si segua la notazione usuale: gli elementi E*k* sono numerati con $k = 0, 1, \ldots.$; l'indice k, espresso in forma binaria, rappresenta i coefficienti del polinomio corrispondente (bit più significativo = coefficiente di grado più alto).

Calcolare E32 $^{-1}$ in GF(2^8) eseguendo tutte le operazioni sulle rappresentazioni polinomiali degli elementi e applicando l'Algoritmo di Euclide Esteso. Esprimere il risultato finale con la notazione E*k*.

$E32 = b(x) = x^5$

1) $m(x) = q_1(x)\,b(x) + r_1(x)$

$q_1(x) = x^3$

$r_1(x) = x^4+x^3+x+1$

$x^8+x^4+x^3+x+1 \;|\; x^5$
$x^8 \qquad\qquad\quad |\; x^3$
x^4+x^3+x+1

2) $b(x) = q_2(x)\,r_1(x) + r_2(x)$

$q_2(x) = x+1$

$r_2(x) = x^3+x^2+1$

$x^5 \;|\; x^4+x^3+x+1$
$x^5+x^4+x^2+x \;|\; x+1$
x^4+x^2+x
x^4+x^3+x+1
x^3+x^2+1

3) $r_1(x) = q_3(x)\,r_2(x) + r_3(x)$

$q_3(x) = x$

$r_3(x) = 1$

$x^4+x^3+x+1 \;|\; x^3+x^2+1$
$x^4+x^3+x \qquad\quad |\; x$
1

$X_0 = 0 \quad X_1 = 1$

$X_2 = -q_1(x) X_1 + X_0 = x^3$

$X_3 = -q_2(x) X_2 + X_1 = (x+1)x^3 + 1 = x^4 + x^3 + 1$

$X_4 = -q_3(x) X_3 + X_2 = (x^4 + x^3 + 1)x + x^3 = \boxed{x^5 + x^4 + x^3 + x} = b^{-1}(x)$

In notazione binaria $b^{-1}(x) = 00111010 = 3A$

Verifica: $x^5(x^5 + x^4 + x^3 + x) \equiv 1 \pmod{m(x)}$

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

Matricola:

Domanda 4

(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 N 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 appunto lo schema di Blom?

$2N$

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

$N(N-1)$

c) Si consideri il caso di tre soli utenti A, B e C, con identificativi pubblici rispettivamente uguali a $r_A = 101$, $r_B = 111$, $r_C = 121$. TA sceglie e tiene segreti a, b, c, e pubblica $p = 947$. Gli utenti A e B però si accordano e si scambiano le informazioni $a_A = 346$, $b_A = 503$, $a_B = 715$, $b_B = 371$.
   - Calcolare i parametri segreti a, b, c.
   - Calcolare le tre chiavi simmetriche distribuite da TA K_{AB}, K_{AC}, K_{BC}.

$$a_A = \begin{cases} a + b\,101 \equiv 346 \pmod{947} \\ a + b\,111 \equiv 715 \pmod{947} \\ b_A = b + c\,101 \equiv 503 \pmod{947} \end{cases}$$

$101^{-1} \equiv 663 \pmod{947}$

$101^{-1} \equiv 872 \pmod{947}$

$10\,b \equiv 369 \pmod{947}$

$b \equiv 321 \pmod{947}$

$a = 346 - 321 \cdot 101 \equiv 123 \pmod{947}$

$c = (503 - 321) \cdot 872 \equiv 555 \pmod{947}$

$K_{AB} = 306$

$K_{AC} = 609$

$K_{BC} = 150$

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 $x^2 \equiv 79 \pmod{751}$ ha soluzione? Se la risposta è sì, calcolarne le radici, altrimenti risolvere $x^2 \equiv -79 \equiv 672 \pmod{751}$. *(2 punti)*

751 primo → l'eq. ha soluzione se $79^{\frac{751-1}{2}} \equiv 1 \pmod{751}$

$79^{375} \equiv -1 \pmod{751} \Rightarrow$ NO

$751 \equiv 3 \pmod 4 \Rightarrow$ l'eq. $x^2 \equiv -79 \pmod{751}$ ha radici

$x = \pm 79^{188} \bmod 751 = \pm 77$ $\quad x_{1,2} \equiv 77, 674 \pmod{751}$

2) Descrivere l'*attacco dell'intruso* al Protocollo di Instaurazione della Chiave di Diffie-Hellman. *(2 punti)*

3) Qual è il vantaggio di usare una modalità di concatenazione (CFB, CBC, ….) di un cifrario a blocchi, se il vettore di inizializzazione è trasmesso in chiaro e non è tenuto segreto con la chiave? *(2 punti)*

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

Matricola:

4) Enunciare il *Teorema Cinese del Resto* generalizzato a K congruenze. *(2 punti)*

5) Disegnare lo schema di un generatore PRBS basato sull'algoritmo *Linear Feedback Shift Register* (LFSR) oppure *Blum-Blum-Shub* (BBS), che generi una sequenza di bit pseudo-casuali di periodo almeno pari a 10^3. Specificare come *garantire* che il periodo sia non inferiore a 10^3. Scegliere lo schema LFSR oppure BBS in base a quanto vi risulta semplice garantire quel periodo minimo (non è necessario calcolare i valori numerici dei parametri, ma è richiesto di spiegare come calcolarli, e quindi come fare la scelta opportuna) *(3 punti)*

6) Descrivere la procedura di *autenticazione* e *cifratura* di un messaggio PGP inviato da Alice a Bob basato sugli algoritmi RSA, 3DES, SHA, DSA (firma El Gamal). *(3 punti)*