

Sicurezza delle Reti

Prof. Stefano Bregni

V Appello d'Esame 2017-18 – 1~~8~~ febbraio 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 $p = 157$, $\alpha = 6$, $\beta = \alpha^a \pmod{p} = 37$, tenendo segreto l'esponente a ($1 < a \leq p-2$).

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

$$A_1 = (r_1, s_1) = (26, 32) \quad P_1 = 20$$

$$A_2 = (r_2, s_2) = (26, 28) \quad P_2 = 24$$

$$A_3 = (r_3, s_3) = (26, 28) \quad P_3 = 28$$

Verificare che le tre firme siano valide.

$$B^r r^s \equiv \alpha^P \pmod{p}$$

$$A_1 \left\{ \begin{array}{l} 37^{26} 26^{32} \equiv 47 \\ 6^{20} \equiv 47 \end{array} \right\} \Rightarrow \text{OK}$$

$$A_2 \left\{ \begin{array}{l} 37^{26} 26^{28} \equiv 153 \\ 6^{24} \equiv 153 \end{array} \right\} \Rightarrow \text{OK}$$

$$A_3 \left\{ \begin{array}{l} 37^{26} 26^{28} \equiv 153 \\ 6^{28} \equiv 154 \end{array} \right\} \Rightarrow \text{NO}$$

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).

$$P_1 = 20 \quad A_1 = (26, 32)$$

$$P_2 = 24 \quad A_2 = (26, 28)$$

$$S \equiv K^{-1} (P - a\Gamma) \pmod{(p-1)} \rightarrow SK \equiv P - a\Gamma \pmod{(p-1)}$$

$$\begin{cases} 32K \equiv 20 - a \cdot 26 \pmod{156} \\ 28K \equiv 24 - a \cdot 26 \pmod{156} \end{cases}$$

$$\begin{cases} 28K \equiv 24 - a \cdot 26 \pmod{156} \end{cases}$$

$$4K \equiv -4 \pmod{156} \quad \text{gcd}(4, 156) = 4 \Rightarrow 4 \text{ soluzioni}$$

$$K \equiv -1 \pmod{39}$$

$$\Rightarrow K_i = -1, 38, 77, 116 \pmod{156}$$

$$\Rightarrow K = 77$$

Da i dati pubblici:

$$\Gamma \equiv \alpha^K \pmod{p}$$

$$6^{77} \equiv 26 \pmod{157}$$

$$32 \cdot 77 \equiv 20 - a \cdot 26 \pmod{156}$$

$$26a \equiv 52 \pmod{156} \quad \text{gcd}(26, 156) = 26 \Rightarrow 26 \text{ soluzioni}$$

$$a_0 \equiv 2 \pmod{6}$$

$$a_i \equiv 2, 8, 14, 20, 26, 32, \dots$$

$$\Rightarrow a = 32$$

Da i dati pubblici:

$$B \equiv \alpha^a \pmod{p}$$

$$6^{32} \equiv 37 \pmod{157}$$

Sicurezza delle Reti

Prof. Stefano Bregni

V Appello d'Esame 2017-18 – 13 febbraio 2019

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 $p = 107$, $\alpha = 6$, $\beta = \alpha^a \pmod{p}$, tenendo segreto l'esponente $a = 50$.

- Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 6$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{9, 10\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β .
- Alice estrae il numero casuale segreto (nonce) $k = 25$ e spedisce il messaggio $P_1 = 100$. Calcolare il messaggio cifrato $C_1 = (r_1, t_1)$.
- 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 $C_2 = (r_2, t_2) = (27, 97)$, $C_3 = (r_3, t_3) = (27, 95)$, $C_4 = (r_4, t_4) = (27, 91)$ e, per altra via, viene a sapere che $P_2 = 50$. Calcolare P_3 e P_4 .

a) p primo $1 < a < p-2$ $p-1 = 106 = 2 \cdot 53$ Test α elem. prim. di \mathbb{Z}_p^* : $\alpha^{\frac{p-1}{q_i}} \neq 1 \pmod{p}$

$$\left. \begin{array}{l} 6^{53} \equiv 106 \pmod{107} \\ 6^2 \equiv 36 \pmod{107} \end{array} \right\} \Rightarrow \begin{array}{l} \alpha = 6 \\ \text{OK} \end{array} \quad (\alpha = 9, 10 \text{ No})$$

$$\beta = \alpha^a \pmod{p} = 6^{50} \pmod{107} = 53$$

b) $r_1 = \alpha^k \pmod{p} = 6^{25} \pmod{107} = 38$
 $t_1 = \beta^k P \pmod{p} = 53^{25} \cdot 100 = 101$

$$\Rightarrow C_1 = (38, 101)$$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod{p}$ $t_2^{-1} \equiv 97^{-1} \equiv 32 \pmod{107}$

$$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod{p} \equiv 50 \cdot 95 \cdot 32 \equiv 60 \pmod{107}$$

$$P_4 \equiv P_2 \frac{t_4}{t_2} \pmod{p} \equiv 50 \cdot 91 \cdot 32 \equiv 80 \pmod{107}$$

($k=100$)

Sicurezza delle Reti

Prof. Stefano Bregni

V Appello d'Esame 2017-18 – 14 febbraio 2019

Cognome e nome:

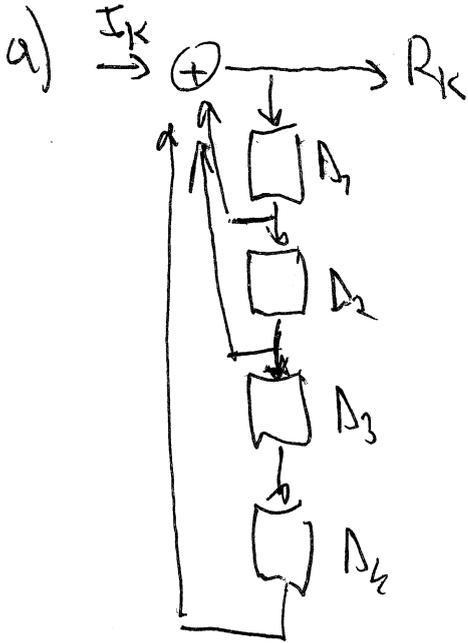
(stampatello)
(firma leggibile)

Matricola:

Domanda 3

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

- a) Si disegni lo schema di uno *scrambler autosincronizzante* avente polinomio caratteristico $P(x) = 1+x+x^2+x^4$, alimentato con tutti "0" e utilizzato come generatore di sequenza PRBS. Si indichino la sequenza binaria in ingresso con $\{I_k\} \equiv \{0\}$ e la sequenza binaria in uscita con $\{R_k\}$.
- b) Si inizializzino gli elementi di ritardo D_i ($i = 1, 2, 3, 4$) con $\{1, 1, 0, 0\}$ al passo iniziale $k = 0$. Ricavare la sequenza PRBS $\{R_k\}$ generata all'uscita, evidenziando la sua periodicit . Qual   il periodo P della sequenza?
- c) Verificare se il polinomio $P(x)$   irriducibile. Se lo fosse, quali sarebbero i valori possibili di P ?



k	I_k	D_{1k}	D_{2k}	D_{3k}	D_{4k}	R_k
0	0	1	1	0	0	0
1	0	0	1	1	0	1
2	0	1	0	1	1	0
3	0	0	1	0	1	0
4	0	0	0	1	0	0
5	0	0	0	0	1	1
6	0	1	0	0	0	1
7	0	1	1	0	0	0

$P = 7$

d) $P(x) = 1 + x + x^2 + x^4$
 Divisibile per x ? No
 Divisibile per $x+1$? Si

$$\begin{array}{r}
 x^4 + x^3 + x^2 + x + 1 \\
 \underline{x^4 + x^3} \\
 x^2 + x + 1 \\
 \underline{x^2 + x} \\
 1 \\
 \underline{x+1} \\
 0
 \end{array}
 \quad \Bigg| \quad
 \begin{array}{r}
 x+1 \\
 \hline
 x^3 + x^2 + 1
 \end{array}$$

$\Rightarrow P(x)$ irriducibile
 $P(x) = (x+1)(x^3 + x^2 + 1)$

Se $P(x)$ irriducibile, $P \setminus 15 \quad P \in \{1, 3, 5, 15\}$

Sicurezza delle Reti

Prof. Stefano Bregni

V Appello d'Esame 2017-18 – 14 febbraio 2019

Cognome e nome:

(stampatello)
(firma leggibile)

Matricola:

Domanda 4

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

Bob adotta il sistema di cifratura a chiave pubblica RSA. Pubblica il modulo $n = 5141$ e due esponenti di cifratura $e_1 = 1521$, $e_2 = 1523$.

- 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 .
- Oscar vuole firmare messaggi impersonando Bob sulla base dei dati pubblici. Calcolare quindi la firma di Bob $A(m)$ per il messaggio di Oscar $m = 7$ utilizzando il valore corretto dell'esponente.

a) $n = 5141 = 53 \cdot 97$ (per tentativi)

$$\varphi(n) = 52 \cdot 96 = 4992 = 2^7 \cdot 3 \cdot 13$$

$$\varphi(\varphi(n)) = 1536$$

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

$$\text{MCD}(1521, 4992) = 39$$

$$\text{MCD}(1523, 4992) = 1$$

$$\left. \begin{array}{l} \text{MCD}(1521, 4992) = 39 \\ \text{MCD}(1523, 4992) = 1 \end{array} \right\} \Rightarrow e = 1523$$

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

con l'Euclide Esteso: $d \equiv 59 \pmod{4992}$

$$A = m^d \pmod{n} = 7^{59} \pmod{5141} = 506$$

Cognome e nome:*(stamatello)**(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) Descrivere un attacco a scelta nello *Schema di Lamport* per l'autenticazione di un host Alice da parte di un server Bob. *(3 punti)*

-
- 2) In IPsec, cos'è una *IP Security Policy*? Qual è la sua funzione principale? A cosa si applica? *(2 punti)*

3) Descrivere sommariamente il processo di autenticazione e cifratura di un messaggio PGP. (3 punti)

4) Nella suite di protocolli *Transport Level Security (TLS)*, quali funzioni svolge *Handshake Protocol*? In particolare, specificare anche quante chiavi crea e per quali scopi. (3 punti)

5) Trovare i fattori primi di $n = 13843$ attraverso l'Algoritmo di Fattorizzazione $p-1$ di Pollard con base $a = 2$. (3 punti)

$$b_1 \equiv 2 \pmod{13843}$$

$$b_2 \equiv 2^2 \equiv 4$$

$$b_3 \equiv 4^3 \equiv 64$$

$$b_4 \equiv 64^4 \equiv 13343$$

$$b_5 \equiv 13343^5 \equiv 8892$$

$$b_6 \equiv 8892^6 \equiv 6547$$

$$\Rightarrow p = 109$$

$$q = 127$$

$$\text{MCD}(3, n) = 1$$

$$\text{MCD}(63, n) = 1$$

$$\text{MCD}(13342, n) = 1$$

$$\text{MCD}(8891, n) = 1$$

$$\text{MCD}(6547, n) = 109$$