

Sicurezza delle Reti

Prof. Stefano Bregni

III Appello d'Esame 2017-18 – 30 agosto 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 cifratura a chiave pubblica di El Gamal e pubblica $p = 107$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 40$.

- 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 $\alpha = \{4, 5\}$. 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*) $k = 26$ 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 $C_2 = (r_2, t_2) = (18, 19)$, $C_3 = (r_3, t_3) = (18, 14)$, $C_4 = (r_4, t_4) = (18, 28)$ e, per altra via, viene a sapere che $P_2 = 99$. Calcolare P_3 e P_4 .

a) p primo $1 < a < p-2$ $p-1 = 106 = 2 \cdot 53$ Test α ed elem. primitivo
di \mathbb{Z}_p^* : $\alpha^{p-1} \not\equiv 1 \pmod{p}$

$\begin{cases} 3^{53} \equiv 1 \\ \text{No} \end{cases}$ $\begin{cases} 4^{53} \equiv 1 \\ \text{No} \end{cases}$ $\begin{cases} 5^{53} \equiv 106 \pmod{107} \\ 5^2 \equiv 25 \end{cases} \Rightarrow \alpha \equiv 5 \text{ OK}$
($\alpha \equiv 3, 4$ No)

$\beta = \alpha^a \bmod p = 5^{40} \bmod 107 = (19)$

b) $r_1 = \alpha^k \bmod p = 5^{26} \bmod 107 = 99$
 $t_1 = \beta^k P \bmod p = 19^{26} \cdot 100 = 16 \Rightarrow C_1 = (99, 16)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod{p}$ $t_2^{-1} \equiv 19^{-1} \equiv 62 \pmod{107}$

$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod{107} \equiv 99 \cdot 14 \cdot 62 \equiv (11)$

$P_4 \equiv P_2 \frac{t_4}{t_2} \equiv 99 \cdot 28 \cdot 62 \equiv (22)$

($k=3$)

Domanda 2

(svolgere su questo foglio nello spazio assegnato) ⁵ (6 punti)

Alice e Bob adottano un sistema di firma cieca RSA. Alice pubblica il modulo $n = 667$ e l'esponente di cifratura $e = 39$. Bob estrae il numero casuale segreto (nonce) $k = 20$ 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 .

$$a) n = 667 = 23 \cdot 29 \quad \phi(n) = 616 = 2^3 \cdot 7 \cdot 11 \quad \phi[\phi(n)] = 240$$

$$k \perp n \text{ OK} \quad e \perp \phi(n) \text{ OK}$$

$$b) d = e^{-1} \bmod \phi(n) = 39^{239} \bmod 616 = 79 \quad (\text{meglio con Euclide E.})$$

$$B \rightarrow A: t = k^e P \bmod n = 20^{39} \cdot 500 \bmod 667 = (165)$$

$$A \rightarrow B: s = t^d \bmod n = 165^{79} \bmod 667 = (545)$$

$$\text{Bob calcola la firma: } A = s/k \bmod n = 545 \cdot 567 \bmod 667 = (194)$$

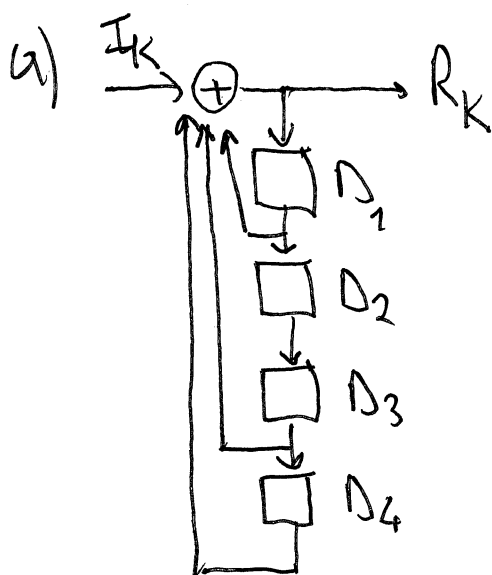
$$\text{dove } k^{-1} \bmod n = 567 \quad (\text{con Euclide E.})$$

$$\text{Verifica: } A = P^d \bmod n = 500^{79} \bmod 667 = 194 \quad (\text{come sopra})$$

Domanda 3

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

- a) Si disegni lo schema di uno *scrambler autosincronizzante* avente polinomio caratteristico $P(x) = 1+x+x^3+x^4$, 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 $\{1, 0, 0, 0\}$ al passo iniziale $k = 0$. Ricavare la sequenza PRBS $\{R_k\}$ generata all'uscita, evidenziando la sua periodicità. Qual è il periodo P della sequenza?
- c) Verificare se il polinomio $P(x)$ è irriducibile. Se lo fosse, quali sarebbero i valori possibili di P ?



b)

| k | I_k | D_{1k} | D_{2k} | D_{3k} | D_{4k} | R_k |
|-----|-------|----------|----------|----------|----------|-------|
| 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| 2 | 0 | 1 | 1 | 1 | 0 | 0 |
| 3 | 0 | 0 | 1 | 1 | 1 | 0 |
| 4 | 0 | 0 | 0 | 1 | 1 | 0 |
| 5 | 0 | 0 | 0 | 0 | 1 | 1 |
| 6 | 0 | 1 | 0 | 0 | 0 | 1 |
| ... | | | | | | |

P=6

c) $P(x) = 1+x+x^3+x^4$
 Divisibile per x ? NO
 Divisibile per $x+1$? SI

$$\begin{array}{r|l}
 x^4 + x^3 + x + 1 & x+1 \\
 \underline{x^4 + x^3} & x^3 + 1 \\
 & x+1 \\
 & \underline{x+1} \\
 & //
 \end{array}$$

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

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

Cognome e nome:

(stampatello)
(firma leggibile)

Matricola:

Domanda 4

(svolgere su questo foglio nello spazio assegnato) (8 punti)

- a) Cos'è una funzione di hash $y = h(x)$?
- b) Definire la proprietà di *unidirezionalità* di una funzione di hash, distinguendola dalla proprietà di *non invertibilità* di una funzione generica. E' possibile definire una funzione di hash invertibile? In che caso? Fare un esempio di funzione di hash non invertibile ma non unidirezionale.
- c) Definire e distinguere le proprietà desiderate per una buona funzione di hash "*debolmente resistente alle collisioni*" e "*fortemente resistente alle collisioni*". Data una funzione candidata $h = h(m)$, quale delle due proprietà vi sarebbe più facile tentare di violare? Perché?
- d) Si consideri una funzione $h_n(x)$ che produce hash di lunghezza $n = 4, 8, 12$ bit. Dati tre hash desiderati $\bar{h}_4, \bar{h}_8, \bar{h}_{16}$, si facciano rispettivamente $H_n = 2^4, 2^8, 2^{12}$ tentativi per ognuno, applicando la funzione a messaggi totalmente casuali di lunghezza qualsiasi. Qual è la probabilità di ottenere lo hash desiderato nei tre casi? Per $n \rightarrow \infty$, la probabilità di successo o insuccesso tende a qualche valore particolare?

$$\begin{aligned} n=4 \quad P &= 1 - \left(1 - \frac{1}{16}\right)^{16} = 0,64392 \\ n=8 \quad P &= 1 - \left(1 - \frac{1}{256}\right)^{256} = 0,63294 \\ n=12 \quad P &= 1 - \left(1 - \frac{1}{4096}\right)^{4096} = 0,63216 \end{aligned}$$

$$\lim_{n \rightarrow \infty} \left(1 - \frac{1}{n}\right)^n = \frac{1}{e}$$

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (12 punti)

(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

- 1) Si consideri un generatore di password composte da 32 caratteri casuali X scelti nell'alfabeto di 16 $\{A, B, \dots, P\}$. (3 punti)
- a) Qual è la quantità di informazione [bit] delle password, se i 16 caratteri sono equiprobabili?
- b) Qual è la quantità di informazione delle password, se invece la probabilità che $X=A$ è 0.50, mentre gli altri 15 caratteri sono equiprobabili?
- c) A cosa tende la quantità di informazione delle password, se invece la probabilità $P(X=A) \rightarrow 1$, mentre le probabilità di presentazione degli altri 15 caratteri tende a 0?

a) $P(X=x_i) = \frac{1}{16}$ $H(X) = - \sum_{i=1}^{16} \frac{1}{16} \log_2 \frac{1}{16} = 4 \text{ bit/carattere (come visto)}$
 $\Rightarrow H(32 \text{ caratteri}) = 128 \text{ bit}$

b) $P(X="A") = 0,50$ $P(X="B") = P(X="C") = \dots = \frac{0,50}{15}$
 $H(X) = - \left[0,50 \log_2 0,50 + \sum_{i=1}^{15} \frac{0,50}{15} \log_2 \frac{0,50}{15} \right] \approx 0,50 + 2,45345 \approx 2,953 \text{ bit/c}$

c) $H(X) = \lim_{\varepsilon \rightarrow 0} \left[-(1-\varepsilon) \log_2 (1-\varepsilon) - \sum_{i=1}^{15} \frac{\varepsilon}{15} \log_2 \frac{\varepsilon}{15} \right] = 0$ $\Rightarrow H(32 \text{ caratteri}) = 94,51 \text{ bit}$

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

(2 punti)

- 3) Nello Schema di Lamport per l'autenticazione di un host Alice da parte di un server Bob, descrivere lo Small-n Attack portato da Oscar a Bob e Alice.

(2 punti)

Cognome e nome:

(stampatello)
(firma leggibile)

Matricola:

- 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 $n = 38191$ attraverso l'Algoritmo di Fattorizzazione $p-1$ di Pollard con base $a = 2$. (2 punti)

$$b_1 \equiv 2 \quad (m \nmid 38191)$$

$$b_2 \equiv 2^2 \equiv 4 \quad (—)$$

$$b_3 \equiv 4^3 \equiv 64 \quad (—)$$

$$b_4 \equiv 64^4 \equiv 11367 \quad (—)$$

$$b_5 \equiv 11367^5 \equiv 20403 \quad (—)$$

$$b_6 \equiv 20403^6 \equiv 28417 \quad (—)$$

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

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

$$\text{mcd}(11366, n) = 1$$

$$\text{mcd}(20403, n) = 1$$

$$\text{mcd}(28417, n) = 181$$

$$\Rightarrow p = 181$$

$$q = n/p = 211$$