Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni IV [illegible] **Appello d'Esame 2012-13 – 25 settembre 2013**

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)

Si consideri l'algoritmo di cifratura di Hill definito come

$$\mathbf{C}_i = \mathbf{P}_i \cdot \mathbf{K} + \mathbf{B} \mod 33$$

dove:

$\mathbf{C}_i$ = coppia i-esima di caratteri cifrati $[C_{1i}\ C_{2i}]$;
$\mathbf{P}_i$ = coppia i-esima di caratteri in chiaro $[P_{1i}\ P_{2i}]$;
$\mathbf{K}$, $\mathbf{B}$ = chiave di cifratura, con

$$\mathbf{K} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \qquad \mathbf{B} = [b_1 \quad b_2].$$

Effettuare un *attacco di tipo testo in chiaro noto*, con

$\mathbf{P} = [1\ 2\ 4\ 1\ 2\ 4]$ $\qquad$ $\mathbf{C} = [1\ 2\ 3\ 3\ 2\ 1]$

e ricavare la chiave $\mathbf{K}$, $\mathbf{B}$.

Cosa c'è di sbagliato in questa cifratura?

$P_1 = (1\ 2)$
$P_2 = (4\ 1)$
$P_3 = (2\ 4)$

$C_1 = (1\ 2)$
$C_2 = (3\ 3)$
$C_3 = (2\ 1)$

$$\begin{cases} C_1 = P_1 K + B \\ C_2 = P_2 K + B \\ C_3 = P_3 K + B \end{cases} \quad \begin{pmatrix} C_1 - C_3 \\ C_2 - C_3 \end{pmatrix} \equiv \begin{pmatrix} P_1 - P_3 \\ P_2 - P_3 \end{pmatrix} K \pmod{33}$$

$$\begin{pmatrix} 1-2 & 2-1 \\ 3-2 & 3-1 \end{pmatrix} \equiv \begin{pmatrix} 1-2 & 2-4 \\ 4-2 & 1-4 \end{pmatrix} K \pmod{33} \Rightarrow \begin{pmatrix} 32 & 1 \\ 1 & 2 \end{pmatrix} \equiv \begin{pmatrix} 32 & 31 \\ 2 & 30 \end{pmatrix} K \pmod{33}$$

$$K = \begin{pmatrix} 32 & 31 \\ 2 & 30 \end{pmatrix}^{-1} \begin{pmatrix} 32 & 1 \\ 1 & 2 \end{pmatrix} \bmod 33$$

$\det \begin{pmatrix} 32 & 31 \\ 2 & 30 \end{pmatrix} \equiv 7 \pmod{33}$ $\quad 7 \nmid 33$ ok $\Rightarrow \exists \left(\begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}^{-1}\right)$

$7^{-1} \bmod 33 = 7^{19} \bmod 33 = 19$

$$\begin{pmatrix} 32 & 31 \\ 2 & 30 \end{pmatrix}^{-1} \equiv \frac{1}{7} \begin{pmatrix} 30 & -31 \\ -2 & 32 \end{pmatrix} \equiv \begin{pmatrix} 9 & 5 \\ 28 & 14 \end{pmatrix} \pmod{33}$$

$$K = \begin{pmatrix} 4 & 5 \\ 28 & 14 \end{pmatrix}\begin{pmatrix} 32 & 7 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 24 & 19 \\ 19 & 23 \end{pmatrix} \qquad \det(K) \equiv 9 \pmod{33}$$

N.B. $\mathrm{mcd}(9,33) = 3 \Rightarrow \nexists\, K^{-1}$

$$B = C_1 - P_1 K \equiv (1\ 2) - (1\ 2)\begin{pmatrix} 24 & 19 \\ 19 & 23 \end{pmatrix} \equiv (1\ 2) - (1\ 32) \equiv (0\ 3) \pmod{33}$$

Verifica:

$$\left.\begin{aligned} C_1 &= P_1 K + B = (1\ 2) \\ C_2 &= P_2 K + B = (3\ 3) \\ C_3 &= P_3 K + B = (2\ 1) \end{aligned}\right\} \text{ok}$$

Mobilità e Sicurezza delle Reti IV
Prof. Stefano Bregni **Appello d'Esame 2012-13 – 25 settembre 2013**

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

Matricola:

Domanda 2

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

Alice e Bob adottano il protocollo di *Diffie-Hellman* per lo scambio della chiave. Alice pubblica $p = 107$ e inizialmente $\alpha = 4$. Alice sceglie $x = 23$ (segreto). Bob sceglie $y = 3$ (segreto).

a) Verificare la correttezza dei dati forniti secondo le ipotesi del protocollo Diffie-Hellman. Se $\alpha = 4$ non risultasse una scelta valida, Alice si corregge e pubblica invece $\alpha = 5$ (anch'esso da verificare). Se anche questa scelta non risultasse valida, Alice e Bob rinunceranno a proseguire (e l'esercizio termina qui).

b) Calcolare i numeri scambiati e la chiave K condivisa.

a) p primo. $1 \leq x \leq p-2$ $1 \leq y \leq p-2$ ok

Test se α elem. primitivo: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $\quad p-1 = 106 = 2 \cdot 53$

$\alpha = 4$ $\begin{cases} 4^{53} \bmod 107 = 1 \\ 4^2 \bmod 107 = 16 \end{cases} \Rightarrow$ NO $\quad \alpha = 5$ $\begin{cases} 5^{53} : \bmod 107 = 106 \\ 5^2 \bmod 107 = 25 \end{cases} \Rightarrow$ ok

b)

A → B $\quad \alpha^x \bmod p = 5^{23} \bmod 107 = 59$

B → A $\quad \alpha^y \bmod p = 5^3 \bmod 107 = 18$

Alice calcola: $K = 18^{23} \bmod 107 = 46$

Bob calcola: $K = 59^3 \bmod 107 = 46$

Domanda 3

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

Alice e Bob adottano un *sistema di firma cieca RSA*. Alice pubblica il modulo $n = 391$ e l'esponente di cifratura $e = 13$. Bob estrae il numero casuale segreto (*nonce*) $k = 12$ e chiede ad Alice di firmare ciecamente il messaggio $P = 32$.

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) $n = 391 = 17 \cdot 23$ $\varphi(n) = 352 = 2^5 \cdot 11$ $\varphi[\varphi(n)] = 160$

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

b) $d = e^{-1} \bmod \varphi(n) = 13^{159} \bmod 352 = ?$ meglio uso Euclide Esteso

$352 = 27 \cdot 13 + 1$ $x_0 = 0$ $x_2 = -27 = 325$ → $d = 325$

$13 = 13 \cdot 1 + 0$ $x_1 = 1$

Bob → Alice: $t = k^e P \bmod n = 12^{13} \cdot 32 \bmod 391 = 261$

Alice → Bob: $s = t^d \bmod n = 261^{325} \bmod 391 = 381$ (slide)

Bob calcola la firma: $A = s/k \bmod n = 381 \cdot 163 \bmod 391 = 325$

$k^{-1} \bmod n = 12^{351} \bmod 391 = ?$ meglio uso Euclide Esteso

$341 = 32 \cdot 12 + 7$ $x_0 = 0$ $x_1 = 1$

$12 = 1 \cdot 7 + 5$ $x_2 = 359$

$7 = 1 \cdot 5 + 2$ $x_3 = 33$

$5 = 2 \cdot 2 + 1$ $x_4 = 326$

$2 = 2 \cdot 1 + 0$ $x_5 = 163$ → $k^{-1} = 163$

Verifica: $P^d \bmod n = 32^{325} \bmod 391 = 325 = A$ calcolato come sopra.

Mobilità e Sicurezza delle Reti IV

Prof. Stefano Bregni Appello d'Esame 2012-13 – 25 settembre 2013

Cognome e nome: *(stampatello)*

Matricola: *(firma leggibile)*

Domanda 4

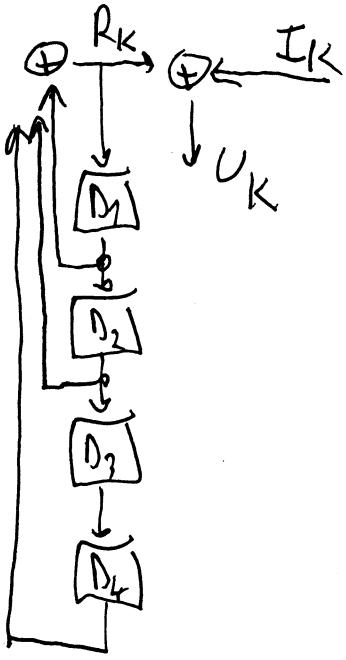
(svolgere su questo foglio nello spazio assegnato) (6 punti)

a) Si disegni lo schema di uno *scrambler additivo* avente polinomio caratteristico $P(x) = 1+x+x^2+x^4$. Si indichi la sequenza binaria in ingresso con $\{I_k\}$, la sequenza binaria in uscita con $\{U_k\}$, la sequenza binaria pseudocasuale generata dallo scrambler con $\{R_k\}$.

b) Si inizializzi lo scrambler con "1" negli elementi di ritardo D_1 e D_2 e con "0" in D_3 e D_4. Lo si alimenti con una sequenza dati composta da tutti "1" in ingresso. Ricavare la sequenza restituita all'uscita $\{U_k\}$, evidenziando la sua periodicità. Qual è il periodo P della sequenza?

c) Verificare se il polinomio $P(x)$ è irriducibile.

a)



b)

Pos. k	I_k	D_{1k}	D_{2k}	D_{3k}	D_{4k}	R_k	U_k	
0	1	1	1	0	0	0	1	
1	1	0	1	1	0	1	0	
2	1	1	0	1	1	0	1	
3	1	0	1	0	1	0	1	
4	1	0	0	1	0	0	1	
5	1	0	0	0	1	1	0	
6	1	1	0	0	0	1	0	
7	1	1	1	0	0	0	1	$P=7$
8								
9								
10								

c) Diviso per X

→ NO

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

$x^3 + x + 1$

$x^2 + x + 1$

x^2

$x + 1$

1 → non è divisibile

Divisibile per $x+1$

$\rightarrow \leq 1$

$$x^4+x^2+x+1 \;\big|\; x+1$$

$$x^4+x^3 \qquad\qquad x^3+x^2+1$$

$$x^3+x^2+x+1$$

$$x^3+x^2$$

$$x+1$$

$$x+1$$

$$0 \;\big|\; \rightarrow \text{divisibile}$$

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

$\Rightarrow P(x)$ non è irriducibile

Mobilità e Sicurezza delle Reti IV
Prof. Stefano Bregni **Appello d'Esame 2012-13 – 25 settembre 2013**

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) Esprimere il *Problema Computazionale di Diffie-Hellman*. Saper risolvere il problema del logaritmo discreto è condizione necessaria, condizione sufficiente, o condizione necessaria e sufficiente per la risoluzione del Problema Computazionale di Diffie-Hellman? *(3 punti)*

2) Esprimere il *Problema di Decisione di Diffie-Hellman*. Sapere risolvere il Problema Computazionale di Diffie-Hellman permette di risolvere il Problema di Decisione di Diffie-Hellman? Sapere risolvere il Problema di Decisione di Diffie-Hellman permette di risolvere il Problema Computazionale di Diffie-Hellman? *(2 punti)*

3) Definire la proprietà di *unidirezionalità* di una funzione di hash. *(2 punti)*

4) In un *firewall*, spiegare in cosa consistono e per cosa si differenziano *Access Control List statiche* e *dinamiche*. Presentare i casi di ACL dinamiche per protocolli con e senza connessione. *(3 punti)*

5) Presentare l'*attacco dell'intruso* al protocollo di scambio delle chiavi di Diffie-Hellman. Descrivere una modifica del protocollo di Diffie-Hellman che permette di evitare questo attacco. *(3 punti)*