Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **IV Appello d'Esame 2013-14 – 18 luglio 2014**

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)

Alice e Bob adottano un *sistema di firma cieca RSA*. Alice pubblica il modulo $n = 319$ e l'esponente di cifratura $e = 17$. Bob estrae il numero casuale segreto (*nonce*) $k = 25$ e chiede ad Alice di firmare ciecamente il messaggio $P = 299$.

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) $n = 319 = 11 \cdot 29$ $\quad \varphi(n) = 280 = 2^3 \cdot 5 \cdot 7$ $\quad \varphi[\varphi(n)] = 96$

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

b) $d = e^{-1} \bmod \varphi(n) = 17^{95} \bmod 280 = 33$ oppure Euclide Esteso (A)

Bob → Alice: $t = k^e P \bmod n = 25^{17} \cdot 299 \bmod 319 = 62$

Alice → Bob: $s = t^d \bmod n = 62^{33} \bmod 319 = 299$

Bob calcola la firma: $A = s/k \bmod n = 299 \cdot 26^9 \bmod 319 = 63$

dove $k^{-1} \bmod n = 25^{279} \bmod 319$ → meglio mano Euclide Esteso (B)

$k^{-1} \equiv 26^9 \pmod{319}$

Verifica: $A = P^d \bmod n = 299^{33} \bmod 319 = 63 = A$ calcolato come sopra

(A)

$280 = 16 \cdot 17 + 8$ $\quad x_0 = 0 \quad x_1 = 1$

$17 = 2 \cdot 8 + 1$ $\quad x_2 = -16$

$8 = 8 \cdot 1 + 0$ $\quad x_3 = 33$

(B)

$319 = 12 \cdot 25 + 19$ $\quad x_0 = 0 \quad x_1 = 1$

$25 = 1 \cdot 19 + 6$ $\quad x_2 = -1$

$19 = 3 \cdot 6 + 1$ $\quad x_3 = 13$

$6 = 6 \cdot 1 + 0$ $\quad x_4 = 268$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2013-14 – 18 luglio 2014**

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 $p = 163$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 128$.

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 $\alpha = 4$, oppure ancora $\alpha = 5$ (da verificare). Se anche queste scelte non risultassero valide, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 18$ e spedisce il messaggio $P = 120$. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob, per un errore di trasmissione, riceve $C' = (r', t') = (11, 22)$. Calcolare il messaggio decifrato da Bob P'.

a) p primo $1 < a \leq p-2$ Tst se α elem. prim. di $\mathbb{Z}_p^*$: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$

$3^{81} \equiv 162$
$3^{54} \equiv 58$
$\Rightarrow \alpha = 3$ OK

$\beta = \alpha^a \bmod p = 3^{128} \bmod 163 = 119$ (S&R)

b) $r = \alpha^k \bmod p = 3^{18} \bmod 163 = 133$

$t = \beta^k P \bmod p = 119^{18} \cdot 120 \bmod 163 = 94$

$\rightarrow C = (133, 94)$

c) $C' = (11, 22)$

$P' = t' \cdot r'^{-a} \bmod p = 22 \cdot 11^{34} \bmod 163 = 134$

Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **IV Appello d'Esame 2013-14 – 18 luglio 2014**

Cognome e nome: *(stampatello)*

(firma leggibile)

Matricola:

Domanda 3

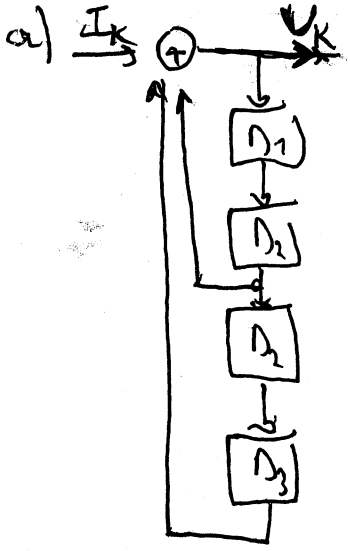
(svolgere su questo foglio nello spazio assegnato) **(5 punti)**

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

b) Si inizializzi lo scrambler con "1" nell'elemento di ritardo D_1 e con "0" in D_2, 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)



$P(x) = 1+x^2+x^4$

b)

Pos. K	I_k	D_{1k}	D_{2k}	D_{3k}	D_{4k}	U_k
0	1	1	0	0	0	1
1	1	1	1	0	0	0
2	1	0	1	1	0	0
3	1	0	0	1	1	0
4	1	0	0	0	1	0
5	1	0	0	0	0	1
6	1	1	0	0	0	1
7	1					

$P = 6$

c) Diviso per X

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

$\Rightarrow$ non è divisibile

Divido per $x+1$

$$\begin{array}{l|l} x^4+x^2+1 & x+1 \\ \hline x^4+x^3 & x^3+x^2 \\ \hline x^3+x^2+1 & \\ x^3+x^2 & \\ \hline 1 & \end{array}$$

$\Rightarrow$ non è divisibile

Divido per x^2+x+1

$$\begin{array}{l|l} x^4+x^2+1 & x^2+x+1 \\ \hline x^4+x^3+x & x^2+x+1 \\ \hline x^3+x+1 & \\ x^3+x^2+x & \\ \hline x^2+x+1 & \\ x^2+x+1 & \\ \hline \emptyset & \end{array}$$

$\Rightarrow$ divisibile

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

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2013-14 – 18 luglio 2014**

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

Matricola:

Domanda 4
(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).

a) Calcolare il prodotto degli elementi E32 × E96 in GF(2^8) eseguendo tutte le operazioni sulle loro rappresentazioni binarie.

E32 = 00100000 $\quad$ M = 100011011

E96 = 01100000

X_0 = E32 = 00100000

X_1 = (00100000) · (00000010) = 01000000

X_2 = (01000000) · (") = 10000000

X_3 = (10000000) · (") = 100000000

100011011

00011011

X_4 = (00011011) · (") = 00110110

X_5 = (00110110) · (") = 01101100

X_6 = (01101100) · (") = 11011000

E32 · E96 = $X_5 + X_6$ = 01101100

11011000

10110100 = E1h0

b) Calcolare $E32^2 = E32 \times E32$ in GF(2^8).

$(E32)^2 = X_5 = 01101100 = E10\beta$

c) Calcolare $E32 \times E4 + E128$ in GF(2^8).

$E32 \times E4 = X_2 = 10000000$

$$\begin{array}{r} X_2 + E128 = \quad 10000000 \\ \quad\quad\quad\quad\quad 10000000 \\ \hline \quad\quad\quad\quad\quad 00000000 \end{array} = E\phi$$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni **IV Appello d'Esame 2013-14 – 18 luglio 2014**

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 $x^2 \equiv 5 \pmod{239}$ ha soluzione? Se la risposta è sì, calcolarne le radici, altrimenti risolvere $x^2 \equiv -5 \pmod{239}$. *(2 punti)*

239 primo → l'eq. ha soluzione se $5^{\frac{239-1}{2}} \equiv 1 \pmod{239}$

$5^{119} \bmod 239 = 1 \Rightarrow$ sì

$239 \equiv 3 \pmod 4 \Rightarrow X = \pm 5^{\frac{239+1}{4}} \bmod 239 = \pm 5^{60} \bmod 239 = \pm 31$

$\Rightarrow X_{1,2} \equiv 31, 208 \pmod{239}$

2) 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)*

3) 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)*

4) Si illustri come i protocolli di distribuzione della chiave simmetrica con autenticazione della TA possono evitare i *replay attack*, facendo anche due esempi. *(3 punti)*

5) Si consideri il meccanismo di memorizzazione cifrata (tramite una funzione unidirezionale $f(x)$) delle password in un file pubblico per il controllo dell'accesso a un sistema. Si descriva in cosa consiste un *attacco del vocabolario*, il meccanismo del *salt* e come il suo utilizzo contrasta questi attacchi. *(4 punti)*