Sicurezza delle Reti

Prof. Stefano Bregni — **IV Appello d'Esame 2020-21 – 17 gennaio 2022**

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 $p = 113$, $\alpha = 5$, $\beta = \alpha^a \bmod p = 93$, tenendo segreto l'esponente a ($1 < a \leq p\text{-}2$).

Bob estrae il numero casuale segreto k (*nonce*) con MCD(k, p-1) = 1. Usando sempre questo stesso valore di k, Bob calcola le seguenti firme A_1 e A_2 per i rispettivi messaggi P_1 e P_2.

$A_1 = (r_1, s_1) = (21, 35)$ $\quad P_1 = 14$
$A_2 = (r_2, s_2) = (21, 47)$ $\quad P_2 = 18$

Oscar intercetta i due messaggi firmati. Sulla base di essi e delle informazioni pubbliche, calcolare k e a (*attacco del nonce ripetuto*).

$s \equiv k^{-1}(P - ar) \pmod{(p-1)} \rightarrow sk \equiv P - ar \pmod{(p-1)}$

$$\begin{cases} 35k \equiv 14 - 21a \pmod{112} \\ 47k \equiv 18 - 21a \pmod{112} \end{cases}$$

$12k \equiv 4 \pmod{112}$ $\quad MCD(12, 112) = 4 \Rightarrow$ 4 soluzioni

$3k \equiv 1 \pmod{28}$ $\quad 3^{-1} \equiv 19 \pmod{28}$

$k_0 \equiv 19 \pmod{28}$

$k_i \equiv 19, 47, 75, 103 \pmod{112}$

$\Rightarrow \boxed{k \equiv 19}$

Dai dati pubblici:
$r \equiv \alpha^k \pmod{p}$
$5^{19} \equiv 21 \pmod{113}$

$35 \cdot 19 \equiv 14 - 21a \pmod{112}$

$21a \equiv 21 \pmod{112}$ $\quad MCD(21, 112) = 7 \Rightarrow$ 7 soluzioni

$3a \equiv 3 \pmod{16}$ $\quad 3^{-1} \equiv 11 \pmod{16}$

$a_0 \equiv 3 \cdot 11 \equiv 1 \pmod{16}$

$a_i \equiv 1, 17, \boxed{33}, 49, 65, 81, 97, \pmod{112} \Rightarrow \boxed{a \equiv 33}$

Dai dati pubbl.
$\beta \equiv \alpha^a \pmod{p}$

Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2020-21 – 17 gennaio 2022**

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (5 punti)

Bob adotta il *sistema di cifratura a chiave pubblica RSA*. Pubblica il modulo $n = 20413$ e un esponente di cifratura scelto tra $e_1 = 37$, $e_2 = 497$, $e_3 = 498$.

a) Fattorizzare n con il metodo di Fermat. Verificare la correttezza dei dati forniti in base alle ipotesi del metodo RSA. Scegliere il valore corretto tra i tre esponenti e_1 , e_2 , e_3.

b) Alice trasmette a Bob il messaggio cifrato $C = 9$, calcolato utilizzando il valore corretto dell'esponente e. Decifrarlo e calcolare il corrispondente messaggio in chiaro P.

a) $n = 20413 = 137 \cdot 149$

$\varphi(n) = 136 \cdot 148 = 20128 = 2^5 \cdot 17 \cdot 37$

$\varphi[\varphi(n)] = 9216$

$\left.\begin{array}{l} MCD(37, 20128) = 37 \\ MCD(497, 20128) = 1 \\ MCD(498, 20128) = 2 \end{array}\right\} \Rightarrow e = 497 \quad (e \perp \varphi(n))$

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

Con Euclide Esteso: $d \equiv 81 \pmod{20128}$

$P = C^d \bmod n = 9^{81} \bmod 20413 = 9903$

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

Matricola:

Domanda 3

(svolgere su questo foglio nello spazio assegnato) (7 punti)

a) Una funzione di hash $h = h(m)$ può essere *invertibile*? Che differenza c'è tra la proprietà di *unidirezionalità* definita per una funzione generica e quella definita per una funzione di hash?

b) Vi viene proposta una funzione di hash $h = h(m)$ asserendo che è resistente alle collisioni. Desiderate provare che non è vero. Per cominciare, proverete a dimostrare che non è fortemente resistente, o debolmente resistente? Facendo cosa? (o tentando di fare cosa?)

c) Una tabella raccoglie i valori di *hash*, di lunghezza $L = 20$ bit, calcolati su $N = 10.000.000$ di file MP3 diversi.

- Qual è la probabilità che almeno due file abbiano lo stesso hash in tabella?

$$P \cong 1 - e^{-10^{14}/(2 \cdot 2^{20})} = 1$$

- Quanto vale questa probabilità, se i file sono solo $N = 2000$?

$$P \cong 1 - e^{-\frac{2000^2}{2 \cdot 2^{20}}} \cong 1 - e^{-1,91} \cong 0,85$$

- Quale dovrebbe essere la lunghezza minima degli *hash*, perché detta probabilità sia <50% ancora su 10.000.000 di file diversi?

$$e^{-\frac{10^{14}}{2M}} > \frac{1}{2} \qquad \frac{10^{14}}{2M} < \ln 2 \qquad M > \frac{10^{14}}{2 \ln 2} = 7,2 \cdot 10^{13}$$

$\Rightarrow$ 46 bit

Domanda 4

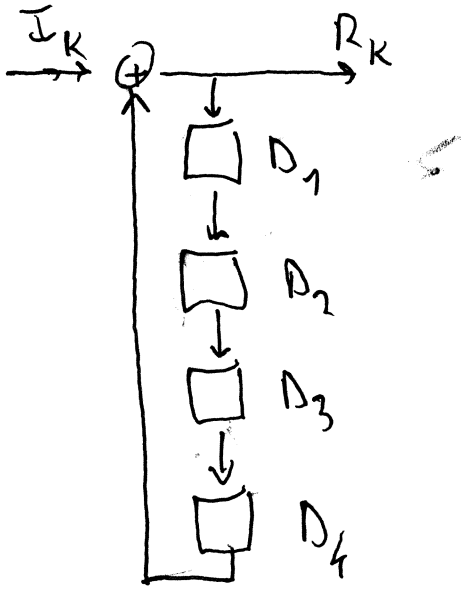
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Si disegni lo schema di un generatore di sequenza PRBS basato su registro a scorrimento LFSR, realizzato come *scrambler autosincronizzante* con polinomio caratteristico $P(x) = 1+x^4$ alimentato con tutti "1". 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 $\{0, 0, 1, 1\}$ 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) Scomporre il polinomio $P(x)$ in fattori irriducibili, se $P(x)$ è riducibile. Perché il periodo P della sequenza $\{R_k\}$ non è un sottomultiplo di 15?

a)



b)

k	I_k	D_{1k}	D_{2k}	D_{3k}	D_{4k}	R_k
0	1	0	0	1	1	0
1	1	0	0	0	1	0
2	1	0	0	0	0	1
3	1	1	0	0	0	1
4	1	1	1	0	0	1
5	1	1	1	1	0	1
6	1	1	1	1	1	0
7	1	0	1	1	1	0
8	1	0	0	0	1	0
9	1					

$P = 8$

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

Sicurezza delle Reti
Prof. Stefano Bregni **IV Appello d'Esame 2020-21 – 17 gennaio 2022**

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

Matricola:

Domanda 5
(rispondere su questo foglio negli spazi assegnati) (13 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) L'equazione $x^2 \equiv 10 \pmod{79}$ ha soluzione? Se la risposta è sì, calcolarne le radici. L'equazione $x^2 \equiv -10 \equiv 69 \pmod{79}$ ha soluzione? Se la risposta è sì, calcolarne le radici. *(2 punti)*

$p=79$ primo → l'eq. ha soluzione se $10^{39} \equiv 1 \pmod{79}$

$10^{39} \equiv 1 \pmod{79} \Rightarrow$ SI

$79 \equiv 3 \pmod 4 \Rightarrow$ l'eq. $x^2 \equiv 10 \pmod{79}$ ha 2 radici

$x^2 \equiv -10 \pmod{79}$ non ha soluzioni

$x \equiv \pm 10^{20} \equiv \pm 22 \pmod{79}$

$\equiv 22, 57$

2) Cos'è un elemento primitivo dell'insieme $\mathbb{Z}_p^*$? Quanti sono gli elementi di $\mathbb{Z}_{233}$? Quanti sono gli elementi di $\mathbb{Z}_{233}^*$? Quanti sono gli elementi primitivi di $\mathbb{Z}_{233}^*$? *(2 punti)*

233, 232, 112

233 primo

3) Se trovassi un algoritmo per risolvere il *Problema Computazionale di Diffie-Hellman* in modo efficiente, questo mi potrebbe essere di aiuto per risolvere il *Problema del Logaritmo Discreto*? In che modo? *(2 punti)*

4) Se dal mio PC in ufficio mi collego con un web browser all'indirizzo https://www.stefanobregni.org, posso dirmi sicuro che il sito sia proprio quello così denominato e non un altro camuffato, oppure no?
L'admin della mia Azienda può osservare che ho visitato questo sito? Può osservare i titoli delle pagine che visito all'interno del sito? *(2 punti)*

5) Per quale ragione può essere consigliabile utilizzare modalità di concatenazione in un cifrario a blocchi, anche se il vettore di inizializzazione è pubblicato e quindi la chiave della modalità non concatenata non viene estesa? *(2 punti)*

6) Un hacker è entrato in possesso del file di sistema dove sono memorizzate le credenziali degli utenti per l'accesso a un server web. Descrivere la procedura che l'Amministratore deve seguire per ricavare la password dell'utente POTUS, se ritiene che la sua password appartenga a un vocabolario di 1000 parole. Di quanto aumenterebbe il tempo necessario all'hacker, se le password sono salvate nel file con un *salt* di 24 bit? *(3 punti)*