Sicurezza delle Reti

Prof. Stefano Bregni — **I Appello d'Esame 2020-21 – 18 giugno 2021**

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) (8 punti)

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 271$, $\alpha = 6$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 17$.

a) 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 $\alpha = \{6, 7\}$. 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 $P_1 = 50$. 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 $C_2 = (r_2, t_2) = (40, 98)$, $C_3 = (r_3, t_3) = (40, 181)$, $C_4 = (r_4, t_4) = (40, 166)$ e, per altra via, viene a sapere che $P_2 = 50$. Calcolare P_3 e P_4.

d) Calcolare per quale valore di k Alice ha calcolato i messaggi C_2, C_3, C_4 del punto c), applicando l'algoritmo Baby Step Giant Step.

a) p primo $1 < \alpha < p-2$ $p-1 = 270 = 2 \cdot 3^3 \cdot 5$ Trk. α elem. prim. $\mathbb{Z}_p^*$:
$\alpha^{(p-1)/q_i} \not\equiv 1 \pmod p$

$6^{135} \equiv 270$
$6^{90} \equiv 242$
$6^{54} \equiv 10$
$\Rightarrow$ $\alpha = 6$ ($\alpha = 7$ No) OK

$\beta = \alpha^a \bmod p = 6^{17} \bmod 271 = 15$

b) $r_1 = \alpha^k \bmod p = 6^{26} \bmod 271 = 14$

$t_1 = \beta^k P_1 \bmod p = 15^{26} \cdot 50 \bmod 271 = 57$

$\Rightarrow C_1 = (14, 57)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $\quad t_2^{-1} = 98^{-1} \equiv 224 \pmod{271}$

$P_3 \equiv P_2 \frac{t_3}{t} \pmod p \equiv 50 \cdot 181 \cdot 224 \equiv 120 \pmod{271}$

$P_4 \equiv P_2 \frac{t_4^2}{t_2} (\cdots) \equiv 50 \cdot 166 \cdot 224 \equiv 140$

d) $6^k \bmod 271 = 40$ $\Rightarrow$ $k = 92$

Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame 2020-21 – 18 giugno 2021**

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

Matricola:

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

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 109$, $\alpha = 6$, $\beta = \alpha^a \bmod p = 15$, 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.

$A_1 = (r_1, s_1) = (42, 43)$ $\quad P_1 = 11$
$A_2 = (r_2, s_2) = (42, 22)$ $\quad P_2 = 14$

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

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

$\begin{cases} 43k \equiv 11 - a42 \pmod{108} \\ 22k \equiv 14 - a42 \pmod{\text{---}} \end{cases}$

$21k \equiv -3 \equiv 105 \pmod{108}$ $\quad MCD(21, 108) = 3 \Rightarrow$ 3 soluz.

$7k \equiv 35 \pmod{36}$ $\quad 7^{-1} \equiv 31 \pmod{36}$

$k_0 \equiv 5 \pmod{36}$

$k_i \equiv 5, (41), 77 \pmod{108}$

$\Rightarrow \boxed{k = 41}$

Dai dati pubblici:
$r \equiv \alpha^k \bmod p$
$6^{41} \equiv 42 \pmod{109}$

$43 \cdot 41 \equiv 11 - a42 \pmod{108}$

$42a \equiv 84 \pmod{108}$ $\quad MCD(42, 108) = 6 \Rightarrow$ 6 soluz.

$7a \equiv 14 \pmod{18}$ $\quad 7^{-1} \equiv 13 \pmod{18}$

$a_0 \equiv 2 \pmod{18}$

$a_i \equiv 2, (20), 38, 56, 74, 92 \pmod{108}$

$\Rightarrow \boxed{a \equiv 20}$

Dai dati pubblici:
$\beta \equiv \alpha^a \pmod{p}$

Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame 2020-21 – 18 giugno 2021**

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

Matricola:

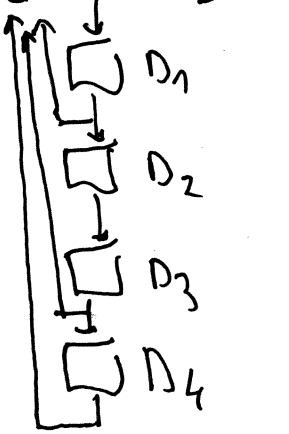
Domanda 3
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Si disegni lo schema di un generatore di sequenza PRBS basato su registro a scorrimento LFSR, realizzato come *scrambler autosincronizzante* con polinomio caratteristico $P(x) = 1+x+x^3+x^4$ alimentato con tutti "0". 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, 1, 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 del periodo P?

a)



b)

k	I_k	D_{1k}	D_{2k}	D_{3k}	D_{4k}	R_k
0	0	0	1	0	0	0
1	0	0	0	1	0	1
2	0	1	0	0	1	0
3	0	0	1	0	0	

$P = 3$

c) $P(x) = x^4+x^3+x+1$

Divisibile per x? NO

per $x+1$? SI

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

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

Se $P(x)$ riducibile: $P < 15$ $\quad P \in \{1, 3, 5, 15\}$

Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame 2020-21 – 18 giugno 2021**

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

Matricola:

Domanda 4
(svolgere su questo foglio nello spazio assegnato) (6 punti)

a) Definire la proprietà di *unidirezionalità* di una funzione di *hash* $h = h(x)$. Specificare per cosa tale definizione si distingue dalla proprietà di *non invertibilità* di una funzione generica $y = y(x)$.

b) Si consideri una ipotetica funzione di *hash* $h(m) = \mathrm{DES}_{K(m)}$("000…"), consistente nella cifratura DES di un blocco di 64 bit "0" con chiave K pari ai primi 56 bit del messaggio m. Si dica se tale funzione $h(m)$ è

- invertibile? (spiegare perché SI o perché NO)

NO

- unidirezionale? (spiegare perché SI o perché NO)

SI

- fortemente resistente alle collisioni? (spiegare perché SI o perché NO; se si risponde NO fornire un esempio di collisione)

NO

c) Un attaccante tenta di ottenere un valore di hash desiderato h_0 calcolando la $h(m)$ del punto b) su variazioni casuali di un messaggio malevolo m. Quanti tentativi sono necessari perché l'attacco abbia successo con probabilità almeno 0.5?

$$P(\text{successo in } n \text{ prove}) = 1 - (1 - 2^{-64})^n$$

$$(1 - 1/2^{64})^n = 1/2 \rightarrow n \cong 2^{63} \cong 9.\ldots \cdot 10^{18}$$

$$n = \frac{\log 1/2}{\log(1 - 2^{-64})} = 1{,}2 \cdot 10^{19}$$

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 2 caratteri, consistenti di 1 consonante e 1 vocale casuali scelti nell'alfabeto Thai, che comprende 44 consonanti e 32 vocali. Qual è la quantità di informazione [bit] delle password, se le consonanti e le vocali sono equiprobabili e scelte indipendentemente una dall'altra? *(2 punti)*

Consonante: $P(X=x_i)=\frac{1}{44}$ $H_1(X)=-\sum_1^{44}\frac{1}{44}\log_2\frac{1}{44}\cong 5{,}46$ bit

Vocale: $P(X=x_i)=\frac{1}{32}$ $H_2(X)=-\sum_1^{32}\frac{1}{32}\log_2\frac{1}{32}=5$ bit

$H=H_1+H_2=10{,}46$ bit

2) Cos'è un elemento primitivo dell'insieme $\mathbb{Z}_p^*$? Quanti sono gli elementi di $\mathbb{Z}_{199}^*$? Quanti sono gli elementi primitivi di $\mathbb{Z}_{199}^*$? *(2 punti)*

198, 120

3) Spiegare perché il *Problema Computazionale di Diffie-Hellman* non può essere più difficile del *Problema del Logaritmo Discreto*, ma non è detto il viceversa. *(2 punti)*

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

Matricola:

4) Un sedicente Stefano Bregni ti contatta, presentando il certificato "SUBJECT: Stefano Bregni" emesso da Verisign. Che procedura segui per sincerarti dell'autenticità del certificato? Se la validazione del certificato va a buon fine, procedi dando per assodato di essere stato contattato da Stefano Bregni, oppure devi fare altro per esserne certo? *(2 punti)*

5) Descrivere lo *Schema di Lamport* per l'autenticazione di un host A da parte di un server B, precisando quali informazioni sono tenute segrete da A e B e quali informazioni sono invece pubbliche o trasferite in chiaro. *(2 punti)*

6) L'Amministratore esamina il file di sistema, dove sono memorizzate le credenziali degli utenti per l'accesso a un server. Se ipotizzo che la password dell'utente BREGNI appartenga a un vocabolario di 50.000 parole, cosa deve fare l'Amministratore per ricavare la sua password dal file? Di quanto aumenta il tempo necessario all'Amministratore, se le password sono salvate nel file con un *salt* di 16 bit? *(2 punti)*