Sicurezza delle Reti

Prof. Stefano Bregni — **V Appello d'Esame 2016-17 – 6 febbraio 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 firma elettronica di El Gamal* e pubblica $p = 163$, $\alpha = 7$, $\beta = \alpha^a \bmod p = 8$, tenendo segreto l'esponente a ($1 < a \leq p\text{-}2$).

a) Bob estrae il numero casuale segreto k (*nonce*) ($k \perp p\text{-}1$). Usando sempre questo stesso valore di k, Bob calcola le seguenti firme A_k per i rispettivi messaggi P_k:

$A_1 = (r_1, s_1) = (19, 28)$ $\quad P_1 = 11$
$A_2 = (r_2, s_2) = (19, 116)$ $\quad P_2 = 13$
$A_3 = (r_3, s_3) = (19, 40)$ $\quad P_3 = 15$

Verificare che le tre firme siano valide.

$\beta^r r^s \equiv \alpha^P \pmod p$

A_1 | $8^{19}\ 19^{28} \equiv 149$; $7^{11} \equiv 149$ $\Rightarrow$ ok

A_2 | $8^{19}\ 19^{116} \equiv 129$; $7^{13} \equiv 129$ $\Rightarrow$ ok

A_3 | $8^{19}\ 19^{40} \equiv 148$; $7^{45} \equiv 127$ $\Rightarrow$ NO

b) Oscar intercetta i tre messaggi (P_k, A_k). Sulla base delle sole firme verificate valide, calcolare k e a (*attacco del nonce ripetuto*).

$P_1 = 11 \quad A_1 = (19, 28)$

$P_2 = 13 \quad A_2 = (19, 116)$

$S \equiv k^{-1}(P - qr) \pmod{(p-1)} \rightarrow sK \equiv P - qr \pmod{(p-1)}$

$$\begin{cases} 28K \equiv 11 - q19 \pmod{162} \\ 116K \equiv 13 - q19 \pmod{162} \end{cases}$$

$88K \equiv 24 \pmod{162} \quad mcd(24, 88) = 2 \Rightarrow$ 2 soluzioni

$44K \equiv 1 \pmod{81} \quad 44^{-1} \equiv 35 \pmod{81}$ (E.E.)

$\Rightarrow K_0 \equiv 35 \pmod{81}$

$K_1 \equiv 35, 116 \pmod{162}$

$\Rightarrow \boxed{K = 35}$

Dai dati pubblici
$r = \alpha^K \bmod p$
$7^{35} \equiv 19$ OK

$28 \cdot 35 \equiv 11 - q19 \pmod{162}$

$q19 \equiv 3 \pmod{162} \quad mcd(19, 162) = 1 \Rightarrow$ 1 soluzione

$19^{-1} \equiv 145 \pmod{162}$

$\Rightarrow \boxed{q \equiv 3 \cdot 145 \equiv 111} \pmod{162}$

Dai dati pubblici:
$\beta \equiv \alpha^q \pmod{p}$
$7^{111} \equiv 8 \pmod{163}$

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (6 punti)

a) Cos'è una funzione di *hash* $y = h(x)$?

b) Definire e distinguere le proprietà di *unidirezionalità* e *non invertibilità* di una funzione di *hash*.

c) Si consideri una funzione $h(x)$ che produce *hash* lunghi 60 bit. Dato un hash h_1, qual è l'ordine di grandezza (cioè: 10 elevato a...?) del numero di messaggi m di lunghezza 100 byte, tali per cui $h(m) = h_1$?

d) Provare che la funzione $h(x) = 2^x \bmod 17$, con x intero, non è *fortemente resistente alle collisioni*, trovando due messaggi qualsiasi m_1 e m_2 tali per cui $h(m_2) = h(m_1)$.

c) $|m| = 2^{800}$ $|h| = 2^{60}$ $\Rightarrow 2^{740} \cong 10^{222}$ mappe m per h_1 $\because h(m) = h_1$

d) Poiché $m_1 \equiv m_2 \pmod{16}$

$m_1 = m_2 + k16$

Domanda 3

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

Bob adotta il *sistema di firma elettronica RSA*. Pubblica il modulo $n = 3827$ e l'esponente di cifratura $e = 1607$.

a) Verificare la correttezza dei dati forniti in base alle ipotesi del metodo RSA.

b) Calcolare la firma di Bob A per il messaggio $m = 33$.

a) $n = 3827 = 43 \cdot 89$ (per tentativi)

$\varphi(n) = 42 \cdot 88 = 3696 = 2^4 \cdot 3 \cdot 7 \cdot 11$ $\quad e \perp \varphi(n)$

$\varphi[\varphi(n)] = 960$

b) $d = e^{-1} \bmod \varphi(n) = e^{\varphi[\varphi(n)]-1} \bmod \varphi(n) = 1607^{959} \bmod 3696$

Meglio usare l'algoritmo di Euclide Esteso:

$3696 = 2 \cdot 1607 + 482$ $\quad x_0 = 0 \quad x_1 = 1$

$1607 = 3 \cdot 482 + 161$ $\quad x_2 = -q_1 x_1 + x_0 = -2$

$482 = 2 \cdot 161 + 160$ $\quad x_3 = -q_2 x_2 + x_1 = 7$

$161 = 1 \cdot 160 + 1$ $\quad x_4 = -q_3 x_3 + x_2 = -16$

$160 = 160 \cdot 1 + 0$ $\quad x_5 = -q_4 x_4 + x_3 = 23 \Rightarrow d = 23$

Verifica: $23 \cdot 1607 \bmod 3696 = 1$

$A = m^d \bmod n = 33^{23} \bmod 3827 = 589$

Domanda 4

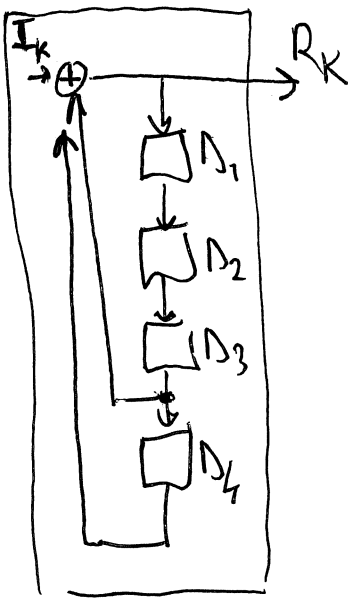
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Si disegni lo schema di uno *scrambler autosincronizzante* avente polinomio caratteristico $P(x) = 1+x^3+x^4$, 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 inizializzi lo scrambler con tutti "1" negli elementi di ritardo D_i. 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.

a)



b)

K	I_K	D_{1K}	D_{2K}	D_{3K}	D_{4K}	R_K
0	0	1	1	1	1	0
1	0	0	1	1	1	0
2	0	0	0	1	1	0
3	0	0	0	0	1	1
4	0	1	0	0	0	0
5	0	0	1	0	0	0
6	0	0	0	1	0	1
7	0	1	0	0	1	1
8	0	1	1	0	0	0
9	0	0	1	1	0	1
10	0	1	0	1	1	0
11	0	0	1	0	1	1
12	0	1	0	1	0	1
13	0	1	1	0	1	1
14	0	1	1	1	0	1
15	0	1	1	1	1	0

P=15

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

Divisibile per x? NO

Divisibile per $(x+1)$? NO

Divisibile per (x^2+x+1)? NO

$x^4 + x^3 + 1 \;|\; x+1$

$x^4 + x^3 \quad\quad x^3$

1

$x^4 + x^3 + 1 \;|\; x^2+x+1$

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

$x^2 + 1$

$x^2 + x + 1$

x

$\Rightarrow P(x) = 1 + x^3 + x^4$ irriducibile

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) Cos'è un *elemento primitivo* $\alpha \in \mathbb{Z}_p^*$? Quanti sono gli elementi primitivi di $\mathbb{Z}_{1019}^*$? *(2 punti)*

$\varphi(1019) = 1018$

2) Si consideri l'equazione $x^2 \equiv a \pmod{n}$, con $n = p \cdot q \cdot r \cdot s$, dove p, q, r, s sono interi primi >2. Quante soluzioni può avere al massimo questa equazione? Dare almeno un cenno di spiegazione. *(2 punti)*

16

3) Perché le firme digitali sono basate sull'applicazione dell'algoritmo di firma all'*hash* del messaggio e non direttamente al messaggio stesso? Applicare l'algoritmo di firma al messaggio stesso migliorerebbe la sicurezza del sistema? *(2 punti)*

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

Matricola:

4) Descrivere brevemente l'attacco *Man-in-the-Middle* al Protocollo di Instaurazione della Chiave di Diffie-Hellman. Come è possibile ostacolarlo? *(2 punti)*

5) Quali sono i differenti ruoli dell'*Autentication Server* e del *Ticket-Granting Server* in Kerberos? *(2 punti)*

6) Fornire un esempio di *chiave monouso* (*One-Time Password*), come può essere generata e come viene utilizzata.*(2 punti)*

7) Descrivere le proprietà di *diffusione* e *confusione*, che secondo Claude Shannon un buon crittosistema dovrebbe avere per ostacolarne l'analisi. *(2 punti)*