

Sicurezza delle Reti

Prof. Stefano Bregni

I Appello d'Esame 2015-16 – 4 luglio 2016

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 $p = 103$, $\alpha = 5$, $\beta = \alpha^a \bmod p = 84$, tenendo segreto l'esponente a ($1 < a \leq p-2$).

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

$$A_1 = (r_1, s_1) = (45, 59) \quad P_1 = 50$$

$$A_2 = (r_2, s_2) = (45, 91) \quad P_2 = 51$$

$$A_3 = (r_3, s_3) = (45, 19) \quad P_3 = 52$$

Verificare che le tre firme siano valide.

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

$$A_1 \left. \begin{array}{l} 84^{45} 45^{59} \equiv 41 \\ 5^{50} \equiv 41 \end{array} \right\} \Rightarrow \text{OK} \quad (\bmod 103)$$

$$A_2 \left. \begin{array}{l} 84^{45} 45^{91} \equiv 58 \\ 5^{51} \equiv 102 \end{array} \right\} \Rightarrow \text{NO}$$

$$A_3 \left. \begin{array}{l} 84^{45} 45^{19} \equiv 98 \\ 5^{52} \equiv 98 \end{array} \right\} \Rightarrow \text{OK}$$

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).

$$P_1 = 50 \quad A_1 = (45, 59)$$

$$P_3 = 52 \quad A_3 = (45, 19)$$

$$S = K^{-1} (P - a r) \pmod{p-1} \rightarrow SK \equiv P - ar \pmod{p-1}$$

$$\begin{cases} 59K \equiv 50 - a \cdot 45 \pmod{102} \\ 19K \equiv 52 - a \cdot 45 \pmod{102} \end{cases}$$

$$40K \equiv 100 \pmod{102} \quad \gcd(40, 102) = 2 \Rightarrow 2 \text{ soluzioni}$$

$$20K \equiv 50 \pmod{51} \quad 20^{-1} \equiv 23 \pmod{51}$$

$$K_0 = 23 \cdot 50 \pmod{51} = 28$$

$$K_1 = K_0 + 51 = 79$$

Da i dati pubblici: $r = \alpha^K \pmod{p}$

$$5^{28} \pmod{103} = 58$$

$$5^{79} \pmod{103} = 45 \Rightarrow K = 79$$

$$19 \cdot 79 \equiv 52 - a \cdot 45 \pmod{102}$$

$$45a \equiv 81 \pmod{102} \quad \gcd(45, 102) = 3 \Rightarrow 3 \text{ soluzioni}$$

$$15a \equiv 27 \pmod{34} \quad 15^{-1} \equiv 25 \pmod{34}$$

$$a_0 = 29$$

$$a_1 = a_0 + 34 = 63$$

$$a_2 = a_0 + 2 \cdot 34 = 97$$

Dei dati pubblici: $\beta = \alpha^a \pmod{p}$

$$5^{29} \pmod{103} = 84 \Rightarrow \textcircled{a=29}$$

Domanda 2

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

Si consideri l'algorithmo di cifratura di Hill definito come

$$C_i = P_i \cdot K + B \pmod{40}$$

dove:

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

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

Effettuare un attacco di tipo testo in chiaro noto, con

$$P = [2 \ 2 \ 3 \ 6 \ 4 \ 3] \quad C = [2 \ 3 \ 3 \ 2 \ 3 \ 1]$$

e ricavare la chiave K, B .

Per i valori ricavati di K e B ,

- esiste un solo C che corrisponde a un certo P ?
- esiste un solo P che corrisponde a un certo C ?

Giustificare le risposte.

$$\begin{cases} C_1 = P_1 K + B \\ C_2 = P_2 K + B \\ C_3 = P_3 K + B \end{cases} \quad \begin{pmatrix} C_1 - C_3 \\ C_2 - C_3 \end{pmatrix} \equiv \begin{pmatrix} P_1 - P_3 \\ P_2 - P_3 \end{pmatrix} K \pmod{40}$$

$$\begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \equiv \underbrace{\begin{pmatrix} -2 & -1 \\ -1 & 3 \end{pmatrix}}_P K \pmod{40}$$

$$\det P = 33 \quad 33^{-1} \equiv 17 \pmod{40} \quad 33 \perp 40$$

$$P^{-1} = 17 \begin{pmatrix} 3 & 1 \\ 1 & 33 \end{pmatrix} \equiv \begin{pmatrix} 11 & 17 \\ 17 & 6 \end{pmatrix} \pmod{40}$$

$$K \equiv \begin{pmatrix} 11 & 17 \\ 17 & 6 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 29 & 39 \\ 23 & 0 \end{pmatrix} \pmod{40}$$

$$\det K = 23 \quad 23 \perp 40 \Rightarrow \exists K^{-1}$$

$$B \equiv C_1 - P_1 K \equiv (2 \ 3) - (2 \ 2) \begin{pmatrix} 29 & 39 \\ 23 & 0 \end{pmatrix} \equiv (2 \ 3) - (24 \ 38) \equiv (18 \ 5)$$

Domanda 3

(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 la funzione SHA-256, che produce hash lunghi 256 bit. Dato un hash h_1 , qual è l'ordine di grandezza (cioè: 10 elevato a...?) del numero di messaggi m di lunghezza 256 byte, tali per cui $h(m) = h_1$?
- d) Provare che la funzione $h(x) = \text{BIP}(2,4)$, con $x \in \mathbb{Z}_n$ per $n = 256$ (x parola di 8 bit), non è *debolmente resistente alle collisioni*, trovando un messaggio m_2 tale per cui $h(m_2) = h(m_1)$ ad esempio con $m_1 = "00000000"$ ($m_i \in \mathbb{Z}_n$).

c) $|m| = 2^{256}$ $|h| = 2^{256} \Rightarrow 2^{1792} \cong 10^{539}$ meno di m
per ogni h_1

d) $m_2 = "11111111"$ (10101010, ...)

Domanda 4

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

- a) Ricavare la sequenza binaria pseudo-casuale $\{x_i\}$ generata dall'algoritmo Blum-Blum-Shab per $p = 19$, $q = 31$, $x = 3$ e determinarne il periodo P .

i	x_i	b_i
0	9	1
1	81	1
2	82	0
3	245	1
4	536	0
5	653	1
6	237	1
7	214	0
8	443	1
9	112	0
10	175	1
11	586	(-3) 0
12	9	1
13		

$P = 12$

$$M = p \cdot q = 19 \cdot 31 = 589$$

$$x_0 \equiv x \pmod{M}$$

$$x_i \equiv x_{i-1}^2 \pmod{M}$$

- b) In base alla teoria, quali sono i valori possibili che può assumere il periodo $P = \pi(x_0)$ del generatore precedente, per valori arbitrari del seme $x_0 = x^2 \in \mathbb{Z}_n$?

Si ricorda che $\pi(x_0)$ divide $\lambda(\lambda(n))$, dove $\lambda(n) := \text{mcm}(\{\phi(p_i^{a_i})\})$ è la Funzione di Carmichael.

$$\lambda(n) = \text{mcm}(18, 30) = 2 \cdot 3^2 \cdot 5 = 90$$

$$18 = 2 \cdot 3^2$$

$$30 = 2 \cdot 3 \cdot 5$$

$$\lambda(\lambda(n)) = \lambda(90) = \text{mcm}(1, 6, 4) = 12$$

$$90 = 2 \cdot 3^2 \cdot 5$$

$$\pi(x_0) \in \{1, 2, 3, 4, 6, 12\}$$

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) Determinare se l'equazione $x^2 \equiv 803 \pmod{839}$ ha soluzione, tramite il calcolo del simbolo di Legendre corrispondente. (2 punti)

$p = 839$ primo

$$\left(\frac{803}{839}\right) \equiv - \left(\frac{839}{803}\right) = - \left(\frac{36}{803}\right) = - \left(\frac{2}{803}\right)^2 \left(\frac{3}{803}\right)^2 = -1$$

\uparrow $m \equiv m \equiv 3 \pmod{4}$ \uparrow $36 \perp 803$ $803 \equiv 3 \pmod{p}$

\Rightarrow non ha soluzione

- 2) Che differenza c'è tra i protocolli di *symmetric key agreement* e *symmetric key distribution*? In cosa consiste un *replay attack* ai protocolli precedenti? Come possono essere impediti i *replay attack*? Fare due esempi. (4 punti)

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

Matricola:

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

-
- 4) Quali sono le tre informazioni fondamentali contenute in un *certificato di identità* in una PKI? Se il certificato è autentico, cosa garantisce? Descrivere la procedura di verifica della sua autenticità. *(2 punti)*

5) Trovare i fattori primi di $n = 20687$ attraverso l'Algoritmo di Fattorizzazione $p-1$ di Pollard con base $a = 2$. (3 punti)

$$b_1 \equiv 2 \pmod{20687}$$

$$b_2 \equiv 2^2 \equiv 4$$

$$b_3 \equiv 4^3 \equiv 64$$

$$b_4 \equiv 64^4 \equiv 59$$

$$b_5 \equiv 59^5 \equiv 2266$$

$$\text{gcd}(3, 20687) = 1$$

$$\text{gcd}(63, 20687) = 1$$

$$\text{gcd}(58, 20687) = 1$$

$$\text{gcd}(2265, 20687) = 157$$

$$\Rightarrow p = 157$$

$$q = n/p = 137$$