

# Sicurezza delle Reti

Prof. Stefano Bregni

I Appello d'Esame 2017-18 – 6 luglio 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  $p = 127$ ,  $\alpha = 2$ ,  $\beta = \alpha^a \bmod p$ , tenendo segreto l'esponente  $a = 65$ .

- Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se  $\alpha = 2$  non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme  $\alpha = \{3, 4, 5\}$ . Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare  $\beta$ .
- Bob estrae il numero casuale segreto (*nonce*)  $k = 19$ . Per questo valore di  $k$ , calcolare la firma di Bob  $A = (r, s)$  del messaggio  $P = 19$ .
- Verificare se anche la firma  $A' = (r', s') = (6, 7)$  è valida per lo stesso messaggio  $P = 19$ . Se è valida, calcolare il valore di  $k$  per cui è stata calcolata da Bob.

$p$  primo  $1 < \alpha < p-1$   $k \in \mathbb{Z}_{p-1}$   $\alpha$  elem. primitivo di  $\mathbb{Z}_p^*$   
Test se  $\alpha$  elem. primitivo:  $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}$   $p-1 = 126 = 2 \cdot 3^2 \cdot 7$   
 $\left. \begin{array}{l} 2^{63} \equiv 1 \\ 2^{42} \equiv 1 \\ 2^{18} \equiv 1 \end{array} \right\} \Rightarrow \alpha = 2 \text{ NO}$   
 $\left. \begin{array}{l} 3^{63} \equiv 126 \\ 3^{42} \equiv 107 \\ 3^{18} \equiv 4 \end{array} \right\} \Rightarrow \alpha = 3 \text{ SI}$   $\alpha = 3$  elem. prim. di  $\mathbb{Z}_{127}^*$

$$\beta = \alpha^a \bmod p = 2^{65} \bmod 127 = 118$$

$$b) r = \alpha^K \bmod p = 3^{19} \bmod 127 = (12)$$

$$s = K^{-1} (P - ar) \bmod (p-1) = 73 (19 - 65 \cdot 12) \bmod 126 = (13)$$

$$K^{-1} \bmod (p-1) = 19^{-1} \bmod 126 = 73 \quad (\text{con E.E.})$$

$$\text{Verifica: } 19 \cdot 73 \equiv 1 \pmod{126} \Rightarrow \boxed{A = (12, 13)}$$

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

$$\left\{ \begin{array}{l} 118^6 \cdot 6^7 \equiv 12 \pmod{127} \\ 3^{19} \equiv 12 \pmod{127} \end{array} \right\} \Rightarrow \begin{array}{l} A' = (6, 7) \\ \text{firmo valido di } P=19 \end{array}$$

$$sK \equiv P - ar \pmod{126}$$

$$7K \equiv 19 - 65 \cdot 6 \pmod{126}$$

$$7K \equiv 7 \pmod{126} \quad \text{MCD}(7, 126) = 7 \rightarrow 7 \text{ soluzioni}$$

$$K_0 \equiv 1 \pmod{18}$$

$$K_i \equiv 1, 19, 37, 55, (73), 91, 109 \pmod{126}$$

$$\text{Dai dati pubblici: } r = \alpha^K \bmod p \quad 6 = 3^K \bmod 127$$

$$\Rightarrow \boxed{K = 73}$$

## Domanda 2

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

Bob adotta il sistema di cifratura a chiave pubblica RSA. Pubblica il modulo  $n = 5251$  e l'esponente di cifratura  $e = 1021$ .

- a) Verificare la correttezza dei dati forniti in base alle ipotesi del metodo RSA.  
 b) Oscar vuole firmare messaggi impersonando Bob sulla base dei dati pubblici. Cosa deve fare? Calcolare la firma di Bob  $A(m)$  per il messaggio  $m = 112$ .

$$a) n = 5251 = 59 \cdot 89 \text{ (primi)} \quad (per\ tentativi)$$

$$\phi(n) = 58 \cdot 88 = 5104 = 2^4 \cdot 7 \cdot 29 \quad e \perp \phi(n)$$

$$\phi[\phi(n)] = 2240$$

$$b) d = e^{-1} \bmod \phi(n) = e^{\phi[\phi(n)]-1} \bmod \phi(n) = 1021^{2239} \bmod 5104$$

Meglio usare l'algoritmo di Euclide Esteso:

$$5104 = 4 \cdot 1021 + 1020$$

$$1021 = 1 \cdot 1020 + 1$$

$$1020 = 1020 \cdot 1 + 0$$

$$x_0 = 0 \quad x_1 = 1$$

$$x_2 = -4 \cdot 1 + 0 = -4$$

$$x_3 = -1(-4) + 1 = 5$$

$$\Rightarrow d = 5$$

$$\text{Verifica: } 5 \cdot 1021 \equiv 1 \pmod{5104}$$

$$A = m^d \bmod n = 112^5 \bmod 5251 = 130$$

Domanda 3

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

Calcolare il logaritmo discreto  $\text{Log}_\alpha(\beta)$  soluzione dell'equazione  $\alpha^x \equiv \beta \pmod{p}$  per  $p = 139$ ,  $\alpha = 3$ ,  $\beta = 40$ , applicando l'algoritmo Baby Step Giant Step.

Prima di tutto, verificare se esiste certamente una soluzione. Per quanti valori di  $\beta \in \mathbb{Z}_p^*$  l'equazione ammette soluzione? per  $\forall \beta$

a) Test  $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p} \Rightarrow \alpha$  radice primitiva di  $\mathbb{Z}_p^*$

$$p-1 = 138 = 2 \cdot 3 \cdot 23 \quad \left. \begin{array}{l} 3^{69} \equiv 138 \\ 3^{46} \equiv 42 \\ 3^6 \equiv 34 \end{array} \right\} \Rightarrow \alpha = 3 \text{ rad. primitiva di } \mathbb{Z}_{139}^*$$

$\Rightarrow \exists$  1 soluzione per  $\forall \beta$

b) Esiste una soluzione per  $\phi(p-1)$  valori di  $\alpha$ , cioè per  $\forall \alpha$  rad. prim.  
 $\phi(p-1) = \phi(138) = 44$

$$c) N = \lfloor p-1 \rfloor + 1 = 12 \quad \alpha^{-1} \equiv 93 \pmod{139} \quad 3^{137}$$

$$\alpha^{-N} \equiv 79 \pmod{139} \quad 93^{12}$$

j	$\alpha^j$	K	$\beta \alpha^{-NK} = 40 \cdot 79^K$
0	1	0	40
1	3	1	102
2	9	2	:
3	27	3	:
4	81	4	:
5	124	5	:
6	34	6	:
7	102	7	:
8	28	8	:
9	84	9	:
10	113	10	:
11	61	11	:

$$\alpha^j \equiv \beta \alpha^{-NK} \pmod{p}$$

$$\alpha^{j+NK} \equiv \beta \pmod{p}$$

$$\Rightarrow x = j + NK = 19$$

$$\text{Verifica: } 3^{19} \equiv 40 \pmod{139}$$

---

**Sicurezza delle Reti**

**Prof. Stefano Bregni**

**I Appello d'Esame 2017-18 – 6 luglio 2018**

**Cognome e nome:**

*(stampatello)*

*(firma leggibile)*

**Matricola:**

---

**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  $p = 23$ ,  $q = 47$ ,  $x = 48$  e determinarne il periodo  $P$ .

$i$	$x_i$	$b_i$
0	142	0
1	706	0
2	95	1
3	377	1
4	518	0
5	236	0
6	565	1
7	330	0
8	800	0
9	48	0
10	142	0
11		

$P = 10$

$$n = p \cdot q = 23 \cdot 47 = 1081$$

$$x_0 \equiv x^2 \pmod{n}$$

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

$$23 \bmod 4 = 3$$

$$47 \bmod 4 = 3$$

$$48 \perp 1081$$

- 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  $\lambda(n) := \text{mcm}(\{\phi(p_i^{q_i})\})$  è la Funzione di Charnichael.

$$\lambda(n) = \text{mcm}(22, 46) = 2 \cdot 11 \cdot 23 = 506$$

$$\lambda[\lambda(n)] = \lambda(506) = \text{mcm}(1, 10, 22) = 2 \cdot 5 \cdot 11 = 110$$

$$\pi(x_0) \in \{1, 2, 5, 10, 11, 22, 55, 110\}$$

$$\boxed{\pi(x_0) \setminus 110}$$

**Domanda 5***(rispondere su questo foglio negli spazi assegnati) (15 punti)**(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).*

- 
- 1) Definire e distinguere le proprietà desiderate per una buona funzione di hash "*debolmente resistente alle collisioni*" e "*fortemente resistente alle collisioni*". Data una funzione candidata  $h = h(m)$ , quale delle due proprietà vi sarebbe più facile tentare di violare? Perché? *(3 punti)*

- 
- 2) Descrivere lo *Schema di Lamport* per l'autenticazione di un host Alice da parte di un server Bob, precisando quali informazioni sono conosciute segretamente da A e B, e quali informazioni sono invece pubbliche o trasferite in chiaro da A o B. Descrivere lo *Small-n Attack* portato da Oscar a Bob e Alice. *(4 punti)*

- 3) Si supponga di avere un sistema di autenticazione di utenti basato su biometria. Il pattern del candidato  $k$  è confrontato con il pattern memorizzato per l'utente  $A$ , misurandone la *distanza*  $d_{kA}$  secondo un'opportuna metrica. Con che criterio si decide la soglia di accettazione  $D$ , per cui il candidato è accettato come  $A$  se  $d_{kA} < D$ ? (2 punti)

- 
- 4) Descrivere in sintesi le principali differenze tra *Transport Mode* e *Tunnel Mode* per l'opzione *Encapsulating Security Payload* (ESP) di IPsec. (3 punti)

- 
- 5) Descrivere in sintesi il principio del protocollo HTTPS. Rispetto al protocollo base HTTP, quali informazioni trasmesse dall'utente che si connette a un server *www* vengono cifrate? Quali protocolli stabiliscono una connessione end-to-end tra i *peer* su *client* e *server*? (percorrere la pila dall'alto al basso) (3 punti)