Sicurezza delle Reti

Prof. Stefano Bregni — **II Appello d'Esame 2020-21 – 6 luglio 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) (6 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 107$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 23$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 3$ 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 β.

b) Bob estrae il numero casuale segreto (*nonce*) $k = 33$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 101$.

c) Verificare se anche la firma $A' = (r', s') = (22, 25)$ è valida da Bob per lo stesso messaggio $P = 101$. Se è valida, calcolare il valore di k per cui è stata calcolata da Bob, scegliendo il metodo più veloce a disposizione.

a) p primo $1 < a < p-2$ $K \perp p-1$ $p-1 = 106 = 2 \cdot 53$

Test se α elem. primitivo: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$

$3^{53} \equiv 106$, $3^2 \equiv 25$ $\Rightarrow$ $\alpha = 3$ (OK) — $\alpha = 4$ NO, $\alpha = 5$ NO

$\beta = \alpha^a \bmod p = 5^{23} \bmod 107 = 59$

b) $r = \alpha^k \bmod p = 5^{33} \bmod 107 = 94$

$s = k^{-1}(P - ar) \bmod (p-1) = 45 \cdot (101 - 23 \cdot 94) \bmod 106 = 5$

$k^{-1} \equiv 33^{-1} \equiv 45 \pmod{106}$

$\Rightarrow A = (94, 5)$

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

$59^{22} \cdot 22^{25} \equiv 73 \pmod{107}$

$5^{101} \equiv 73 \pmod{107}$

$\Rightarrow A' = (22, 25)$ firma valida di $P = 101$

Si può risolvere $5^K \equiv 22 \pmod{107}$

oppure $5K \equiv P - ar \pmod{p-1}$

$25K \equiv 131 - 23 \cdot 22 \pmod{106}$

$25K \equiv 19 \pmod{106}$ $\quad MCD(25, 106) = 1 \rightarrow$ 1 soluzione

$\Rightarrow K \equiv 19 \cdot 17 \equiv 5 \pmod{106}$ $\quad 25^{-1} \equiv 17 \pmod{106}$

$\Rightarrow \boxed{K = 5}$

Sicurezza delle Reti
Prof. Stefano Bregni — **II Appello d'Esame 2020-21 – 6 luglio 2021**

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 $n = 16241$ e un esponente di cifratura scelto tra $e_1 = 1517$, $e_2 = 2705$, $e_3 = 2841$.

a) 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 $C = 31$, calcolato utilizzando il valore corretto dell'esponente e. Decifrarlo e calcolare il corrispondente messaggio in chiaro P.

a) $n = 16241 = 109 \cdot 149$ (primi)

$\varphi(n) = 108 \cdot 148 = 15984 = 2^4 \cdot 3^3 \cdot 37$

$\varphi[\varphi(n)] = 5184$

$\left.\begin{array}{l} MCD(1517, 15984) = 37 \\ MCD(2705, 15984) = 1 \\ MCD(2841, 15984) = 3 \end{array}\right\} \Rightarrow e = 2705 \quad (e \perp \varphi(n))$

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

Con Euclide Esteso: $d \equiv 65 \pmod{15984}$

$P = C^d \bmod n = 31^{65} \bmod 16241 = 2$

Sicurezza delle Reti
Prof. Stefano Bregni — **II Appello d'Esame 2020-21 – 6 luglio 2021**

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

Matricola:

Domanda 3
(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 $p = 19$, $q = 43$, $x = 20$ e determinarne il periodo P.

i	x_i	b_i	
0	400	0	
1	685	1	
2	267	1	
3	210	0	
4	799	1	
5	324	0	
6	400	0	

$P = 6$

$m = p \cdot q = 19 \cdot 43 = 817$

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

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

$19 \bmod 4 = 3$

$43 \bmod 4 = 3$

$20 \perp 817$

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 $\lambda(n)$ è la Funzione di Charmichael, calcolabile come

$$\lambda(n) = \text{mcm}\left(\left\{\lambda\left(p_i^{a_i}\right)\right\}\right) \qquad \lambda\left(p^k\right) = \begin{cases} \frac{1}{2}\varphi\left(p^k\right) & \text{se } p = 2,\ k \geq 3 \\ \varphi\left(p^k\right) & \text{altrimenti} \end{cases}$$

$\lambda(n) = \text{mcm}(18, 42) = 2 \cdot 3^2 \cdot 7 = 126$

$\lambda[\lambda(n)] = \lambda(126) = \text{mcm}(1, 6, 6) = 6$ $\qquad \pi(x_0) \mid 6$

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

Domanda 4
(svolgere su questo foglio nello spazio assegnato) (7 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) Definire la proprietà di *resistenza forte alle collisioni* di una funzione di *hash* $h = h(x)$. Specificare per cosa tale definizione si distingue dalla proprietà di *resistenza debole alle collisioni.*

c) Avete letto che SHA-3 è ritenuta fortemente resistente alle collisioni. Desiderate diventare famosi provando che non è vero. Per cominciare, proverete a dimostrare che non è fortemente resistente, o debolmente resistente? Facendo cosa? (o tentando di fare cosa?) Che metodo pensate di seguire?

d) Avete scelto una funzione di *hash* che restituisce valori di lunghezza $L = 64$ bit. In una tabella, avete memorizzato i valori di *hash* calcolati su un miliardo di file diversi. Qual è la probabilità che almeno due file abbiano lo stesso hash in tabella?

$N = 2^{64} \cong 1.85 \cdot 10^{19}$

$r = 10^9$

$P \cong 1 - e^{-r^2/2N} \cong 1 - e^{-0,0271} \cong 0,02674$

Sicurezza delle Reti
Prof. Stefano Bregni **II Appello d'Esame 2020-21 – 6 luglio 2021**

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) Cos'è un *elemento primitivo* dell'insieme $\mathbb{Z}_p^*$?
Cos'è un *residuo quadratico* dell'insieme $\mathbb{Z}_p^*$?
Si calcolino tutti i residui quadratici dell'insieme $\mathbb{Z}_{11}^*$, partendo dalle potenze dell'elemento primitivo più piccolo di $\mathbb{Z}_{11}^*$. Esaminando i risultati ottenuti, si dica quali sono le radici quadrate di -2 (mod 11). *(3 punti)*

$\alpha = 2$

$2^5 \equiv 10$
$2^2 \equiv 4$ $\rightarrow$ ok
$\pmod{11}$

$2^0 \equiv 1 \pmod{11}$
$2^2 \equiv 4$
$2^4 \equiv 5$
$2^6 \equiv 9 \rightarrow \sqrt{9} \equiv \sqrt{-2} \equiv \pm 2^3 \equiv \pm 8 \equiv \{3, 8\}$
$2^8 \equiv 3$

$\alpha_9 = \{1, 3, 4, 5, 9\}$

2) 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)*

3) 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)*

4) Se utilizzo HTTPS con un browser web, l'Amministratore della rete attraverso cui mi collego a Internet conosce l'indirizzo IP del server a cui mi collego? Conosce i titoli delle pagine che visito? *(2 punti)*

5) Enunciare il *Teorema Cinese del Resto* generalizzato a K congruenze. *(2 punti)*

6) A invia in messaggio a B utilizzando PGP. Con che chiave A cifra il messaggio? Con che chiave A firma il messaggio? A deve trasmettere una chiave a B? Come? *(2 punti)*