Sicurezza delle Reti

Prof. Stefano Bregni **II Appello d'Esame 2022-23 – 20 luglio 2023**

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 cifratura a chiave pubblica di El Gamal* e pubblica $p = 293$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 45$.

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 $\alpha = \{9, 10\}$. 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*) $k = 16$ e spedisce il messaggio $P_1 = 12$. 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 $C_2 = (r_2, t_2) = (111, 4)$, $C_3 = (r_3, t_3) = (111, 40)$, $C_4 = (r_4, t_4) = (111, 77)$ e, per altra via, viene a sapere che $P_2 = 18$. Calcolare P_3 e P_4.

a) p primo $1 < \alpha < p-2$ $\quad p-1 = 292 = 2^2 \cdot 73$

Test se α elem. prim. di $\mathbb{Z}_p^*$: $\alpha^{(p-1)/q_i} \not\equiv 1 \pmod p$

$$\begin{cases} 3^{146} \equiv -1 \\ 3^4 \equiv 81 \end{cases} \Rightarrow \alpha = 3 \text{ OK} \quad (\alpha = 9, 10 \text{ no})$$

$\beta = \alpha^a \bmod p = 3^{45} \bmod 293 = 200$

b) $r_1 = \alpha^k \bmod p = 3^{16} \bmod 293 = 40$

$t_1 = \beta^k P_1 \bmod p = 200^{16} \cdot 12 \bmod 293 = 45 \Rightarrow C_1 = (40, 45)$

c) $\dfrac{t_2}{P_2} \equiv \dfrac{t_3}{P_3} \equiv \dfrac{t_4}{P_4} \equiv \beta^k \pmod p \qquad t_2^{-1} \equiv 4^{-1} \equiv 220 \pmod{293}$

$P_3 \equiv P_2 \dfrac{t_3}{t_2} \pmod p = 18 \cdot 40 \cdot 220 \equiv 180 \pmod{293}$

$P_4 \equiv P_2 \dfrac{t_4}{t_2} \pmod p = 18 \cdot 77 \cdot 220 \equiv 200 \pmod{293}$

(firme calcolate per $k = 15$)

Sicurezza delle Reti
Prof. Stefano Bregni — **II Appello d'Esame 2022-23 – 20 luglio 2023**

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (7 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 101$, $\alpha = 5$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 90$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 5$ 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) Bob estrae il numero casuale segreto (*nonce*) $k = 89$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 30$.

c) Verificare se anche la firma $A' = (r', s') = (28, 90)$ è valida da Bob per lo stesso messaggio $P = 30$

d) Se è valida, calcolare il valore di k per cui è stata calcolata da Bob, scegliendo il metodo più conveniente (non *Baby Step Giant Step*).

a) p primo $1 < a < p-2$ $\quad k \perp p-1$

$p-1 = 100 = 2^2 \cdot 5^2$

Test se α el. prim. di $\mathbb{Z}_p^*$: $\alpha^{(p-1)/q_i} \not\equiv 1 \pmod p$

$$\left.\begin{array}{l} 7^{50} \equiv -1 \\ 7^{20} \equiv 84 \end{array}\right\} \Rightarrow \begin{array}{l} \alpha = 7 \\ \text{OK} \end{array} \quad (\alpha = 5,6 \text{ NO})$$

$\beta = \alpha^a \bmod p = 7^{90} \bmod 101 = 14$

b) $r = \alpha^k \bmod p = 7^{89} \bmod 101 = 2$

$s = k^{-1}(P - ar) \bmod (p-1) = 9(30 - 90 \cdot 2) \bmod 100 = 50$

$k^{-1} \equiv 89^{-1} \equiv 9 \pmod{100}$ $\quad \Rightarrow A = (2, 50)$

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

$$\left.\begin{array}{l} 14^{28} \cdot 28^{90} \equiv 6 \pmod{101} \\ 7^{30} \equiv 6 \pmod{101} \end{array}\right\} \Rightarrow A' = (28, 90) \text{ firma valida di } P = 30$$

d) Invece di risolvere $7^K \equiv 28 \pmod{101}$, meglio:

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

$90K \equiv 30 - 90 \cdot 28 \pmod{100}$

$90K \equiv 10 \pmod{100}$ $MCD(90,100) = 10 \Rightarrow$ 10 soluzioni

$9K \equiv 1 \pmod{10}$ $9^{-1} \equiv 9 \pmod{10}$

$K_0 = 9 \pmod{100}$

$K_i = 9, 19, 29, 39, 49, 59, 69, 79, 89, 99 \pmod{100}$

$\Rightarrow K = 79$

Dai dati pubblici:

$\alpha^K \equiv r \pmod{p}$

$7^K \equiv 28 \pmod{101}$

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

Matricola:

Domanda 3

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

Bob adotta il *sistema di cifratura a chiave pubblica RSA.* Pubblica il modulo $n = 17063$ e un esponente di cifratura scelto tra $e_1 = 1001$, $e_2 = 1003$, $e_3 = 1005$.

a) Fattorizzare n con il metodo di Pollard. 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 $C = 15$, calcolato utilizzando il valore corretto dell'esponente e. Decifrarlo e calcolare il corrispondente messaggio in chiaro P.

a) $n = 17063 = 113 \cdot 151$ (Pollard)

$\varphi(n) = 112 \cdot 150 = 2^5 \cdot 3 \cdot 5^2 \cdot 7 = 16800$

$\varphi[\varphi(n)] = 3840$

$MCD(1001, 16800) = 7$ NO
$MCD(1003, 16800) = 1$ OK
$MCD(1005, 16800) = 5$ NO

$\Rightarrow e = 1003$ $(e \perp \varphi(n))$

Pollard $(a=2)$

$b_1 \equiv 2 \pmod{17063}$

$b_2 \equiv 2^2 \equiv 4$ $(\sim)$ $MCD(3, n) = 1$

$b_3 \equiv 4^3 \equiv 64$ $(\sim)$ $MCD(63, n) = 1$

$b_4 \equiv 64^4 = 4287$ $(\sim)$ $MCD(4286, n) = 1$

$b_5 \equiv 4287^5 \equiv 13138$ $(\sim)$ $MCD(13137, n) =$
$= 151$

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

Con Euclide Esteso:

$d \equiv 67 \pmod{16800}$

$\underline{P} = C^d \bmod n =$

$= 15^{67} \bmod 17063 =$

$= 3827$

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

Matricola:

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

a) Spiegare cosa significa affermare che una <u>*generica funzione*</u> $y = y(x)$ è *invertibile*, ma *unidirezionale*.

b) Spiegare cosa significa affermare che una <u>*funzione di hash*</u> $h = h(x)$, necessariamente *non invertibile*, è *unidirezionale*.

c) Si consideri una ipotetica funzione di *hash* definita come $h(m) = (r \cdot t) \bmod p$, dove (r, t) è la cifratura a chiave pubblica di El Gamal $E_{p,\alpha,\beta,k}(P)$ di $P = 1$ con parametri pubblici p = primo grande e sicuro, $\alpha = 2$, $\beta = 2$, calcolata con il *nonce* $k = m$. Scrivere l'espressione $h(m) = (r \cdot t) \bmod p$.

$r = \alpha^k \bmod p = 2^m \bmod p$

$t = \beta^k P \bmod p = 2^m \bmod p$

$\Rightarrow h(m) = 2^{2m} \bmod p$

Si dica se tale funzione $h(m)$ è

- invertibile? (spiegare perché SI o perché NO)

NO

- unidirezionale? (spiegare perché SI o perché NO)

SI

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

NO $m_2 = m_1 + k\frac{p-1}{2}$

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) Trovare i parametri (*a, b*) del *Cifrario Affine* (mod 26) che cifra "nyarlathotep" in "ryedlejzujqx". *(3 punti)*

Alfabeto	
0	a
1	b
2	c
3	d
4	e
5	f
6	g
7	h
8	i
9	j
10	k
11	l
12	m
13	n
14	o
15	p
16	q
17	r
18	s
19	t
20	u
21	v
22	w
23	x
24	y
25	z

$E_k(x) = ax + b \bmod 26$

"a" → "e" $\quad 4 \equiv a \cdot 0 + b \pmod{26} \quad \Rightarrow b = 4$

"h" → "z" $\quad 25 \equiv a7 + 4 \pmod{26}$

(scelgo "h" perché $7 \perp 26$)

$7a \equiv 21 \pmod{26}$

$a \equiv 21 \cdot 15 \equiv 3 \pmod{26} \quad \Rightarrow a = 3$

2) Un hacker è entrato in possesso del file di sistema dove sono memorizzati gli hash delle password degli utenti per l'accesso a un server. Sappiamo che la funzione di hash $h = h(x)$ utilizzata *non è unidirezionale*. L'hacker sarà in grado di ricavare le password degli utenti? *(2 punti)*

Sicurezza delle Reti
Prof. Stefano Bregni **II Appello d'Esame 2022-23 – 20 luglio 2023**

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

Matricola:

---

3) Dopo laboriose ricerche, su Astalavista hai trovato un certificato emesso da DigiCert a nome SUBJECT: <www.whitehouse.gov>. *(3 punti)*

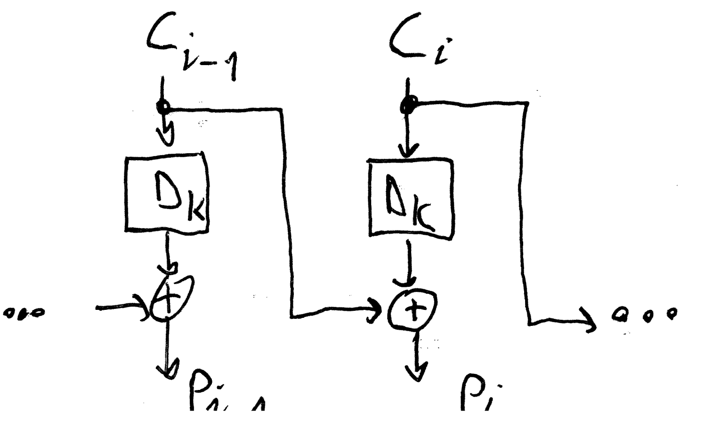
a) Che procedura segui per verificare l'autenticità del certificato?
b) Qual è l'informazione più importante che apprendi dal certificato?
c) Dopo la verifica a), il certificato risulta valido. Tuttavia, la Casa Bianca contattata in proposito dichiara di non avere nulla a che fare con questo certificato. Quale segreto potrebbe avere violato l'impostore che ha creato il certificato?

---

4) Si consideri il protocollo di Diffie-Helman. A cosa serve? Definirne le variabili, i valori scambiati e il risultato finale, specificando quali di questi sono pubblici e quali segreti. *(2 punti)*

---

5) Si consideri un cifrario a blocchi concatenato secondo la modalità *Cipher Block Chaining* (CBC), in cui cifratura e decifratura sono svolte rispettivamente come $C_i = E_K(P_i \oplus C_{i-1})$ e $P_i = C_{i-1} \oplus D_K(C_i)$, C_0 è il vettore di inizializzazione, la dimensione dei blocchi P_i e C_i è 256 bit. Se il flusso cifrato $\{C_i\}$ subisce errori di trasmissione puramente casuali con tasso ε molto piccolo (ossia, gli errori sono rari e isolati), quale sarà il tasso di errore sul flusso decifrato $\{P_i\}$? Per rispondere, disegnare lo schema a blocchi del processo di decifrazione. *(2 punti)*



$\Rightarrow 129\,\varepsilon$