

Sicurezza delle Reti

Prof. Stefano Bregni

II Appello d'Esame 2023-24 – 25 luglio 2024

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) (7 punti)

Bob adotta il sistema di cifratura a chiave pubblica di El Gamal e pubblica $p = 127$, $\alpha = 6$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 40$.

- Si assuma che tutti i dati forniti rispettino le ipotesi del metodo di El Gamal e, in particolare, che α sia un elemento primitivo di \mathbb{Z}_p^* . Calcolare β .
- Alice estrae il numero casuale segreto (nonce) $k = 16$ e spedisce il messaggio $P = 100$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.
- Bob riceve $C' = (r', t') = (105, 69)$. Calcolare il messaggio decifrato da Bob P' .
- Calcolare il valore di k per cui Alice ha calcolato $C' = E[P]$ applicando l'algoritmo BSGS (bastano le prime 7 righe della tabella).

a) p primo $1 < \alpha \leq p-2$ $p-1=126=2 \cdot 3^2 \cdot 7$ Test se α elem. prim. $\in \mathbb{Z}_p^*$
 $\alpha^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$
 $\alpha^{\frac{p-1}{3}} \not\equiv 1 \pmod{p}$
 $\alpha^{\frac{p-1}{7}} \not\equiv 1 \pmod{p}$
 $\left. \begin{array}{l} 6^3 \equiv 126 \\ 6^42 \equiv 127 \\ 6^{18} \equiv 4 \end{array} \right\} \Rightarrow \alpha = 6$
 $\beta = \alpha^a \bmod p = 6^{40} \bmod 127 = 70$

b) $r = \alpha^k \bmod p = 6^{16} \bmod 127 = 30$
 $t = \beta^k P \bmod p = 70^{16} \cdot 100 \bmod 127 = 26 \Rightarrow C = (30, 26)$

c) $P' = t' \cdot r'^{-a} = 69 \cdot 105^{-40} \bmod 127 = 69 \cdot (-22)^{86} = 100$

d) $6^k \bmod 127 = 105 \Rightarrow k = 77$

$$N = [p-1] = 12$$

$$\alpha^{-1} = 6^{-1} \equiv -21 \pmod{127}$$

$$\alpha^{-N} \equiv 94 \pmod{127}$$

$$k \equiv 5 + 12 \cdot 6 \equiv 77 \pmod{126}$$

j	α^j	K	α^{-NK}	$\beta \alpha^{-NK}$
0	1	0	1	70
...
5	29	6	16	29

Domanda 2

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

Bob adotta il sistema di firma elettronica di El Gamal e pubblica $p = 109$, $\alpha = 6$, $\beta = \alpha^a \bmod p = 41$, tenendo segreto l'esponente a ($1 < a \leq p-2$).

Bob estrae il numero casuale segreto k (nonce) con $\text{MCD}(k, p-1) = 1$. Usando sempre questo stesso valore di k , Bob calcola le seguenti firme A_1 e A_2 per i rispettivi messaggi P_1 e P_2 .

$$A_1 = (r_1, s_1) = (69, 59) \quad P_1 = 20$$

$$A_2 = (r_2, s_2) = (69, 87) \quad P_2 = 24$$

Oscar intercetta i due messaggi firmati. Sulla base di essi e delle informazioni pubbliche, calcolare k e a (attacco del nonce ripetuto).

$$s \equiv k^{-1}(P - ar) \pmod{p-1} \rightarrow sk \equiv P - ar \pmod{p-1}$$

$$\begin{cases} 59k \equiv 20 - a \cdot 69 \pmod{108} \\ 87k \equiv 24 - a \cdot 69 \pmod{108} \end{cases}$$

$$28k \equiv 4 \pmod{108} \quad \text{MCD}(28, 108) = 4 \Rightarrow 4 \text{ soluzioni}$$

$$7k \equiv 1 \pmod{27} \quad 7^{-1} \equiv 4 \pmod{27}$$

$$k_0 \equiv 4 \pmod{27} \quad k_i \equiv 4, 31, 58, 85 \pmod{108}$$

$$\Rightarrow \boxed{k = 85}$$

Dai dati pubblici:

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

$$69 = 6^k \bmod 109$$

$$59 \cdot 85 \equiv 20 - a \cdot 69 \pmod{108}$$

$$69a \equiv -27 \pmod{108} \quad \text{MCD}(69, 108) = 3 \Rightarrow 3 \text{ soluzioni}$$

$$23a \equiv -9 \pmod{36} \quad 23^{-1} \equiv 11 \pmod{36}$$

$$a_0 \equiv -9 \cdot 11 \equiv 9 \pmod{36}$$

$$a_i \equiv 9, 45, 81 \pmod{108}$$

$$\Rightarrow \boxed{a = 45}$$

Dai dati pubblici:

$$\beta \equiv \alpha^a \pmod{p}$$

$$41 \equiv 6^a \pmod{109}$$

Domanda 3

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

- a) Ricavare la sequenza binaria pseudo-casuale $\{x_i\}$ generata dall'algoritmo Blum-Blum-Shab per $p = 31$, $q = 67$, $x = 5$ e determinarne il periodo P . I primi p, q e il seme iniziale x rispettano le ipotesi del metodo?

i	x_i	b_i
0	25	1
1	625	1
2	149	1
3	1431	1
4	1916	0
5	997	1
6	1203	1
7	1617	1
8	1823	1
9	129	1
10	25	1
11	:	:
	:	:
	:	:

\uparrow
 $\pi = 10$
 \downarrow

$$n = p \cdot q = 31 \cdot 67 = 2077$$

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

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

$$49 \equiv 3 \pmod{4}$$

$$59 \equiv 3 \pmod{4}$$

$$5 \perp 31 \cdot 67 = 2077$$

$$\left. \begin{array}{l} 49 \equiv 3 \pmod{4} \\ 59 \equiv 3 \pmod{4} \end{array} \right\} \Rightarrow 5$$

- 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 Carmichael, calcolabile come

$$\lambda(n) = \text{lcm}(\{\lambda(p_i^{a_i})\}) \quad \lambda(p^k) = \begin{cases} \frac{1}{2} \phi(p^k) & \text{se } p = 2, k \geq 3 \\ \phi(p^k) & \text{altrimenti} \end{cases}$$

$$\lambda(n) = \text{lcm}(30, 66) = 2 \cdot 3 \cdot 5 \cdot 11 = 330$$

$$\lambda[\lambda(n)] = \lambda(330) = \text{lcm}(2, 4, 10) = 20$$

$$\pi(x_i) \in \{2, 4, 5, 10, 20\}$$

Domanda 4

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

a) Definire la proprietà di *resistenza debole alle collisioni* di una funzione di hash $y = h(x)$.

b) Un Trojan memorizza i valori di *hash* calcolati con SHA2-256, troncati agli ultimi 32 bit per risparmiare memoria, su tutti i file JPG scaricati da un archivio di 1000 immagini. La probabilità P che almeno due JPG di essi abbiano lo stesso *hash* è vicina a 1, vicina a 0, o qualche valore intermedio? Conviene scommettere sul fatto che ci siano almeno due hash uguali?

$$P \approx 1 - e^{-N^2/2^{m+1}}$$

$$N = 1000$$

$$m = 32$$

$$\rightarrow P \approx 1 - e^{-\frac{10^6}{8 \cdot 10^4}} \approx 0$$

c) E' facile verificare che una certa *funzione di hash* $h = h(x)$ non è *unidirezionale*. Un signore memorizza in un file sul suo server i valori degli hash $h_i = h(p_i)$ di tutte le password p_i dei suoi clienti, ignorando che la funzione $h = h(x)$ è facilmente violabile. I clienti devono digitare la loro password per accedere al loro portafoglio di dati sul server. Se un hacker riesce a leggere il file, riuscirà a ricavare le password dei clienti e ad accedere ai dati dei clienti?

d) Hai proposto alla tua Azienda di adottare la funzione di hash $h(m) = \text{DES}_m("00...0")$, definita come la cifratura DES di un blocco di 64 zeri con chiave pari agli ultimi 56 bit (i 56 bit meno significativi) del messaggio m . Per verificarne la robustezza, l'Azienda mette a disposizione un premio di 10.000 euro per il primo che riesca a vincere una delle seguenti sfide pubbliche a tua scelta:

- X
- 1) provare entro 1 ora dal bando che $h(m)$ non è unidirezionale;
 - 2) provare entro 1 ora dal bando che $h(m)$ non è fortemente resistente alle collisioni;
- Se nessuno vince la sfida da te scelta, il premio va a te.
Quale delle due sfide scegli di bandire? Perché?

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) Trovare i parametri
- (a, b)
- del Cifrario Affine (mod 26) che decifra "pghtcdbadul" in "nyarlathotep".

(2 punti)

$$C = E_K(P) = aP + b \pmod{26}$$

$$P = D_K(C) = (C - b)a^{-1} \pmod{26}$$

$$\begin{matrix} \text{"c"} \\ \downarrow D_K \end{matrix} \rightarrow \begin{matrix} \text{"a"} \\ \downarrow D_K \end{matrix} \Rightarrow 0 \equiv (2 - b)a^{-1} \pmod{26} \Rightarrow \boxed{b = 2}$$

$$\begin{matrix} \text{"a"} \\ \downarrow D_K \end{matrix} \rightarrow \begin{matrix} \text{"o"} \\ \downarrow D_K \end{matrix} \Rightarrow 14 \equiv (0 - b)a^{-1} \pmod{26} \Rightarrow a^{-1} = -7$$

$$a^{-1} \equiv -7 \equiv 19 \pmod{26}$$

$$a \equiv 19^{-1} \equiv 11 \pmod{26} \Rightarrow \boxed{a = 11}$$

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

- 2) Uno scrambler auto-sincronizzante non è utile per crittografare dati da trasmettere su un canale non sicuro e moltiplica il tasso di errore sul canale di un fattore
- M
- (ordine dello scrambler). A che scopo viene quindi utilizzato? (2 punti)

- 3) Per
- $p = 433$
- (primo), quanti elementi
- $\alpha \in \mathbb{Z}_p^*$
- hanno Ordine = 432? Quanti hanno Ordine = 5?

Cos'è un residuo quadratico dell'insieme \mathbb{Z}_p^* ? Quanti sono i residui quadratici in \mathbb{Z}_{433}^* ?

(3 punti)

$$\phi(432) = 144 \text{ elementi con ordine} = 432$$

$$0 \text{ elementi con ordine} = 5$$

$$216 \text{ residui quadratici}$$

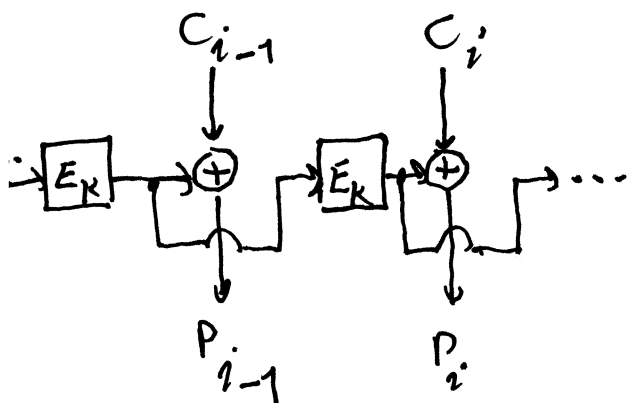
- 4) Si consideri un generatore di password consistenti di 10 simboli casuali scelti nell'alfabeto Fremmen, che comprende in tutto 27 caratteri (lettere) e 9 cifre (non c'è lo zero), più lo spazio " ". Qual è la quantità di informazione [bit] delle password, se i simboli sono scelti indipendentemente una dall'altro, la probabilità che un simbolo sia un carattere è 65%, che sia una cifra è 25%, che sia uno spazio è 10%? (2 punti)

$$H(X) = -\left(0,65 \log_2 \frac{0,65}{27} + 0,25 \log_2 \frac{0,25}{9} + 0,10 \log_2 0,10\right) =$$

$$= 3,495 + 1,292 + 0,332 = 5,12 \text{ bit/simbolo}$$

$$H(10 \text{ simboli}) = 51,2 \text{ bit}$$

- 5) Si consideri un cifrario a blocchi concatenato secondo la modalità *Output FeedBack Mode (OFB)*, in cui cifratura e decifratura sono svolte rispettivamente come $C_i = P_i \oplus E_K^{(i)}(C_0)$, $P_i = C_i \oplus E_K^{(i)}(C_0)$, C_0 è il vettore di inizializzazione, la dimensione dei blocchi P_i e C_i è 2048 bit. Disegnare lo schema a blocchi del processo di decifrazione. Il flusso cifrato $\{C_i\}$ viene trasmesso da A a B, ma subisce errori di trasmissione puramente casuali con tasso ε . Quale sarà il tasso di errore sul flusso decifrato $\{P_i\}$, nei due casi $\varepsilon = 10^{-5}$ e $\varepsilon = 0.5$? (2 punti)



- 6) Su Astalavista, hai trovato un certificato in cui leggi, tra le altre cose:

Issuer name: TrueServices.Inc;
 Period of validity: from 1/1/1990 to 31/12/2199;
 Subject name: VATICAN.ORG;
 Public Key of the Subject: X
 Signature: Y.

Come verifichi che il certificato sia valido, se il tuo browser non riesce a validarlo automaticamente? Per validarlo, che informazione devi reperire?