Crittografia e Sicurezza

A.A. 2006/2007

Giacomo Verticale

Esercizi di Crittografia e Sicurezza

Esercitazioni del corso di *Crittografia e Sicurezza* tenuto dal prof. Maurizio Decina.

Giacomo Verticale
giacomo.verticale@polimi.it
www.elet.polimi.it/upload/vertical/

1

Aritmetica modulare

1.1 GCD e algoritmo di Euclide

Esercizio 1.1 *Calcolare* $d = \gcd(360, 294)$ *in due modi:*
1. *fattorizzando ciascuno dei numeri e poi fattorizzando d;*
2. *usando l'algoritmo di Euclide.*

Soluzione Osserviamo che

$$360 = 6^2 \times 10 = 5 \times 3^2 \times 2^3$$
$$294 = 2 \times 3 \times 7^2$$

Il gcd è il prodotto dei fattori comuni, ciascuno preso con l'esponente minore. Quindi

$$d = 3 \times 2 = 6$$

Definiamo:

$$r_0 = \max(a, b)$$
$$r_1 = \min(a, b)$$

Il nostro scopo è scrivere una sequenza di espressioni del tipo:

$$r_0 = q_1 r_1 + r_2$$
$$\dots$$
$$r_{j-2} = q_{j-1} r_{j-1} + r_j$$
$$\dots$$

Dove j è l'indice della espressione, r_j e q_j sono numeri interi. L'algoritmo è inizializzato con:

$$r_0 \leftarrow a$$
$$r_1 \leftarrow b$$
$$j \leftarrow 0$$

L'algoritmo termina quando $r_j = 0$ e si ha $d = \gcd(a, b) = r_{j-1}$.

j	r_j	
0	360	–
1	294	–
2	66	$360 = 1 \cdot 294 + 66$
3	30	$294 = 4 \cdot 66 + 30$
4	6	$30 = 5 \cdot 6 + 0$
5	0	–

Quindi $d = \gcd(360, 294) = 6$.

Esercizio 1.2 *Trovare $d = \gcd(841, 294)$ ed esprimere d come combinazione lineare dei due numeri.*

Soluzione L'algoritmo di Euclide esteso permette di trovare i coefficienti s e t tali per cui:

$$\gcd(a, b) = r_0 s + r_1 t$$
$$\text{con}$$
$$r_0 = \max(a, b)$$
$$r_1 = \min(a, b)$$

Si definiscono le seguenti ricorrenze:

$$s_j = \begin{cases} 1 & \text{se } j = 0 \\ 0 & \text{se } j = 1 \\ s_{j-2} - q_{j-1} s_{j-1} & \text{se } j \geq 2 \end{cases}$$

e

$$t_j = \begin{cases} 0 & \text{se } j = 0 \\ 1 & \text{se } j = 1 \\ s_{j-2} - q_{j-1} s_{j-1} & \text{se } j \geq 2 \end{cases}$$

Per come sono definiti s_j e t_j, vale sempre la seguente relazione:

$$r_j = r_0 s_j + r_1 t_j$$

Quindi i valori s, t che permettono di esprimere il gcd come combinazione lineare dei due numeri sono i coefficienti s_j, t_j ottenuti in corrispondenza di $r_j = \gcd(a, b)$, ovvero dell'ultimo resto non nullo.

La tabella mostra tutti i passaggi dell'algoritmo mettendo in evidenza r_j, q_j e il calcolo dell'espressione $r_j = r_0 s_j + r_1 t_j$.

j	r_j	q_j		s_j	t_j	$r_0 s_j + r_1 t_j$
0	841	–	–	1	0	841
1	294	2	–	0	1	294
2	253	1	$841 = 2 \cdot 294 + 253$	1	-2	253
3	41	6	$294 = 1 \cdot 253 + 41$	-1	3	41
4	7	5	$253 = 6 \cdot 41 + 7$	7	-20	7
5	6	1	$41 = 5 \cdot 7 + 6$	-36	103	6
6	1	6	$7 = 1 \cdot 6 + 1$	43	-123	1
7	0	–	$6 = 6 \cdot 1 + 0$	-294	841	0

Poiché l'ultimo resto non nullo si ottiene per $j = 6$, i due numeri sono primi tra loro e i coefficienti cercati sono $s = 43$ e $t = -123$.

Normalmente non scriveremo tutte le colonne della tabella (che contengono molte ripetizioni), ma semplicemente le espressioni $r_{j-2} = q_{j-1}r_{j-1} + r_j$ e le colonne s_j e t_j.

	s_j	t_j
–	1	0
–	0	1
$841 = 2 \cdot 294 + 253$	1	-2
$294 = 1 \cdot 253 + 41$	-1	3
$253 = 6 \cdot 41 + 7$	7	-20
$41 = 5 \cdot 7 + 6$	-36	103
$7 = 1 \cdot 6 + 1$	43	-123
$6 = 6 \cdot 1 + 0$	-294	841

1.2 Algoritmo di Euclide con polinomi

Esercizio 1.3 *Si consideri lo spazio dei polinomi $f(x)$ con coefficienti reali in cui il coefficiente di grado massimo è unitario. Due polinomi $f(x)$ e $g(x)$ si dicono primi fra loro se* $\gcd(f(x), g(x)) = 1$.

Trovare $d(x) = \gcd(x^4 + x^2 + 1, x^2 + 1)$ e trovare i polinomi $s(x)$ e $t(x)$ tali per cui $d(x) = s(x)f(x) + t(x)g(x)$.

Soluzione

	$s_j(x)$	$t_j(x)$
–	1	0
–	0	1
$x^4 + x^2 + 1 = x^2 \cdot (x^2 + 1) + 1$	1	$-x^2$
$x^2 + 1 = (x^2 + 1) \cdot 1 + 0$	$-(x^2 + 1)$	$x^4 + x^2 + 1$

$$d(x) = 1$$
$$s(x) = 1$$
$$t(x) = -x^2$$

Infatti $1 = 1 \cdot (x^4 + x^2 + 1) - x^2 \cdot (x^2 + 1)$.

Esercizio 1.4 *Calcolare $d(x) = \gcd(x^4 - 4x^3 + 6x^2 - 4x + 1, x^3 - x^2 + x - 1)$.*

Soluzione

	$s_j(x)$	$t_j(x)$
–	1	0
–	0	1
$x^4 - 4x^3 + 6x^2 - 4x + 1 = (x - 3)(x^3 - x^2 + x - 1) + (2x^2 - 2)$	1	$-(x - 3)$
$x^3 - x^2 + x - 1 = (\frac{1}{2}x - \frac{1}{2})(2x^2 - 2) + (2x - 2)$	$-\frac{1}{2}(x - 1)$	$\frac{1}{2}(x^2 - 4x + 5)$
$2x^2 - 2 = (x + 1)(2x - 2) + 0$	$\frac{1}{2}(x^2 + 1)$	$-\frac{1}{2}(x^3 - 3x^2 + 3x + 1)$

L'ultimo resto non nullo è $2x - 2 = 2(x - 1)$. Prendiamo come gcd il polinomio monico $x - 1$.

$$\begin{aligned} d(x) &= x - 1 \\ u(x) &= -\frac{1}{4}x + \frac{1}{4} \\ v(x) &= \frac{1}{4}x^2 - x + \frac{5}{4} \end{aligned}$$

Esercizio 1.5 *Se un polinomio $f(x)$ ha radici multiple, esse sono radici di* $\gcd(f(x), f'(x))$. *Trovare la radice multipla del polinomio $x^2 - 2x^3 - x^2 + 2x + 1$.*

Soluzione

$$f'(x) = 4x^3 - 6x^2 - 2x + 2$$

$$\begin{aligned} x^4 - 2x^3 - x^2 + 2x + 1 &= \left(\frac{1}{4}x - \frac{1}{8}\right)\left(4x^3 - 6x^2 - 2x + 2\right) + \left(-\frac{5}{4}x^2 + \frac{5}{4}x + \frac{5}{4}\right) \\ 4x^3 - 6x^2 - 2x + 2 &= \left(-\frac{16}{5}x + \frac{8}{5}\right)\left(-\frac{5}{4}x^2 + \frac{5}{4}x + \frac{5}{4}\right) + 0 \end{aligned}$$

Quindi la radice multipla è $x^2 - x - 1$. Infatti

$$x^4 - 2x^3 - x^2 + 2x + 1 = (x^2 - x - 1)^2$$

1.3 Teorema cinese del resto

Esercizio 1.6 *Trovare le soluzioni della seguente congruenza:*

$$3x \equiv 4 \pmod 7$$

Soluzione Si consideri che

$$3^{-1} \cdot 3x \equiv 3^{-1} \cdot 4 \pmod 7$$

Usando l'algoritmo di Euclide possiamo ricavare che

$$3 \cdot 5 = 15 = 7 \cdot 2 + 1 \equiv 1 \pmod 7$$

Quindi l'inverso di 3 è 5. Possiamo scrivere:

$$\begin{aligned} 5 \cdot 3x &\equiv 5 \cdot 4 \pmod 7 \\ x &\equiv 20 \bmod 7 \equiv 6 \pmod 7 \end{aligned}$$

La soluzione è quindi:

$$x = 6 + 7k, \quad \forall k \in \mathbb{Z}$$

Esercizio 1.7 *Trovare le soluzioni del seguente sistema di congruenze:*

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{16} \end{cases}$$

Soluzione Il teorema cinese del resto garantisce che la soluzione esiste se $m_i = \{3, 5, 11, 16\}$ sono primi tra loro a coppie. È facile verificare che 3, 5 e 11 sono primi e che $16 = 2^4$, quindi non esistono fattori in comune.

Si definiscono quindi:

$$\begin{aligned} a_i &= \{2, 3, 4, 5\} \\ m_i &= \{3, 5, 11, 16\} \\ M &= \prod_{i=1}^{4} m_i = 3 \cdot 5 \cdot 11 \cdot 16 = 2640 \\ z_i &= \frac{M}{m_i} \\ y_i &= z_i^{-1} \pmod{m_i} \\ x &= \sum_{i=1}^{4} a_i y_i z_i \bmod M \end{aligned}$$

Nel caso in esame:

i	a_i	m_i	z_i	y_i
1	2	3	880	1
2	3	5	528	2
3	4	11	240	5
4	5	16	165	13

Quindi:

$$x = 2 \cdot 1 \cdot 880 + 3 \cdot 2 \cdot 528 + 4 \cdot 5 \cdot 240 + 5 \cdot 13 \cdot 165 \equiv 1973 \pmod{2640}$$

1.4 Residui quadratici

Esercizio 1.8 *Calcolare* $\left(\frac{91}{167}\right)$.

Soluzione Osserviamo che 167 è primo, quindi si può usare la definizione di simbolo di Legendre:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{se } a \text{ è un quadrato} \pmod{p} \\ -1 & \text{altrimenti} \end{cases}$$

Inoltre $167 \equiv 3 \pmod 4$, quindi a è un quadrato $\bmod p$ se e solo se:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Nel nostro caso dobbiamo calcolare $\left(91^{83} \bmod 167\right)$. Per svolgere il calcolo usiamo l'algoritmo Square-and-Multiply.

i	c_i	$z \pmod{167}$
6	1	$1^2 \times 91 = 91$
5	0	$91^2 = 98$
4	1	$98^2 \times 91 = 53$
3	0	$53^2 = 137$
2	0	$137^2 = 65$
1	1	$65^2 \times 91 = 41$
0	1	$41^2 \times 91 = 166$

Quindi

$$91^{83} \equiv 166 \equiv -1 \pmod{167}$$

allora 91 non è un quadrato e il simbolo di Legendre vale -1:

$$\left(\frac{91}{167}\right) = -1$$

Esercizio 1.9 *Calcolare* $\left(\frac{91}{167}\right)$ *usando la legge di reciprocità quadratica.*

Soluzione Osserviamo che $91 = 7 \times 13$, quindi:

$$\left(\frac{91}{167}\right) = \left(\frac{7}{167}\right)\left(\frac{13}{167}\right)$$

La legge di reciprocità dice che:

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{se } m \equiv n \equiv 3 \pmod{4} \\ \left(\frac{n}{m}\right) & \text{altrimenti} \end{cases}$$

Nel nostro caso:

$$\begin{aligned} 167 \bmod 4 &= 3 \\ 7 \bmod 4 &= 3 \\ 13 \bmod 4 &= 1 \end{aligned}$$

Quindi:

$$\left(\frac{91}{167}\right) = -\left(\frac{167}{7}\right)\left(\frac{167}{13}\right)$$

Applichiamo la proprietà per cui, se $a \equiv b \pmod{p}$ e $\gcd(a, p) = 1$:

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

e otteniamo

$$\left(\frac{91}{167}\right) = -\left(\frac{6}{7}\right)\left(\frac{11}{13}\right)$$

Osserviamo che $6 \equiv -1 \pmod{7}$, quindi:

$$\left(\frac{6}{7}\right) = \left(\frac{-1}{7}\right) = (-1)^{(7-1)/2} = (-1)^3 = -1$$

Osserviamo che $11 \equiv -2 \pmod{13}$ e che $13 \equiv 5 \pmod{8}$, quindi:

$$\left(\frac{11}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right) = (-1)^{(13-1)/2} \cdot (-1) = -1$$

Quindi il risultato è:

$$\left(\frac{91}{167}\right) = -(-1)(-1) = -1$$

Esercizio 1.10 *Valutare il simbolo di Legendre* $\left(\frac{1801}{8191}\right)$ *fattorizzando solo i numeri pari.*

Soluzione Calcoliamo innanzitutto $\gcd(1801, 8191)$.

j	r_j	
0	8191	–
1	1801	–
2	987	$8191 = 4 \cdot 1801 + 987$
3	814	$1801 = 1 \cdot 987 + 814$
4	173	$987 = 1 \cdot 814 + 173$
5	122	$814 = 4 \cdot 173 + 122$
6	51	$173 = 1 \cdot 122 + 51$
7	20	$122 = 2 \cdot 51 + 20$
8	11	$51 = 2 \cdot 20 + 11$
9	9	$20 = 1 \cdot 11 + 9$
10	2	$11 = 1 \cdot 9 + 2$
11	1	$9 = 4 \cdot 2 + 1$
12	0	$2 = 2 \cdot 1 + 1$

Osserviamo che:

$$\begin{gathered} 1801 \bmod 4 = 1 \\ 8191 \bmod 4 = 3 \\ 8191 \bmod 1801 = 987 \\ \gcd(8191, 1801) = 1 \end{gathered}$$

Applicando la legge di reciprocità:

$$\left(\frac{1801}{8191}\right) = \left(\frac{8191}{1801}\right) = \left(\frac{987}{1801}\right)$$

Osserviamo ancora che:

$$\begin{gathered} 1801 \bmod 4 = 1 \\ 987 \bmod 4 = 3 \\ 1801 \bmod 987 = 814 \\ \gcd(987, 1801) = \gcd(8191 \bmod 1801, 1801) = 1 \\ 987 \bmod 8 = 3 \end{gathered}$$

Quindi:

$$\left(\frac{987}{1801}\right) = \left(\frac{814}{987}\right) = \left(\frac{2}{987}\right)\left(\frac{407}{987}\right) = -\left(\frac{407}{987}\right)$$

Osserviamo ancora che:

$$\begin{gathered} 407 \bmod 4 = 3 \\ 987 \bmod 4 = 3 \\ 987 \bmod 407 = 173 \\ \gcd(407, 987) = 1 \end{gathered}$$

Quindi:

$$-\left(\frac{407}{987}\right) = \left(\frac{173}{407}\right)$$

Osserviamo ancora che:

$$\begin{gathered} 407 \bmod 4 = 3 \\ 173 \bmod 4 = 1 \\ 987 \bmod 407 = 61 \\ \gcd(407, 173) = 1 \end{gathered}$$

Quindi:

$$\left(\frac{173}{407}\right) = \left(\frac{61}{173}\right)$$

Osserviamo ancora che:

$$\begin{gathered} 61 \bmod 4 = 1 \\ 173 \bmod 4 = 1 \\ 173 \bmod 61 = 51 \\ \gcd(61, 173) = 1 \end{gathered}$$

Quindi:

$$\left(\frac{61}{173}\right) = \left(\frac{51}{61}\right)$$

Osserviamo ancora che:

$$\begin{gathered} 61 \bmod 4 = 1 \\ 51 \bmod 4 = 3 \\ 61 \bmod 51 = 10 \\ \gcd(61, 51) = 1 \\ 51 \bmod 8 = 3 \end{gathered}$$

Quindi:

$$\left(\frac{51}{61}\right) = \left(\frac{2}{51}\right)\left(\frac{5}{51}\right) = -\left(\frac{5}{51}\right)$$

Osserviamo ancora che:

$$\begin{aligned} 5 \bmod 4 &= 1 \\ 51 \bmod 4 &= 3 \\ 51 \bmod 5 &= 1 \\ \gcd(5, 51) &= 1 \end{aligned}$$

Quindi:

$$-\left(\frac{5}{51}\right) = -\left(\frac{1}{5}\right) = -1$$

Esercizio 1.11 (Cifrario di Hill su $\mathbb{Z}_4$) *Il messaggio binario in chiaro $P =$ `011000110100` viene cifrato usando un cifrario di Hill su $\mathbb{Z}_4$. Il cifrario usa come chiave una matrice K con dimensione 2×2.*

1. *Dire che condizioni deve rispettare la chiave K.*
2. *Cifrare il messaggio P considerando il caso*

$$K = \begin{pmatrix} 0 & 1 \\ 3 & 3 \end{pmatrix}$$

3. *Decifrare il messaggio ottenuto al passo precedente*
4. *Usando la coppia messaggio in chiaro / messaggio cifrato ottenuta ai punti precedenti, effettuare un attacco di tipo* known plaintext *e ricavare la chiave K.*

Soluzione

1. La chiave K deve rispettare le seguenti due condizioni:

$$\begin{cases} \det(K) \neq 0 \\ \gcd(\det(K), 4) = 1 \end{cases}$$

   Notare che, per convenzione, la 2 implica la 1.
2. Per prima cosa convertiamo il messaggio binario in elementi di $\mathbb{Z}_4$. Poiché gli elementi sono $\{0, 1, 2, 3\}$ la cosa più semplice è convertire ogni coppia di bit in un numero. Pertanto il messaggio diventa:

$$P = \begin{pmatrix} 1 & 2 & 0 & 3 & 1 & 0 \end{pmatrix}$$

   La chiave è una matrice 2×2, quindi il testo in chiaro deve essere diviso in vettori P_i di due elementi:

$$\begin{aligned} P_1 &= \begin{pmatrix} 1 & 2 \end{pmatrix} \\ P_2 &= \begin{pmatrix} 0 & 3 \end{pmatrix} \\ P_3 &= \begin{pmatrix} 1 & 0 \end{pmatrix} \end{aligned}$$

   Procediamo quindi applicando la formula:

$$C_i = P_i \cdot K \pmod 4$$

$$\begin{aligned} C_1 &= \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 3 & 3\end{pmatrix} = \begin{pmatrix}6 & 7\end{pmatrix} = \begin{pmatrix}2 & 3\end{pmatrix} \pmod 4 \\ C_2 &= \begin{pmatrix}0 & 3\end{pmatrix}\begin{pmatrix}0 & 1\\ 3 & 3\end{pmatrix} = \begin{pmatrix}9 & 9\end{pmatrix} = \begin{pmatrix}1 & 1\end{pmatrix} \pmod 4 \\ C_3 &= \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 3 & 3\end{pmatrix} = \begin{pmatrix}0 & 1\end{pmatrix} \pmod 4 \end{aligned}$$

Quindi il testo cifrato C risulta:

$$C = \begin{pmatrix}2 & 3 & 1 & 1 & 0 & 1\end{pmatrix}$$

che, espresso in binario, diventa $C = 101101010001$.

3. Occorre per prima cosa calcolare la matrice inversa della chiave:

$$K^{-1} = \frac{1}{-3}\begin{pmatrix}3 & -1\\ -3 & 0\end{pmatrix} \pmod 4$$

Occorre trovare l'elemento inverso di -3 in $\mathbb{Z}_4$. Ma $-3 \equiv 1 \pmod 4$, e l'inverso di 1 è ancora 1, quindi:

$$K^{-1} = \begin{pmatrix}3 & 3\\ 1 & 0\end{pmatrix} \pmod 4$$

Calcoliamo il testo in chiaro:

$$\begin{aligned} P_1 &= \begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}3 & 3\\ 1 & 0\end{pmatrix} = \begin{pmatrix}9 & 6\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix} \pmod 4 \\ P_2 &= \begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}3 & 3\\ 1 & 0\end{pmatrix} = \begin{pmatrix}4 & 3\end{pmatrix} = \begin{pmatrix}0 & 3\end{pmatrix} \pmod 4 \\ P_3 &= \begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}3 & 3\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\end{pmatrix} \pmod 4 \end{aligned}$$

Quindi il testo in chiaro è:

$$P = \begin{pmatrix}1 & 2 & 0 & 3 & 1 & 0\end{pmatrix}$$

4. Dobbiamo costruire una equazione del tipo:

$$\begin{pmatrix}P_i\\ P_j\end{pmatrix} K = \begin{pmatrix}C_i\\ C_j\end{pmatrix}$$

dove le righe P_i, C_i e P_j, C_j sono due coppie testo in chiaro / testo cifrato di lunghezza due.

Risolvendo rispetto alla matrice delle incognite otterremo la chiave. Per risolvere l'equazione la matrice del testo in chiaro deve essere invertibile; dovremo tenere presente questo fatto nello scegliere le righe della matrice.

Fortunatamente la matrice costruita usando P_1 e P_2 va bene, infatti:

$$\det\begin{pmatrix}1 & 2\\ 0 & 3\end{pmatrix} = 3$$

che non è né nullo né multiplo di 2.

Quindi possiamo scrivere:

$$K = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix} == \frac{1}{3} \begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}$$
$$= 3 \begin{pmatrix} 4 & 7 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 3 & 3 \end{pmatrix} \pmod 4$$

Nella equazione precedente si è posto $1/3 \equiv 3 \pmod 4$, per calcolare l'inverso di 3 è possibile usare l'algoritmo di Euclide esteso, oppure si può osservare che $3 \cdot 3 = 9 \equiv 1 \pmod 4$.

1.5 Cifratura con matrici

Esercizio 1.12 *Alice e Bob usano una tecnica di cifratura affine basata sull'aritmetica in $\mathbb{Z}_{10}$. L'algoritmo di cifratura è la espressione:*

$$C_i = P_i \cdot K + B \pmod{10}$$

I vettori riga 1×2 C_i e P_I contengono rispettivamente la coppia i-esima di numeri cifrata e in chiaro, mentre la chiave è composta dalla matrice K e dal vettore B.

La chiave condivisa è:

$$K = \begin{pmatrix} 3 & 7 \\ 2 & 7 \end{pmatrix}$$
$$B = \begin{pmatrix} 4 & 9 \end{pmatrix}$$

1. *Verificare che K sia una chiave valida.*
2. *Cifrare il messaggio:*
$$P = \begin{pmatrix} 6 & 7 & 3 & 9 & 3 & 6 \end{pmatrix}$$
3. *Decifrare il messaggio cifrato.*
4. *Portare un attacco di tipo* known-plaintext *e trovare la chiave (K e B).*

Soluzione Perché K sia valida devono essere rispettate le seguenti condizioni:

$$\begin{cases} \det(K) \neq 0 \\ \gcd(\det(K), 10) = 1 \end{cases}$$

Nel nostro caso abbiamo che $\det(K) = 7$ e le due condizioni sono rispettate.

Scomponiamo il messaggio P in 3 vettori riga:

$$P_1 = \begin{pmatrix} 6 & 7 \end{pmatrix}$$
$$P_2 = \begin{pmatrix} 3 & 9 \end{pmatrix}$$
$$P_3 = \begin{pmatrix} 3 & 6 \end{pmatrix}$$

Calcoliamo i testi cifrati:

$$C_1 = \begin{pmatrix} 6 & 7 \end{pmatrix} \begin{pmatrix} 3 & 7 \\ 2 & 7 \end{pmatrix} + \begin{pmatrix} 4 & 9 \end{pmatrix} = \begin{pmatrix} 6 & 0 \end{pmatrix}$$
$$C_2 = \begin{pmatrix} 3 & 9 \end{pmatrix} \begin{pmatrix} 3 & 7 \\ 2 & 7 \end{pmatrix} + \begin{pmatrix} 4 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix}$$
$$C_3 = \begin{pmatrix} 3 & 6 \end{pmatrix} \begin{pmatrix} 3 & 7 \\ 2 & 7 \end{pmatrix} + \begin{pmatrix} 4 & 9 \end{pmatrix} = \begin{pmatrix} 5 & 2 \end{pmatrix}$$

Il testo cifrato è quindi:

$$C = \begin{pmatrix} 6 & 0 & 1 & 3 & 5 & 2 \end{pmatrix}$$

Per decifrare il messaggio occorre invertire la matrice K. L'algoritmo di decifratura è l'espressione:

$$P = CK^{-1} - BK^{-1}$$

$$K^{-1} = \frac{1}{7} \begin{pmatrix} 7 & -7 \\ -2 & 3 \end{pmatrix} \bmod 10$$

L'inverso di $7 \pmod{10}$ si può trovare usando l'algoritmo esteso di Euclide:

r_j	q_j		s_j	t_j
10	–	–	1	0
7	1	–	0	1
3	2	$10 = 1 \cdot 7 + 3$	1	-1
1	3	$7 = 2 \cdot 3 + 1$	-2	3
0	–	$3 = 3 \cdot 1 + 0$	7	-10

L'inverso di 7 è 3, infatti:

$$7 \cdot 3 \bmod 10 = 21 \mod 10 = 1$$

Quindi:

$$K^{-1} = 3 \begin{pmatrix} 7 & 3 \\ 8 & 3 \end{pmatrix} \bmod 10 = \begin{pmatrix} 1 & 9 \\ 4 & 9 \end{pmatrix}$$
$$-BK^{-1} = - \begin{pmatrix} 4 & 9 \end{pmatrix} \begin{pmatrix} 1 & 9 \\ 4 & 9 \end{pmatrix} = \begin{pmatrix} 0 & 3 \end{pmatrix}$$

Calcoliamo i testi in chiaro:

$$P_1 = \begin{pmatrix} 6 & 0 \end{pmatrix} \begin{pmatrix} 1 & 9 \\ 4 & 9 \end{pmatrix} + \begin{pmatrix} 0 & 3 \end{pmatrix} = \begin{pmatrix} 6 & 7 \end{pmatrix}$$
$$P_2 = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 9 \\ 4 & 9 \end{pmatrix} + \begin{pmatrix} 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 9 \end{pmatrix}$$
$$P_3 = \begin{pmatrix} 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 9 \\ 4 & 9 \end{pmatrix} + \begin{pmatrix} 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 6 \end{pmatrix}$$

Per scoprire la chiave dato un insieme di coppie P_i, C_i, occorre scrivere un sistema di equazioni:

$$C_1 = P_1K + B \tag{1.1}$$
$$C_2 = P_2K + B \tag{1.2}$$
$$C_3 = P_3K + B \tag{1.3}$$

Sottraendo la (1.3) alla (1.2) e alla (1.1), si ottiene una nuova equazione in cui la costante B non è presente e da cui si può ricavare la matrice K:

$$\begin{pmatrix} C_1 - C_3 \\ C_2 - C_3 \end{pmatrix} = \begin{pmatrix} P_1 - P_3 \\ P_2 - P_3 \end{pmatrix} K \tag{1.4}$$

$$K = \begin{pmatrix} P_1 - P_3 \\ P_2 - P_3 \end{pmatrix}^{-1} \begin{pmatrix} C_1 - C_3 \\ C_2 - C_3 \end{pmatrix} \tag{1.5}$$

$$K = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 1 & -2 \\ -4 & 1 \end{pmatrix} \tag{1.6}$$

Perché l'attacco abbia successo è necessario che la matrice dei testi in chiaro sia invertibile. Poiché:

$$\det \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix} = 9$$

la matrice è invertibile e non ci sono fattori comuni con 10, pertanto l'inversa è unica:

$$K = \frac{1}{9} \begin{pmatrix} 3 & -1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ -4 & 1 \end{pmatrix} = 9 \begin{pmatrix} 7 & -7 \\ -12 & 3 \end{pmatrix} = \begin{pmatrix} 63 & -63 \\ -108 & 27 \end{pmatrix}$$
$$K \equiv \begin{pmatrix} 3 & 7 \\ 2 & 7 \end{pmatrix} \pmod{10}$$

Da notare che $9^{-1} \equiv 9 \pmod{10} = 9$, infatti $9 \cdot 9 \bmod 10 = 1$.

Trovato K si può usare la (1.1) per trovare B:

$$B = C_1 - P_1K = \begin{pmatrix} 6 & 0 \end{pmatrix} - \begin{pmatrix} 2 & 1 \end{pmatrix} = \begin{pmatrix} 4 & -1 \end{pmatrix}$$
$$B \equiv \begin{pmatrix} 4 & 9 \end{pmatrix} \pmod{10}$$

Esercizio 1.13 *Calcolare x tale che $x^2 \equiv 76 \pmod{167}$.*

Soluzione Prima di tutto verifichiamo se l'equazione ha soluzione. Siccome 167 è primo, 76 è un quadrato se

$$76^{\frac{167-1}{2}} = 76^{83} \equiv 1 \pmod{167}$$

Per verificare che $76^{83} \bmod 167 = 1$ si può usare l'algoritmo Square-and-Multiply:

i	c_i	$z \pmod{167}$
6	1	$1^2 \times 76 = 76$
5	0	$76^2 = 98$
4	1	$98^2 \times 76 = 114$
3	0	$114^2 = 137$
2	0	$137^2 = 65$
1	1	$65^2 \times 76 = 126$
0	1	$126^2 \times 76 = 1$

Siccome $167 \equiv 3 \pmod 4$, si può usare la formula veloce per estrarre le radici:

$$x = \pm 76^{\frac{167+1}{4}} \bmod 167 = \pm 76^{42} \bmod 167$$

Anche qui possiamo usare l'algoritmo Square-and-Multiply:

i	c_i	$z \pmod{167}$
5	1	$1^2 \times 76 = 76$
4	0	$76^2 = 98$
3	1	$98^2 \times 76 = 114$
2	0	$114^2 = 137$
1	1	$137^2 \times 76 = 97$
0	0	$97^2 = 57$

Come è facile verificare, $x = \pm 57$.

Esercizio 1.14 *Calcolare x tale che* $x^2 \equiv 100 \pmod{231}$.

Soluzione Poiché $231 = 3 \times 7 \times 11$, il problema si riconduce a trovare la soluzione del sistema:

$$\begin{aligned} x^2 &\equiv 100 \equiv 1 \pmod 3 \\ x^2 &\equiv 100 \equiv 2 \pmod 7 \\ x^2 &\equiv 100 \equiv 1 \pmod{11} \end{aligned}$$

Per verificare che la soluzione esista, calcoliamo i numeri di Legendre:

$$\begin{aligned} \left(\frac{1}{3}\right) &= 1 \\ \left(\frac{2}{7}\right) &= 2^{\frac{7-1}{2}} \bmod 7 = 1 \\ \left(\frac{2}{7}\right) &= 1 \end{aligned}$$

Quindi la soluzione esiste. Osservando poi che $3 \equiv 7 \equiv 11 \pmod 4$, si può usare la formula per calcolare velocemente le radici:

$$\begin{aligned} x &\equiv \pm 1 \pmod 3 \\ x &\equiv \pm 2^{\frac{7+1}{4}} \equiv 4 \pmod 7 \\ x &\equiv \pm 1 \pmod{11} \end{aligned}$$

Il teorema del resto cinese ci permette di trovare la x cercata. Definiamo:

$$\begin{aligned} z_1 &= 231/3 = 77 \quad y_1 \equiv 77^{-1} \equiv 2^{-1} \equiv 2 \pmod 3 \\ z_2 &= 231/7 = 33 \quad y_2 \equiv 33^{-1} \equiv 5^{-1} \equiv 3 \pmod 7 \\ z_3 &= 231/11 = 21 \quad y_3 \equiv 21^{-1} \equiv 10^{-1} \equiv 10 \pmod{11} \end{aligned}$$

Per trovare gli inversi possiamo osservare che $z_1 \equiv -1 \pmod 3$ e $z_3 \equiv -1 \pmod{11}$, quindi y_1 e y_3 sono gli inversi di se stessi. Per y_2 usare l'algoritmo di Euclide esteso:

r_i	q_i	s_i	t_i
7	$--$	1	0
5	1	0	1
2	2	1	-1
1	2	-2	3

Combinando le soluzioni negli $2^3 = 8$ casi otteniamo le 8 radici:

$$x \equiv 1 \cdot 77 \cdot 2 + 4 \cdot 33 \cdot 3 + 1 \cdot 21 \cdot 10 \equiv 67 \pmod{231}$$
$$x \equiv -1 \cdot 77 \cdot 2 + 4 \cdot 33 \cdot 3 + 1 \cdot 21 \cdot 10 \equiv 221 \pmod{231}$$
$$x \equiv 1 \cdot 77 \cdot 2 - 4 \cdot 33 \cdot 3 + 1 \cdot 21 \cdot 10 \equiv 199 \pmod{231}$$
$$x \equiv -1 \cdot 77 \cdot 2 - 4 \cdot 33 \cdot 3 + 1 \cdot 21 \cdot 10 \equiv 122 \pmod{231}$$
$$x \equiv 1 \cdot 77 \cdot 2 + 4 \cdot 33 \cdot 3 - 1 \cdot 21 \cdot 10 \equiv 109 \pmod{231}$$
$$x \equiv -1 \cdot 77 \cdot 2 + 4 \cdot 33 \cdot 3 - 1 \cdot 21 \cdot 10 \equiv 32 \pmod{231}$$
$$x \equiv 1 \cdot 77 \cdot 2 - 4 \cdot 33 \cdot 3 - 1 \cdot 21 \cdot 10 \equiv 10 \pmod{231}$$
$$x \equiv -1 \cdot 77 \cdot 2 - 4 \cdot 33 \cdot 3 - 1 \cdot 21 \cdot 10 \equiv 164 \pmod{231}$$

1.6 Crittosistema di Rabin

Esercizio 1.15 (Crittosistema di Rabin) *Si consideri un testo composto dalle sole 26 lettere maiuscole codificate con numeri interi progressivi. Si consideri 'A' = 65, 'B' = 66 e così via fino a 'Z' = 90.*

Alice e Bob comunicano usando un crittosistema di Rabin. La chiave pubblica di Alice è

$$m = p \cdot q = 209$$

La chiave privata (ovvero la coppia p, q) è tenuta segreta.

Bob cifra, lettera per lettera, il seguente messaggio: "WADE" e lo invia ad Alice. Eve, che conosce le prime due lettere del messaggio in chiaro ma ignora le ultime due, ottiene una copia del messaggio cifrato.

1. *Cifrare il messaggio*
2. *Spiegare come può Eve ricavare la chiave privata di Alice.*
3. *Decifrare la parte restante del messaggio.*

Soluzione

1. Il messaggio in chiaro P è la sequenza:

$$P = \begin{pmatrix} 87 & 65 & 68 & 69 \end{pmatrix}$$

Il messaggio cifrato M si ottiene elevando al quadrato modulo m.

$$C_i = P_i^2 \bmod 209$$

$$C = \begin{pmatrix} 45 & 45 & 26 & 163 \end{pmatrix}$$

2. Ricordiamo che ad ogni M_i corrispondono 4 possibili P_i. Supponiamo che le quattro radici di M_i siano $\pm r$ e $\pm s$, allora $\gcd(r+s, pq)$ sarà uguale a p oppure a q. Nel caso in esame notiamo che i numeri 87 e 65 vengono entrambi cifrati con 45. Calcoliamo quindi il massimo comune denominatore:

$$\gcd(87+65, 209) = \gcd(152, 209) = 19.$$

   Per cui i due fattori di m sono $q = 19$ e $p = 209/19 = 11$.
3. Per decifrare sfruttiamo il Teorema Cinese del Resto. Partiamo da $M_3 = 26$. Dobbiamo prima risolvere le equazioni modulo p e q. Definiamo $m_1 = p$ e $m_2 = q$. Dopodiché risolviamo il sistema di equazioni:

$$a_i^2 = 26 \mod m_i$$

$$\begin{cases} a_1^2 &= 26 \mod 11 = 4 \\ a_2^2 &= 26 \mod 19 = 7 \end{cases}$$

   Usando le regole per risolvere i quadrati modulo k con $k \equiv 3 \pmod 4$ otteniamo:

$$\begin{cases} a_1 &= 4^{\frac{11+1}{4}} \mod 11 = 4^3 \mod 11 = 9 \\ a_2 &= 7^{\frac{19+1}{4}} \mod 19 = 7^5 \mod 19 = 11 \end{cases}$$

   Si verifica facilmente che le radici cercate esistono e coincidono con i valori trovati. Ora bisogna combinare tra loro le soluzioni. L'algoritmo prevede che si calcoli:

$$\begin{aligned} z_i &= 209/m_i \\ y_i &= z_i^{-1} \mod m_i \\ x &= \sum_i (\pm a_i) y_i z_i \mod 209 \end{aligned}$$

   Calcoliamo:

$$\begin{aligned} z_1 &= 19 \\ z_2 &= 11 \end{aligned}$$

$$\begin{aligned} y_1 &= 19^{-1} \mod 11 \\ y_2 &= 11^{-1} \mod 19 \end{aligned}$$

   Per trovare y_1 e y_2 possiamo usare il teorema di euclide esteso oppure il teorema di Fermat. Risulta:

$$\begin{aligned} y_1 &= 7 \mod 11 = 7 \\ y_2 &= 7 \mod 19 = 7 \end{aligned}$$

$$x = \begin{cases} 9 \cdot 19 \cdot 7 + 11 \cdot 11 \cdot 7 \mod 209 = 163 \\ 9 \cdot 19 \cdot 7 - 11 \cdot 11 \cdot 7 \mod 209 = 141 \\ -9 \cdot 19 \cdot 7 + 11 \cdot 11 \cdot 7 \mod 209 = 68 \\ -9 \cdot 19 \cdot 7 - 11 \cdot 11 \cdot 7 \mod 209 = 46 \end{cases}$$

Delle quattro soluzioni ottenute teniamo solo $x = 68 =$ 'D' perché le altre soluzioni non corrispondono a lettere del nostro alfabeto.

Per $M_4 = 163$ procediamo allo stesso modo, ottenendo $x = 69 =$ 'E'.

2

Campi finiti

2.1 Anelli di Polinomi

2.1.1 Algoritmo di Euclide

Esercizio 2.1 *Siano $f(x) = x^4 + x^3 + x^2 + 1$ e $g(x) = x^3 + 1$ polinomi con coefficienti in $\mathbb{Z}_2$. Trovare $d(x) = \gcd(f(x), g(x))$ ed esprimelo come combinazione lineare di f e g.*

Solutione

$r(x)$		$s(x)$	$t(x)$
$x^4 + x^3 + x^2 + 1$		1	0
$x^3 + 1$		0	1
$x^2 + x$	$x^4 + x^3 + x^2 + 1 = (x+1)(x^3+1) + x^2 + x$	1	$-(x+1)$
$x + 1$	$x^3 + 1 = (x+1)(x^2+x) + (x+1)$	$-(x+1)$	x^2
0	$x^2 + x = x(x+1) + 0$	$\cdots$	$\cdots$

Per effettuare le divisioni tra polinomi ricordiamo che si applica la lunga divisione e che siamo in algebra modulo 2 (quindi $1 + 1 = 0$).

$$
\begin{array}{rrrrr|l}
x^4 & +x^3 & +x^2 & & +1 & x^3+1 \\
\cline{6-6}
x^4 & & & x & & x+1 \\
\cline{1-5}
 & x^3 & +x^2 & +x & +1 & \\
 & x^3 & & & 1 & \\
\cline{1-5}
 & & x^2 & +x & & \\
\cline{1-4}
\end{array}
$$

$$
\begin{array}{rrrr|l}
x^3 & & & +1 & x^2+x \\
\cline{5-5}
x^3 & +x^2 & & & x+1 \\
\cline{1-3}
 & x^2 & & 1 & \\
 & x^2 & +x & & \\
\cline{1-3}
 & & x & +1 & \\
\cline{1-4}
\end{array}
$$

Il gcd è $d(x) = x + 1$ e può essere scritto come:

$$x + 1 = (x+1)(x^4 + x^3 + x^2 + 1) + x^2(x^3 + 1)$$

Esercizio 2.2 *Trovare il fattore multiplo in $f(x) = x^4 - x^2 + 1 \in \mathbb{Z}_3[x]$.*

Soluzione Se un fattore è multiplo, è presente sia in $f(x)$ che in $f'(x)$, pertanto comparirà nel $\gcd(f, f')$.

Nel caso in esame $f'(x) = 4x^3 - 2x = x^3 + x$.

$r(x)$	$q(x)$
$x^4 - x^2 + 1$	$--$
$x^3 + x$	x
$x^2 + 1$	x
0	$--$
$\cdots$	

Quindi $\gcd(f, f') = x^2 + 1$.

2.2 Cifrari

Esercizio 2.3 (S-box AES semplificato) *Un S-box opera come segue:*

- *i 4 bit in ingresso $(b_0 b_1 b_2 b_3)$ sono convertiti in un polinomio $N(x)$ di grado 3 con coefficienti in $\mathbb{Z}_2$;*
- *il polinomio $N(x)$ viene considerato un elemento di $GF(16) = \mathbb{Z}_2[x]/(x^4 + x + 1)$ e invertito, ottenendo l'elemento $N^{-1}(x)$; l'inverso di 0 è convenzionalmente posto a 0;*
- *i coefficienti di $N^{-1}(x)$ sono usati per formare un nuovo polinomio $N(y) \in \mathbb{Z}_2[y]/(y^4 + 1)$;*
- *l'output del S-box sono i coefficienti del polinomio $M(y)$ costruito come segue:*

$$M(y) = N(y) \cdot a(y) + b(y) \bmod (y^4 + 1) \tag{2.1}$$

con

$$a(y) = y^3 + y^2 + 1 \tag{2.2}$$

$$b(y) = y^3 + 1 \tag{2.3}$$

$$\tag{2.4}$$

1. *Dati i bit in ingresso `1000`, calcolare l'output del S-box.*
2. *Verificare che $\mathbb{Z}_2[y]/(y^4 + 1)$ non forma un campo.*
3. *Verificare che $a(y)$ è invertibile in $\mathbb{Z}_2[y]/(y^4 + 1)$ e trovare $a^{-1}(y)$.*
4. *Trovare lo S-box inverso a quello dato.*
5. *Decifrare la sequenza di bit `1000`.*

Soluzione La sequenza di bit 1000 corrisponde al polinomio $N(x) = x^3$. Occorre trovare l'inverso di $x^3 \pmod{x^4 + x + 1}$. Usiamo l'algoritmo di Euclide per i polinomi e otteniamo:

$r(x)$	$q(x)$		$s(x)$	$t(x)$
$x^4 + x + 1$	$--$		1	0
x^3	x		0	1
$x + 1$	$x^2 + x + 1$	$x^4 + x + 1 = x \cdot x^3 + (x + 1)$	1	x
1	$x + 1$	$x^3 = (x^2 + x + 1)(x + 1) + 1$	$x^2 + x + 1$	$x^3 + x^2 + x + 1$
0	$\cdots$			

Quindi $N^{-1}(x) = x^3 + x^2 + x + 1$. Tenendo presente che $x^4 = x + 1$ verifichiamo che $N(x)N^{-1}(x) = 1$:

$$\begin{aligned}(x^3 + x^2 + x + 1)x^3 &= (x^3 + x^2 + x + 1)xxx \\ (x^3 + x^2 + x + 1)x &= x^4 + x^3 + x^2 + x = x^3 + x^2 + 1 \\ (x^3 + x^2 + 1)x &= x^4 + x^3 + x = x^3 + 1 \\ (x^3 + 1)x &= x^4 + x = 1\end{aligned}$$

Definiamo il polinomio $N(y) = y^3 + y^2 + y + 1$ e calcoliamo $M(y)$:

$$\begin{aligned}M(y) &= (y^3 + y^2 + y + 1)(y^3 + y^2 + 1) + (y^3 + 1) \bmod (y^4 + 1) = \\ &= (y^6 + y^3 + y + 1) + (y^3 + 1) \bmod (y^4 + 1) = \\ &= y^6 + y \bmod (y^4 + 1) = \\ &= y^2 + y\end{aligned}$$

L'output del S-box è `0110`.

Il polinomio $y^4 + 1$ è riducibile, infatti $y^4 + 1 = (y + 1)^4$. Quindi $\mathbb{Z}_2[y]/(y^4 + 1)$ non forma un campo.

Il polinomio $a(y)$ è invertibile $\pmod{y^4 + 1}$ se $\gcd(a(y), y^4 + 1) = 1$. Al solito procediamo con l'algoritmo di Euclide

$r(x)$	$q(x)$		$s(x)$	$t(x)$
$y^4 + 1$	$--$		1	0
$y^3 + y^2 + 1$	$y + 1$		0	1
$y^2 + y$	y	$y^4 + 1 = (y^3 + y^2 + 1)(y + 1) + (y^2 + y)$	1	$y + 1$
1	$y^2 + y$	$(y^3 + y^2 + 1)y + 1$	y	$y^2 + y + 1$
0	$\cdots$			

Come è facile verificare, $a^{-1}(y) = y^2 + y + 1$.

Noto $M(y)$, lo S-box inverso è composto dai seguenti passi.

- Si calcola

$$\begin{aligned}N(y) &= M(y)a^{-1}(y) + a^{-1}(y)b(y) \bmod (y^4 + 1) = \\ &= M(y)(y^2 + y + 1) + (y^3 + y^2) \bmod (y^4 + 1)\end{aligned}$$

- A partire da $N(y)$ si costruisce il polinomio $N^{-1}(x) \in GF(16)$.
- Si calcola l'inverso $N(x)$.

La sequenza `1000` corrisponde al polinomio $M(y) = y^3$. Il polinomio N(y) vale:

$$\begin{aligned}N(y) &= y^3(y^2 + y + 1) + (y^3 + y^2) \bmod (y^4 + 1) = \\ &= y^5 + y^4 + y^2 \bmod (y^4 + 1) = \\ &= y + 1 + y^2 = y^2 + y + 1\end{aligned}$$

Il polinomio da invertire in GF(16) è $N^{-1}(x)x^2 + x + 1$ che ha come inverso $(x^2 + x)$. Infatti:

$$\begin{aligned}(x^2 + x + 1)(x^2 + x) &= x^4 + x^3 + x^2 + x^3 + x^2 + x = x^4 + x \pmod{x^4 + x + 1} \\ &= (x + 1) + x = 1\end{aligned}$$

Esercizio 2.4 *Mostrare che* $r(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ *è irriducibile. Trovare l'inverso moltiplicativo di* $(2x + 1) \bmod r(x)$.

Soluzione Se $r(x)$ fosse riducibile, sarebbe divisibile per un polinomio $d(x)$ di grado inferiore (grado uno). I polinomi di grado 1 sono:

$$\begin{aligned} x \\ x+1 \\ x+2 \\ 2x = 2 \cdot x \\ 2x+1 = 2(x+2) \\ 2x+2 = 2(x+1) \end{aligned}$$

Non considerando i polinomi che sono uguali a meno di una costante moltiplicativa, restano tra polinomi: $x, x+1, x+2$:

$$x^2 + 1 = x \cdot x + 1 \tag{2.5}$$
$$x^2 + 1 = (x+2)(x+1) + 2 \tag{2.6}$$
$$\tag{2.7}$$

Quindi $(x^2 + 1)$ non è riducibile.
Per calcolare $(2x + 1)^{-1}$ usiamo l'algoritmo di Euclide:

$r(x)$	$q(x)$		$s(x)$	$t(x)$
x^2+1	$--$		1	0
$2x+1$	$2x+2$		0	1
2	$\cdots$	$x^2+1 = (2x+2)(2x+1)+2$	1	$x+1$
$\cdots$				

Per comodità si riporta la divisione $\frac{x^2+1}{2x+1}$. Nello svolgimento ricordiamo sempre che $x^2 = -1 = 2$.

$$\begin{array}{rrr|l} x^2 & & +1 & -x+1 \\ \cline{4-4} x^2 & -x & & -x-1 \\ \cline{1-2} & x & +1 & \\ & x & -1 & \\ \cline{2-3} & & 2 & \end{array}$$

Quindi possiamo scrivere che

$$(2x + 1)(x + 1) \bmod (x^2 + 1) = 2$$

e l'inverso di $2x + 1$ sarà $(-x - 1) \equiv (2x + 2)$.

Alternativamente potevamo calcolare l'inverso come $(2x + 1)^{9-2} \bmod (x^2 + 1)$ usando Square-and-Multiply.

1	$1^2 \times (2x+1) = (2x+1)$
1	$(2x+1)^2 \times (2x+1) = (-x+1)^3 = -x^3 + 1 = -x(-1) + 1 = x + 1$
1	$(x+1)^2 \times (2x+1) = (x^2+2x+1)(2x+1) = 2x(2x+1) = 4x^2 + x = 2x + 2$

Esercizio 2.5 (Cifrario di Hill su $GF(4)$) *Il messaggio binario in chiaro $P =$ `011000110100` viene cifrato usando un cifrario di Hill su $GF(4)$. Come usale, gli elementi del campo sono la classe dei resti modulo $r(x) = x^2 + x + 1$. Il cifrario usa come chiave una matrice K con dimensione 2×2.*

1. *Dire che condizioni deve rispettare la chiave K.*
2. *Cifrare il messaggio P considerando il caso*
$$K = \begin{pmatrix} 0 & 1 \\ x+1 & x+1 \end{pmatrix}$$
3. *Decifrare il messaggio ottenuto al passo precedente*
4. *Usando la coppia messaggio in chiaro / messaggio cifrato ottenuta ai punti precedenti, effettuare un attacco di tipo* known plaintext *e ricavare la chiave K.*

Soluzione

1. La chiave K deve rispettare le seguenti condizioni:
$$\begin{cases} \det(K) \neq 0 \\ \gcd(\det(K), x^2 + x + 1) = 1 \end{cases}$$
Notare che, poiché operiamo in un campo, la seconda è sempre vera per qualunque K che rispetti la 1.
2. Per prima cosa convertiamo il messaggio binario in elementi di $GF(4)$. Poiché gli elementi sono $\{0, 1, x, x+1\}$ la cosa più semplice è convertire ogni coppia di bit in un polinomio. Pertanto il messaggio diventa:
$$P = \begin{pmatrix} 1 & x & 0 & x+1 & 1 & 0 \end{pmatrix}$$
La chiave è una matrice 2×2, quindi il testo in chiaro deve essere diviso in vettori P_i di due elementi:
$$\begin{aligned} P_1 &= \begin{pmatrix} 1 & x \end{pmatrix} \\ P_2 &= \begin{pmatrix} 0 & x+1 \end{pmatrix} \\ P_3 &= \begin{pmatrix} 1 & 0 \end{pmatrix} \end{aligned}$$
Procediamo quindi applicando la formula:
$$C_i = P_i \cdot M \pmod 4 \tag{2.8}$$
$$\begin{aligned} C_1 &= \begin{pmatrix} 1 & x \end{pmatrix} \begin{pmatrix} 0 & 1 \\ x+1 & x+1 \end{pmatrix} = \begin{pmatrix} x^2+x & x^2+x+1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \end{pmatrix} \pmod{x^2+x+1} \\ C_2 &= \begin{pmatrix} 0 & x+1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ x+1 & x+1 \end{pmatrix} = \begin{pmatrix} x^2+2x+1 & x^2+2x+1 \end{pmatrix} \\ &= \begin{pmatrix} x & x \end{pmatrix} \pmod{x^2+x+1} \\ C_3 &= \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ x+1 & x+1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \end{pmatrix} \pmod{x^2+x+1} \end{aligned}$$
Quindi il testo cifrato C risulta:
$$C = \begin{pmatrix} 1 & 0 & x & x & 0 & 1 \end{pmatrix}$$
che, espresso in binario, diventa $C =$ `010010100001`.

3. Occorre per prima cosa calcolare la matrice inversa della chiave:

$$K^{-1} = \frac{1}{-(x+1)} \begin{pmatrix} x+1 & -1 \\ -(x+1) & 0 \end{pmatrix} = x \begin{pmatrix} x+1 & 1 \\ x+1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 1 & 0 \end{pmatrix} \pmod{x^2+x+1}$$

Nel fare questo calcolo si consideri che $\frac{1}{x+1} \equiv x$, infatti $x(x+1) = x^2 + x = x+1+1 = x$.

Calcoliamo il testo in chiaro:

$$\begin{aligned} P_1 &= \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & x \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & x \end{pmatrix} \pmod{x^2+x+1} \\ P_2 &= \begin{pmatrix} x & x \end{pmatrix} \begin{pmatrix} 1 & x \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2x & x^2 \end{pmatrix} = \begin{pmatrix} 0 & x+1 \end{pmatrix} \pmod{x^2+x+1} \\ P_3 &= \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix} \pmod{x^2+x+1} \end{aligned}$$

Quindi il testo in chiaro è:

$$P = \begin{pmatrix} 1 & x & 0 & x+1 & 1 & 0 \end{pmatrix}$$

4. Dobbiamo costruire una equazione del tipo:

$$\begin{pmatrix} P_i \\ P_j \end{pmatrix} K = \begin{pmatrix} C_i \\ C_j \end{pmatrix}$$

dove le righe P_i, C_i e P_j, C_j sono due coppie testo in chiaro / testo cifrato di lunghezza due.

Risolvendo rispetto alla matrice delle incognite otterremo la chiave. Per risolvere l'equazione la matrice del testo in chiaro deve essere invertibile; dovremo tenere presente questo fatto nello scegliere le righe della matrice.

Fortunatamente la matrice costruita usando P_1 e P_2 va bene, infatti:

$$\det \begin{pmatrix} 1 & x \\ 0 & x+1 \end{pmatrix} = x+1$$

che non è nullo.

Quindi possiamo scrivere:

$$\begin{aligned} K &= \begin{pmatrix} 1 & x \\ 0 & x+1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 \\ x & x \end{pmatrix} = \frac{1}{x+1} \begin{pmatrix} x+1 & -x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ x & x \end{pmatrix} \\ &= x \begin{pmatrix} x+1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ x & x \end{pmatrix} = \begin{pmatrix} x+1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ x & x \end{pmatrix} \\ &= \begin{pmatrix} 1 & x+1 \\ 0 & x \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ x & x+1 \end{pmatrix} = \begin{pmatrix} x^2+x+1 & x^2+x \\ x^2 & x^2 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ x+1 & x+1 \end{pmatrix} \pmod{x^2+x+1} \end{aligned}$$