Euclides i el xifrat de clau compartida, la multiplicació del camperol rus i l'intercanvi de claus

Jordi Pujolàs

Departament de Matemàtica, UdL

11è DITMAE

Centre de Formació Integrat Ferran Sunyer i Balaguer

dissabte 12 de març de 2022

fFSB fundació FERRAN SUNYER I BALAGUER

Ajuntament de Figueres Alt Empordà

UAB Universitat Autònoma de Barcelona

Generalitat de Catalunya Departament d'Educació

Multiplicació del camperol rus

$$13 \times 7 = ??$$

Posem en una columna les meitats successives d'un factor (descartant els residus) i a l'altra els doblats de l'altre factor:

13	7
6	14
3	28
1	56

Algorisme: el producte buscat és la suma dels valors de la 2a columna tals que a la 1a tinguin un valor senar

$$13 \times 7 = 7 + 28 + 56 = 91$$

Multiplicació del camperol rus

L'algorisme funciona perquè podem reduir les operacions a tan sols multiplicar per 2 i sumar 7 ("Double & Add") i fer-les en un ordre determinat pel 13. Si posem

$$A \to \text{ sumar 7}, \quad D \to \text{ multiplicar per 2}$$

i diem "posicions senars $\leftrightarrow$ instrucció DA" i "parells $\leftrightarrow$ D", aleshores obviant el darrer 1, anant de baix a dalt i començant per 7 tenim

$$\begin{array}{c|c|c} 13 & s & DA \\ 6 & p & D \\ 3 & s & DA \\ 1 & s & DA \end{array} \quad \to \quad \begin{array}{c|c} D & 14 \\ A & 21 \\ D & 42 \\ D & 84 \\ A & 91 \end{array}$$

$$91 = 2 \cdot (2 \cdot (2 \cdot 7 + 7)) + 7$$

De la 1a columna realment importa la representació en binari de 13. Fes un altre exemple: $17 \cdot 19$?

Aritmètica del rellotge

Si els humans calculem amb enters, els ordinadors amb residus.
Exemple: si son les nou i passen 4 hores, seran la una:

$$9 + 4 = 13 \equiv 1 \pmod{12}$$

i no les 13 ni les 25. Si son les onze i passen tres vegades 9 hores seran les dues

$$11 + 3 \cdot 9 = 38 \equiv 2 \pmod{12}.$$

Els ordinadors calculen residus en rellotges amb moltíssimes hores.
Exemple:

$$31^2 \pmod{71} \equiv 38, \qquad \underbrace{7^{41}}_{35\text{dígits}} \pmod{311} \equiv 169$$

Ei: $7^{41} = 44.567.640.326.363.195.900.190.045.974.568.007$;-O
Aquestes operacions les fan amb un algorisme bessó del camperol rus que fa servir "elevar al quadrat" en lloc de "multiplicar per 2" i "multiplicar" enlloc de "sumar": S $\leftrightarrow$ D, X $\leftrightarrow$ A

Exponenciació binària

Es vol calcular

$$b^k \pmod{p}$$

- Expressar k en binari (amb el bit més significatiu a l'esquerra)
- Convertir els 1's en "SX" i els 0's en "S".
- Obviar el bit 1 de més a l'esquerra (i per tant la primera instrucció SX)
- Efectuar les operacions a b de manera seqüencial i d'esquerra a dreta

$S \rightarrow$ elevar al quadrat mòdul p

$X \rightarrow$ multiplicar per 2 mòdul p

Exponenciació binària

Exemple:

$$7^{13} \pmod{23} = ??$$

$$13 = (1101)_2 \rightarrow SXSXSSX \rightarrow SXSSX$$

$$\begin{array}{c|c} S & 7^2 \pmod{23} \equiv 49 \pmod{23} \equiv 3 \\ X & 3 \cdot 7 \pmod{23} \equiv 21 \\ S & 21^2 \pmod{23} \equiv (-2)^2 \pmod{23} \equiv 4 \\ S & 4^2 \pmod{23} \equiv 16 \\ X & 16 \cdot 7 \pmod{23} \equiv 112 \equiv 20 \end{array}$$

Intercanvi de claus de Diffie-Hellman

El protocol fixa uns paràmetres (g, m), les claus secretes de dos comunicants son k_1, k_2 i les respectives claus públiques $g^{k_1} \pmod m, g^{k_2} \pmod m$. Aleshores la clau compartida pels dos comunicants és

$$g^{k_1 k_2} \pmod m = g^{k_2 k_1} \pmod m = g^{k_1 k_2} \pmod m$$

El fet d'estar als exponents fa que s'estableixi comunicació entre les dues parts mantenint segures les claus secretes: calcular exponents és un problema difícil que no se sap solucionar gaire més bé que anar provant.

Exemple:

$$(g, m) = (7, 23), k_1 = 13, k_2 = 5$$

$$g^{k_1} \pmod m = 7^{13} \pmod{23} \equiv 20$$

$$g^{k_2} \pmod m = 7^{5} \pmod{23} \equiv 17$$

$$20^{5} \pmod{23} \equiv 10$$

$$17^{13} \pmod{23} \equiv 10$$

Advanced Encryption Standard

AES Video

1 caràcter ASCII $\leftrightarrow$ 1 byte $\leftrightarrow$ 2 hexadecimals

$$02 \to 00000010 \to 0x^7 + 0x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 1x + 0 = x$$

$$aa \to 10101010 \to 1x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x + 0 = x^7 + x^5 + x^3 + x$$

$$\dots$$

$$m(x) = x^8 + x^4 + x^3 + x + 1 \equiv 0$$

Com que

$$x(x^7 + x^3 + x^2 + 1) = 1 \pmod{m(x)}$$

la component de l'AES anomenada S-box envia 02 a $10001101 = b_7 b_6 \dots b_1 b_0$, i després fa una transformació lineal fixa...

Advanced Encryption Standard

$$\begin{pmatrix} s_0 \\ s_1 \\ s_1 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Per tant $02 \leftrightarrow 77$, i per a un bloc de dos hexadecimals qualsevol, es fa el mateix: la S-box calcula l'invers en l'aritmètica del rellotge en versió polinomis: amb un rellotge de $m(x)$ hores ;-)

Enters $\leftrightarrow$ Polinomis

AES S-Box càlculs tabulats per Kaisa Nyberg

Algorisme d'Euclides per al $mcd(a, b)$

- Fer la taula de divisions successives $a = q \cdot b + r$ amb el residu viatger fins arribar al residu $mcd(a, b) = mcd(b, r)$, el darrer diferent de 0.

	q_1	q_2	q_3	$\dots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\dots$	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4	$\dots$	$r_n = mcd(a, b)$	0	

S'aprofiten els càlculs d'aquest algorisme per a calcular inversos amb l'aritmètica del rellotge sempre que a i b no comparteixin factors comuns, $mcd(a, b) = 1$. Cal:

- reconstruir la identitat de Bézout

$$1 = u \cdot a + v \cdot b$$

a partir de la taula anterior posant cada residu com $r = D - q \cdot d$ començant pel residu $r_n = 1$. Observeu que a cada divisió efectuada es compleix $r_{i-1} = q_{i+1} r_i + r_{i+1}$

Algorisme d'Euclides

- trobar u, v amb la divisió entera per "desplegar residus" remuntant cap a l'esquerra la fila dels residus de la taula, fins que tan sols quedin a i b. Sempre s'arriba a la identitat de Bézout!
- $b^{-1} \pmod{a} = v \pmod{a}$ i també $a^{-1} \pmod{b} = u \pmod{b}$

Exemple:

$$17^{-1} \pmod{23} = ??$$

	1	2	1	5
23	17	6	5	1
6	5	1	0	

$$1 = 6-1\cdot 5 = 6-1\cdot(17-2\cdot 6) = 3\cdot 6-17 = 3\cdot(23-17)-17 = 3\cdot 23-4\cdot 17$$

$$17^{-1} \pmod{23} \equiv -4 \pmod{23} \equiv 19$$

$$17 \cdot 19 = 323 = 322 + 1 = 14 \cdot 23 + 1$$

Exemple:

$$34^{-1} \pmod{55} = ??$$

	1	1	1	1	1	1	1	2
55	34	21	13	8	5	3	2	1
21	13	8	5	3	2	1	0	

$$1 = 3-1\cdot 2 = 8-5-1\cdot(5-3) = 8-2\cdot 5+3 = 21-13-2\cdot(13-8)+(8-5) =$$

$$21-3\cdot 13+3\cdot 8-5 = 55-34-3\cdot(34-21)+3\cdot(21-13)-(13-8) =$$

$$55-4\cdot 34+6\cdot 21-4\cdot 13+8 = 55-4\cdot 34+6\cdot(55-34)-4\cdot(34-21)+21-13 =$$

$$7\cdot 55-14\cdot 34+5\cdot 21-13 = 7\cdot 55-14\cdot 34+5\cdot(55-34)-(34-21) =$$

$$12\cdot 55-20\cdot 34+21 = 12\cdot 55-20\cdot 34+(55-34) = 13\cdot 55-21\cdot 34$$

$$34^{-1} \pmod{55} \equiv -21 \pmod{55} \equiv 34$$

Bonus:

$$\frac{55}{34} = 1 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{2}}}}}}$$

Gràcies