11è Dissabte Transfronterer de les Matemàtiques de l'Alt Empordà
"Euclides i el xifrat de clau compartida, la multiplicació del camperol rus i l'intercanvi de claus"

Taller Dissabte, 12 de març de 2022

Activitat 1: **Diffie-Hellman** Per a aquesta activitat, els participants del taller es distribueixen per parelles, i els monitors disposen d'un registre de les parelles participants. Aquesta primera activitat consisteix a simular un intercanvi de claus entre els dos integrants de cada parella.

i) Cada participant A_i identifica la seva clau secreta a partir de la seva data de naixement, com en el següent exemple: com que A_i ha nascut el 12 de març del 2008, aleshores la clau secreta de A_i és

$$k_{s_i} = 12 + 03 + 08 = 23$$

Amb una mica de sort, aquest nombre hauria de complir $1 < k_{s_i} < 52$ i no hauria d'haver-hi massa repeticions de claus entre els assistents. Encara que hauria de ser secreta, comuniqueu amb discreció la vostra clau als monitors del taller, per si apareix alguna inconsistència. Si hi ha repeticions o alguna clau surt de rang, el monitor sumarà una xifra aleatòria a k_{s_i} si cal i reduirà el resultat mòdul 53.

ii) El protocol de Diffie-Hellman que farem anar té paràmetres

$$(g, m) = (2, 53)$$

iii) Cadascun dels assistents calcula la seva clau pública k_{p_i} a partir de la seva clau secreta k_{s_i} amb llapis i paper seguint l'algorisme del camperol rus explicat a la xerrada:

$$k_{p_i} = 2^{k_{s_i}} \pmod{53}$$

- Expressar k_{s_i} 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

$$S \rightarrow \text{ elevar al quadrat mòdul 53}$$
$$X \rightarrow \text{ multiplicar per 2 mòdul 53}$$

iv) Quan acaba de fer el càlcul de la seva clau pública, cada participant A_i s'aixeca de la cadira i porta un paperet amb la seva **clau pública** k_{p_i} al monitor SCHM, que fa de canal segur.

vi) El monitor SCHM efectua l'intercanvi de claus : dona a cada membre de la parella $\{A_i, A_{i+1}\}$ la clau pública de l'altre. Per exemple, SCHM dóna k_{p_1} a A_2 i k_{p_2} a A_1.

vii) Els membres de cada parella tornen al seu lloc i calculen la clau k_c que *compartiran* amb la seva parella quan vulguin establir una comunicació segura. Per exemple, a la primera parella (A_1, A_2) el participant A_1 calcula

$$k_{p_2}^{k_{s_1}} \pmod{53}$$

i el participant A_2 calcula

$$k_{p_1}^{k_{s_2}} \pmod{53}.$$

Els càlculs cal fer-los seguint l'algorisme del camperol rus de nou. Si tot ha anat bé tindrem un únic valor $k_{p_2}^{k_{s_1}} \pmod{53} = k_{p_1}^{k_{s_2}} \pmod{53}$, que és la clau compartida k_c pels integrants de la parella.

viii) En acabat, cada membre de la parella s'aixeca de la cadira i mostra el seu resultat al SCHM.

ix) El SCHM verifica que els dos valors calculats pels membres dela mateixa paerlla coincideixen i dona per establerta la comunicació entre ells. Resulten premiades les tres primeres parelles en establir comunicació, segons l'ordre validat pel SCHM.

Activitat 2: **AES** A la segona activitat, els participants de cada parella xifren la seva clau compartida k_c de l'activitat anterior amb una versió ultrasimplificada de l'Advanced Encryption Standard, el criptosistema de clau simètrica de la xerrada. Si no s'ha pogut trobar la clau compartida, alternativament cada participant xifra la seva clau secreta k_{s_i}.

i) Per xifrar k_c es calcula

$$k_c^{-1} \pmod{53}$$

seguint l'algorisme d'Euclides.

- Fer la taula de divisions successives $D = q \cdot d + r$ fins arribar al residu 1.

	q_1	q_2	q_3	$\dots$	q_{n-1}	q_n	q_{n+1}
53	k_{s_i}	r_1	r_2	$\dots$	r_{n-2}	r_{n-1}	$r_n = 1$
r_1	r_2	r_3	r_4	$\dots$	$r_n = 1$	0	

- Cal reconstruir la identitat de Bézout

$$1 = u \cdot 53 + v \cdot k_c$$

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

$$r_{i-1} = q_{i+1} r_i + r_{i+1}$$

- Per trobar u, v cal anar substituïnt i remuntant cap a l'esquerra la fila dels residus de la taula, fins que tan sols quedin el 53 i la clau k_c. Sempre s'arriba a la identitat de Bézout!

- El resultat és $k_c^{-1} \pmod{53} = v$.

ii) Cada participant calcula $v \pmod{53}$. Atenció que si v surt negativa cal sumar-li 53 les vegades que calgui fins que es compleixi $0 \leq v \leq 53$.

iii) Cada participant efectua el producte $k_c \cdot v = 1 \pmod{53}$ i el mostra als monitors. Les tres parelles que xifrin la clau més ràpidament tenen premi.