Si ho amague, ho trobes?
Aritmètica del rellotge

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

El xifrat RSA

Aquest mètode es basa en la dificultat de trobar els factors primers d'un número n que siga producte de dos primers molt granes. En principi és el mateix tenir els dos números primers que tenir el seu producte: donats dos números es fàcil multiplicar-los, i donat un número és teòricament possible factoritzar-lo en producte de números primers[1]. Però quan parlem d'un número de dimensió 1024 bits (309 xifres en sistema decimal), intentar factoritzar-lo és computacionalment impracticable.

Els ordinadors troben amb rapidesa números primers grans i també poden multiplicar-los en una mil·lèsima de segon per tal d'obtenir un resultat de dues-centes xifres. Per exemple, açò es fa cada vegada que es visita una pàgina segura, el navegador genera sobre la marxa una nova clau d'usar i tirar. Però, quan costa descompondre en factors primers un número amb dues-centes xifres? És pràcticament impossible, açò és el que garanteix la seguretat del sistema.

El RSA és un algoritme asimètric que xifra en bloc y que utilitza una clau distribuïda públicament i altra privada guardada en secret pel seu propietari. Si dues persones A i B es volen comunicar amb aquest mètode és el receptor B qui té *tota* la clau; l'emissor A coneix la part pública de la clau, que serveix per xifrar missatge. El receptor guarda acuradament la part privada de la clau, que val per desxifrar.

Anem a fer tots plegats els passos que s'han de seguir per enviar un missatge. Per tal d'entendre bé el procés utilitzarem números petits i xifrarem caràcter a caràcter. Calcula cadascun dels valors dels passos i completa les taules.

1. Generación de las claves (por parte del receptor del mensaje)

Pas 1. El receptor B selecciona dos números primers suficientment grans, p y q.
Per exemple, p =17 i q =2.

Pas 2. Troba $N = p \times q = 17 \times 2 = 34$.

Pas 3. Calcula la funció indicador d'Euler: $\Phi(N) = (p-1)\cdot(q-1) = 16 \times 1 = 16$

Aquesta funció ens proporciona la quantitat de números primers relatius amb N i menors que N. Açò vol dir que hi ha 16 números enters x, tals que mcd (34, x)=1.

Pas 4. Selecciona un número e menor que $\Phi(N)$ i tal que mcd(e, $\Phi(N)$) = 1. Agafem e =3 posat que mcd (3,16) = 1.

[1] Una forma possible de descompondre un número n en els seus factors és provar a dividir-lo por tots els números enters positius compresos entre 2 i l'arrel de n. Per suposat, al llarg del temps els matemàtics han inventat altres mètodes de factorització més eficients, però cap d'ells ha aconseguit un algoritme amb un ordre de complexitat que permeta factoritzar en un temps raonable números tan grans com els utilitzats en RSA actualment, tot i amb la potència dels millors ordinadors d'avui en dia.

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

Pas 5. Calcula l'invers de e en un rellotge amb $\Phi(N)$ hores. És a dir el número d que verifique que: $e \times d \equiv 1 (\text{mod } \Phi(N))$
Si $e = 3$ pots comprovar que $d = 11$, si el rellotge té 16 horas: $3 \times 11 = 33 = 1 (\text{mod} 16)$
Precisament el petit teorema de Fermat i el resultat d'Euler garanteixen que aquest número existeix i és únic. Els càlculs anteriors es poden fer amb relativa facilitat. Per obtenir d es pot gastar l'algoritme estès d'Euclides (consulta l'apartat per a saber més)

Pas 6. La clau pública està constituïda per $(N, e) = (34, 3)$ i la secreta per $(N, d) = (34, 11)$
Ara que B ja té la clau, anuncia la part pública a tothom que ens vulga enviar missatges (la mateixa clau pública serveis per a qualsevol persona que se vulga comunicar amb ell). La clau secreta la conserva amb zel el receptor. Aquest parell de claus és tal que tot i coneixent una d'elles és quasi impossible calcular l'altra.

2. Xifrat del missatge (per part de l'emissor)

Per xifrar, l'emissor A realitza els passos següents:
Pas 7. Localitza la clau pública del destinatari per tal de conèixer els valores de **N** i e.
En el nostre cas: $(N, e) = (34, 3)$

Pas 8. Utilitza la funció: $C \equiv M^e \ (\text{mod } N)$ sent M del missatge original i C del xifrat.

Text clar	V	I	E	N	È	S
Text expressat en números (M)	26	8				
Missatge xifrat $C \equiv M^e \ (\text{mod } N)$	32	2				

Pas 9. Envia al destinatari el criptograma C.

3. Desxifrat del criptograma per pare del receptor

Pas 10. Si el destinatari B vol recuperar el missatge que ha rebut fa servir la seva clau privada d per a calcular: $M \equiv C^d \ (\text{mod } N)$

Text rebut	32	2	30	21	30	25
Text desxifrat: $D = C^d \ (\text{mod } N)$	26	8				
Text clar	V	I				

Amb aquest exemple has après a xifrar utilitzant un sistema de clau pública però no oblides que en realitat és prou més complicat ja que en la nostra simulació s'han usat valors de p, q i e molt petits i s'ha xifrat caràcter a caràcter. En la realitat es fan servir números primers enormes i es xifra en bloc però açò requereix l'ús de càlculs tan enormes que fan falta ordinadors de gran potència per calcular-los.

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL