UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Superior d'Enginyeries Industrial, Aeroespacial i Audiovisual de Terrassa

Treball Fi de Diploma

Criptosistemes de clau pública: són segures les teves comunicacions?

Public key cryptosystems: Are your comunications safely?

Autor: MªÁngeles Lozano Corella

Tutor:Albert Masip-Álvarez

Diploma en ciència tecnologia i societat

2023

It may well be doubted whether human

ingenuity can construct an enigma of this

kind which human ingenuity may not,

by proper application,resolve

(E.A.Poe,El escarabajo de oro)

Es pot dubtar de si l'enginy humà
pot construir un enigma d'aquest tipus
que l'ingeni humà no pot resoldre,
mitjançant l'aplicació adequada.
(E.A.Poe,El escarabajo de oro)

Resum

Des de el S.V aC els espartans i atenencs ,ja van utilitzar un mètode criptogràfic per a guanyar la guerra, anomenat Scitala. Després els romans també van utilitzar missatges xifrats. La Xifra de Cèsar : consistia en la substitució de determinades lletres per altres lletres segons una regla fixa.

I així, fins avui, que amb la societat de la informació estem contínuament enviant i rebent missatges per la qual cosa necessitem que hi hagi uns protocols, que ens garanteixen la seguretat d'aquests. Per això miraré d'esbrinar com funciona la RSA: Criptosistemes de Clau Pública, que és un dels mètodes que utilitzen varis estaments públics per garantir la seguretat de les nostres comunicacions.

Paraules clau: missatges, algoritmes ,xifrat i desxifrat.

Abstract

From the S.V BC the spartans and athenians, they already used one a cryptographic method mode to win the war,called Scitala ,later the romans also used encrypted messages,Caesar's Cipher:consisted of the substitution of certain letters by other letters according to a fixed rule.

And so until today that with the information society,we are continuously receiving messages.Therefore, we need to have protocols,which guarantee the security of these.So I will try to find out how RSA works;Public Key Cryptosystems, methods used by various public authorities to guarantee the security of our communications.

Key words:messages,algorithms,encryption and decryption,

Índex de continguts

1.Introducció

Justificació: Em va interessar aquets tema després de veure la pel·lícula “The Imitation Game” on el matemàtic Alan Turing junt amb un equip de criptoanalistes, van desxifrar els codis secrets que els nazis utilitzaven a la màquina Enigma durant la Segona Guerra Mundial. Aquest fet va contribuir a que Alemanya perdés la guerra i a evitar milers de morts. Aquesta fita històrica m’ha portat a interessar-me pel llenguatge secret dels codis que utilitzem a diari sense ser-ne conscients.

Actualment tota la informació la tenim en format digital i això ens facilita la rapidesa, transport i ús d’aquesta al mateix temps, però, ens comporta problemes de seguretat amb les dades sensibles de salut, financeres, telefòniques o de xarxes socials a les que no tothom hauria de tenir-hi lliure accés, únicament aquelles persones o entitats autoritzades.

Des de la implantació l’any 1999 de la llei Oficial de Protecció de Dades (LOPD), tots els organismes oficials estan obligats a garantir la seguretat de les nostres dades. Un dels mitjans que s’utilitzen per aconseguir-ho és la criptografia i un dels mètodes més utilitzat fins ara la RSA, que ja s’està superant amb els ordinadors quàntics.

2.Objectius

General: Esbrinar com la criptologia asimètrica o de clau pública (RSA) ens proporciona comunicacions segures a través de canals insegurs, és a dir, permet que dues persones A i B puguin enviar missatges per un canal que pugui ser interceptat per una tercera persona E, de manera que només les persones autoritzades A i B puguin llegir el missatge. Concretament veurem la part matemàtica basada en les

propietats dels nombres primers en la que es fonamenta la RSA per les següents finalitats:

- Generar claus
- Xifrar els missatges
- Desxifrar els missatge

Específic: aplicar la Criptografia de Clau Pública (RSA) a una de les seves aplicacions: la signatura digital.

3.Metodologia

Consulta de llibres i articles de la referència sobre tècniques criptogràfiques de protecció de dades. Intentar mitjançant exercicis entendre el criptograma RSA. Entrevistar a encarregats de gestionar la firma digital de Greintec (Gremi d'instal·ladors Terrassa i Comarca)

Capítol 1. mètodes matemàtics utilitzats en criptografia: l'RSA

1.1 Conceptualització

La Criptografia Asimètrica o Criptografia de Clau Pública, és un mètode criptogràfic que utilitza un parell de claus per a l'enviament de missatges:

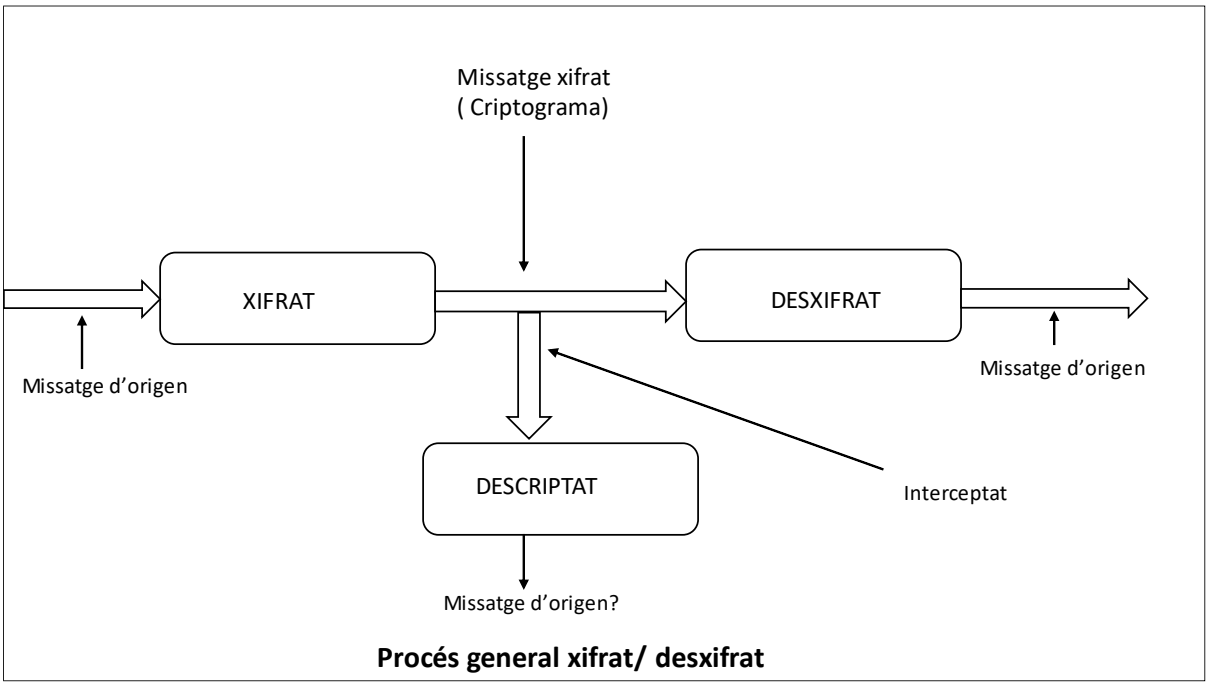
- Clau pública : s'utilitza per xifrar els missatges
- Clau privada: s'utilitza per desxifrat els missatges

Què esperem d'un sistema criptogràfic? :

- Autenticitat : establir una cosa o persona com l'autenticitat
- Confidencialitat: assegurar-se que la informació es només accessible per a les persones amb accés autoritzat.
- No repudiació : permet provar que les dades han estat enviades i que ni emissor ni/o receptor poden negar la emissió i/o recepció.
- Integritat : assegurar-se que la informació no ha estat modificada.

En criptografia ,l'RSA és un algoritme de xifratge de clau pública, fou descrit per Ron Rivest, Adi Shamir i Len Adleman a l'institut de Tecnologia de Massachusetts el 1977.Les lletres RSA corresponen a les inicials del seus cognoms.

És el primer i més utilitzat algoritme d'aquest tipus i és vàlid tan per xifrar com per signar digitalment. La seguretat d'aquets algoritme rau en el problema de la factorització de nombres enters. Aquest algoritme RSA serà segur mentre no el superi la Criptografia Quàntica.



Procés general xifrat/ desxifrat

1.1.1 Nombres primers i coprimers

Definició: Un nombre p>1 es denomina primer si és divisible entre 1 i p únicament, de manera que p=1·p. Així, es compleix que p no pot ser descrit pel producte de dos nombres positius més petits. Serien exemples de nombres primers el 2,5,7,13,19...

1.1.2 El teorema fonamental de l'aritmètica

El teorema fonamental de l'aritmètica afirma que cada nombre natural pot ser descrit com el producte de nombres primers; tot i no ser evident, cada descomposició és única. Per exemple, $50=2\cdot5^2$ o $130=2\cdot5\cdot13$.

Hi ha un problema en la factorització de nombres enters, ja que quan volem descriure un nombre molt gran no trobem cap algoritme clàssic que resolgui el problema en un temps polinòmic. L'algoritme RSA depèn de la seva impossibilitat.

1.1.3 Quants nombres primers hi ha?

El teorema d'Euclides afirma que hi ha infinits nombres primers. Per demostrar aquesta afirmació suposem que tenim una llista de nombresprimers:p_1, p_2,p_3, ,,,,,p_r veurem com hi ha un nombre primer que no consta en la llista. Suposem que tenim un numero N, on N= p_1, p_2.p_3, ,,,,,p_{r+1}. Si N no és divisible per cap nombre primer, llavors N és primer (i no apareixia en la llista). Si N és divisible entre un nombre primer p, llavors aquest nombre p no estava en la llista, ja que p : (N- p_1, p_2.p_3, ,,,,,p_r)= p:1 .Per exemple tenim una llista amb els nombres 13,19,17,23. Tenim N=13·19·23·17+1=96578. El nombre 96578 é p_1, p_2.p_3, ,,,,,p_{r+1}s divisible entre 2, de manera que 2 és primer i no estava en la llista.

Podem demostrar el teorema d'Euclides pel mètode de reducció al absurd: suposem que tenim un p màxim. Si agafem un nombre N, tal que N= p_1, p_2.p_3, ,,,,,p_{max+1},N serà un nombre primer major que p màxim ja que no és divisible entre cap nombre primer, donant de residu 1; això fa que N=N·1. Per exemple: suposem que 7 és el nombre primer més gran. Si N=2·3·5·7+1=211, 211 és un nombre primer major que 7.

1.4 La funció φ d'Euler

Hi ha nombres que són primers entre ells, és a dir, només tenen com a comú divisor l'1 i el -1; aquests nombres també s'anomenen nombres coprimers. La funció φ d'Euler afirma que quan n és un nombre enter positiu, llavors φ(n) és el numero de nombres enters positius menors que n i que són coprimers amb n. Per exemple: φ(7)=6, ja que 1,2,3,4,5,6 són coprimers amb 7 i menors que ell. Així com φ(6)=2

(1,5) i φ(12)=4 (1,5,7,11). Aquesta funció dona lloc a diferents propietats que podem utilitzar:

- Si n és un nombre primer p, llavors φ(p)=p-1: φ(13)=12, φ(7)=6 o φ(5)=4.
- Si n és un nombre primer p, llavors φ(pk)=pk-pk-1=pk·(1-1:p): φ(25)=φ(52)= 52·(1- 1:5)=20 o φ(343)=φ(73)=73·(1-1:7)=294.
- Si dos nombres m i n són coprimers, llavors φ(m·n)= φ(n)·φ(m): φ(13·7)=φ(91)=φ(13)·φ(7)=12·6=72 o φ(4·3)=φ(12)=φ(4)·φ(3)=2·2=4.
- Si un nombre n=p1k·p2k'·p3k''·...·pmk^ m-1, es compleix que φ(n)=n·(1-1:p1)·(1-1:p2)·...·(1-1:pm): si n=22·73·3=4116, φ(4116)=4116·(1-1:2)·(1-1:7)·(1-1:3)=1176.

1.2 Aritmètica modular

El fet de classificar els nombres en parells i imparells és una eina summament poderosa. Els nombres parells deixen residu 0 quan els dividim entre 2 i els imparells residu 1. La idea és que, si substituïm el numero 2 per qualsevol nombre n, llavors els nombres es poden classificar en funció del residu que deixen al dividir-los entre n.

Definició: diem que dos nombres a i b són congruents mòdul n si deixen el mateix residu quan els dividim entre n. Tenim llavors que si a=q·n+r i b=t·n+r, b-a=(t-q)·n. Diem doncs que a≡b (mod n) quan a és congruent amb b mòdul n. Per exemple,

2=0·3+2, 5=1·3+2, 20=6·3+2 i 29=9·3+2; això implica que 2≡5≡20≡29 (mod 3). Podem observar que cada nombre és congruent mòdul n amb un i només un dels nombres 0,1,2,3,4,...,n-1. Per exemple, cada nombre és congruent mòdul 4 amb 0,1,2 o 3: 221=4·55+1 o 221≡1 (mod 4).

1.2.1 Propietats

Si tenim que a≡b (mod n) i c≡d (mod n), llavors a+c≡b+d (mod n), a-c≡b-d (mod n) i a·c≡b·d (mod n). Per exemple, operem 639·437 (mod 7): 639=7·91+2 i 437=7·62+3. Per tant, 639≡2 (mod 7) i 437≡3 (mod 7). Si apliquem la propietat anterior, tenim que 639·437≡2·3≡6 (mod 7); el resultat és 6. Operem ara 632^2 (mod 633): 632=633·1-1. Tenim que 632≡-1 (mod 633), per tant, $632^2≡(-1)^2$ (mod633), el que implica que $632^2≡1$ (mod 633); el resultat és 1.

1.2.2 L'INVERS D'UN NOMBRE

Què trobem quan intentem dividir, per exemple, 2:3 (mod 7)? 2:3=2·(1:3) i $1:3=3^{-1,}$ però, què és llavors l'invers d'un nombre mòdul n? Trobem que l'invers d'a mòdul n és un nombre enter b mòdul n tal que a·b≡1 (mod n), que és igual a a^{-1} (mod n). Exemplifiquem-ho resolent 2:3 (mod 7): 2:3=2·(1:3) (mod 7), $1:3=3^{-1}$ (mod 7) i 3·5=7·2+1; això implica que 5 sigui l'invers de 3 (mod 7), ja que 3·5≡1 (mod 7). Com que $2·3^{-1}=2·5=10$ (mod 7) el resultat és 10. Hem de tenir en conte que l'invers d'un nombre mòdul n no sempre existeix. Per exemple, no existeix l'invers de 3 (mod 6), ja que 0·3≡0 (mod 6), 1·3≡3 (mod 6), 2·3≡0 (mod 6), 3·3≡3 (mod 6), 4·3≡0 (mod 6) i 5·3≡3 (mod 6).

Computació d'inversos

L'algoritme d'Euclides és un mètode eficaç que serveix per trobar el màxim comú divisor de dos nombres. Posem un exemple per explicar com funciona: m.c.d (48,18)=6. Primer dividim el nombre gran entre el petit: 48=18·2+12. A continuació, dividim el divisor anterior entre el residu: 18=12·1+6. Repetim el procediment fins a obtenir residu 0; el divisor és llavors el resultat: 12=6·2+0. Provem-ho amb nombres més grans; m.c.d (1934,128)=2: 1934=128·15+14, 128=14·9+2 i 14=2·7+0. Fem el m.c.d (1448,1936)=8: 1936=1448·1+488, 1448=488·2+472, 488=472·1+16, 472=16·29+8 i 16=8·2+0. Computem també el m.c.d (252,105)=21: 252=105·2+42, 105=42·2+21 i 42=21·2+0. Podem observar que si 21 és el m.c.d (252,105) també és el m.c.d (105,252- 105), és a dir, de 105 i 147. Tenim doncs que el m.c.d pot ser expressat com la suma de dos nombres originals, cadascun multiplicat per un nombre enter. Si dos nombres a i n són coprimers, llavors l'invers d'a mòdul n existeix. Segons l'algoritme d'Euclides, hi ha nombres enters x,y tals que $x \cdot a+y \cdot n=1$ i $x \cdot a-1=-y \cdot n$. Si $x \cdot a \equiv 1 \pmod{n}$, llavors x és l'invers d'a mòdul n per definició. D'aquesta manera, podem computar inversos mòdul n molt eficaçment utilitzant l'algoritme d'Euclides; trobarem l'invers de 8 (mod 11): el m.c.d (8,11)=1 (són coprimers), ja que 11=8·1+3, 8=3·2+2, 3=2·1+1 i 2=1·2+0. Tenim llavors que 3=11-8, 2=8-2(3) i 1=3-2. Ara operem i substituïm: 1=3-(8-2·3), 1=3-8+2(3), 1=3(3)-8, 1=3(11-8)-8, 1=3(11)-3(8)-8 i 1=3(11)-4(8). Per tant, $1 \equiv -4(8) \pmod{11}$; com que -4+11=7,canvie el -4 pel 7. Obtenim llavors que $1 \equiv 7 \cdot 8 \pmod{11}$; així, 7 és l'invers de 8 (mod 11).

1.2.3 EL TEOREMA D'EULER

El teorema d'Euler afirma que si tenim un nombre m>1 i un altre nombre enter a, i a i m són coprimers, llavors $a^{\varphi(m)}=1 \pmod m$. Aquest teorema és útil quan volem trobar residus de divisions molt grans;per exemple, el residu de 3^{50} entre 14 (a=3, m=14): $3^{\varphi(14)}=1 \pmod{14}$, $\varphi(14)=\varphi(7\cdot2)=\varphi(7)\cdot\varphi(2)=6\cdot1=6$ i $3^6=1 \pmod{14}$. Posem 3^{50} en funció de 6 ($50=6\cdot8+2$): $3^{50}=(3^6)^8\cdot3^2\equiv x \pmod{14}$. Resolem l'equació: si $3^6=1 \pmod{14}$, llavos $(1)^8\cdot3^2\equiv x \pmod{14}$; $9\equiv x \pmod{14}$, de manera que 9 és el residu i el resultat que buscàvem. Fem el residu de dividir 7^{63}entre 15 (a=7, m=15): $7^{\varphi(15)}=1 \pmod{15}$, $\varphi(15)=\varphi(3\cdot5)=\varphi(3)\cdot\varphi(5)=2\cdot4=8$ i $7^8=1 \pmod{15}$. Posem 7^{63} en funció de 8 ($63=8\cdot7+7$): $7^{63}=(7^8)^7\cdot7^7\equiv x \pmod{15}$. Resolem l'equació: si $7^8=1 \pmod{15}$, llavors $(1)^7\cdot7^7\equiv x \pmod{15}$; $7^7\equiv x \pmod{14}$, on 7^7 és el residu. Trobem el residu de dividir $(-29)^{30}$ entre 11 (a=-29, m=11): $(-29)^{\varphi(11)}=1 \pmod{11}$, $\varphi(11)=10$ i $(-29)^{10}=1 \pmod{11}$. Posem $(-29)^{30}$ en funció de 10 ($30=10\cdot3$): $(-29)^{30}=((-29)^{10})^3\equiv x \pmod{11}$. Resolem l'equació: si $(-29)^{10}=1 \pmod{11}$, llavos $(1)^3\equiv x \pmod{11}$; $1\equiv x \pmod{11}$, on 1 és el residu.

1.2.4 EL PETIT TEOREMA DE FERMAT

El petit teorema de Fermat anuncia que si p és un nombre primer i a és un nombre que pertany als nombres naturals, llavors $a^p\equiv a \pmod p$. Si a i p són coprimers, llavors $a^{p-1}\equiv1\pmod p$. Aquest teorema té diferents aplicacions; per exemple: verifiquem si $5^{38}\equiv4 \pmod{11}$. Com que 5 i 11 són nombres coprimers,$5^{10}\equiv1 \pmod{11}$. Posem 5^{38} en funció de 10: $38=10\cdot3+8$, per tant, $(5^{10})^3\cdot5^8\equiv1^3\cdot5^8\equiv5^8 \pmod{11}$. $5^8=(5^2)^4$, $5^2=11\cdot2+3$, $5^2\equiv3 \pmod{11}$, $(5^2)^4\equiv3^4$ (mo11), $5^{38}\equiv5^8\equiv3^4\equiv81\equiv4 \pmod{11}$ i $81=11\cdot7+4$. Comprovem així que sí que es verifica. Comprovem si $6^{36}\equiv3 \pmod{13}$: $6^{12}\equiv1$ (mod

13) i 36=12·3; així mateix, $(6^{12})^3=6^{36}$ i $(6^{12})^3\equiv1^3\equiv1$ (mod 13). Per tant, podem afirmar que no es compleix, ja que és congruent amb 1 (mod 13), no amb 3. Calculem el residu de dividir 7^{44} entre 13: $7^{12}\equiv1$ (mod 13) i 44=12·3+8; per tant, ((mod 13), $10^4=(10^2)^2$, $10^2=100=13\cdot7+9\equiv9$ (mod 13), $10^4=(10^2)^2\equiv9^2$ i $9^2=81=13\cdot6+3\equiv3$ (mod 13); el residu és 3.

1.2.5 TEOREMA XINÈS DEL RESIDU

El teorema xinès del residu afirma que si $x\equiv b_1(\text{mod } m_1), x\equiv b_2(\text{mod } m_2)$.....

$x\equiv b_k(\text{mod } m_k)$ llavors el m.c.d $(m_i,m_j) = 1$, sempre que i i j siguin nombres diferents.

Exemplifiquem-ho trobant el valor de x en el següent sistema d'equacions:

$x\equiv4(\text{mod}12)(x=12.k+4)$
$x\equiv3$ (mod 7)

El m.c.d (12,7)=1. $x\equiv3$ (mod 7)=12·k+4, 3-4 (mod 7)=12k, -1=12k (mod 7) i 6 (-1+7)=12k (mod 7). Com que $12\equiv5$ (mod 7), $6\equiv5k$ (mod 7). Trobem el valor de k aconseguint un residu 6: 5=7·0+5 (no), 2·5=7·1+3 (no), 3·5=7·2+1 (no) i 4·5=7·2+6 (sí), el que implica que $k\equiv4$ (mod 7) (7n+4=k). Seguim resolent l'equació: x=12k+4, x=12(7n+4)+4, x=84n+48+4 i x=84n+52, el resultat de l'equació. Resolem ara el sistema d'equacions:

$x\equiv29$ (mod 6) (x=6k+29)

$x\equiv14$ (mod 11)

El m.c.d (6,11)=1. $x\equiv14$ (mod 11)=6k+29 i 14-29=6k. Com que -15=6k, podem dir que 7 (15+11+11) (mod 11)=6k. Trobem llavors el valor de k. Necessitem residu

7:6·1=11·0+6 (no), 6·2=11·1+1 (no) i 6·3=11·1+7 (sí), el que implica que k=3. Si k=3 (mod 7), x=6k+29=6·3+29=47. La x=47.

1.3 Explicació matemàtica de l'algoritme.

Alice elabora la clau pública

Primer triem dos nombres primers aleatoris p i q de l'ordre de 2^{1024} o 2^{4096} aproximadament. Nosaltres exemplifiquem el procés utilitzant nombres més petits, ja que així les operacions són assequibles. Agafem doncs p=3 i q=13.

Computem p·q=n i φ(n). Segons el teorema fonamental de l'aritmètica, la descomposició del nombre n és única: n=3·13=39. Utilitzem la quarta propietat de la funció φ d'Euler per trobar φ(n): 39=3·13, de manera que φ(39)=39·(1-1:3)·(1-1:13)=24.

Triem un nombre aleatori e tal que m.c.d (e,φ(n))=1. El m.c.d (e,24)=1; e=29. El m.c.d (29,24)=1. Ho comprovem amb l'algoritme d'Euclides: 29=24·1+5, 24=5·4+4, 5=4·1+1 i 4=1·4+0.

Fem públics els nombres (n,e), ja que són la clau pública per xifrar el missatge. La clau pública=(39,29).

Bob elabora la clau privada

A continuació, computem d, l'invers d'e mòdul φ(n), de manera que e·d≡1 (mod φ(n)). Computem l'invers de 29 (mod 24) mitjançant l'algoritme d'Euclides: 5=29-24, 4=24-4·5, 1=5-4, 1=5-(24-4·5), 1=5-24+4·5, 1=5·5-24, 1=5(29-24)-24, 1=5(29)-5(24)-24 i 1=5(29)-6(24). Com que 1≡5·29 (mod 24), 5 és l'invers, d=5.

Alice elabora, xifra i envia el missatge

Volem enviar un missatge, m, tal que m sigui un nombre enter, de manera que $1 \leq m < n$. Agafem m=20, ja que $1 \leq 20 < 39$. El missatge xifrat serà M, on $M=m^e \pmod n$. $M=20^{29} \pmod{39}$; per computar aquesta operació, utilitzem el Teorema d'Euler, ja que realment busquem el residu de dividir 20^{29} entre 39: $20^{\varphi(39)}=1 \pmod{39}$, $\varphi(39)=24$ i $20^{24}=1 \pmod{39}$. Posem 20^{29} en funció de 24: $29=24 \cdot 1+5$, així $20^{24} \cdot 20^5 \equiv x \pmod{39}$. $1 \cdot 20^5 \equiv x \pmod{29}$, $20^5 \equiv x \pmod{29}$, $20^5=39 \cdot 82051+11$ i $20^{29} \pmod{39}=11$, obtenint M=11.Enviem el missatge xifrat M, en el nostre cas, M=11.

Bob desxifra el missatge

Per desxifrar el missatge computem $M^d \pmod n$. Observem primer com: $e \cdot d=t \cdot \varphi(n)+1$, de manera que $e \cdot d \equiv 1 \pmod{\varphi(n)}$, on d és l'invers d'e $(\text{mod } \varphi(n))$. $29 \cdot 5=t \cdot 24+1$; si resolem l'equació, tenim que $(29 \cdot 5-1):24=6$, per tant t=6. Si $M=m^e$, llavors $(m^e)^d=m^{e \cdot d}=m^{t \cdot \varphi(n)+1}=(m^{\varphi(n)})^t \cdot m^1$. Observem com $m^1=m$ i $(m^{\varphi(n)})^t=1^t \pmod n \equiv 1 \pmod n$. Tenim així doncs que $(m^{\varphi(n)})^t \cdot m^1 \equiv 1 \cdot m \equiv m \pmod n$, obtenint m, el missatge original. Exemplifiquem-ho: $M=11=20^{29}$, $20^{29})^5=20^{6 \cdot 24+1}=(20^{24})^6 \cdot 20^1$, $(20^{24})^6=1^6 \pmod{39} \equiv 1 \pmod{39}$ i $(20^{24})^6 \cdot 20^1 \equiv 1 \cdot 20 \equiv 20 \pmod{39}$; com podem observar, hem obtingut m=20, el missatge original.

CAPITOL 2 : SIGNATURA DIGITAL

La signatura digital és una aplicació de la la Criptografia de Clau Pública que ens permet signar qualsevol missatge digital de manera anàloga a com signen a la correspondència ordinària. Ja que vàlida la autenticitat e integritat del missatge o document digital.

La signatura digital han de ser fàcils de fer i verificar i difícils de falsificar.

Degut a problemes amb l'ús de les dades personals obtingudes , sobretot de les xarxes socials, s'ha fet necessària la protecció de les dades personals (DP). Tenint en compte que els estats de la UE protegien el dret a la intimitat en el món físic s'ha vist necessari també protegir els ciutadans europeus de les DP digitals recollides informàticament.

Des del 25 de maig de 2018 s'aplica el Reglament Europeu de Protecció de Dades (RGPD) , la Agencia Española de Protección de Datos (AEPD) i l'Autoritat Catalana de Protecció de Dades (APDCAT). El RGPD és un marc normatiu que haurà de ser completat sense cap contradicció per part de les legislacions nacionals.Aquest reglament de la UE i de les agències estatals ha estat necessari degut als constants abusos de gegants tecnològics com Facebook, Google, Twitter, Instagram i altres xarxes socials que podien eludir els controls de les Agències Nacionals de Protecció de Dades (PD).

El passat 5 de març, l'hospital va patir un ciberatac,amb un robatori de dades de pacients i

Professionals ,els ciberatacants van demanar un rescat de 4,5 milions de dòlars per alliberar les dades i no publicar-les ,el govern no va cedir a cap mena de xantatge o extorsió.

2.1 DADES PERSONALS

Ara anem a definir el concepte clau de les dades:

2.1.- QUÈ ÉS UNA DADA DE CARÀCTER PERSONAL ?

Les dades de caràcter personal són qualsevol informació referent a les persones físiques. depenent del tipus de dades aquestes poden ser:

IDENTIFICATIVES (nom, cognoms, DNI, telèfon)

REFERITS a la situació laboral, financera, salut, ...

CATEGORIES ESPECIALS DE DADES (origen ètnic o racial, opinions polítiques, religioses, genètics, orientació sexual, ...)

. **Per què hem de protegir les nostres dades personals?**

Les dades personals pertanyen a la persona a qui es refereixen, cadascú de nosaltres és titular de les seves dades personals, per tant, són propietat nostra, podem decidir a qui les volem donar i a qui no les volem donar si no estem ben segurs, (hi ha algunes excepcions on estem obligats a facilitar-les: contractes laborals, administració pública per a l'exercici de les seves competències...) . Perquè és un dret fonamental: el Dret Fonamental a la Protecció de Dades Personals.

Per tenir el control de les nostres dades, per saber perquè es faran servir, i

especialment protegir el nostre honor i la nostra intimitat personal i Per garantir i

protegir les llibertats públiques i els drets fonamentals de les persones.

2.2 COM S'OBTÉ UN CERTIFICAT DIGITAL

Informació donada per les encarregades de la seva gestió a l'empresa Greintec, de la Cecot de Terrassa, les senyores : Marina Pallàs López i Cristina Sunyer Iranzo.

Un certificat digital el pot obtenir:

- una persona física (a títol personal)
- una persona jurídica (i representa al col·lectiu professional i/o empresarial al que pertany).

La documentació que cal per fer el certificat digital de una persona jurídica :

- Escriptures de constitució de l'empresa.
- Targeta del NIF de l'empresa.
- DNI de la persona de l'empresa que tingui poders.
- Número de telèfon i e-mail que ha de constar al certificat.
- Registre Mercantil.

Per a una persona física cal que acrediti les seves dades amb el DNI .

Els passos són USUARI ⟷ GESTOR ⟷ CERTIFICADORA

La FNMT-RCM (Fábrica Nacional de Moneda y Timbre -Real Casa de la Moneda)

És el proveïdor de serveis de certificació públic a través de CERES (Certificació Espanyola), que permet autentificar i garantir els tràmits amb la Administració, a través d'internet de manera totalment segura.

Només ens cal entrar a la pàgina https://www.cert fnmt.es i seguir les indicacions o bé anar a una gestoria ,per que et facin el tràmit.

El preu d'aquest certificat és de 14 euros i té una validesa de 2 anys, renovables per altres 2anys.

2.3 COM FUNCIONA LA SIGNATURA ELECTRÒNICA?

Per poder utilitzar la signatura electrònica cal haver obtingut prèviament un certificat digital.

La signatura digital es basa en la criptografia asimètrica ,que utilitza dos claus diferents :clau pública i clau privada:

La clau privada ,és una clau que només coneix i posseeix el seu titular, per desxifrar la informació S'emmagatzema en un dispositiu d'ús privat, targeta criptogràfica u ordinador..

La clau pública, pot ser coneguda per tothom ,i és necessària per xifrar la informació.

Aquestes dues claus compleixen dues regles fonamentals:

1. Les dades que es codifiquen amb una només podran descodificar-se amb l'altra.
2. No es pot deduir una clau a partir de l'altra.

Una vegada que tenim el certificat digital ,ja podem fer les gestions signades electrònicament ,i aquesta signatura té el mateix valor legal que la firma manuscrita.

3.CONCLUSIONS

Actualment vivint en una societat digital, quasi totes les nostres activitats ,ja les gestionen via Internet:

- Educació a distància (o bé envien els treball via e-mail)
- Salut a distància, sobre tot arrel de la pandèmia.
- Teletreball.
- Gestions amb les Administracions (declaració de la renda com exemple).
- Gestions amb els bancs.
- Jocs amb qualsevol usuari del món.
- I la relació amb amics i familiars ,mitjançant diferents aplicacions.

Tot això m'ha fet preguntar-me , si són segures les nostres comunicacions?

I per una part he trobat ,que gràcies a la criptografia si tenim cert grau de seguretat i que hi ha lleis a nivell europeu i estatal de protecció de les nostres dades.

A més aquet tipus de comunicació ,ens facilita la vida, és ràpida no perdem temps fent cues i és econòmica ,estalviem paper ; per tant també és més ecològica per el planeta ,encara que també genera una empremta digital.

Però per altre costat , hem tingut noticies de hackeig de dades a Hospitals, intents continus de estafes bancàries ,junt a informacions sobre Intel·ligència Artificial (IA) preocupants. Concretament ,Geoffrey Hinton, pioner a IA ,a una entrevista publicada a The New York Times (1 de maig de 2023),abandona Google i adverteix dels perills d'aquesta tecnologia si no s'utilitza bé.

També crec ,que com usuaris, en general o bé por falta de coneixements o per falta de conscienciació no posem els mitjans necessaris ,per augmentar la seguretat de les nostres comunicacions.

3.2 LIMITACIONS DEL ESTUDI

En primer lloc la falta de temps .

També hauria estat bé , fer una enquesta sobre ús i coneixements del que hi ha darrera de la signatura digital i altres recursos que utilitzen a diari, com xarxes socials.

Veure com es generem les contrasenyes de targes bancaries.

3.3 CONTINUÏTAT DE l'ESTUDI

Veure altres tipus de criptografia com DES (per xifrar textos en blocs de 64 bits) , AES (Advanced Encryption Standard) és un xifrat en blocs de dades de 128 bits i comparar-les amb la RSA.

REFERÈNCIES

Brunet J,M; Ventura E ,(2001): *Informació i Codis*. Ed. .UPC.

Fuster A; De la Guia D; Hernández LL; Montoya F (2003) :Técnicas *Criptograficas. de Protección de Datos.* Ed.Ra-Ma.

Stewart I,(1998):*De aquí al infinito* .Ed. Crítica..

https://es.m.wikipedia.org/wiki/Criptografia.

https://aepd.es

AGRAÏMENTS

En primer lloc ,vull agrair als professors Tomàs Herreros i Albert Masip-Álvarez el seu suport acadèmic.

En segon lloc, als meus companys de classe pel seu suport emocional.

En tercer lloc, a les encarregades de la gestió de Signatura digital ,de l'empresa Greintec,de la Cecot de Terrassa ,les senyores Marina Pallàs i Cristina Sunyer ,que em van explicar com s'obté un certificat digital.

ANNEXOS

ANNEX 1

CRIPTOSISTEMAS DE CLAVE PÚBLICA
¿Son seguras tus comunicaciones?

UPC

M.Ángeles Lozano
Tutor:Albert Masip-Alvarez

INTRODUCCIÓN

Actualmente tenemos toda la información en formato digital esto nos facilita la rapidez, transporte y uso de los datos.
Pero al mismo tiempo también nos crea problemas con la seguridad en nuestras comunicaciones.

Para averiguar que grado de seguridad tienen, vamos a estudiar el criptosistema de mayor difusión y relevancia : la RSA

RESULTADOS

La criptografía nos está facilitando la vida: como aplicación la Firma Digital.

Gracias a ella las gestiones que hacemos a diario ,son más rápidas y seguras ; al mismo tiempo cuidamos al planeta con el ahorro de papel.

OBJETIVO

El objetivo del trabajo es ver como se generan las claves para cifrar y descifrar los mensajes que utilizamos a diario ,tanto en redes sociales como para gestiones administrativas .Y asi garantizar su fiabilidad mediante la firma digital

¿Cómo funcionan las claves RSA?

METODOLOGIA

Se han consultado los datos en libros y en la web.Tambiéh se ha consultado a los gestores de la firma digital de Greintec (Gremi de instaladores de Terrassa y Comarca)

Algoritmo de cifra asimétrica RSA

En febrero de 1978 Ron Rivest, Adi Shamir y Leonard Adleman proponen un algoritmo de cifra de clave pública: RSA

Pasos del algoritmo

1. Cada usuario elige un grupo $n = p \cdot q$ (pueden y de hecho son distintos)
2. Los valores p y q no se hacen públicos.
3. Cada usuario calcula $\phi(n) = (p-1)(q-1)$.
4. Cada usuario elige una clave pública e de forma que $1 < e < \phi(n)$ y que cumpla con la condición: $\text{mcd}[e, \phi(n)] = 1$.
5. Cada usuario calcula la clave privada $d = \text{inv}[e, \phi(n)]$.
6. Se hace público el grupo n y la clave e.
7. Se guarda en secreto la clave d. También guardará p y q puesto que en la operación de descifrado usará el Teorema del Resto Chino.

Cifra: $C = N^{eR} \bmod n_R$ Firma: $C = h(M)^{dE} \bmod n_E$

CONCLUSIONES

En la sociedad digital en la que vivimos,casi todas nuestras actividades las gestionamos vía internet.
Gracias a la criptografía. tenemos cierto grado de seguridad en nuestras comunicaciones.
Pero como usuarios,bien por falta de conocimientos o por despreocupación, cada dia nos llegan noticias de hackeos de datos o intentos de estafas.
Por tanto aún queda mucho que hacer en cuanto a seguridad .

REFERENCIAS

Fuster A;De la Guia D; Hernández LL;Montoya F (2003) : Técnicas Criptográficas de Protección de Datos .Ed .Ra-Ma
https://es.m.wikipedia.org/wiki/Criptografia
foto1: https://www.ionos.es/digitalguide/servidors/seguridad/clav3-rsa
foto2:https://tutorialesenlinea.es/257-claves-rsa/amp.html