

TP9 - Criptografía

Alumno: Juan Cruz Mateos
Mat. 15134

1) Encriptar con los caracteres de la [a-z,A-Z] sin ñ, acentos y caracteres especiales la siguiente frase: **Como PeZ en el Agua**

a) En Cesar salto 3.

encriptado = Frpr Shc hq ho Djxd

b) En Cesar salto 20.

encriptado = WIGI jyt yH yF UAOu

2) Encriptar con los caracteres de la [a-z] sin ñ, acentos y caracteres especiales la siguiente frase: **como pez en el agua**

a) En Cesar salto 3.

encriptado = frpr shc hq ho djxd

b) Con vigénere, palabra clave: "ventilado".

encriptado = xszh xpz hb zp nzcl

3) Codificar la encriptación y desencriptación de frases.

a) Cesar: resuelto en **cesar.py**

b) Cesar Modificado: resuelto en **cesar-salto-palabra.py**

c) Vigénere: resuelvo en **vigenere.py**

4) Trabajo en equipo. Uno encripta y otro desencripta. Encriptar y desencriptar la siguiente frase:

“El cifrado César, es una de las técnicas más simples; consiste en reemplazar cada letra por otra que se encuentra un número fijo de posiciones más adelante.”

Aplicar:

a) Cesar salto 10.

Encriptado (Noelia Echeverría) =

Ñu mroBkny MdCkBg ñC Ewk ññ ukC DdmwrmkC vcC CrvzuñCi mywCrCDñ ñw BññvzukJkB
mknk uñDBk zyB yDBk AEñ Cñ ñwmEñwDBk Ew wgvñBy orsy ññ zyCrmywñC vcC
knñukwDñj

Desencriptado (Juan Cruz Mateos) =

El cifrado César, es una de las técnicas más simples; consiste en reemplazar cada letra por otra que se encuentra un número fijo de posiciones más adelante.

b) Cesar salto 5 palabra clave "SeCReTo".

Encriptado (Noelia Echeverría) =

va ,RSióf;f tWjóia .j lcó ;. aój kW,cR,ój bVj jRbga.jé ,fcjRjk. .c i..bgaóqói ,ó;ó a.kió gfi fkió hl.
j. .c,l.ckió lc cZb.if SRTf ;. gfjR,Rfc.j bVj ó;.aóck.í

Desencriptado (Juan Cruz Mateos) =

El cifrado César, es una de las técnicas más simples; consiste en reemplazar cada letra por otra que se encuentra un número fijo de posiciones más adelante.

c) Vigénere, palabra clave: "Ventilado".

Encriptado (Noelia Echeverría) =

ro oBnCagD p,Ftzi ev Jae px sls wiXquviD móH gmyJsosb qcqFBAEe hB fiqFxvaCof gnwi
vewGV tBL wErd Fii Fx mxcsaxEt Cx n.AZvB ypto gs dsFBksopsg pfM iññoaxqs

Desencriptado (Juan Cruz Mateos) =

El cifrado César, es una de las técnicas más simples; consiste en reemplazar cada letra por otra que se encuentra un número fijo de posiciones más adelante.

d) El cuadrado de Polibio.

Encriptado (Noelia Echeverría) =

4824 13191633111428 467834113384 1534 362611 1415 241134 3578132619131134 257734
3419252924153485 1328263419343515 1526 33151525292411431133 13111411 2415353311
292833 28353311 323615 3415 152613361526353311 3626 268325153328 16192228 1415
29283419131928261534 257734 111415241126351586

Desencriptado (Juan Cruz Mateos) =

El cifrado César, es una de las técnicas más simples; consiste en reemplazar cada letra por otra que se encuentra un número fijo de posiciones más adelante.

e) Método de los Confederados. Clave = "NoTenemosClave"

Encriptado (Noelia Echeverría) =

kA WnswnsI ,ftwwL tf zAf pt EDE upháxWfG qfI MLxqHj;ñ WtAxuINH pñ ÑjRBcpñEnH vDob
Hj.HU uCw BJLD CvA xR t.hljzJLD Gñ JbZtet snvE wH BpOnPxbrxx yiM DofHfáJYe

Desencriptado (Juan Cruz Mateos) =

El cifrado César, es una de las técnicas más simples; consiste en reemplazar cada letra por otra que se encuentra un número fijo de posiciones más adelante.

f) Transposición.

Transposición = 5, 2, 1, 3, 4

Encriptado (Noelia Echeverría) =

ilE corfadaC éss,r e u naaed lc stésinca m áslismpcse; snosinet emr eealpazd rcat aleoar pr rote
aques e ncneurta m nnúfreo djio s eponcioáse me sadealnt.

Desencriptado (Juan Cruz Mateos) =

El cifrado César, es una de las técnicas más simples; consiste en reemplazar cada letra por otra que se encuentra un número fijo de posiciones más adelante.

5) Trabajando en equipo. (Juan Cruz Mateos, Noelia Echeverría)

a) Generar con PGP las claves.

gpg --gen-key

Clave publica generada:

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mQGNBGGnq6wBDACu3C5rvJVIIeifdAoERz4QN7o9fHJa93Wg8ChNrmO5SHZMUW8F
UfY9Kw/UCJwnhebgSH/XMNPqP+5iUwVA8/Wk7Yc5VGcMNpAwNNdY7PQbb21/BEJX
SgFbXtykoGr5X7la/sjX5UbjgH+OVqOpn/Z9E0mUJ4xFkNShrkZJIcAOUjMkBN3
NeXWg79Y+29+D3vAJ0Sjxaii7LpK15y1IaJasBGz633GF8Z3DFkgUE31BqTdTnGh
86vEk/alaX+SkxO03nmQEHJ1yDoyDdflitEJT9J/IhMhKMwXAI/SFIELWlDatsel
6hP0rlZkQFOAnJGMznVwzBpu6p8C03DMiyj8O3mJg8VLj7wMPihUFIR8n7AQzT3r
ReaswqYTmZKQScfi7OCl6rrJxuuAWGuyYIaePqu6b1Vcl0Rbb3opt9RauaNSA4FG
SyfleVF7V8J0S/406Mrh8EPiKDtyIbi/xanSGIC4icCRpUyGXmvDsqVtavMS+cp7
5j9zh1qqga7ClgkAEQEAAABQISnVhbiBDcnV6IE1hdGVvcyA8anVhbmN6bXRAZ21h
aWwuY29tPokB1AQTAQoAPhYhBOIVFBfTu2OeWM6YVxc2qcuBk/18BQJhp6usAhsD
BQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAJEBc2qcuBk/18GpgMAIqe
0kh9nOhfWPdUDNVJfdoRs1lm4DD4s1ZhhpZKKVWomGsTeZ830bfmiKMruLC6uvNc
oLJCrvLxwRMKvHelK++H7pJ/SFy7SIsxwxGtyZN2SK94VglrYx08qLLv/o/DpStS
9pst+FiIuNP8bnbB/WxhePEPwDunISqRiqn4ysRAiZYxErEU1So6LJUImLlwlYel
nRXxvTfz6FJ91oGv8bJAMQYoxslcInPxakyFBqiPD2n+0h7I3LZh022U6wcNHHE5
rEjU74vn49JVdx//h2RrmxoTHmbVB2EoVKQPTf7dl4IjujKv8ogOWUeNSLohZIIH
8MvTAj6t/KOn869QqoCmbf+y2vpKHgUGmBIShRsTQGcIeUlnHeq7+qgPPEwCe04G
JpDVt/Mm0aLkrKUNZ/vzNYGSTc7n0LbG1P40TOevMzNMu29Tm0x7bjLATc2X15lC
TAD+fN8QcRZkul7GBMUPoLuvFvrc4RHwrt9fG2cWslkXmghTmPBQz67vE90m7rkB
jQRhp6usAQwAsh0Sa1bLCshmf0xWufOPSte+NgKcga3UA1iHuGdz1AtDV/u4Z6NO
YjOq+DsEHQV3XqpvtJTQ4+OVgaFWf0rEh45ZphVq+kWJh9frer0z8YS/VtJedrKD5
5n6XB1xQn9rvr4mwUh/HET6drms3nKylA6pCgarpUnPF6J6pkZMWZHS5mEpDZ9LBr
EnW3b5hSScaOPT/yP42Hol1diQpvAAI0Zl3Crhc/X4qUKA2LCnYB/aO28BCrTV5A
NGKSsTHgaH23vgEHKIX0pRn2hrPdSNFbXq1RUz6+Hki46elSgMLK9RwtjfhY77f
a/IYVzmmdES4jaFL/HuqbWEG3QzqHRPcEYYBTRnKBU1GJhqPmkVGEPOcu/6lI7Cv
0KKuJLleMezudK1YTTn+qg7390VpnRdJhVYeqLA61T1NR3cuHLgI6+j9/5MLPxIN
jkCM63GRJVClnu1hAJZ1RmuFQIr1GBr0AY90RwwnYJggWKficyZX0YEaEJlhy1t
uj260TimzmjfABEBAAGJAbwEGAEEKACYWIQTpVRQX07tjnljOmFcXNqnLgZP9fAUC
YaerrAibDAUJA8JnAAAKCRAXNqnLgZP9fExPC/0euHOv1rAzSOaBNWiCYENWKuAc
PjFoEcX8gzNvdQvrTVPeYbqBjfiWxwWknnsQD7GyNKZpVfQXkiBHJapzBQSajU2C
y8KWMkmRV7VEUiOvqpqthfQAKetAIZ/PMkyIHLr0vpal3OPZGZmmIVjZ0cnLQskm
WTelfzJd0uDeEgu7OISwsEguhPHKKO7RZqqotFgmKociOdURz83d3z3oJTkqOqzw
bHLti2OfK2bB5OX/91E3M09PpQcrUMV+8Xhp8gDeAOMjz2fJ91VO/69KLqHlRZWm
yOnzpQRlAz1X2KweIcSbk86kP8ULOCsro7rpDws5Twwe5OgiP60+/4YfFeq7K6
WnYSBjnS2G+sAmAYi4T1yPPAJR8fTV+BDXPCt/VvYigTlzoMe1r8vqW/r6DYyIs
7PT/RBs1gucIplzWMwcrGiU+oqM3di/k6/HrB9TrUDS2JWpx7sJkgeOjfoZQ6xzZ
3m4JrjMefMQr5H9ze+l47z/d/EQkFfmKG4Knd94=
=JX7Z
```

-----END PGP PUBLIC KEY BLOCK-----

b) Intercambiarlas con su compañero.

gpg --armor --output publicKey.asc --export Juan Cruz Mateos

Clave public de Noelia Echeverria

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mQGNBGGnDl8BDACgulQQqUrelhybflQjN3Xx+nx6buFgzwG5Hzmnbk+kWRaqu8zf
liIMLdSj9FoKGI61AiNXqh3rlnuThxJ5kf+DBRiNno2rfFs61mRyxeRvVeJJyj1E
UThmPtyG7PV0wADhPjrMnAUXvthUnHFvfEZ23aRcGwnPp2ce3u2GIggig1xrqtK5
kaM6kwr5NqSXD/v3xp8hUrsisnC4l8igDDkNI0lHgSo60qeAOJNTkC84BJFctzQI
igQyxZZDsv+hD+9K8kd20jfYcg+ijcze+7jWIXVcb3C6rj2UpcsTLDH0z0HnieMX
xTvAaZ5MdlBVOMJscL6TgCnz32Fd+UI3fIXHD6JSY+FJjivt9iIyRU00MJ6jeb/F
uLwzyld1rbLNXQMtR3E654lPqk3h6FlyN5FeKeW9WWDltmkA9VLGKUQRZTwgm0/n
1YH7kib/H0xgXLy40b8o3RC5z2jJK6PydLR+mn2Qx0YZm+lKJvciLgHMhbwqF7GC
sbJTAJNwRnfs1ucAEQEAAAbQmTm9lGlhIDxub2VsaWEuZWNoZXZlcnJpYTA4QGdt
YWlsLmNvbT6JAdQEEwEKAD4WIQSD1uHt/fN/qJcmAoyrBdCy+UVh6wUCYacOXwIb
AwUJA8JnAAULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRCrBdCy+UVh67BsC/9x
gdSGd4QUvf/aymBan73Q7o7gXNSZ8Jh3rmYADfjuvEs+Ua63wVU1jk740GophBo6
hBsiANW/6GiC3R/iFRNQdsakpBUG8ZkkUXldcKSG+sBtyoZHbOIIQDsA/MQqY9vN
zSIEynIEF7zzE/FkzsLfH+b62jWiqQ9r9xq0z4pcLW66Xy8hjMVojF7zfFSiNYdF
gajaitVCTVGHUG5e9U3a2ur4lI3WkIevF6bvvoOILU3xoTcopXvwf62uVINBmOd8
0L2htwcqr83P0t5ayvTqjBqHpyifAusPvZjWAoiSRrXATQhF+uUZsxmPodP0P4ZH
VWbbqqcuulPDIsuiQrYQgDEmWAHUXY9xqx3J6nVKhfhuwM+XDm7eZKu+MZhG96gS
99T1NwcY9dMQmvCbw4JBCvxaIO3jIVIj+BtFO8d++x/8gEOq9NpYQI/dliprDRqe
yh6EzDeGNDcGpkbj0KufdcUX50b/NQLlr5eofEQ0eL8vjfCYCfp1MxASiYvFuCC5
AY0EYacOXwEMAOEEN8x+0t59qiQ97YzTUclNN+CysZKWbflaqKw0d3eVADIKc/Ik
STpSpVbO/lFoX2Uvm0Pb08b08A75+PfeyYpSt2KqlMwlt6x83uLIRFuMCDDl49Fn
yP3VeLYEZ94Xu51tWzZRzi414pq1lMfciHFFkorOCjbAoSf5VECnwDbQsRrvQd1W
AMD+VFyzvx59JUe8FS/HJicogPi8xe7jDAw3JrFy6ZYPHBx6WAQ/4ZpzbH5wEbiP
p++1v2JGykZ8hxx/TnyHdLpZaDn2Utd8JisCvMPISvDRd+uLcKsqyx+R9tKdEN+S
FOKerSIJGv+HR2O6z5oOg48Jag3VGCxauF+Tm4ACbdpacFFksdCjVYTofoUwHWGx
+BSuabeeZ3Bsu0eR43CTI72S276xfRgMJm5MIuW63PdQY6kEAp5kWaMo/jqzGUKT
SjrBbR07k7k4wV5cW8K/pENLQOmPnumfrzka9UQs0AAGBiJ09i5ZzwKhl+oO4EHr
CRpGWSwvrJGfyQARAQABiQG8BBgBCgAmFiEEg9bh7f3zf6iXJgKMqwXQsvlFYesF
AmGnDl8CGwwFCQPCZwAACgkQqWwXQsvlFYevJhwwAm8WluZ/rPwiSvIdUrNRWmUhk
ca04B0tANlYoWec/THjfx6hw1GRMvCe7uy6m04WR3aIyfANY0O/Hd15dy7hI59+t
xFpxm2Mix9HJ7sfa3Y7sbLymiQG+4MnRfK46MM29GlR0apcJDSboI2kQVNxt7+2Q
pOo4mDzN+8Lf5vx2OH8Fy4aNUA9QZTxo4x1S763arOjsShUGQpq4dck0Hwyg51wm
VoMpzdT53gd9V6dPIPPQ643Umgy8/XQvDqWGbElr9YeKaCiXEbNZnSIU2aIG963EQ
ME4ArLnrCRvImOzG3a9xkmqyW0O9441kGmkiH4jk3KzF65KVn15JENGBTL65x5q
825ZGv20nbvDEq47Mj5wfChp73Vfej+kYjuO3ckJgJvaq8kmlHIewl8rjJ7HeMqF
ejrPjuUO71RjoYTfwFKpd9glZfM7eb44V8fqY5xFenAeGGU6uL8yPkQQmcadDPs3
fkrwWRRehySZpn/cwPIeM+itZn6MEDYguxV8sjpS
=Lc3g
```

-----END PGP PUBLIC KEY BLOCK-----

c) Cifrar un mensaje y enviarlo. Del otro extremo descifrar.

noelia.txt fue cifrado por Noelia Echeverria utilizando:

gpg --armor --recipient juanczmt@gmail.com --encrypt noelia.txt

-----BEGIN PGP MESSAGE-----

hQGMA3a8ZV4a6s7aAQwAhoMltyjnQNjwmljuTUxIqYTXrrlZApM3dcjfKXr7Z7sH
fl60e+QWSMkfZFBsBkPhohTl4kb/jWSDwy9dWt5MLBv2LFGFhv+/KnUeGX+VJQpr
AJBSc1nFO/OwEquFhCgnBVQbRSpnVYaCSC/bNPVFE9k3WFvTz0PSyoxIeWqgsXm3
xYEPu+vKqzuFhTX9fKhVdlIWodYtH6ui4uIkYAiG3oF5vbf6vrxMv/WFVcM8ZYz
kdsZ8UJ08qS0+p2PM601Wlo6O7fjTN0Zst9Df5mo6hkC9eWApF44Ypo/g+/JFZzs
vsAWVLRciosT9Vl32vatMz3bwHkgw9H7Cr9bmu0AiLHwGrMM08THx45t6r8jnOXk
2AKKw6VsavW56ZUoiNdtjIxzP0C7DltuKa5WJnCjNVfebPYVGumkTinGywnb7qy
SVZtN4alWHWGcy21jcbYzZPtFuLAXdMuHlUmuWGVJ+of+f1ZDmRxngq9hCoBLYVp
zYgVd7+xkVoOBt4F7gli0lYBKGOdyQSasLaX0wH0RteqtAerwcNXhFtNpPrmDEig
xeQV1qGYBSXyKXMxn4JHnBOoUd/kCvfOpgdZSJ9/akJs2Hrbzdt6MFr7JP5G5Ih7
Vii7YCoiSA==
=h/pn
-----END PGP MESSAGE-----

Al desencriptar con: `gpg --decrypt noelia.txt.asc` se obtuvo

gpg: encrypted with 3072-bit RSA key, ID 76BC655E1AEACEDA, created 2021-12-01
"Juan Cruz Mateos <juanczmt@gmail.com>"
Noelia tiene sueño

d) Firmar un mensaje y enviarlo. Del otro extremo verificar.
main.go fue firmado con:
`gpg --clearsign main.go`

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

package main

import "fmt"

```
func main() {  
    fmt.Println("Esto esta firmado")  
}
```

-----BEGIN PGP SIGNATURE-----

iQGzBAEBCgAdFiEE6VUUF9O7Y55YzphXFzapy4GT/XwFAMGnsTkACgkQFzapy4GT
/XzNDgwArUyYwcPd7AyJtksjDSovwKtJAaXcgfeQEXeZK88nBuJQnrJRjYQe//g
ffWyxXznxkNewlsI6+3HC6LyCMUybl55sQzWIEX+se4JaQFAjprA+dPfP+iDtQfF
n8Jy+u9x00L57TmY89o84R3xx1q6Pak1rcF/0JqCaoxmzR5xN8WUa7B6eT/sXDPU
aIE8b2evwpLGHObLJLEIRtHrDCzTKgMbnu/8g/BqLHSxaZOicK5m2NZrbJtEV4s1
BdXhgeHdDhBdTzFriJCu/gm6C39lADTRWqW5TL4K8pz/VrJgaCXHFit9cVLj+9LX
9YkF2DCWYpn4lntSmC77gvdULZUGGCpvKX68EKYcMoj/tXTIQhStcD/lrazdFoUe
bQzqa6CzoIGrChNjQscK61GFIAXUgaR15vGk2lROkKp8TxZU1GXi4bRHnH+skYu8
xg3Rlv1FkSq0hRuQjOvbQlc2qk/iA3e9531Z+1F7HtL5Ur6Qg17ZTXciXsY7WRwH
CiHsqoek
=64Kz
-----END PGP SIGNATURE-----

y enviado a Noelia Echeverría para verificar

el resultado de `gpg --verify main.go.asc` fue:

```
gpg: Signature made Wed Dec 1 15:50:33 2021 -03
gpg: using RSA key E9551417D3BB639E58CE98571736A9CB8193FD7C
gpg: Good signature from "Juan Cruz Mateos <juanczmt@gmail.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner. Primary key fingerprint: E955
1417 D3BB 639E 58CE 9857 1736 A9CB 8193 FD7C
```

e) Busque un tercer compañero y arme un anillo de confianza.

Crear un anillo de confianza consiste en tener claves de gente firmada por otra gente que la han firmado y que con su firma aseguran que esa clave es realmente de quien dice ser y no ha sido alterada. Si por ejemplo tenemos las personas A y B. Las personas A y B son amigas y se intercambian entre ellas las claves públicas, verifican sus fingerprints para ver que las claves son las correctas y quedan para ver las claves que se han pasado son correctas. Entonces una vez verificado que todo es correcto cada uno firma la clave de su amigo. Ahora si por ejemplo yo obtengo la clave de B y veo que está firmada por A (que es una persona que conozco y en la que confié) entonces me fío de que esa clave es la clave correcta de B y la puedo usar. Si por un casual quisiera firmar la clave de B con mi firma para avalar que su clave es buena sería bueno que me pusiese en contacto con él y verificaremos la clave.

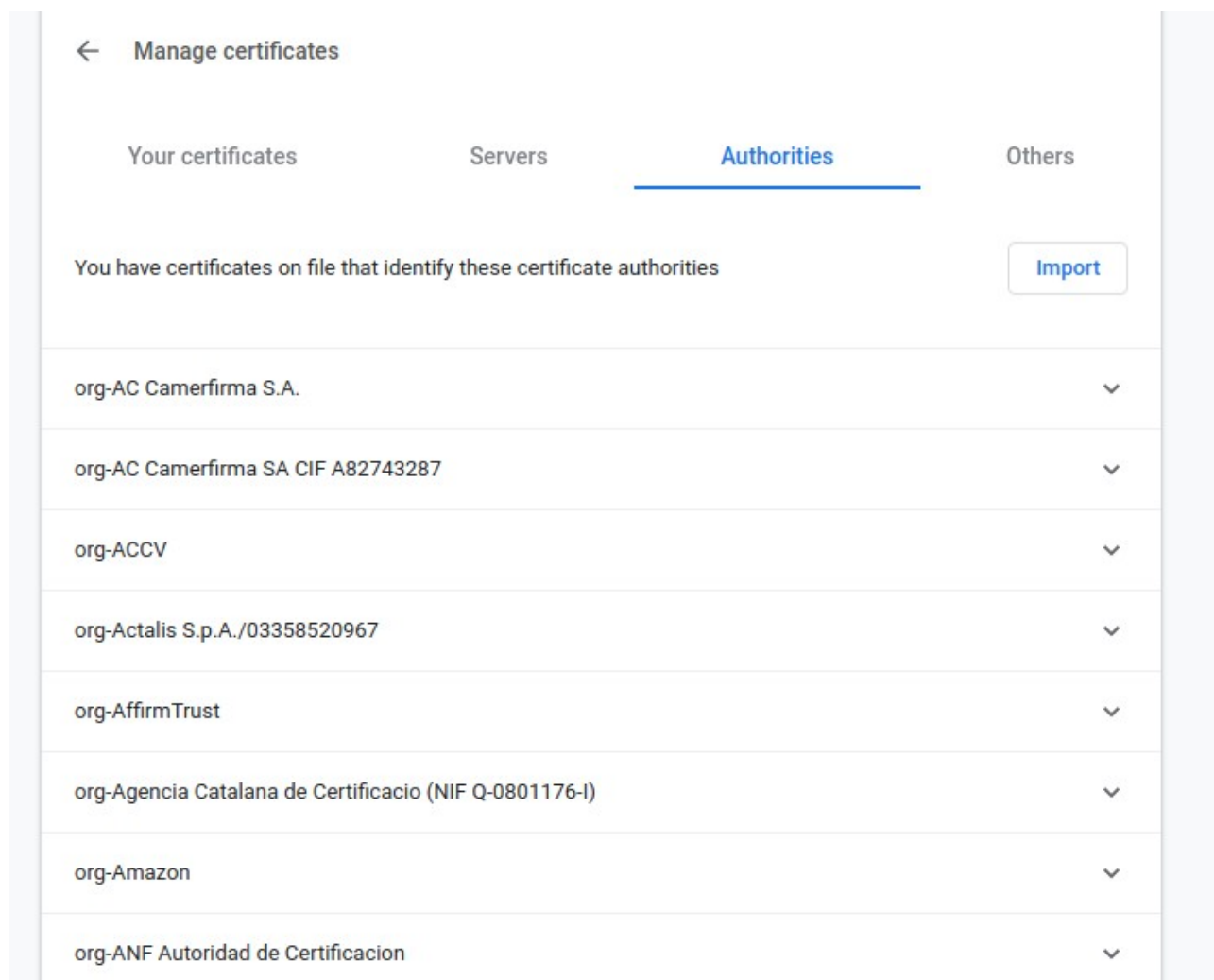
6) Busque en su computadora de qué manera están firmados los programas que instala (o los drivers del sistema operativo).

Sistema operativo:

- Distributor ID: Ubuntu
- Description: Ubuntu 21.10
- Release: 21.10

Los programas se encuentran firmados utilizando `gpg` y MD5, SHA256, SHA512, entre otros algoritmos, son utilizados para verificar la integridad de los archivos.

7) Revise su navegador o browser y verifique que certificados tiene instalados.



8) Describa los pasos a seguir por una empresa en Argentina, para obtener una firma digital válida en el país. (Ministerio de Modernización, ONTI).

Los certificados que se otorgan de la AC-ONTI (con token) o de la AC-MODERNIZACIÓN (sin token) son únicamente para personas humanas. Ambas tienen la misma validez jurídica.

La firma digital con token sirve para firmar cualquier tipo de documento.

Es una herramienta tecnológica que nos permite asegurar la autoría de un documento o mensaje y verificar que su contenido no haya sido alterado. La firma digital otorga: validez jurídica, autenticidad e integridad del documento y seguridad.

Requerimientos

- Documento Nacional de Identidad (DNI) y tener número de CUIL o CUIT.
- No es necesario presentar la Nota de Envío de Datos impresa.

- Se debe adquirir un dispositivo criptográfico (token) que cumpla con el estándar FIPS 140-2 nivel 2 o superior, que soporte claves RSA de 2048 bits. Los mismos deberán estar homologados por NIST National Institute of Standards and Technology de acuerdo a lo establecido en la Política Única de Certificación de la AUTORIDAD CERTIFICANTE de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (AC ONTI).
- Para validar los archivos firmados digitalmente se deberá incorporar la cadena de certificados emitidos por AC-Raíz, que incluye todos los certificados de las autoridades certificadoras públicas y privadas. No es requisito excluyente al momento de tramitar la firma.

Pasos:

1. Sacá un turno en la Autoridad de Registro más cercana o consulta en AR con turnero propio. Al momento de completar el formulario del punto 2, deberá seleccionar la misma Autoridad de Registro. De no coincidir, el oficial de registro no podrá emitir el certificado.

2. Deberá completar el formulario (<https://pki.jgm.gov.ar/app/Signature/Request/Hardware/CertificateRequest.aspx>) con los datos personales y de la organización. El correo electrónico ingresado al momento de completar el formulario debe ser personal (únicamente del titular de la solicitud, sin excepción), en “Aplicación” seleccionar “Ninguna” y en “Autoridad de Registro” la misma que haya seleccionado al momento de solicitar el turno. En datos de organización completar con "No aplica" en todos los campos.

3. Volver a verificar que los datos coincidan con el DNI del solicitante, y luego seleccionar “Enviar Datos de Solicitud de Certificado”. En esta instancia el solicitante aun NO posee un certificado de firma digital.

4. El solicitante recibirá automáticamente en el correo electrónico declarado un link de verificación al que deberá acceder para confirmarlo, el cual tiene una vigencia de 24hs. Pasado ese lapso de tiempo, si el solicitante no confirmó el mail, deberá cargar nuevamente la solicitud.

Si la fecha del turno para presentarse ante la AR excede los 20 días hábiles luego de haber completado el formulario, el mismo se rechazará automáticamente y deberá volver a cargar sus datos

5. Para finalizar el trámite, deberá presentarse personalmente sin excepción ante la Autoridad de Registro donde solicitó el turno con el dispositivo criptográfico y el DNI original.

6. En la autoridad de registro:

El oficial de registro realiza las validaciones correspondientes y el soporte técnico de firma digital verifica los requisitos del dispositivo criptográfico. Según sea el caso, el oficial de registro habilita a “solicitar certificado” para continuar con el trámite, o bien rechaza la solicitud.

El solicitante valida los datos enviados (en el punto 1), inserta su dispositivo criptográfico y completa la solicitud, generando sus claves en el mismo.

El oficial de registro aprobará la solicitud e instalará el certificado en el dispositivo, o eventualmente la rechazará. El sistema envía luego un correo electrónico a la dirección validada del titular, informando la emisión del certificado en el cual figuran dos datos importantes (Número de serie del certificado y PIN de revocación), por lo que debe conservarse.

Información importante:

- El trámite es personal y de modalidad presencial.
- Si durante la vigencia del plazo de validez de su certificado se produce alguna modificación en los datos incluidos en el mismo (nombre, apellido, CUIL o correo electrónico), usted deberá revocarlo y volver a tramitar un nuevo certificado presencialmente.
- Los certificados que se otorgan son únicamente para personas humanas.