PAC 2. Criptografía

Sílvia Sanvicente García

2 novembre 2021

Exercici 1

Sigui $h : \{0, 1, \ldots, 2^{2048} - 1\} \longrightarrow \{0, 1, \ldots 2^{256} - 1\}$ una funció hash tal que

$$x_1 \equiv x_2 \pmod{2^{32}} \Rightarrow h(x_1) = h(x_2)$$

(a) És h resistent a segona pre-imatges?

(b) És possible calcular eficientment col·lisions?

(a) Resistent a segones pre-imatges vol dir que no és possible $h(x_1) = h(x_2)$ si $x_1 \neq x_2$.

$x_1 \equiv x_2 \pmod{2^{32}}$ vol dir que x_1 és congruent amb x_2 mòdul 2^{32} si 2^{32} és divisor de $(x_1 - x_2)$.

Si $(x_1 - x_2)\ mod\ 2^{32} = 0$, llavors $h(x_1) = h(x_2)$.

Aquesta funció hash no és resistent a segones pre-imatges atès que podem trobar valors per a x_1 i x_2 que compleixin $mod[(x_1 - x_2), 2^{32}] = 0$. Com per exemple, $x_1 = 21474836480$ i $x_2 = 17179869184$.

(b) Si, es podria realitzar un atac per força bruta on es busquessin de manera aleatòria dos valors que complissin la condició $mod[(x_1 - x_2), 2^{32}] = 0$. Per simplificar el càlcul es podria cercar una única incògnita $mod[a, 2^{32}] = 0$ i aïllar-la, donant l'equació $a = 2^{32}n,\ n \in \mathbb{Z}$. Un cop trobada a, aquesta es podria descompondre en dos enters, x_1 i x_2.

Exercici 2

De tots és conegut que la seguretat del RSA està relacionada amb la dificultat de factoritzar nombres a partir d'una certa grandària. Però de fet, si a partir de N és possible calcular $\varphi(N)$ de manera eficient, la seguretat del RSA també queda en dubte. Imagina que $N = 667$ és un mòdul RSA i saps que $\varphi(N) = 616$. Calcula els factors de N sense factoritzar N.

RSA utiliza la funció totient d'Euler:

$\phi(n) = \phi(pq) = (p-1)(q-1) = pq - p - q + 1$

Substituïm pq per n:

$\phi(n) = n - p - n/p + 1$

Multipliquem per p a cada costat de l'equació per treure la fracció:

$\phi(n)p = np - p^2 - n + p$

Arreglem l'equació per tenir una expressió quadràtica:

$\phi(n)p - np + p^2 + n - p = 0$

$p^2 + \phi(n)p - np - p + n = 0$

$p^2 + (\phi(n) - n - 1)p + n = 0$

Substituïm n i $\phi(n)$ pels valors que ens donen i resolem l'equació:

$p^2 + (616 - 667 - 1)p + 667 = 0$

$p^2 - 52p + 667 = 0$

$p = \frac{52 \pm \sqrt{(-52)^2 - 4 \cdot 667}}{2}$

$p = \frac{52 \pm \sqrt{36}}{2}$

$p_1 = 29$ i $p_2 = 23$

Els factors de N serien 29 i 23.

Exercici 3

Alícia observa que el xifrat del Cèsar és completament insegur pel que decideix modificar aquest xifrat de la següent manera. Per començar assignem a cada lletra de l'alfabet una representació numèrica tal com feia el Cèsar, i després xifra i desxifra de la següent manera:

$$I(x) = ax + b \mod 26$$
$$D(i) = (i - b)a^{-1} \mod 26$$

on $a \in \mathbb{Z}_{26}$ tal que $MCD(a, 26) = 1$. Pots ajudar a Alícia i implementar-ho en python? Utilitza el teu programa per desxifrar el següent text que Alícia t'ha enviat des de Londres.

Per resoldre l'exercici s'han programat les funcions següents en Python:

```
##############################################
# Silvia Sanvicente, 1 nov 2021              #
# Fonaments de ciberseguretat                #
# PAC 2, Exercici 3                          #
##############################################

# funcio per encriptar
def encriptar(a, b, missatge):
    # lletres del alfabet angles
    alfabet = "abcdefghijklmnopqrstuvwxyz"
    resultat = ""
    for lletra in missatge:
        # busquem el index de la lletra al alfabet
        x = alfabet.find(lletra)
        # apliquem I(x) = ax + b mod 26
        index = (a*x + b) % 26
        # concatenem el resultat amb els anteriors
        resultat = resultat + alfabet[index]
    return resultat

# funcio per desencriptar
def desencriptar(a, b, missatge):
    # lletres del alfabet angles
    alfabet = "abcdefghijklmnopqrstuvwxyz"
    resultat = ""
    for lletra in missatge:
        # busquem el index de la lletra al alfabet
        i = alfabet.find(lletra)
        # apliquem D(i) = (i - b)a^-1 mod 26
        index = ((i - b) * pow(a, -1, 26)) % 26
        # concatenem el resultat amb els anteriors
        resultat = resultat + alfabet[index]
    return resultat

# valor de a i b
a = 19
b = 23

# fem una prova amb "hola"
#print(encriptar(a, b, "hola"))
```

```
#print(desencriptar(a, b, "adyx"))

# desencriptem el text del exercici
missatge = "yxbvhnivuxutkodirautjxuxrqejdkvhncxjdrjtqvibvhnitcxceb" \
           "yaivxivyxjtdkxcxxrqyxtkodirautjxtyxuvyvrautjxpnvbvkodj" \
           "xvkyxwiduvjjtocvyxtkoixvbuinjunixjdrwnuxjtdkxytuduvygt" \
           "kjnyxuxrqyxrxuvtsxtvbwvjtxyrvkuyxtkodirxjtojdkutkhncxv" \
           "knkxjdrwnuxcdixdjtijnyxkuxuixgebcvyvbsxisvbcvjdrwnuxcd" \
           "ivbwvixxtsovstbuvtsvknkxbeitvcvbuakcxicbwidudjdybreudc" \
           "vbivhyvbvtkvbtyyvtbjdkjvqncvbwvirtktrtuexivybwdbbtqyvb" \
           "itbjdbxyxtkoixvbuinjunixtdxyxwiowtxtkodirxjtoyxjtqvibv" \
           "hnitcxcjdrwiekwidhixrxitqxbbcvcxcvbrvuxcxcvbxistnbrxpn" \
           "tkxitsxisvbcvjdrwnuxcdivbtuduvypnvydihxktuexjtovkuvkhn" \
           "ttgxyditjdrnkitbjbtyxtkodirxjtojdkotcvkjtxytkgdynjixcx" \
           "wdhnebxiitqxixyvbrxkbcxyuivbwvibdkvbwvivsvrwyvjdkgviut" \
           "kubvxtsivktkodirxjtowitgtyvhtxcx"
print(desencriptar(a, b, missatge))
```

La funció per desencriptar retorna:

```
laseguretatinformhticatambzconegudacomciberseguridadzsl
hrearelacionadaamblainformhticailatelemhticaquesenfocae
nlaproteccifdelainfraestructuracomputacionalitotelvincu
latamblamateixaiespecialmentlainformacifcontingudaenuna
computadoraocirculantatravzsdelesxarxesdecomputadorespe
raaixfexisteixenunaszriedesthndardsprotocolsmztodesregl
eseinesilleisconcebudesperminimitzarelspossiblesriscosa
lainfraestructuraioalaprfpiainformaciflaciberseguridadc
omprznprogramaribassdedadesmetadadesarxiusmaquinarixarx
esdecomputadoresitotelquelorganitzacifentenguiivalorico
munriscsilainformacifconfidencialinvolucradapoguzsarrib
aralesmansdaltrespersonesperexempleconvertintseaixrenin
formacifprivilegiada
```

Si corregim les paraules amb accents i posem espais, comes i punts, obtenim el text següent:

```
La seguretat informatica, tambe coneguda com a ciberseguretat, es l'area
    relacionada amb la informatica i la telematica que s'enfoca en la
    proteccio de la infraestructura computacional i tot el vinculat amb la
    mateixa i, especialment, la informacio continguda en una computadora o
    circulant a traves de les xarxes de computadores. Per aixo, existeixen
    una serie d'estandards, protocols, metodes, regles, eines i lleis
    concebudes per minimitzar els possibles riscos a la infraestructura i o
    a la propia informacio. La ciberseguretat compren programari, bases de
    dades, metadades, arxius, maquinari, xarxes de computadores i tot el que
     l'organitzacio entengui i valori com un risc si la informacio
    confidencial involucrada pogues arribar a les mans d'altres persones per
     exemple, convertint-se aixi en informacio privilegiada.
```