Week 7 - 25/11/2022

Exercício 1

```
-----BEGIN DH PARAMETERS-----
MIICCAKCAgEAux0Gojz+Dg6hCLPKAsphVM5GzoBBSdFaqBHPePiiEWJGPUrMY/0G
poNJyk1ltbA+BMDE7IjHV68ZDfm179UE2TXOqrfeMpNEhfKFIdO4CfiCM+AG9/i5
Q/MA1lujWtJdsP+qEYzaQ0HIeyaMW7GUudwYhJs+9VFWhLtnvKn/Sav6RYs914s6
vI+3kNHOZp+kHT8DKyLvhC915O9CWonl37azGdedMQKlsC/s52JU2G5cJ6BMqnH9
vbxZnbyGWkTX9gUx1jBFHwodjyAOOToYHwUlyuh3OYqasV1HnAWhw/hjSZMwveuI
D1w+fqo5PH3pciO5y+soEKj55RJrKxwXvXnH+tELHEsD4NnFUuJIyLPukTrcKU9Z
FenXW6UoO69k7aIybx6D7Qtuc+i5UJfLjDJI06j9Du8AZpFGLHctB/vsDmZyq21Q
QynaDPXVAQC7Bbs2M4Z8S28xbX21cz19vSz5uJiWW1erN4tpMB9Ac4DKAknefam4
oHtf0UM91yAQoeKhLhqm5qopgSJ/9MiVhEmzPQh3SCmMo9vfnIegBzj2IOF+/UNC
5H3zLA/jemk6WpnzjyuZNr+rQcGLukSCeLA0UBYsBakez+0UnOgzua/zIF/Smc0F
k3pOlB86P4OhC7CO+cIFxIMQ7aFyQsqLkrEJ4AxWZOwY9rqV8iSnozMCAQI=
-----END DH PARAMETERS-----
```

Exercício 2

```
-----BEGIN X9.42 DH PARAMETERS-----
MIIELAKCAgEAh/pVNCPkeQvetk5HygBmQ6dnKdEbkS3567AAxr36HeyeNIADwlqM
+ZKNnxYlGcWgOkzKL8xXHYjV0Ys7nBsgTNPB5UjXG5iAwvbsge7k9COGmbPHZF+r
MtmEjot6ueqD0ksa2ny16VaAYjXmgl7lz5Gqh/7tlVx2YtsxPJ5UEKSE/YO1wWLs
Y3n0WmJAKImCnVjtveCbanViU8A0fj8aOhdQHSGXbEtwjDJRfWSUhTqQtXBLuzmM
8qlYTMyv9yaV0+od+KPpJFy0omHnftmVWS8RmzTM2vj2RsM/w1HCzD6e/Kg326VT
sk66a7MY8GlyJ1JuyliPQ6G8x/4LhKwuCQ3OjpzpRIKA0hINllF45BISqi8IW/UR
6jA3jJJWytPtlj8zsNw9HwJhvusY9YYJUTugTh3Tk5Sf/Sdn68xIF+D0v4aOkwai
0J6qRzC7nEdnJn/020EZrZpvm+WZpZHN23v/a77XWUwUZQUUFoPI3E+cJ30UtXYP
UVCkKFU1F0ys6quzFb+XY6Ao4kWUNtBCW0P1VzaGxg+Jgp5jmeu/qgsOrgxFCAj1
FsLSJmUqRLSEsglIgwmsYNZ4ICSKr2EwDICD796sxTXgSswrv2RwWAcspiDPIqbP
X/Mdv7z6F/3wuXE9/nI0BkEuGiDPFxzvcv1US/sogLWUtnp3oSiXK30CggIAft+y
A8xtPKBxxFdvpwKaPws/6IIsKQFB/ci44xSM/dShK2EyeyFSmpzi7t1at0MI3jiI
l1LRhrwCm6WwMS+b3fBoT16t7FL51uYkI9S2PKY/oNzYjPFwgBjBh83i59bbFq96
oIYdhFEitYkfg//zHkoZFtcy2dOyr4ydqfqweMtuKZ4Uje9pfUYc/e2Iu9gHseLV
bgAunrj09v/9ekHW382/5c3IzuHIrDI2b/BQ36RmvDyF1PyzeXFwBXkRRzhX2mob
9nE1HRmjZuEjBMcCwpX9U1+hSvuvFZMynK70ZG92zmsjSqa+2FFBtmeSe+WPVdLk
+ZcOLfkqj7PiMjY5gDGD9PoVwldBTiSYyaN9XZ6BE4tpWJyr8XSETszbFRG+qhjD
1TZDdl3Yixdj33u/0/NGpsgquBa/4ce4N/2gaS/6OUOX5C2xclOTMWE/9FPP1urD
jk3B1LYkEsZStrWVkpK41rGOJIEtYlTUEv3Urfd+yfFW93DEy8Iwd6JrZaYHOdtT
kaISgyAXzAerfCCPpjj9C66nl6duijI58x94vBdstW47EBfSK58H6X7zge8koo1I
U0klT6wLMGY5djgETzuoP/RsBfeAOhQhM1Bj0xxDTUm9yxspjzYiPQpS+SFpqwqy
wrpgftlatQBGj7uTgZesYZk9jtZEydForsTbxFUCIQDI7RUYzMSAaEr738cxhStD
6hFl8aT/HXwOaxF8IxSAwQ==
-----END X9.42 DH PARAMETERS-----
```

Exercício 3

A primeira abordagem demora bastante mais tempo pois tem que obedecer às regras tradicionais de primos Diffie Hellman, isto é, seja o primo gerado *p*, para *p* ser admissível, *(p-1)/2* terá também que ser primo. Esta regra (não aplicada na geração do segundo parâmetro DH), leva a que o conjunto de números primos que são elegíveis seja bastante mais reduzido, tornando assim mais exigente a computação destes mesmos primos (o que explica a diferença considerável no tempo de cálculo do exercício 1 para o exercício 2).

Código para verificar a estrutura:

```
#!/usr/bin/env sage -python
import sys
import numpy as np
import sage as sg
from sage.all import *

payload = 0xBB1D06A23CFE0E0EA108B3CA02CA6154CE46CE804149D15AA811CF78F8A2

toCheck = (payload - 0x1)//2

print(is_pseudoprime(toCheck)) #True
```

Exercício 5

Código de resolução:

```
#!/usr/bin/env sage -python
import sys
import numpy as np
from sage.all import *

#Calcular Y

p = 1373
g = 2
y = 871

Y = (g^y)%p

print('Y enviado pelo Bob: ' + str(Y))

# Descobrir o Expoente secreto da Alice

X = 974

_,gA,_ = xgcd(X,p) #g^a vai ser o inverso multiplicativo do valor enviad

if(gA < 0): #Condição necessária pois não existem logaritmos de números
    gA = gA + p

secExp = log(gA,g).n() #Expoente Secreto

print('Expoente secreto da Alice: ' + str(secExp))
```

Exercício 6

Problema CDH:

O problema CDH consiste na capacidade de, dado *g^a* e *g^b*, se conseguir computar *g^ab*, tornando possível computar o segredo partilhado com apenas informação disponível no canal.

Problema DDH:

O problema DDH, consiste num problema de indistinguibilidade, ou seja, conhecendo *g^a* e *g^b*, ser capaz de distinguir, com uma probabilidade superior a 1/2, *g^ab* de um *g^c* em que *c* é um expoente aleatório. Ou seja, ser capaz de distinguir o segredo partilhado de um elemento aleatório.

Resposta:

Dadas as definições acima descritas, assumindo a existência de um algoritmo que resolva CDH, esse mesmo algoritmo, dadas as informações disponíveis no problema DDH, é capaz de, dado um *g^a* e um *g^b*, calcular *g^ab* e por fim comparar com o valor facultado, avaliando se é de facto o segredo ou um elemento aleatório e resolvendo assim também DDH.