

Cibersegurança

Instruções de utilização e estrutura do trabalho do módulo 1

Regime: Noturno

Grupo: G11

Alunos:

- Alexandre Silva 47192

- Diogo Cunha 47109

Introdução

Este documento tem como objetivo a apresentar a organização e as instruções necessárias para correr os *scripts* do trabalho desenvolvido pelo G11 da turma noturna.

Este documento está organizado da seguinte forma:

- **Organização do trabalho:** apresenta organização decidida para as funções desenvolvidas;
- **Bibliotecas usadas;**
- **Instruções de utilização:** apresenta os passos necessários para executar os *scripts* desenvolvidos.

Organização do trabalho

O trabalho desenvolvido foi organizado da seguinte maneira na diretória TP1:

- **libs.txt:** ficheiro que contém as dependências (bibliotecas) dos *scripts* desenvolvidos;
- Diretória **src/**
 - **__init__.py:** criado para que a pasta *src* seja interpretada como um módulo de *python*;
 - **G11_DSA.py:** contém as funções desenvolvidas para a implementação da assinatura digital DSA, ou seja, contém as funções pedidas entre as alíneas 1 e 4;
 - **G11_Attacks.py:** contém as funções para atacar a assinatura digital DAS, ou seja, contém as funções pedidas das alíneas 5 e 6
 - **G11_Timing.py:** contém o teste usado para medir o tempo que demora a quebrar a assinatura digital, através de força bruta, dependendo do tamanho da chave. Contém também os tempos obtidos;
 - **test_G11.py:** contém vários *unit test cases* usados para testar as funções desenvolvidas.

Bibliotecas usadas

Neste trabalho foi usada apenas uma biblioteca. A biblioteca **sympy**.

Esta biblioteca serviu de auxílio para gerar números primos aleatórios e verificar se um número era primo.

Instruções de utilização

No desenvolver do trabalho foi criado um ambiente virtual do *python* para não instalar as bibliotecas usadas diretamente no computador de cada um e para que cada utilizador (alunos e professor) tenham as mesmas condições ao correr os *scripts*, evitando assim problemas como conflitos de versões entre bibliotecas entre dois utilizadores, fácil gestão das bibliotecas usadas, versões diferentes de *python*, etc.

Para ativar o ambiente virtual basta seguir os seguintes passos:

1. Abrir um terminal na pasta TP1.
2. Executar: **python -m venv ENV_TP1**
3. Executar: **pip install -r libs.txt**

No passo 2, o ambiente já está ativado se a pasta ENV_TP1 for criada e no terminal se encontrar o nome do ambiente atrás do diretória atual, como na seguinte figura:

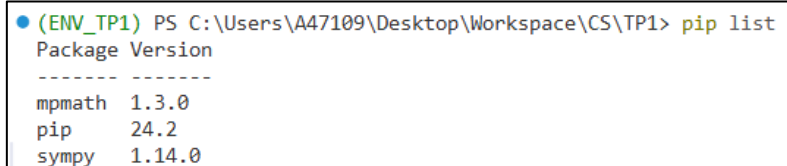


```
(ENV_TP1) PS C:\Users\A47109\Desktop\Workspace\CS\TP1>
```

Figura 1 – Resultado do comando **python -m venv ENV_TP1**

Só no passo 3 é que o ambiente se encontra pronto para correr os *scripts* pois este passo instala as bibliotecas utilizadas neste trabalho.

Para garantir que as bibliotecas foram instaladas, é possível correr o comando **pip list** e verificar o seguinte *output* no terminal:



```
(ENV_TP1) PS C:\Users\A47109\Desktop\Workspace\CS\TP1> pip list
Package Version
-----
mpmath  1.3.0
pip     24.2
sympy   1.14.0
```

Figura 2 – Output do comando **pip list**

Por fim, para correr os *scripts* através da pasta *src* basta executar o comando: **python .\src\SCRIPT_NAME.py**

Dos *scripts* apresentados anteriormente, é possível correr:

- test_G11.py
- G11_Timing.py