



Escola de Engenharia  
**Universidade do Minho**

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA  
**Mestrado em Engenharia Informática**  
*Engenharia de Segurança*

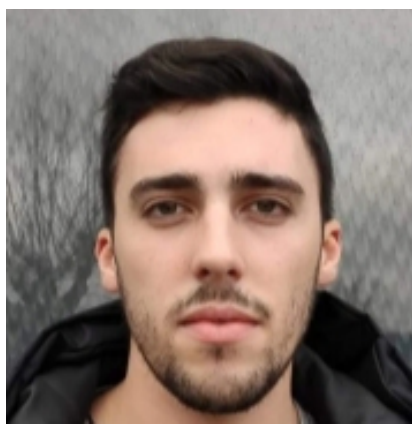
## *Aula 2*

**17 de Fevereiro de 2020**

## **Grupo 1**



Ricardo Pereira a73577



Tiago Ramires pg41101

Braga, 25 de Fevereiro de 2020

# 1. Números aleatórios/pseudoaleatórios

## 1.1 Pergunta P1.1

- `head -c 32 /dev/random | openssl enc -base64` - demorou 0.014 segundos;
- `head -c 64 /dev/random | openssl enc -base64` - demorou 0.007 segundos;
- `head -c 1024 /dev/random | openssl enc -base64` - demorou 3 minutos e 11.087 segundos;
- `head -c 1024 /dev/urandom | openssl enc -base64` - demorou 0.011 segundos.

Em sistemas do tipo *Unix* existem funcionalidades que geram números pseudoaleatórios com base no "ruído" recolhido pelos vários controladores do dispositivo. Os arquivos */dev/random* e */dev/urandom* têm essa finalidade havendo uma ligeira diferença entre os dois. O primeiro (*/dev/random*), bloqueia a obtenção dos *bytes* pseudoaleatórios enquanto a quantidade de entropia requerida não tiver sido atingida e o segundo (*/dev/urandom*), normalmente retorna um resultado imediato facilitando o processo e reutilizando a entropia do sistema.

Assim ficamos a perceber o porquê de os dois primeiros comandos serem rápidos - a quantidade de dados pedidos é relativamente baixa, o que não requer grande entropia. Já o terceiro comando é bem mais demorado, uma vez que a quantidade de dados aleatórios pedidos é elevada e, por esse motivo o sistema bloqueia até que exista entropia suficiente para a geração desses *bytes* pseudoaleatórios. Por fim, o último comando pede o mesmo número de dados mas obriga a que estes sejam gerados a partir do arquivo */dev/urandom*, diminuindo substancialmente a qualidade de pseudoaleatoriedade mas garantindo sempre bastante rapidez.

## 1.2 Pergunta P1.2

- `head -c 1024 /dev/random | openssl enc -base64` - demorou 0.007 segundos;
- `head -c 1024 /dev/urandom | openssl enc -base64` - demorou 0.007 segundos.

O software *HAVEGE* explora as alternâncias dos estados do *hardware* volátil interno e usa-os como fontes de incerteza, isto é, aumenta a quantidade de entropia que já se tinha, e assim, é previsível que o primeiro comando que dantes demorava minutos, seja obtido quase instantaneamente, tal como o segundo. Executando os comandos, as previsões confirmam-se, tendo até

os tempos medidos coincido.

## 2. Partilha/Divisão de segredo (*Secret Sharing/Splitting*)

### 2.1 Pergunta P2.1

O programa em questão pede ao utilizador um determinado segredo que o mesmo queira partilhar e dividir e uma palavra chave para tornar esse segredo acessível apenas por quem a conhecer. Para o reconstituir, o utilizador pode posteriormente desvendar esse segredo utilizando um de outros dois executáveis que podem requer todas ou apenas algumas partes nas quais foi dividido.

#### Parte A

Para podermos responder à questão, tivemos inicialmente que gerar o par de chaves e construir e gerar o respetivo certificado:

- `openssl genrsa -aes128 -out private-key.pem 1024`
- `openssl req -key private-key.pem -new -x509 -days 365 -out mykey.crt`

Posteriormente, executou-se o comando `python createSharedSecret-app.py 8 5 4110173577 private-key.pem`, onde 8 é o número de partes em que o segredo é dividido, 5 o número de partes necessárias para a reconstrução do segredo, 4110173577 o identificador do segredo e `private-key.pem` o par de chaves necessário para a construção do segredo.

O resultado foram 8 objetos *JWT* que foram escritos no *STDOUT*.

#### Parte B

Para reconstruirmos o segredo inicial podemos utilizar o executável que necessita apenas de algumas partes em que o segredo foi dividido - `recoverSecretFromComponents-app.py` - ou podemos utilizar o executável que requer todas as partes em que o segredo foi dividido - `recoverSecretFromAllComponents-app.py`.

A principal diferença útil entre um e outro acontece quando existe a necessidade de alteração de segredo que requer a "autorização" de todas as partes que nele intervêm. Por outro lado, se se quiser "facilitar" a alteração do segredo reduz-se o número de partes necessárias para a sua

reconstituição.

## 4. Algoritmos e tamanhos de chaves

### 4.1 Pergunta P4.1

- **Algoritmo de assinatura utilizado:** *RSA* com *SHA256*.
- **Algoritmo da chave pública utilizado:** *RSA*.
- **Tamanho da chave pública:** *4096 bits*

```

ricardo@noone:~/Downloads$ openssl x509 -in cert.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            01:a2:92:29:c8:88:b3:1b:a4:79:f6:7a:55
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = AT, L = Vienna, ST = Austria, O = ARGE DATEN - Austrian Society for Data Protection, OU = GLOBALTRUST Certification Service, CN = GLOBALTRUST, emailAddress = info@globaltrust.info
        Validity
            Not Before: Jun 12 00:00:00 2015 GMT
            Not After : Sep 18 00:00:00 2036 GMT
        Subject: C = AT, ST = Wien, L = Wien, O = e-commerce monitoring GmbH, OU = GLOBALTRUST Certification Service, CN = GLOBALTRUST QUALIFIED 1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (4096 bit)
            Modulus:
                00:d9:d5:9b:3d:03:19:e4:f8:f7:be:c3:45:43:53:
                7e:74:4d:4f:5f:a3:be:65:2f:ad:e7:7e:f6:87:b5:
                ed:fe:1d:59:68:9a:77:80:2e:9b:f2:9d:15:55:c7:
                0d:6b:cf:3a:a1:f3:76:3d:6c:ac:f0:5e:04:64:b5:
                99:13:4b:45:24:df:16:e0:12:b4:04:8b:90:94:25:
                0d:6b:cf:3a:a1:f3:76:3d:6c:ac:f0:5e:04:64:b5:
                99:13:4b:45:24:df:16:e0:12:b4:04:8b:90:94:25:
                53:73:ec:c3:7f:90:0b:de:f2:56:17:41:1d:8e:bf:
                0e:34:5b:25:6e:9b:5c:9c:88:95:b8:47:ea:2f:da:
                6f:41:bb:53:90:7f:f3:13:94:7a:af:8a:2d:57:a7:
                9a:e3:39:ed:f6:b7:ec:59:66:de:62:24:91:2a:42:
                54:67:6c:83:9e:f9:b1:d0:21:35:da:30:40:c7:67:
                55:73:01:ec:39:40:4a:cc:91:5c:a3:d6:6a:2b:da:
                44:81:1b:c3:2a:e0:85:a7:96:5b:16:ad:21:59:17:
                be:21:cf:13:cb:cd:ac:8b:fe:04:ce:4a:04:34:80:
                ae:3f:d2:54:87:49:b6:29:6c:9b:e8:67:a3:c1:e9:
                ed:03:91:7f:1a:57:b2:e3:a0:3f:e1:77:e7:89:41:
                11:5d:04:c5:a1:99:a8:18:59:5f:3a:cd:56:ce:04:
                0b:e9:a1:18:8c:0c:a4:fb:46:1d:10:c4:b7:77:9f:
                b2:65:b7:4a:68:22:f8:8d:9c:0e:30:68:c9:de:42:
                4b:ff:7c:62:18:6b:83:01:65:cf:87:47:e5:b0:a4:
                2a:11:08:fa:73:7d:60:b6:33:31:c0:3e:c5:15:35:
                3f:fd:71:96:70:5e:29:d9:00:50:0d:7a:15:8f:72:
                40:2e:4d:fa:4b:51:5f:cb:9d:84:0e:1c:f7:82:d4:
                99:f3:97:2d:53:19:02:9e:fb:c8:3e:6f:75:08:f1:
                10:24:af:3a:f2:f9:d7:d5:ac:1e:1c:dc:64:f0:3b:
                6c:9a:93:09:c5:e7:5f:d0:34:24:1f:9e:b1:93:45:
                da:9c:6d:51:50:fb:60:c4:f3:85:8c:80:36:6e:eb:
                79:17:c7:73:0d:a6:82:f9:f1:ec:46:c2:1a:9d:88:

```

**Figura 4.1:** 1ª parte do resultado

```

79:17:c7:73:0d:a6:82:f9:f1:ec:46:c2:1a:9d:88:
12:49:09:cd:e5:75:63:b3:df:c2:d6:ad:d6:e5:9b:
8d:07:c6:c1:fb:cb:9f:da:16:51:6a:64:e3:fd:da:
00:af:86:5c:b7:31:ee:a1:52:77:1b:37:17:c2:9d:
f2:89:f3:10:88:0d:1a:82:65:b7:b7:5b:61:f7:46:
a7:b4:9a:75:e7:ce:79:ce:6b:81:2f:7f:ae:44:5c:
5a:92:04:be:cf:1a:61:cc:a6:ac:fa:f4:16:fe:95:
e8:61:de:c4:0b:ef:23:f7:d5:9f:be:02:cd:8c:3b:
f2:31:65
Exponent: 3 (0x3)
X509v3 extensions:
  X509v3 Basic Constraints: critical
    CA:TRUE, pathlen:0
  X509v3 Key Usage: critical
    Certificate Sign, CRL Sign
  X509v3 Subject Key Identifier:
    23:BD:9C:59:A4:B9:33:BF:75:44:DD:D0:14:43:84:D6:2C:10:78:A0
  X509v3 Authority Key Identifier:
    keyid:C0:01:D5:E0:78:1F:2F:74:3A:E3:EB:C0:21:52:A6:04:EE:26:CB:A
4
Authority Information Access:
  OCSP - URI:http://ocsp.globaltrust.eu
  CA Issuers - URI:http://service.globaltrust.eu/static/globaltrus
t2006-der.cer
  CA Issuers - URI:http://service.globaltrust.eu/static/globaltrus

X509v3 CRL Distribution Points:

  Full Name:
    URI:http://service.globaltrust.eu/static/globaltrust2006.crl

X509v3 Certificate Policies:
  Policy: 1.2.40.0.36.1.1.8.1
    CPS: http://www.globaltrust.eu/certificate-policy.html
  Policy: 0.4.0.1456.1.1

Signature Algorithm: sha256WithRSAEncryption
78:4a:8f:f3:c6:fd:d5:97:c4:75:29:c0:28:3a:7b:02:31:bb:
d8:a5:63:e1:91:47:66:13:cb:0f:b4:41:f4:36:d4:ea:16:a4:
de:d3:0c:e9:90:8f:ba:fa:15:8e:0e:b4:9d:df:ff:24:3e:38:
dc:eb:27:1d:94:95:62:f9:8c:88:91:37:f3:26:4d:48:3c:fa:
ff:3e:38:20:93:a0:ab:c6:53:d2:ea:49:ee:e7:d1:c4:ee:aa:
89:43:40:67:95:17:64:03:39:08:42:19:51:56:01:95:a2:49:
e4:39:14:e6:09:7d:de:d5:90:e7:1b:dd:2e:13:cc:42:7e:f1:
5e:85:d6:ea:20:5a:2d:ae:6b:5b:38:de:9e:2f:12:c1:38:7b:
f8:44:87:e0:1c:16:fc:11:97:88:7b:65:65:a4:e1:8c:42:ea:
72:1e:4b:f0:34:70:fa:47:40:e5:d4:46:92:00:da:23:60:d7:

```

**Figura 4.2:** 2ª parte do resultado

```
89:43:40:67:95:17:64:03:39:08:42:19:51:56:01:95:a2:49:
e4:39:14:e6:09:7d:de:d5:90:e7:1b:dd:2e:13:cc:42:7e:f1:
5e:85:d6:ea:20:5a:2d:ae:6b:5b:38:de:9e:2f:12:c1:38:7b:
f8:44:87:e0:1c:16:fc:11:97:88:7b:65:65:a4:e1:8c:42:ea:
72:1e:4b:f0:34:70:fa:47:40:e5:d4:46:92:00:da:23:60:d7:
c9:76:4d:8b:7b:ab:97:a0:e0:a8:c3:d3:e5:3f:fb:63:10:3b:
fd:b9:86:cd:10:06:de:3e:58:a9:85:40:7e:da:6b:4d:6a:3d:
1f:e7:34:ed:4c:c8:80:b5:48:07:4d:bd:c1:0a:93:79:1c:d0:
ac:7c:d1:48:b7:1f:e0:cf:bd:68:b2:75:07:4b:81:b9:ba:5e:
98:1a:49:fc:ee:b3:f4:8e:c3:8c:c4:8a:0f:08:cd:6c:ea:dd:
49:a9:79:56:27:18:8c:a3:c8:2d:67:5b:d3:1a:f9:fa:ae:ca:
81:08:12:48:74:ac:b5:ba:4e:ef:cf:a8:8c:0f:17:a9:ff:cf:
b2:18:34:16:07:bd:db:da:7c:24:e2:03:b5:ae:c4:31:e4:8f:
e9:fe:7c:2a:fc:bb:70:f9:78:f2:c6:1f:7d:0c:1b:f7:81:e4:
9f:fb:21:bf:f0:82:ea:fa:32:f5:11:67:99:c9:df:ba:d8:e1:
cd:9b:83:3e:72:fb:09:74:3e:63:36:0a:7a:3c:c7:9d:0b:64:
27:dd:d8:c3:6e:de:3b:a8:09:5d:12:7f:41:69:63:db:9f:57:
6f:ef:0d:09:7c:22:24:d0:46:dd:e3:ec:92:c2:7e:f8:b7:b3:
b1:99:6d:23:d5:c9:5e:4b:20:c8:4b:44:78:2a:93:27:6b:85:
cf:34:ff:a4:3f:42:b0:f6:33:0e:2c:fe:25:ac:7e:68:4f:81:
06:be:e0:02:7b:d8:fa:ad:fa:f6:dd:55:1d:ea:57:44:f9:de:
38:90:c6:9d:a7:92:51:d0:52:a5:ff:49:cb:25:0d:9d:ce:f8:
20:ba:c8:98:c4:69:74:d3:12:bb:2e:b3:21:b9:a8:1f:70:2d:
0b:3e:b0:63:54:5e:bd:a3
```

**Figura 4.3:** 3ª parte do resultado