Weronika Domczewska 323621 30.11.2020

Sprawozdanie poprawkowe ze sprawdzianu 1

Zadanie 1

- $\rho\frac{Du}{Dt} = (\rho\frac{\partial u}{\partial t} + \mathbf{u}\cdot\nabla\mathbf{u}) = -\nabla\bar{p} + \nabla\cdot\{\mu(\nabla\mathbf{u} + \nabla\mathbf{u})^T - \frac{2}{3}(\nabla\cdot u)\mathbf{I}\} + \rho\mathbf{g}$
- $\tilde{f}(\xi) = \int_{-\infty}^{\infty} f(x)e^{-2\pi ix\xi}dx$
- $\mathbb{P}(\hat{X}_n - z_1 - \frac{\alpha}{2}\frac{\sigma}{\sqrt{n}} \leq \mathbb{E}X \leq \hat{X}_n - z_1 - \frac{\alpha}{2}\frac{\sigma}{\sqrt{n}}) \approx 1 - \alpha$
- $$\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} \otimes \begin{bmatrix}0 & 5\\ 6 & 7\end{bmatrix} = \begin{bmatrix}1\begin{bmatrix}0 & 5\\ 6 & 7\end{bmatrix} & 2\begin{bmatrix}0 & 5\\ 6 & 7\end{bmatrix}\\ 3\begin{bmatrix}0 & 5\\ 6 & 7\end{bmatrix} & 4\begin{bmatrix}0 & 5\\ 6 & 7\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0 & 5 & 0 & 10\\ 6 & 7 & 12 & 24\\ 0 & 15 & 0 & 20\\ 18 & 21 & 24 & 28\end{bmatrix}$$

Zadanie 2

1.

```
weronika@weronika-VirtualBox:~/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/weronika/.ssh/id_rsa): klucz_git
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in klucz_git
Your public key has been saved in klucz_git.pub
The key fingerprint is:
SHA256:JldMeN21BRDGnsvBHrcr7mu2WEsXUkIMDlhTJOUTBhY weronika@weronika-VirtualBox
The key's randomart image is:
```

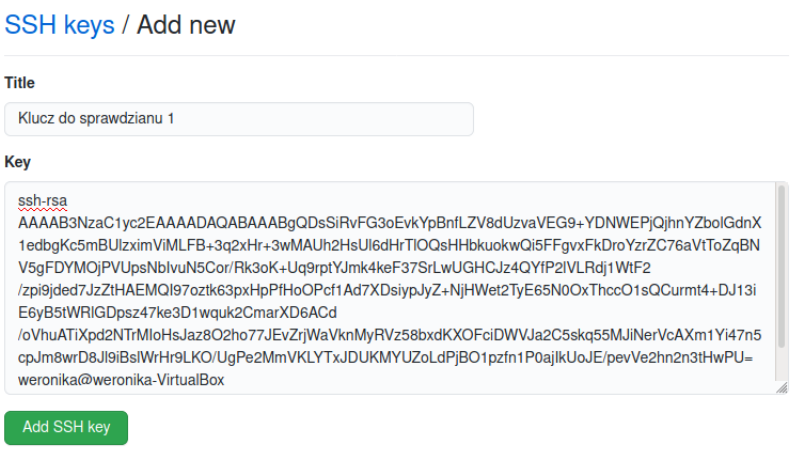
Analogicznie wygenerowałam klucz do serwera.

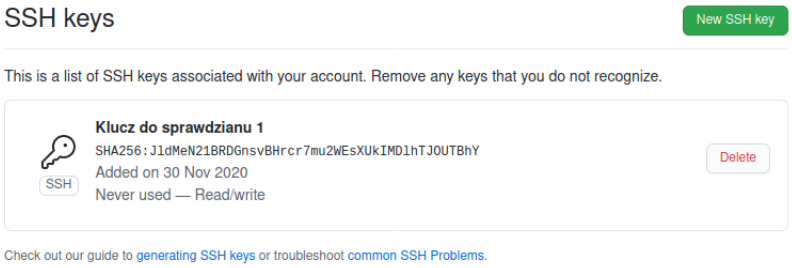
2.

```
weronika@weronika-VirtualBox:~/.ssh$ ssh-copy-id -i ~/.ssh/klucz_ssh.pub d323621@pwi.ii.uni.wroc.pl
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/weronika/.ssh/klucz_ssh.pub"
The authenticity of host 'pwi.ii.uni.wroc.pl (156.17.4.60)' can't be established.
ECDSA key fingerprint is SHA256:t7wSHC5+lROzhY/Hir13kkYXCWIGaC5K1NMQlIbxY4c.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'd323621@pwi.ii.uni.wroc.pl'"
and check to make sure that only the key(s) you wanted were added.
```

Przełącznik -i (identity file) zapewnia dodanie jedynie wybranego przez nas klucza.

3.





4.

```
weronika@weronika-VirtualBox:~/.ssh$ cat config
Host pwi-sprawdzian
        HostName pwi.ii.uni.wroc.pl
        User d323621
        IdentityFile ~/.ssh/klucz_ssh
        ForwardAgent yes
```

5. Klucz lokalny przekierowuję poprzez dodanie do pliku konfiguracyjnego opcji `ForwardAgent yes`

```
ForwardAgent
        Specifies whether the connection to the authentication agent (if any) will be forwarded to the remote
        machine.  The argument may be yes, no (the default), an explicit path to an agent socket or the name of
        an environment variable (beginning with '$') in which to find the path.

        Agent forwarding should be enabled with caution.  Users with the ability to bypass file permissions on
        the remote host (for the agent's Unix-domain socket) can access the local agent through the forwarded
        connection.  An attacker cannot obtain key material from the agent, however they can perform operations
        on the keys that enable them to authenticate using the identities loaded into the agent.
```

Zadanie 3

1.

```
weronika@weronika-VirtualBox:~$ ssh pwi-sprawdzian
Linux pwi 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Nov 30 15:07:14 2020 from 90.156.8.78
d323621@pwi:~$ git clone git@github.com:weronikadomczewska/PWI-sprawdzian-d323621.git
fatal: destination path 'PWI-sprawdzian-d323621' already exists and is not an empty directory.
d323621@pwi:~$ ls
PWI-sprawdzian-d323621
d323621@pwi:~$ rm -rf PWI-sprawdzian-d323621/
d323621@pwi:~$ git clone git@github.com:weronikadomczewska/PWI-sprawdzian-d323621.git
Cloning into 'PWI-sprawdzian-d323621'...
The authenticity of host 'github.com (140.82.121.4)' can't be established.
RSA key fingerprint is SHA256:nThbg6kXUpJWGl7E1IGOCspRomTxdCARLviKw6E5SY8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'github.com,140.82.121.4' (RSA) to the list of known hosts.
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
```

Generowanie kolejnego klucza na zdalnym komputerze jest "brzydkie", ponieważ klucz jest jak nasz podpis - pozwala nas zidentyfikować w jednoznaczny sposób. Kiedy generujemy drugi klucz, utrudniamy identyfikację.
2.
Pobrałam plik przy pomocy `wget http://www.ii.uni.wroc.pl/~lisu/zadanie.tar.gz`
Wypakowałam plik przy pomocy polecenia `tar -xvf zadanie.tar.gz`
Znaczenie przełączników:
`-x` - wypakuj plik
`-v` - pokaż postęp wypakowywania (informacje o wypakowanych plikach)
`-f` - nazwa archiwum do wypakowania

Skomitowałam wszystko przy pomocy poleceń `git add .` oraz `git commit`

3.

```
   32  echo -n d323621 | md5sum
   33  find -name d44d6db6d4914e64e1f3f5e2ff509eca
   34  cd ./zadanie/b97e53755343e2bb57a7208e882bbc59/650d83d0e073f5dc4737941941e150a4/52e9bc351e8ad7283b1926d44d3a8b24
4d6db6d4914e64e1f3f5e2ff509eca
   35  ls
   36  cat zadanie.txt
```

Znaczenie przełączników w `echo`:
`echo` - wypisz na konsolę `-n` - nie dodawaj na koniec znaku nowej linii
`|` - przekieruj output `echo` do następnego programu
`md5sum` - program do wyznaczania funkcji skrótu MD5 ze stringa

Znaczenie przełączników w `find`:
`-name` - szukaj w folderze po nazwie
Zadania z pliku `zadanie.txt`:

```
W pliku users.db znajduje się lista maili wraz z hasłami użytkowników spotify.
------------------------------------------------------------
Zadanie jest proste i składa się z 2 podpunktów:
1) Trzeba dowiedzieć się jaki jest procentowy stosunek
    użytkowników z polski do wszystkich którym wykradziono hasła.
    Czego można użyć jako Bashowego kalkulatora?

2) Stworzyć nowy plik o nazwie passwords.txt w którym
    znajdą się TYLKO hasła w pliku users. Każde w osobnej linii.

------------------------------------------------------------
Oczywiście jak w całym sprawdzianie nie zależy mi tylko na wyniku, ale i na poleceniach
    terminala których użyliście by go uzyskać
```

Podpunkt 1
Jako kalkulatora używam `python3`.

```
Python 3.7.3 (default, Jul 25 2020, 13:03:44)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> plik = open("users.db").readlines()
>>> for linia in plik:
...
KeyboardInterrupt
>>> pol = 0
>>> for linia in plik:
...     if "POLAND" in linia:
...             pol += 1
...
>>> pol
328
>>> procent = pol/len(plik)
>>> procent
0.013978265501811209
>>>
```

Użytkownicy z Polski stanowili około 1.4% użytkowników

Podpunkt 2

```
8ad7283b1926d44d3a8b24/d44d6db6d4914e64e1f3f5e2ff509eca$ cat users.db | sed -E 's/^.+:(.+?)\s\|.+\|.+$/\1/g' > passwords.
txt
```

Znaczenie komend:
`cat` - wypisz zawartość pliku
`sed` - program do dokonywania zmian w tekście
`-E` - użyj rozszerzonych instrukcji RE
`s` - zamień
wyrażenie regularne - od początku do końca linii znajdź cokolwiek co występuje przynajmniej raz, następnie dwukropek, potem hasło złożone z czegokolwiek, co występuje przynajmniej raz (? - wyszukujemy do pierwszego wystąpienia znaku białego), następnie szukamy pipe, po nim cokolwiek, pipe i cokolwiek do końca linii
`\1` - zastąp całą linię znalezionym hasłem
`g` - zastąp w całym pliku
`> passwords.txt` - przekieruj wynik do pliku passwords.txt

Bibliografia:

- https://www.digitalocean.com/community/tutorials/how-to-configure-custom-connection-
- https://linuxize.com/post/using-the-ssh-config-file/
- https://oeis.org/wiki/List_of_LaTeX_mathematical_symbols
- https://regexr.com/
- https://www.geeksforgeeks.org/sed-command-in-linux-unix-with-examples/