

Kolokwium 1

Jacek Długopolski

30 listopada 2020

Zadanie 1

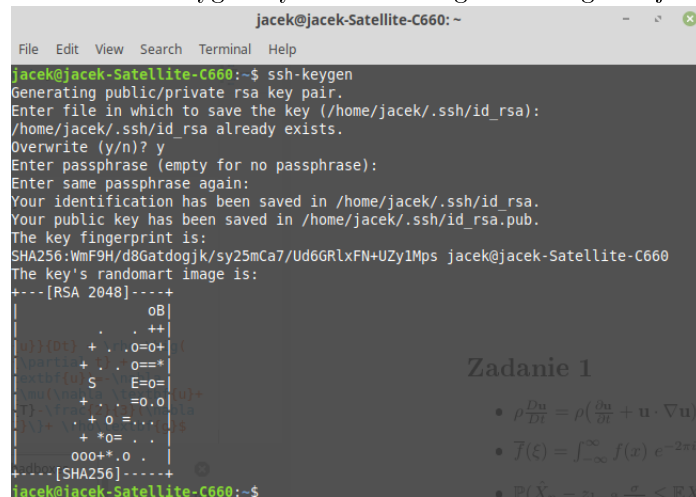
- $\rho \frac{D\mathbf{u}}{Dt} = \rho \left(\frac{\partial \mathbf{u}}{\partial t} + \mathbf{u} \cdot \nabla \mathbf{u} \right) = -\nabla \bar{p} + \nabla \cdot \{ \mu (\nabla \mathbf{u} + (\nabla \mathbf{u})^T - \frac{2}{3} (\nabla \cdot \mathbf{u}) \mathbf{I} \} + \rho \mathbf{g}$
- $\bar{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi} dx$
- $\mathbb{P}(\hat{X}_n - z_{1-\frac{\alpha}{2}} \frac{\sigma}{\sqrt{n}} \leq \mathbb{E}X \leq \hat{X}_n + z_{1-\frac{\alpha}{2}} \frac{\sigma}{\sqrt{n}}) \approx 1 - \alpha$
- $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} = \begin{bmatrix} 1 & \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} \\ 3 & \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 & 5 & 0 & 10 \\ 6 & 7 & 12 & 14 \\ 0 & 5 & 0 & 10 \\ 6 & 7 & 12 & 14 \end{bmatrix}$

Zadanie 2

1. Generuję lokalnie dwa klucze ssh poleceniem:

`ssh-keygen`

Polecenie `ssh-keygen` wywołane bez argumentów generuje klucz RSA.



```
jacek@jacek-Satellite-C660: ~  
File Edit View Search Terminal Help  
jacek@jacek-Satellite-C660:~$ ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/jacek/.ssh/id_rsa):  
/home/jacek/.ssh/id_rsa already exists.  
Overwrite (y/n)? y  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/jacek/.ssh/id_rsa.  
Your public key has been saved in /home/jacek/.ssh/id_rsa.pub.  
The key fingerprint is:  
SHA256:WmF9H/d8Gatdogjk/sy25mCa7/Ud6GRLxFN+UZy1Mps jacek@jacek-Satellite-C660  
The key's randomart image is:  
+--[RSA 2048]-----+  
|          oB|  
|      .  ++|  
|o) (DT) + . 0=0+|  
|p=) + . 0=*|  
|xH (S) E=0=|  
|u(y) + . 0.0+|  
|T) + . 0 =...|  
|) + . 0 =...|  
| + *0= . .|  
|____000+*.0 .|  
+---[SHA256]-----+  
jacek@jacek-Satellite-C660:~$
```

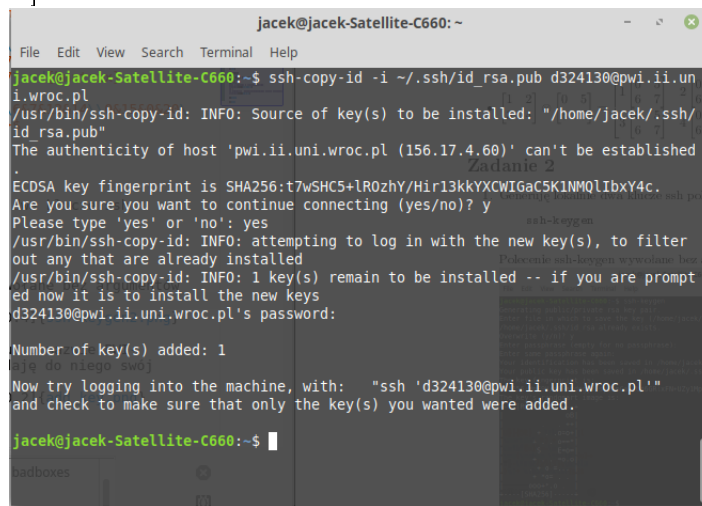
Zadanie 1

- $\rho \frac{D\mathbf{u}}{Dt} = \rho \left(\frac{\partial \mathbf{u}}{\partial t} + \mathbf{u} \cdot \nabla \mathbf{u} \right)$
- $\bar{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi} dx$
- $\mathbb{P}(\hat{X}_n - z_{1-\frac{\alpha}{2}} \frac{\sigma}{\sqrt{n}} \leq \mathbb{E}X \leq \hat{X}_n + z_{1-\frac{\alpha}{2}} \frac{\sigma}{\sqrt{n}}) \approx 1 - \alpha$

2. Przenoszę klucz na zdalny serwer używając polecenia:

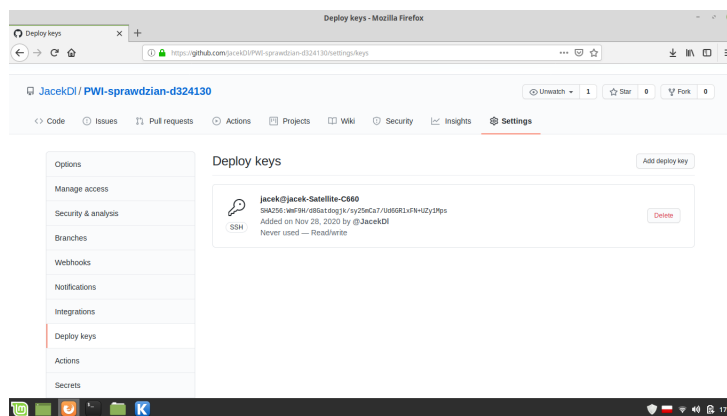
```
ssh-copy-id -i ~/.ssh/id_rsa.pub d324130@pwi.ii.uni.wroc.pl
```

-i identityfile Use only the key(s) contained in identityfile (rather than looking for identities via ssh-add(1) or in the defaultIDfile)[man ssh-copy-id]



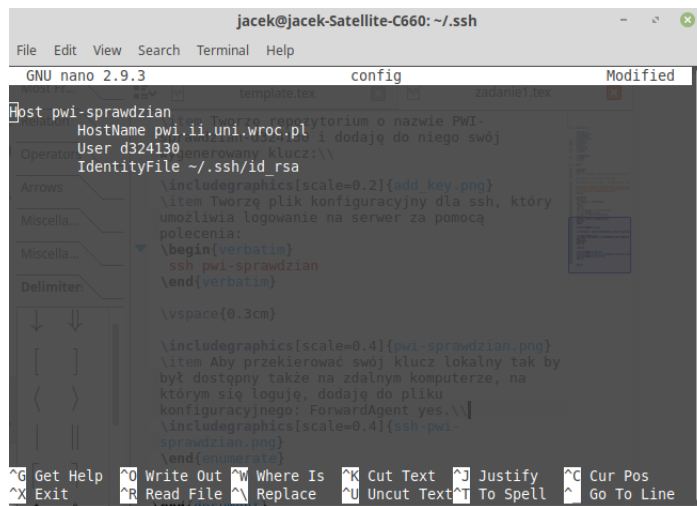
```
jacek@jacek-Satellite-C660: ~  
File Edit View Search Terminal Help  
jacek@jacek-Satellite-C660:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub d324130@pwi.ii.uni.wroc.pl  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/jacek/.ssh/id_rsa.pub"  
The authenticity of host 'pwi.ii.uni.wroc.pl (156.17.4.60)' can't be established  
ECDSA key fingerprint is SHA256:t7wSHC5+lr0zHY/Hir13kkYXCWIGaC5K1NMQLibxY4c.  
Are you sure you want to continue connecting (yes/no)? y  
Please type 'yes' or 'no': 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  
d324130@pwi.ii.uni.wroc.pl's password:  
  
Number of key(s) added: 1  
Now try logging into the machine, with: "ssh 'd324130@pwi.ii.uni.wroc.pl'" and check to make sure that only the key(s) you wanted were added.  
jacek@jacek-Satellite-C660:~$
```

3. Tworzę repozytorium o nazwie PWI-sprawdzian-d324130 i dodaję do niego swój wygenerowany klucz:



4. Tworzę plik konfiguracyjny dla ssh, który umożliwia logowanie na serwer za pomocą polecenia:

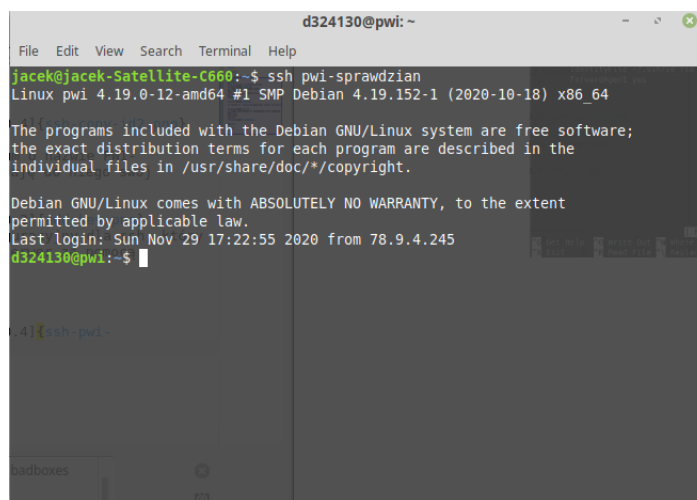
```
ssh pwi-sprawdzian
```



The screenshot shows a terminal window with the title 'jacek@jacek-Satellite-C660: ~/.ssh'. The nano text editor is open, editing a file named 'config'. The file contains the following text:

```
Host pwi-sprawdzian
  HostName pwi.ii.uni.wroc.pl
  User d324130
  IdentityFile ~/.ssh/id_rsa

  \includegraphics[scale=0.2]{add_key.png}
  \item Tworzę reperytorium o nazwie PWI-
  \item Tworzę plik konfiguracyjny dla ssh, który
  \item umożliwia logowanie na serwer za pomocą
  polecenia:
  \begin{verbatim}
    ssh pwi-sprawdzian
  \end{verbatim}
  \vspace{0.3cm}
  \includegraphics[scale=0.4]{pwi-sprawdzian.png}
  \item Aby przekierować swój klucz lokalny tak by
  był dostępny także na zdalnym komputerze, na
  którym się loguję, dodaję do pliku
  konfiguracyjnego: ForwardAgent yes.\
  \includegraphics[scale=0.4]{ssh-pwi-
  sprawdzian.png}
  \end{document}
```



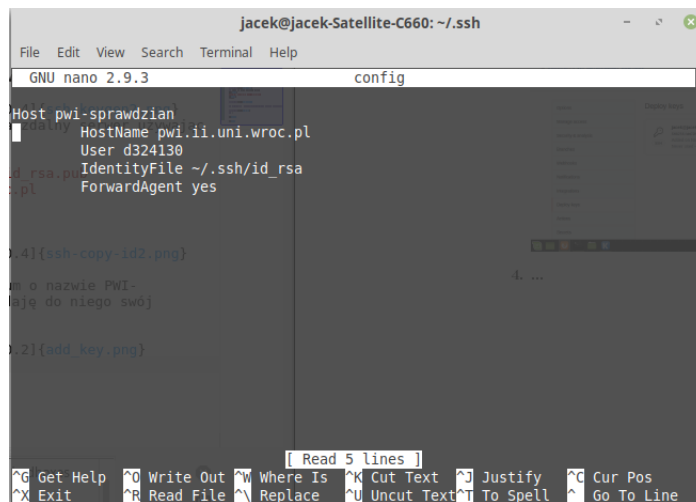
The screenshot shows a terminal window with the title 'd324130@pwi: ~'. The terminal displays the output of the command 'ssh pwi-sprawdzian'. The output is as follows:

```
jacek@jacek-Satellite-C660:~$ 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: Sun Nov 29 17:22:55 2020 from 78.9.4.245
d324130@pwi:~$
```

5. Aby przekierować swój klucz lokalny tak by był dostępny także na zdalnym komputerze, na którym się loguję, dodaję do pliku konfiguracyjnego: ForwardAgent yes.

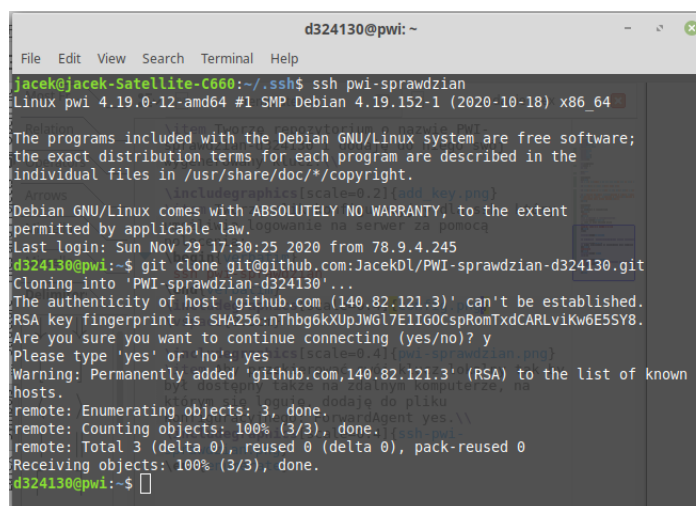


Rozwiązanie polegające na wygenerowaniu kolejnego klucza jest 'brzydkie', ponieważ tworzy również klucz prywatny, który pozostaje na zdalnym komputerze.

Zadanie 3

1. Loguję się na pwi.ii.uni.wroc.pl. Klonuję repozytorium z GitHuba poleceniem:

```
git clone git@github.com:JacekDl/PWI-sprawdzian-d324130.git
```



2. Pobieram poleceniem wget plik ze strony:

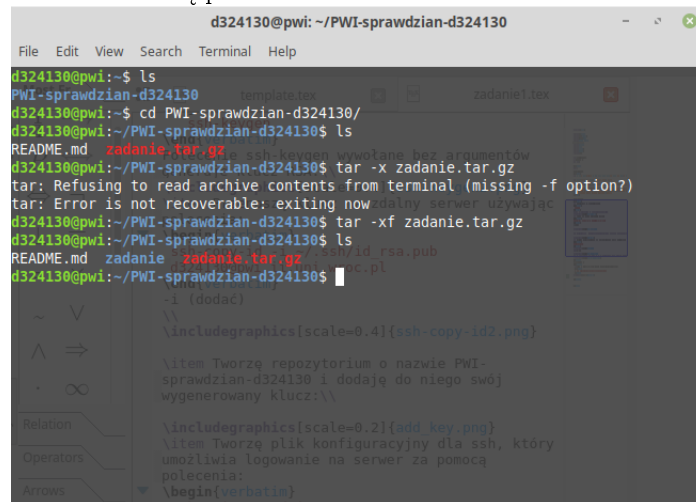
```
wget http://www.ii.uni.wroc.pl/~lisu/zadanie.tar.gz
```

Następnie wypakowuję ten plik w repozytorium:

```
tar -xf zadanie.tar.gz
```

-x wyodrębnia pliki

-f określa nazwę pliku archiwum tar

A screenshot of a terminal window titled 'd324130@pwi: ~/PWI-sprawdzian-d324130'. The terminal shows the following commands and output:

```
d324130@pwi:~$ ls
PWI-sprawdzian-d324130
d324130@pwi:~$ cd PWI-sprawdzian-d324130/
d324130@pwi:~/PWI-sprawdzian-d324130$ ls
README.md  zadanie.tar.gz
d324130@pwi:~/PWI-sprawdzian-d324130$ tar -x zadanie.tar.gz
tar: Refusing to read archive contents from terminal (missing -f option?)
tar: Error is not recoverable: exiting now
d324130@pwi:~/PWI-sprawdzian-d324130$ tar -xf zadanie.tar.gz
d324130@pwi:~/PWI-sprawdzian-d324130$ ls
README.md  zadanie  zadanie.tar.gz  ssh/id_rsa.pub
d324130@pwi:~/PWI-sprawdzian-d324130$
```

I komituję zmiany:

```
git add .
git commit -m "Dodano pliki z archiwum tar"
```

3. Wyliczam funkcję skrótu MD5 ze stringa d324130 poleceniem:

```
echo -n "d324130" | md5sum
```

-n nie dolicza znaku nowej linii na końcu napisu podanego jako argument
[www.bytfreaks.net]

```
d324130@pwi: ~  
File Edit View Search Terminal Help  
d324130@pwi:~$ echo -n "d324130" | md5sum  
7eccfe492d21bf21d0f8e788aba5d7bd -  
d324130@pwi:~$  
\begin{verbatim}  
git clone git@github.com:JacekDl/PWI-  
  sprawdzian-d324130.git  
\end{verbatim}  
\includegraphics[scale=0.4]{gitclone.png}  
\item Pobieram poleceniem wget plik ze strony:  
\begin{verbatim}  
wget http://www.ii.uni.wroc.pl/~lisu/  
  zadanie.tar.gz  
\end{verbatim}  
Następnie wypakowuję ten plik w repozytorium:  
\begin{verbatim}  
tar -xvf zadanie.tar.gz  
\end{verbatim}  
-x wyodrębnia pliki\\  
-f określa nazwę pliku archiwum tar\\  
\includegraphics[scale=0.4]{tar.png}\\  
I komituję zmiany:  
  
\end{enumerate}
```

Odnajduję w gąszczu pobranych folderów katalog:

```
find -name "7eccfe492d21bf21d0f8e788aba5d7bd"
```

```
d324130@pwi: ~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7...  
File Edit View Search Terminal Help  
5294a893bf7f394081aee670dbb07864 bc44cf067c774918f1f0172b9b3a82e3  
581ed6549131526fd6e89368e7ffd081 c8646ec970158541b21d64a805fa1db5  
5ec2424ff3ca9087bb6f43ef9c7a065d d089ca5020f5ffd91db572d7092c7dda  
62084588c149c62b82a33b02fbaafc04 d753127100ac9d12c51b6c6b94e8a452  
6305d57f8c9a598f6a271c5e5de2022c e8db5f9da18b0611a01ca55be90fd70  
671434f9e489641418ec491b874abd1c f2c7dd88657a1e28db388ea50242c08f  
6a8385ce85cbf636fc07c0d8bd55a503 fdb733f327f602436a44f2994e30ccd7  
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie$ man find  
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie$ man find  
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie$ find -name ^C  
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie$ find -name 7eccfe492d21bf21d0f8e78  
8aba5d7bd  
./b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3  
033c650c1c8450d77df2/7eccfe492d21bf21d0f8e788aba5d7bd  
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie$ cd ./b07ad8e0d38ce8c8d112f9c7cb4ab  
4a8/29b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d  
21bf21d0f8e788aba5d7bd  
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29  
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21  
d0f8e788aba5d7bd$ ls  
users.db  zadanie.txt  
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29  
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21  
d0f8e788aba5d7bd$  
\end{enumerate}
```

Następnie wykonuję polecenia z zadania:

a) Sprawdzam jaki jest procentowy stosunek użytkowników z Polski do wszystkich którym wykradziono hasła:

```
grep -c "Country" users.db  
grep -c "Country = POLAND" users.db
```

I wykorzystuję pythona do obliczeń:

```
d324130@pwi: ~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7...
File Edit View Search Terminal Tabs Help

d324130@pwi: ~/PWI-sprawdzian-d324130... x jacek@jacek-Satellite-C660: ~/pwi/lista03 x

users.db  zadanie.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ grep -c "Country" users.db
23460
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ grep -c "Country = POLAND" users.db
326
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ 326*100/23460
-bash: 326*100/23460: No such file or directory
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ 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.
>>> 326*100/23460
1.3895993179880648
>>>
```

Wynik $\approx 1,39\%$

b) Tworzę nowy plik passwords.txt do którego zapisuję tylko hasła z users.db poleceniami:

```
touch passwords.txt
sed 's/.*://' users.db > passwords.txt
sed -i 's/|.*//' passwords.txt
```

-i działa w miejscu - modyfikuje plik podany w komendzie

```
d324130@pwi: ~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7...
File Edit View Search Terminal Help

d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ ls
passwords.txt  users.db  zadanie.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ sed 's/.*://' users.db > passwords.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ ls
passwords.txt  users.db  zadanie.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ nano passwords.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ sed -i 's/|.*//' passwords.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ nano passwords.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$
```

W wyniku czego otrzymuję plik zawierający tylko hasła:

```
d324130@pwi: ~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7...
File Edit View Search Terminal Help
GNU nano 3.2 passwords.txt
ahn4584657
3030steff
bloempot
lry75smm
ColaHummel
qwertyuiop
something
ian880831
sanglier
Nicefish27
de29do18
adam2002
ADinarte5
Ju041978
Monica189087
goku77@goku77
Totempole33
peartree15
add_key.png
config.png
find.png
gitclone.png
ssh-keygen.png
ssh-keygen2.png
ssh-pwi-
sprawdzian.png
tar.png
zadanie1.log
zadanie1.pdf
zadanie1.tex
[ Read 23465 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^M Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```