Public/private key generation and data decryption

This document will explain how to generate a public/private keypair that can be used to encrypt and decrypt sensitive user information for the MediaDiary application.

What is a public/private key pair?

A public/private keypair is a linked pair of keys that can be used to encrypt and decrypt data. In our case encryption can be done with the 'public' key, this key can be shared with anyone without compromising security. Other people can then use this key to encrypt data so that only the person with the corresponding 'private' key can decrypt it and read the information.

Generating a public/private key pair

For the MediaDiary app we are making use of a tool that is already built into all major operating systems (windows, linux and macOs). This tool is called ssh-keygen, and has to be accessed from the command line.

you can generate a key with the command `ssh-keygen -t rsa -b 4096`

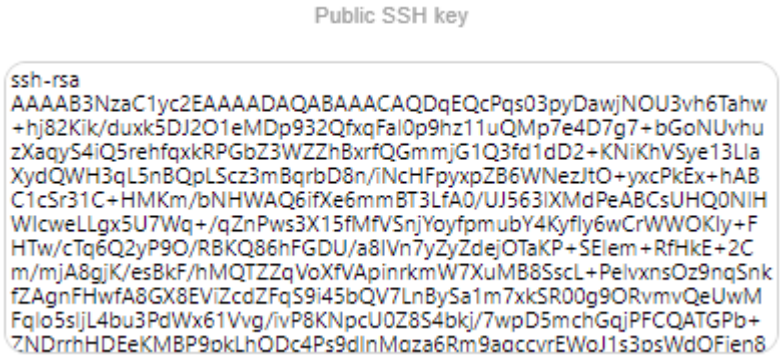
Afterwards you have to specify the location and name of the keypair, although a default is provided.

```
C:\Users\jordy>ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\jordy/.ssh/id_rsa): F:\example_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in F:\example_key.
Your public key has been saved in F:\example_key.pub.
The key fingerprint is:
SHA256:EeYWBR63DLsVpYH0K+IvSgsj63dsm1ayPNrUxeNWjb4 jordy@DesktopBoi
The key's randomart image is:
+---[RSA 4096]----+
|       .O+=..    |
|       +.X =     |
|        * *      |
|       ..+ .o    |
|      . S+.o .   |
|     o.oo.+      |
|. o +.=. o .     |
| o =oXo..    .   |
|o...B=o..  E     |
+----[SHA256]-----+
```

Doing this two files will be generated. in the above example an `example_key` file and an `example_key.pub` file will be generated. the `.pub` file contains the public key which can be used on the MediaDiary app. The `example_key` file (without .pub) is the private key, you should not share this with anyone, and it should not leave the computer you generated it on, as this reduces the security of the private key.

Making a survey with the public key

When making a survey the public key is necessary, the public key file can be opened with a text editor, then you can simply copy paste the key into the public SSH key field.



Make sure to leave no extra spaces or new lines behind the key, this could potentially change the key and mess up encryption.

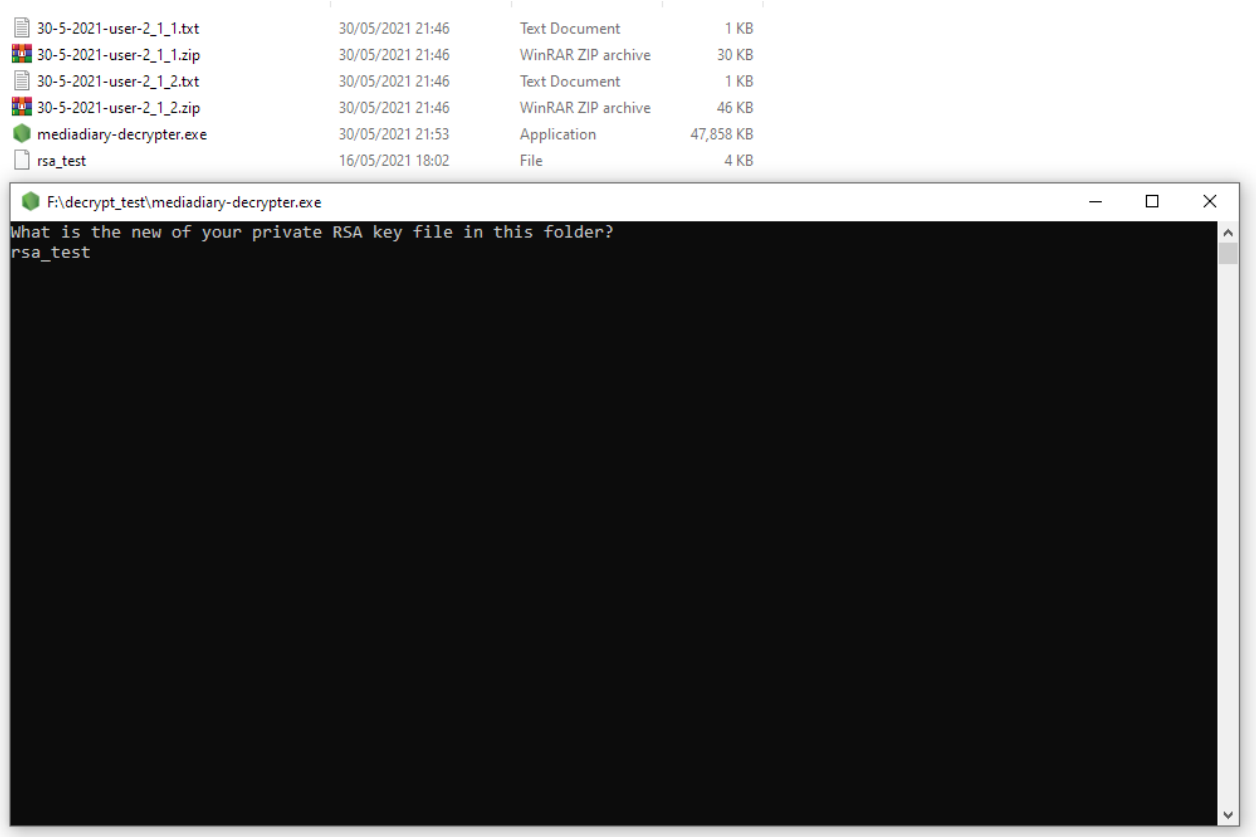
Decrypting survey responses with the private key

When you receive responses you receive named pairs of encrypted zip files and text files containing the encrypted password.

A tool has been created to simplify the decryption of the responses: mediadiary-decrypter. This tool will decrypt the contents of the zip files and place them into corresponding folders:

How to use the mediadiary-decrypter:

1. Place the .zip files and their passwords into a folder
2. Place the mediadiary-decrypter.exe in the same folder
3. Place or copy your private key file into the same folder
4. Run the mediadiary-decrypter.exe
5. Enter the name of your private key file



Now the executable will create a folder for each user and date, containing the responses for that user on that day