Exam #0

1. Encrypt given text with use of given algorithms

**Input:**

Imagination is more important than knowledge. For knowledge is limited, whereas imagination embraces the entire world, stimulating progress, giving birth to evolution. Albert Einstein

* 1. AES Encrypt

**Key:** 357538782F413F444353252176453432

**IV:** fdzggsdfsadasd

**Mode:** CBC

**Input:** RAW

**Output:** HEX

**Output:**

0fbd4ed95eb94db49162f8ec20d028ce

* 1. Blowfish Encrypt

**Key:** 53425435

**IV:** 423

**Mode:** CBC

**Input:** RAW

**Output:** HEX

**Output:**

2bb847a5ba15c6e5

1. Decode given text:

a)

SW5mb3JtYXRpb24gc2NpZW5jZSBpcyBhIGZpZWxkIHByaW1hcmlseSBjb25jZXJuZWQgd2l0aCB0aGUgYW5hbHlzaXMsIGNvbGxlY3Rpb24sIGNsYXNzaWZpY2F0aW9uLCBtYW5pcHVsYXRpb24sIHN0b3JhZ2UsIHJldHJpZXZhbCwgbW92ZW1lbnQsIGRpc3NlbWluYXRpb24sIGFuZCBwcm90ZWN0aW9uIG9mIGluZm9ybWF0aW9uLg==

Information science is a field primarily concerned with the analysis, collection, classification, manipulation, storage, retrieval, movement, dissemination, and protection of information.

I used a wizard stick that automaticly helped me to find right method

b)

4c75626c696e20697320746865206e696e7468206c617267657374206369747920696e20506f6c616e6420616e6420746865207365636f6e64206c6172676573742063697479206f66204c657373657220506f6c616e642e20497420697320746865206361706974616c20616e64207468652063656e746572206f66204c75626c696e20566f69766f646573686970202870726f76696e6365292077697468206120706f70756c6174696f6e206f66203333392c3638322028446563656d6265722032303138292e204c75626c696e20697320746865206c61726765737420506f6c69736820636974792065617374206f66207468652056697374756c6120526976657220616e6420697320617070726f78696d6174656c7920313730206b696c6f6d65747265732028313036206d696c65732920746f2074686520736f75746865617374206f662057617273617720627920726f61642e

Lublin is the ninth largest city in Poland and the second largest city of Lesser Poland. It is the capital and the center of Lublin Voivodeship (province) with a population of 339,682 (December 2018). Lublin is the largest Polish city east of the Vistula River and is approximately 170 kilometres (106 miles) to the southeast of Warsaw by road.

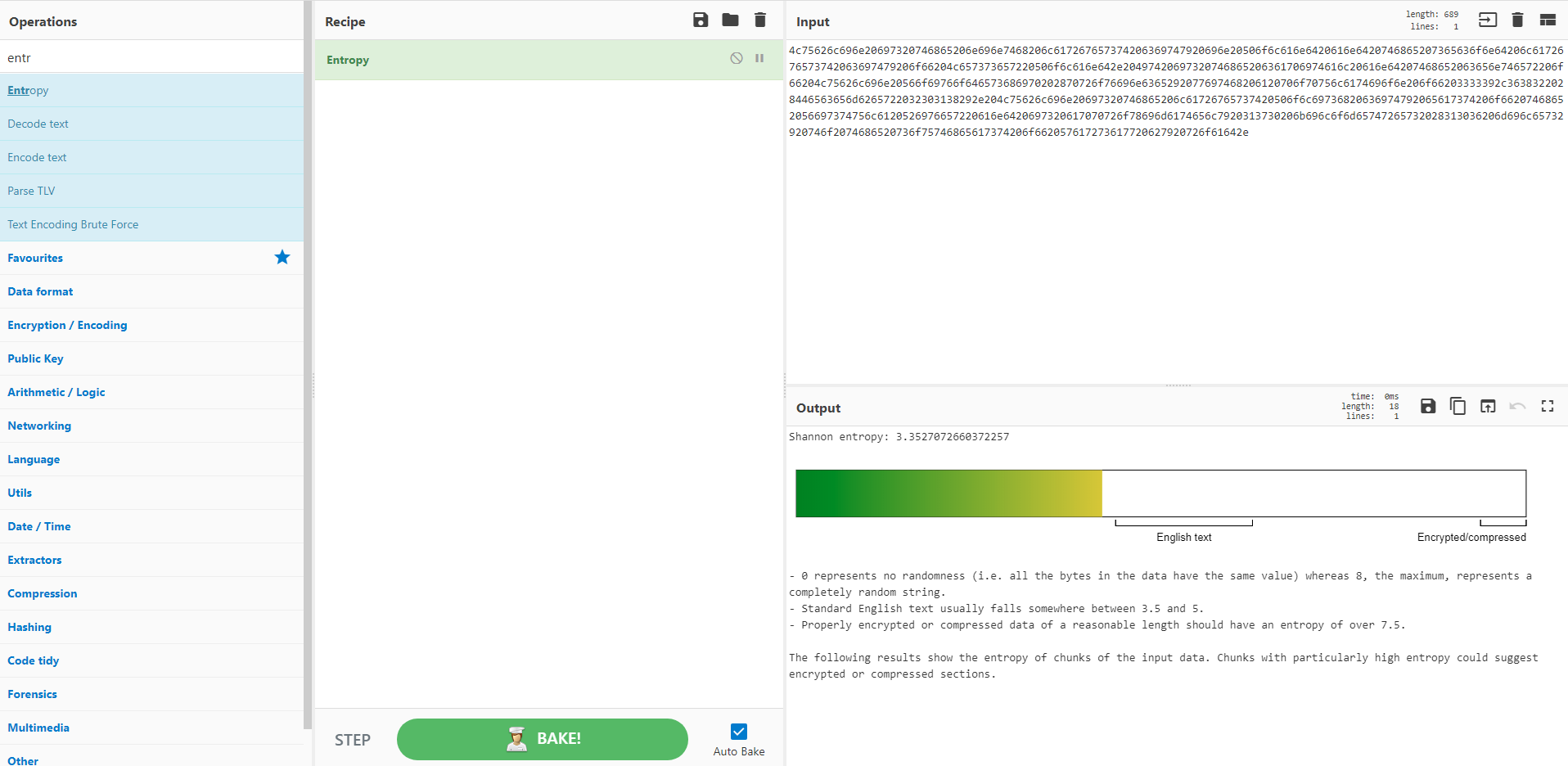
I used special Recipe “From Hex” to decode this text

1. Measure Shannon entropy of given code:

a)

4c75626c696e20697320746865206e696e7468206c617267657374206369747920696e20506f6c616e6420616e6420746865207365636f6e64206c6172676573742063697479206f66204c657373657220506f6c616e642e20497420697320746865206361706974616c20616e64207468652063656e746572206f66204c75626c696e20566f69766f646573686970202870726f76696e6365292077697468206120706f70756c6174696f6e206f66203333392c3638322028446563656d6265722032303138292e204c75626c696e20697320746865206c61726765737420506f6c69736820636974792065617374206f66207468652056697374756c6120526976657220616e6420697320617070726f78696d6174656c7920313730206b696c6f6d65747265732028313036206d696c65732920746f2074686520736f75746865617374206f662057617273617720627920726f61642e

Measure entropy is: 3.3527072660372257



b)

PK........æ.ÐN...N....p.......file.txt.T×..!.]I¤É8.²ÿ.y..D=i¯øL}ÚÞæy|.Ðb.5|¥'¥Î#

ª.É|zÙËãÔ.uJ¼¾N5,¹¯).UÓÛÉ'«¬ÙDyiÙÓ.·VÏ2{þè=$Àúrqg.£^µtùB¹Ëý¸WE..S¿.v\öçÄ®vn\..&Qu¼SIì¼.ºÏ®.Ú.¤1.#¬òhv.æêÎ.=¤±1..m¯õÄzmÃ´.Pn&|¼ºêÎzás.#$Op..16.h[.(Bõj-.Ïù.e

¦ßôE..js¹4#5}'¶¤·¯ìp.÷L2v¡.>V@º.¥Vop`a.¾øxíÝ»eÛAÛ]

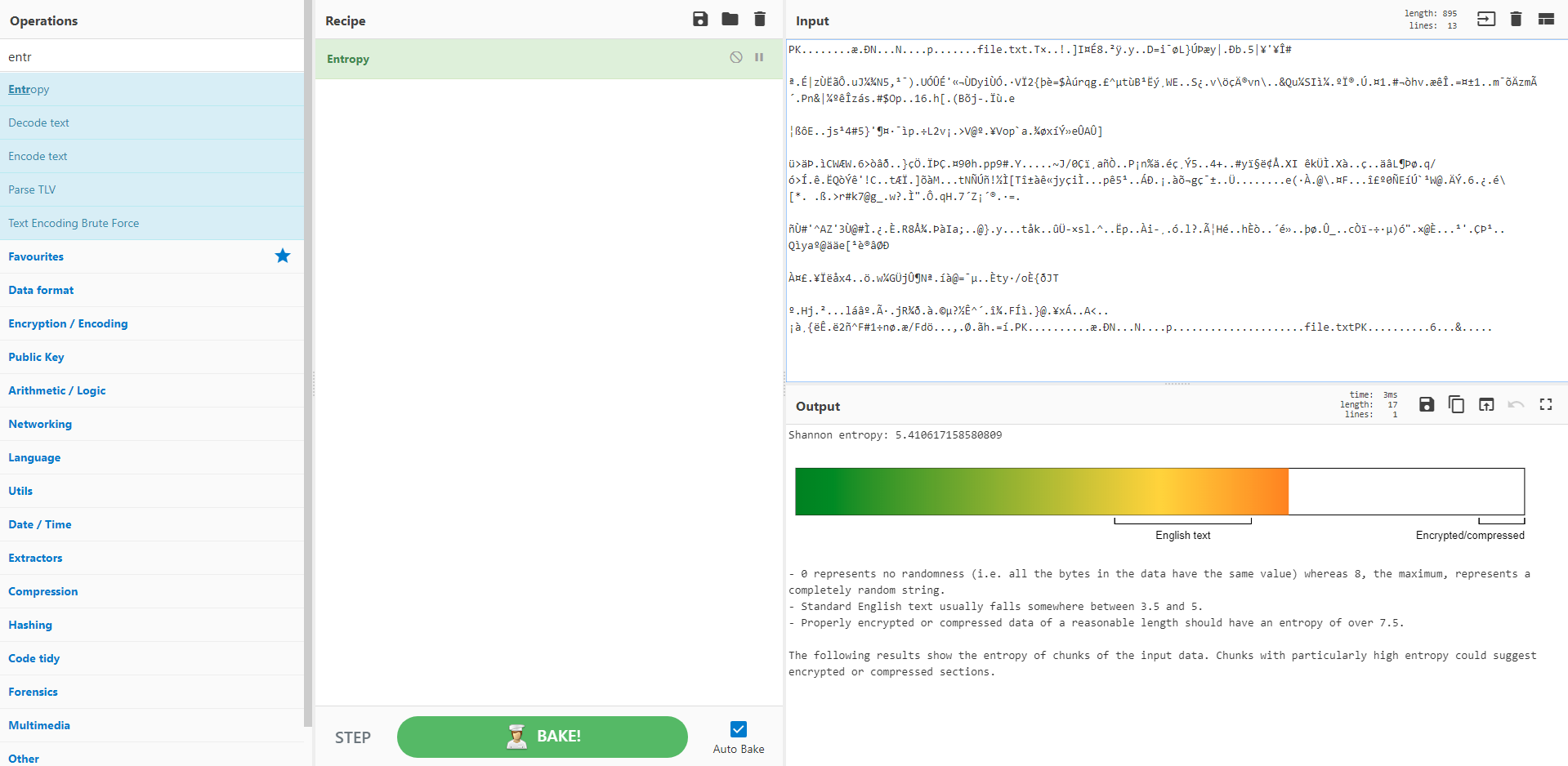
ü>äÞ.ìCWÆW.6>òâð..}çÖ.ÏÞÇ.¤90h.pp9#.Y.....~J/0Çï¸añÒ..P¡n%ä.éç¸Ý5..4+..#yï§ë¢Å.XI êkÜÌ.Xà..ç..äâL¶Þø.q/ó>Í.ê.ËQòÝê'!C..tÆÏ.]õàM...tNÑÚñ!½Ì[Tî±àê«jyçiÌ...pê5¹..ÁÐ.¡.àõ¬gç¯±..Ü........e(·À.@\.¤F...î£º0ÑEíÚ`¹W@.ÄÝ.6.¿.é\[\*. .ß.>r#k7@g\_.w?.Ì".Ô.qH.7´Z¡´®.·=.

ñÙ#'^AZ'3Ù@#Ì.¿.È.R8Å¾.ÞàIa;..@}.y...tåk..ûÜ-×sl.^..Ëp..Ài-¸.ó.l?.Ã¦Hé..hÈò..´é»..þø.Û\_..cÒï-÷·µ)ó".×@È...¹'.ÇÞ¹.. Qìyaº@ääe[¹è®âØÐ

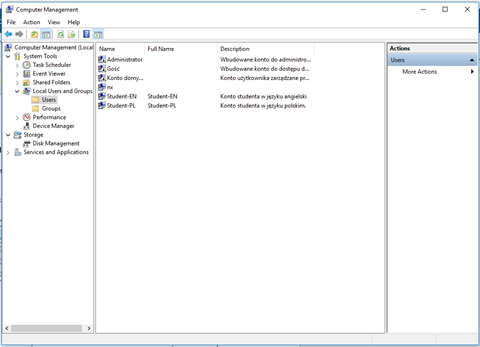
À¤£.¥Ïëåx4..ö.w¼GÜjÛ¶Nª.íà@=¯µ..Èty·/oÈ{ðJT

[º.Hj.²...láâº.Ã·.jR¾ð.à.©µ?½Ê^´.î¾.FÍì.}@.¥xÁ..A<..¡à¸{ëÊ.ë2ñ^F#1÷nø.æ/Fdö...,.Ø.ãh.=í.PK..........æ.ÐN...N....p.....................file.txtPK..........6](mailto:º.Hj.²...láâº.Ã·.jR¾ð.à.©µ?½Ê^´.î¾.FÍì.}@.¥xÁ..A<..¡à¸{ëÊ.ë2ñ^F#1÷nø.æ/Fdö...,.Ø.ãh.=í.PK..........æ.ÐN...N....p.....................file.txtPK..........6)...&.....

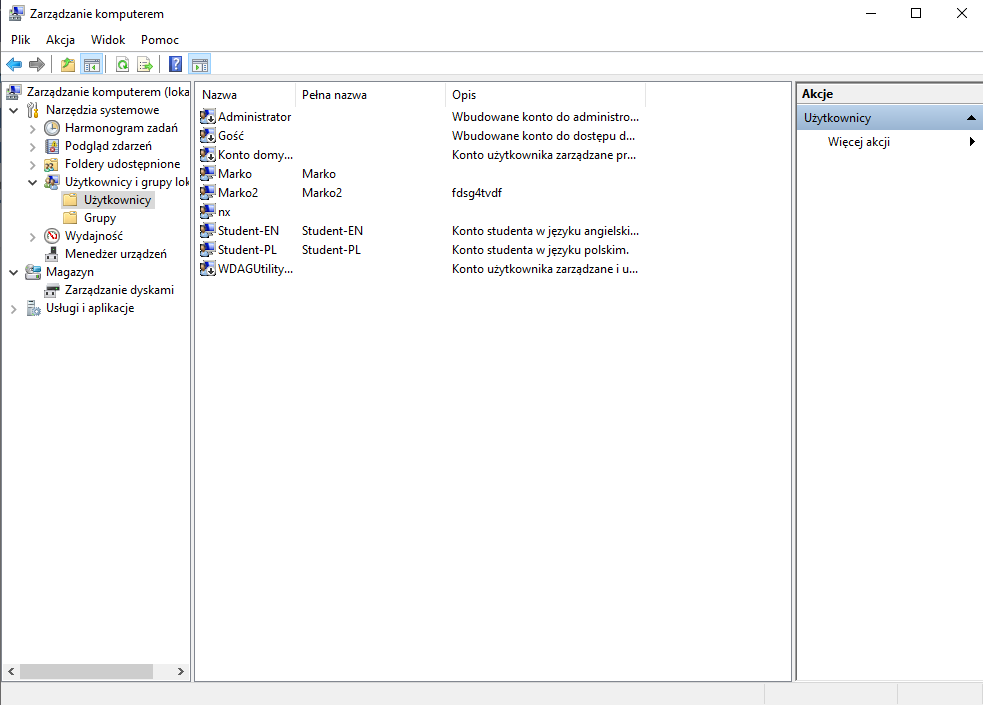
Measure entropy is: 5.410617158580809



1. Check the list of users (right mouse button on "My Computer", command manage).



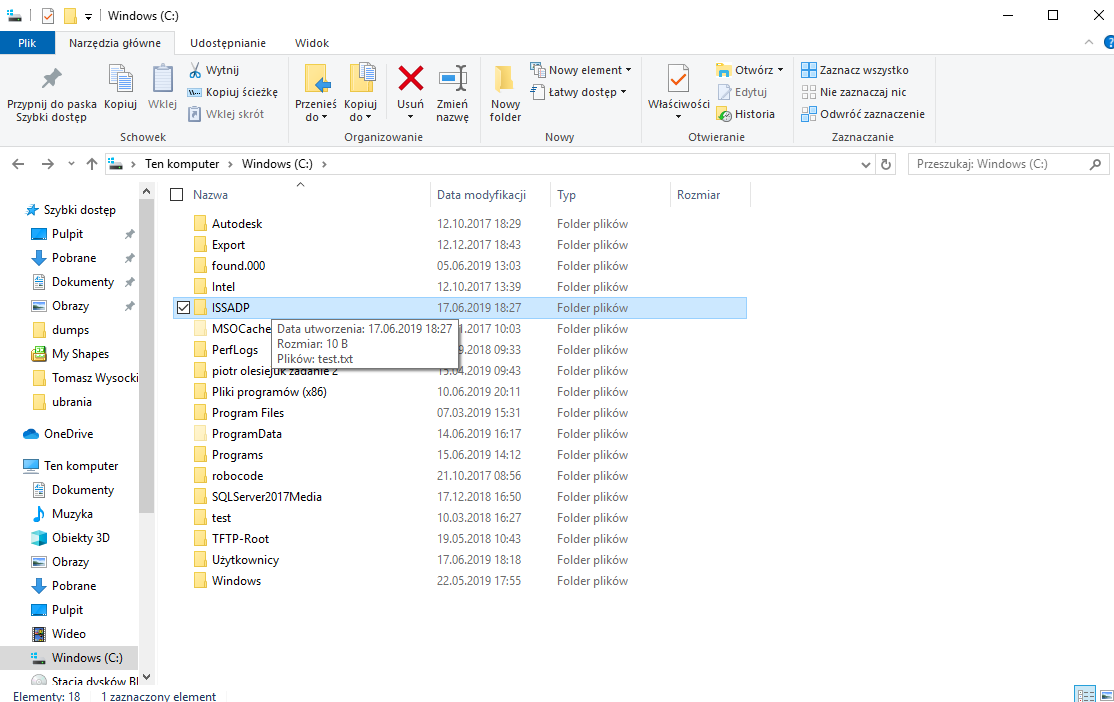
1. Create user [your name] and [your name 2], set passwords for users and change passwords when logging in for the first time.



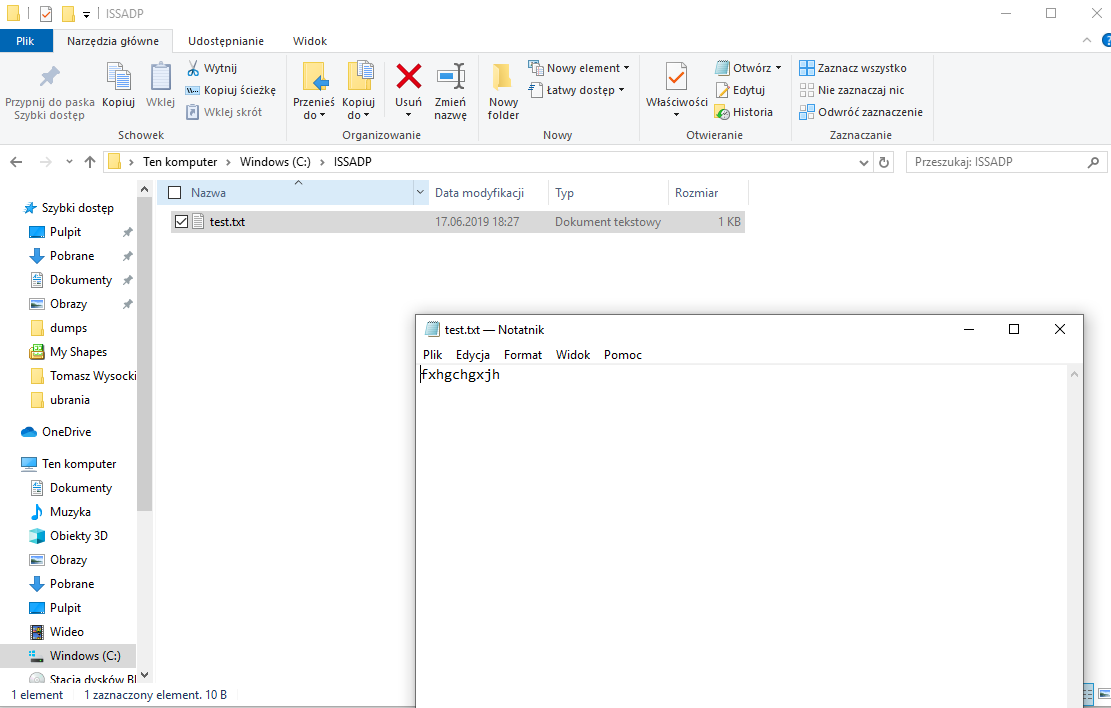
1. Check that you can log in and change your password when you log in for the first time.

I can’t take any screenshot, but i changed the password, its working

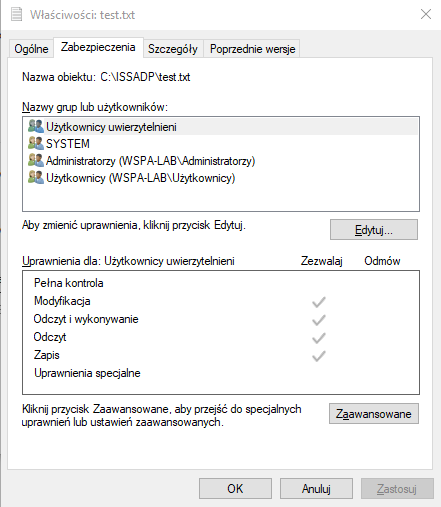
1. Create a ISSADP folder on the local disk.



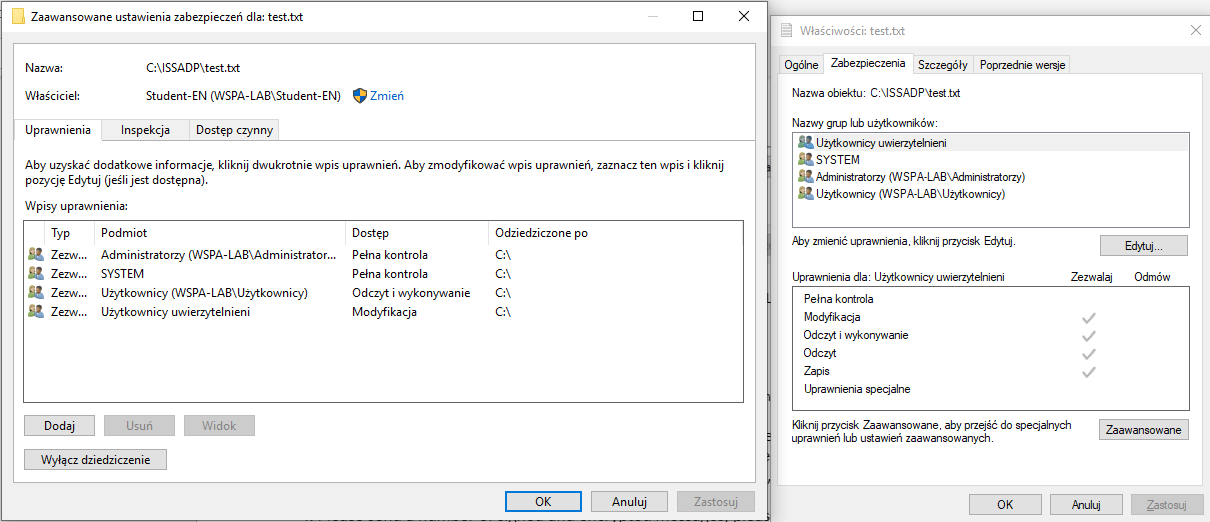
1. Create a test.txt text file with any content in the directory.



1. In the properties of this file we check if there are options available in the Security tab. If the tab is not available, you should find an option to enable this feature.

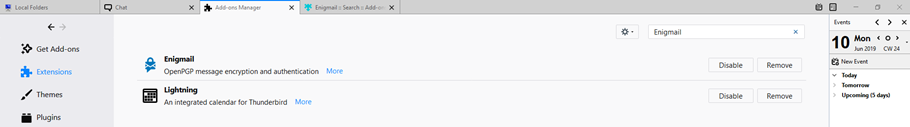


1. Check which options are available in the simple Access Control List and the advanced Access Control List for the file.

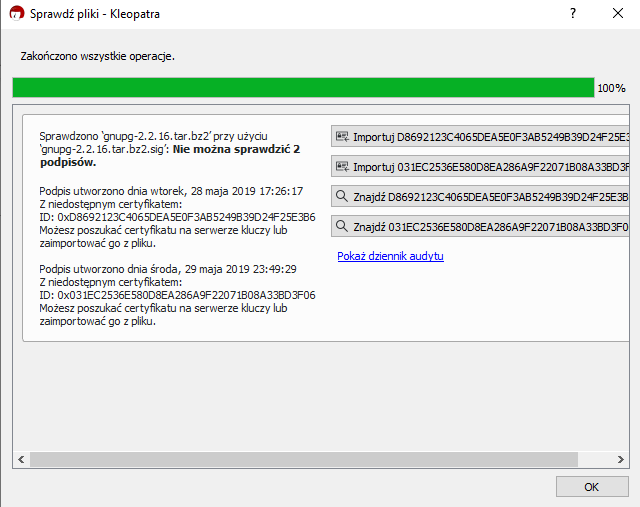


1. Encrypting and signing e-mail continued, generating keys, signing and encrypting files

1. Please install the Enigmail plugin into the Mozilla Thunderbird e-mail client

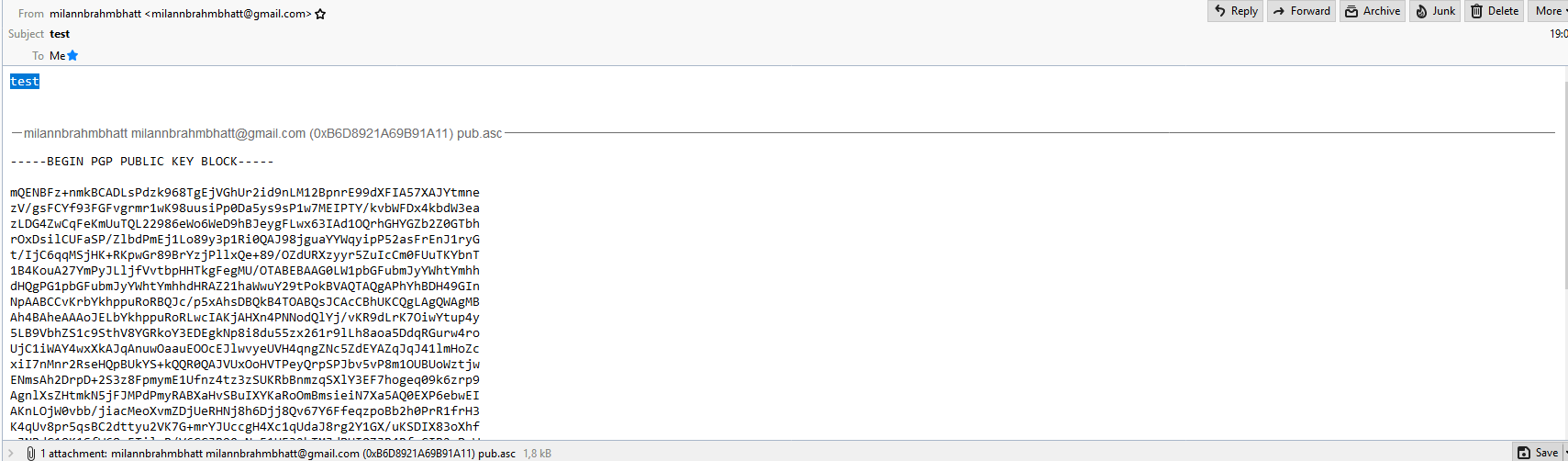


2. To use the plugin, you must install the GnuPG prog ram that the Enigmail add-on uses.

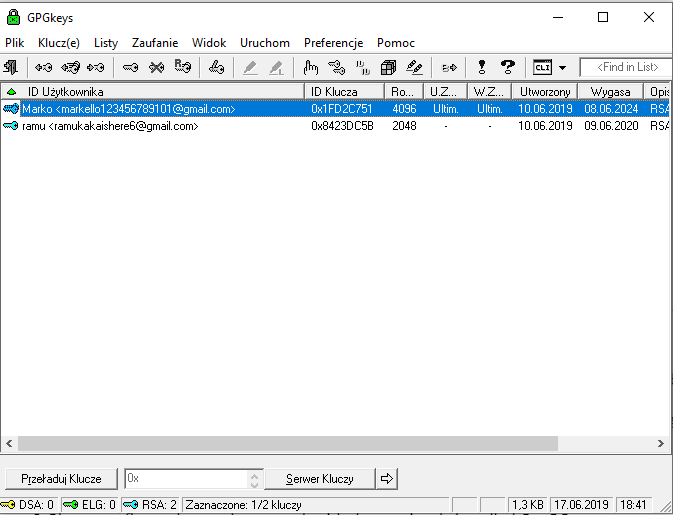


3. The program must be properly configured and a key generated, which will then be used to sign and encrypt the message.

4. Please send a number of signed and encrypted messages, please check how the messages signed and encrypted when accessing the mail by the web client. should any operations be carried out earlier?



5. Please install the GPGshell program, which is an overlay for the GnuPG program with a graphical interface.



6. Please configure the overlay to work with the previously installed GnuPG program.

7. Please familiarize yourself with the functions of the GPGshell program.



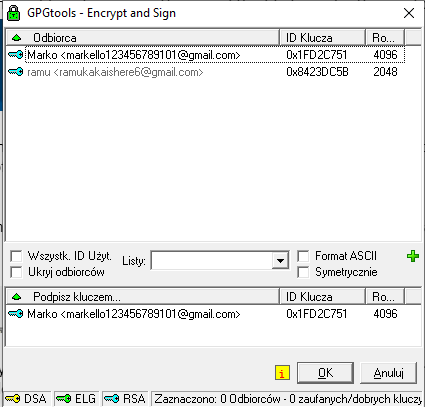
8. Please sign any file in two ways. Then send the file to each other and check the effect.



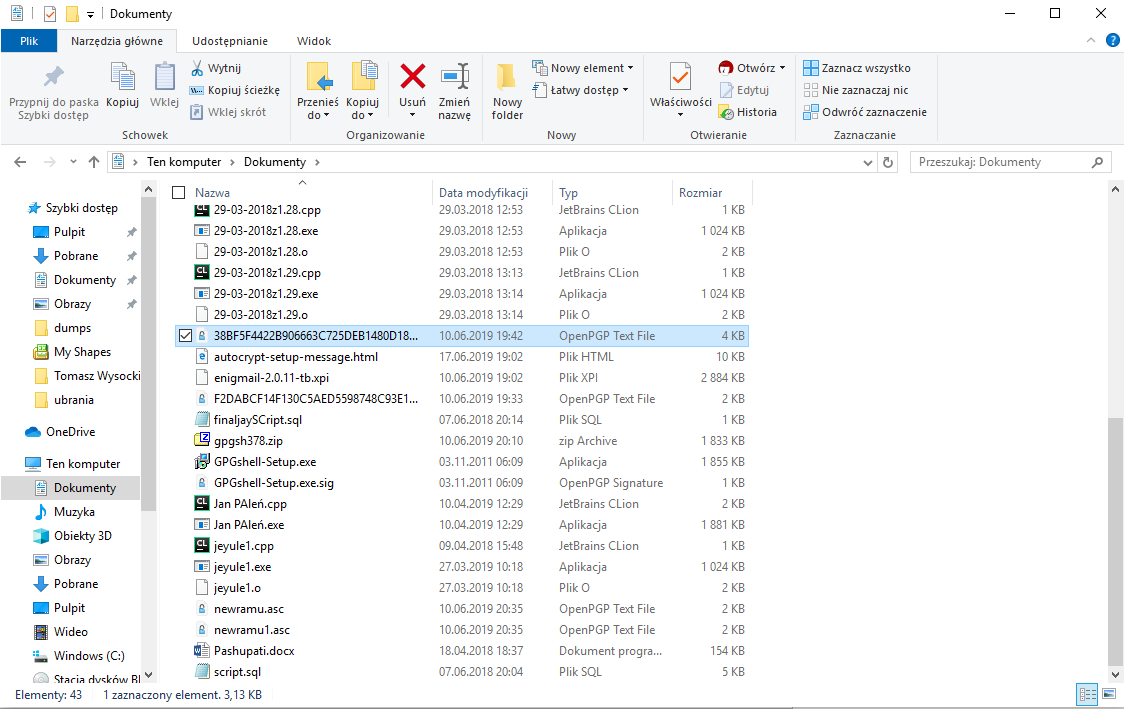
9. Please sign the text file in the form of a detached signature and then change the contents of the file and verify the signature of this file.

10. Please encrypt and sign any file, send it among yourself and try to read its contents.





11. Please try to copy the text to the clipboard and then write it down and paste it into a text document, send it to each other and verify the signature.



12. Please encrypt the text from the clipboard, put it in a text file, exchange it among yourself and finally decrypt and verify the signature.



13. Please encrypt the file with a symmetric key.

Command to encrypt the file test.txt using a symmetric key

*gpg -c test.txt*

Command to decrypt the encrypted file

*gpg -o output.txt test.txt.gpg*

14. Please cancel any key you used and then check the effect.

*gpg -o output.txt -d test.txt.gpg*