# **Practical**

## **Simple AES Problem**

Yasmin has intercepted email traffic between the Master and one of their agents.  **See if you can decrypt the message**.

Master:  Agent 4, execute instructions contained in the attached message [MastersOrder1563.b64](https://learn.vccs.edu/courses/314236/files/92777907/preview).  As usual, the message is encrypted with AES in ECB mode and then Base64 encoded (The Master is too busy to deal with nonces and tags.)  Use the 42nd entry in your book of keys.

Master:  Agent 4, you have not executed my order.  Why?

Agent 4:  Uh, I can’t find my book of keys.

Master:  You idiot!  Look harder!

Agent 4:  Sir, the book of keys was accidentally burned.

Master:  Accidentally!?  By whom!?  Idiot!  I’ll get you the key.

Master:  Dual hearts rule

Instructor note:  In case you can’t find the file [MastersOrder1563.b64](https://learn.vccs.edu/courses/314236/files/92777907/preview), here’s the content

TGFj6ocA5LRj7lFX23zZLTJVZwIJ9ecPDeJ3zt98m8gZGlf0gzuHFRYXrqwOD+TdLbbx5GsUhl3m\nLLQBosBVwXGTOMi5PPaj6QkjLgukWAQcKAFRlFTlj00m7dgB2r+KCLF6i6PWrRU5jvHynL5vy1ut\nWCOtu70kG0wRpXIP4DxdJf2vOkrkJzJ5gq+5dim4Lungicy9LhN03v2WNHiz+q8zaEawXBktXQp+\ndw5nYgX3vLBDbKJ4H6bkSzCBvKScYXxBwNVQJFJABnRsBWtArA==

Note:  Hints are base64.  Easy place to decode base64:  
[https://www.base64decode.org/ (Links to an external site.)](https://www.base64decode.org/)

Hint 1:   
VGhpcyBzaG91bGQgYmUgYWxtb3N0IGlkZW50aWNhbCB0byB0aGUgQUVTLk1PREVfRUNCIGV4YW1wbGUgaW4gQ3J5cHRvIEhvbWV3b3JrIDQu

Hint 2:  
SWYgeW91IGFyZSBwYXN0aW5nIHRoZSBiYXNlNjQgaW50byB5b3VyIFB5dGhvbiwgbWFrZSBzdXJlIGl0IGlzIG9uZSBsb25nIHN0cmluZyB3aXRoIG5vIGNhcnJpYWdlIHJldHVybnMvbGluZSBmZWVkcy4=

Hint 3:  
Y29kZWNzIGFuZCBBRVMgYm90aCB3YW50IGlucHV0IG9mIHR5cGUgYnl0ZXMuICBVc2Ugc29tZXN0cmluZy5lbmNvZGUoKSB0byBjaGFuZ2Ugc3RyaW5nIHRvIGJ5dGVzLiAgVXNlIHNvbWVieXRlcy5kZWNvZGUoKSB0byBjaGFuZ2UgYnl0ZXMgdG8gc3RyaW5nLg==

## **Hash Problem**

Whilst on the Cyberman spaceship, Graham comes across a terminal.  A sticky note near the terminal says, “The credentials for the next account are in file.”  Graham lists the files in the terminal and sees 100 files, file0.txt through file99.txt.  He looks back at the note to see which file he needs, but the sticky note was torn off just after “file”.

Help Graham find the file he needs. All but one of the files are identical; the different file is the one you want. A simple loop that takes the hash of each file is one way to do it. It does not matter which form of hash (MD5, SHA-1, etc.) you use, as we do not expect malicious files that create hash collisions. (There are other ways to solve this if you do not like hashes.)

The files are in [**hashfiles.zip**](https://learn.vccs.edu/courses/314236/files/92777927/preview).  There are 100 files, so put the zip file in its own subdirectory before you unzip.  It could make a mess.  Just sayin’.

**What is the content of the file that contains the credentials?**

Easy way to decode hints:  [https://www.base64decode.org/ (Links to an external site.)](https://www.base64decode.org/)

Terminal Hint 1: Both Linux (md5sum, sha256sum, etc.) and Windows (Get-Filehash) will allow you to use a wild card (\*) in place of the filename to take the hash of every file in a directory. Once you have all the hashes printed out, it is easy to see which file is different.

Python Hint 1: It is easy to do hashes in Python. If you have PyCryptodome installed, you can use this:  
from Crypto.Hash import MD5  
MD5.new(b'this is what I want to hash').hexdigest()

If you don’t have PyCryptodome installed, this works well:  
import hashlib  
hashlib.md5(b'this is what I want to hash').hexdigest()  
Note: the input must be type bytes, b';dlfja;s' or variable.encode()

Python Hint 2  
aW1wb3J0IGhhc2hsaWIKCndpdGggb3BlbignZmlsZTAudHh0JykgYXMgZmg6CiAgICBjb250ZW50ID0gZmgucmVhZCgpLmVuY29kZSgpCm15aGFzaCA9IGhhc2hsaWIubWQ1KGNvbnRlbnQpLmhleGRpZ2VzdCgpCnByaW50KG15aGFzaCk=

Another way Hint:  
RmluZCBhIHdvcmQgaW4gdGhlIGZpcnN0IGZpbGUgdGhhdCB5b3UgZ3Vlc3MgbWlnaHQgbm90IGJlIGluIHRoZSBmaWxlIHRoYXTigJlzIGRpZmZlcmVudApVc2UgZ3JlcCB0byBmaW5kIGEgZmlsZSB0aGF0IGRvZXNu4oCZdCBoYXZlIHRoZSB3b3JkIHlvdSBjaG9zZQpUaGVyZSBpcyBhIGZsYWcgaW4gZ3JlcCBmb3Igbm90IG1hdGNoClVzZSB0aGUgLXIgZmxhZyBmb3IgcmVjdXJzaXZl

## **Cybermen Elliptic Problem**

The Doctor gets on Graham’s terminal on the Cybermen spaceship and immediately fires up Wireshark to see what traffic she can capture.  After examining several TCP streams, she finds an interesting one.

Cybermen Master:  Prepare to receive encrypted message.  Use [Cybermen Elliptic Curve Procedure](https://learn.vccs.edu/courses/314236/files/92777920/preview).  My public key is 17, 23.

Cyberman15:  Acknowledge.  My public key is 17, 88

Cybermen Master:  Message follows.

'+7aYffNYPs+qMlBmPs/9x1FJ+7KhmbudPronEdIWtSUPfvLBwIeEDv4QuHqjMaSWRJ+5OP6n9Ich\nOEiM6CoRD84oF8KppHAulvMNrQTsyco=\n'

[Cybermen Elliptic Curve Procedure is here](https://learn.vccs.edu/courses/314236/files/92777920/preview)[Preview the document](https://learn.vccs.edu/courses/314236/files/92777920/preview)  
[Message as a file is here](https://learn.vccs.edu/courses/314236/files/93176489/preview)

Your job is to decrypt the message (duh 😊).

Hint 1 VGhlIEN5YmVybWVuIGhhdmUgY2hvc2VuIGEgbW9kdWx1cyAoMjExKSBhbmQgY3VydmUgdGhhdCByZXN1bHRzIGluIDIzMiBwb2ludHMuICBJIGd1ZXNzIHlvdSBjb3VsZCBnZXQgYWxsIDIzMiBwb2ludHMgZnJvbSB0aGUgY2FsY3VsYXRvciBhbmQgdGhlbiBicmVhayBvbmUgb2YgdGhlIHB1YmxpYyBrZXlzIHRvIGdldCBhIHByaXZhdGUga2V5LiAgVGhhdCB3b3VsZCBiZSBhIHJlYWwgcGFpbiwgdGhvdWdoLiAgVGhlcmUgaGFzIGdvdCB0byBiZSBhbiBlYXNpZXIgd2F5Lg==

Hint 2  
QmVmb3JlIHlvdSB0cnkgdG8gYnJlYWsgYW55b25l4oCZcyBrZXksIHB1dCB0aGVpciBjdXJ2ZSwgZmllbGQsIGFuZCBiYXNlIHBvaW50IFAgaW50byB0aGUgY2FsY3VsYXRvciBhbmQgcGxheSB3aXRoIE4uICBZb3UgbWF5IGZpbmQgdGhlcmUgYXJlIG5vdCBtYW55IGNob2ljZXMgZm9yIHRoZSBzaGFyZWQga2V5Lg==

Hint 3  
WW91IGNvdWxkIGp1c3QgbGlzdCBhbGwgdGhlIHBvc3NpYmxlIHggY29vcmRpbmF0ZXMgZnJvbSB0aGUgaGludCBiZWZvcmUuICBDb252ZXJ0IHRoZSB4IGNvb3JkaW5hdGVzIHRvIHNlc3Npb24ga2V5cyBhbmQgc2VlIGlmIG9uZSBvZiB0aGVtIGRlY3J5cHRzIHRoZSBtZXNzYWdlLg==