

Homework #9: Crypto

Assignment Details

This homework is due by Monday, April 19th at **11:59PM** ET. Remember there are no late submissions for the homework so please complete it by then.

For this assignment, be sure to document your process, don't just give the answers! Write as if you were explaining to yourself before you figured it out.

Please add the following header to your assignment:

Name: {Firstname Lastname}

UID: {Your UID}

Honor Pledge: *I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.*

Assignment Goal: Apply basic cryptography techniques learned in lecture to the following problems.

Assignment Questions

Question 1 [20 points]: Find the source text from the following strings. (Hint: Cyberchef and <https://www.dcode.fr/en> are great!)

1. Y21zYzM4OHV7ZW5jb2RpbmchPWWuY3J5cHRpb24tcmlnaHQ/fQ==
2. pzpf388h{prnfre_jnfa'g_gung_fzneg}

Question 2:

- We got word that the Bank of Xandar had a data breach and account credentials were leaked. Could you check if `thanos@sna.pp` is in the breach, and if so, tell us their password? (Cracking the entire list does not take long)

The leaked db: (format is `username:cryptoed_password`)

0843089856@sna.pp:05c8408037876647859a737751d4a37b
09265481511@sna.pp:8a4f4a016092956c6ab3119e03867eb2
camilaniky@sna.pp:b0fffb222e73e50f0f8d029b62f82a9c
60985bucaneros15@sna.pp:55c5aed38095529b6dae76bd06fbee35
iloveang*@sna.pp:cc47d539b10517ef6fb62c47ed514361
va40ni@sna.pp:01f5210f2aeb22b39fa924103a0a6950
nayeliscarlett@sna.pp:f0ead30b23d683eb61f36cd6cc844366
PORelmundo8@sna.pp:19022d7ca1e1c79bf42a9ddf451688c9
thanos@sna.pp:e12d61611e2c9780b36e62db6b9668b3
raremen@sna.pp:216e871f9ca090baaa3282ea28d77b2c
lanikque@sna.pp:716c63e240f1f2d3038993edf4f3c1be
NOT4USE@sna.pp:0c44e88854c090c71de3bbbec9175ebe
culobonito@sna.pp:369b73a566dc49a3bb96fa78fc731712
Falcons!@sna.pp:d5faaa50d5b0ff4f50d4ab7cffc4bbe2
CIPHERUS@sna.pp:1d790d204a728cc990475f70dae7a141
doobie4@sna.pp:3240d803d6d01490c0dbe07e6aa7d393
supercalypso@sna.pp:3e9ff02f7b26ae8accd0246f1613afb5
0815383375@sna.pp:522e539b8c52e839b658352a2ea08eda
sorryjose@sna.pp:55073cbf8f40cbb4b434c40391e0c631
marylou131@sna.pp:5df09cf0f9bcf3c25eb29926bbd6051e
4961375@sna.pp:e82792ece6974170144478c832f6997b
darylkrystel@sna.pp:59a15ea5c8d270359cc9ff673d0811d8
nas123@sna.pp:46d3620c3b995e0b692de7083d769b48
politistul@sna.pp:950e75b3078d478e9635090d7766a17a
mydangiu@sna.pp:6d4421397a405da8e9b9daef125b0284
issac0812@sna.pp:7263959d118b222ee368ca009d9fdb6a
78Calvin7@sna.pp:c5a1985a9cf9b9105366d6a47423e62f
arpi92@sna.pp:0c7a911ab8da78f7a37529a79afa8d13
Reginald5@sna.pp:93e3be5beadb36ea08b111f005d4e3a5
onatcoh@sna.pp:7de2874a2757220bfd54e23b25f57e11
023173624@sna.pp:eea3c42bbef0b8bf303a13a2d8a93d1c
9229165@sna.pp:24e94e6a9a5b3bc186afecd26baaffd6
129312jj@sna.pp:0540376b1e5d9dcc470bdd39865ee2cc
07080520@sna.pp:cac0a03af770d15f6fe0936a967fbd56
conniecute@sna.pp:aa1e188eaeead4773a7975b3482a2ab6
tefy69@sna.pp:bc499c727ab52688e053b9513bb591a7
aranhas@sna.pp:41b6fda4d2f39628c384dcc3b429d2c1
linger3@sna.pp:5c5e3f7b392631c6b631e42f7c12aa87
yanuck89@sna.pp:4ff8e24ad8e8b04a00b3bc38e42f1de1
asghxfd@sna.pp:629fff443b67d98655abe7ba00fffc0da
ocean24712@sna.pp:14ec49142801356c35175a27c22e9c15
joom_ae@sna.pp:0f1a4449bc38b9196d6ef3a43a69494e
bigboy97@sna.pp:1655bfc5b43b191970de3b1695c32e28
4201179514@sna.pp:002d461a0b173107dcfff47633d49c52
chloe lowie@sna.pp:9185908a8142636d9101bc60ad34c549
kopink5@sna.pp:273a704e4d45bc79e5156d387ab5b301
9700238264@sna.pp:d4b41e0b0cf25f6e3c30cee21f8660ab
trilogy333@sna.pp:16354b0f33f6e2c5963ae36db8e7c121
32868254@sna.pp:dce4aa2dbd0e4fa6ee2068767dd06497
poolst@sna.pp:842ee5f774eb89619173d952e39b5ee5

Hint: To specify hash type in `john` use `-format="Raw-MD5"`.

Hint #2: You should take a look at the infamous rockyou password wordlist :)

Question 3:

- [We had some technical difficulties making this question - enjoy the lighter hw!]

Scoring

This homework will be out of 90 points total.

Partial credit will be awarded where possible, as long as a good-faith attempt was made.

Point breakdown:

- Question 1 - 30 points (15 points each)
- Question 2 - 40 points
- ~~Question 3 - 0 points~~
- Formatting - 20 points
 - Make sure to talk through the process, not just show the answers!