

Crypto Lab
Sec-250
Your Name Here

Caesar Cipher

Caesar Cipher uses a key called a Shift, which transposes cleartext 'x' amount of times to the right, which results in ciphertext.

cleartext	c	a	t
Shift (Rotate +10)			
ciphertext	m	k	d

Encrypt & decrypt the following **without** online resources, just like the Romans!

1. (ROT3) smegael = **vphjdho**
2. (ROT4) frodo = **jvshs**
3. (ROT9) **gandalf** = pjwmjuo
4. (ROT13) **caesar salad** = pnrjne fnynq

Brute force time ... There's no shift provided, so try all possibilities to decode!

5. **They are taking the hobbits to isengard** = Maxr tkx mtDBGz max ahuubml mh blxgztkw.
 6. What is the shift? **ROT19**
-

Now, look for the row marked 'c' in the left-most column (the key), and the 'c' in the top-most row (plaintext). The intersection of that column and row contains 'e' (ciphertext).

7. Rinse & repeat for the remaining cyphertext, again **without** online resources ... Vive le cryptage!

Message:	c	y	b	e	r	i	s	l	i	f	e
Key:	c	n	c	s	c	n	c	s	c	n	c
Encrypted:	e	l	d	w	t	v	u	d	k	s	g

Completed tabled

Railfence

When you rearrange plaintext in a "wave" pattern (down, down, up, up, down, down, etc.), it is called railfence encryption.

Ex: This plaintext of "happy" looks like this with 3 rails (read: 3 rows) -

```
h   y
 a  p
   p
```

Then when read line-by-line, we get the cyphertext of "hyapp".

8. Decrypt the following ciphertext "crsyectba" built using 3 rails.
cybercats

9. Is Railfence a substitution or transposition cipher? Explain why.

It is a transposition cipher because the letters are rearranged but they are not changed(ie not substituted for other letters

Hashes

We learned how different hash functions produce a unique fixed string of data that should always match to verify data integrity, as long as the data doesn't change.

1. Open a browser to : <https://defuse.ca/checksums.htm>

2. Enter the following phrase into the text area:

Cryptography is as much fun as a person can have!

a. Click "Calculate Checksums"

Are the checksum lengths the same? **No**
How many characters long is each checksum?

MD5 = **32**

SHA1 = **40**

SHA512 = **128**

b. Please take a Snip of results!

The screenshot shows a web interface with a title "Checksums" and a table of results. The table lists various checksum algorithms and their corresponding 32-character MD5, 40-character SHA1, and 128-character SHA512 hashes.

Algorithm	Checksum
md5	584a00726ce415dd0259d94392c5402f
LM	df222ee06aee1a6e3695417d0cc8ee74
NTLM	e331713297be40ec73ea12bb7973798e
sha1	cb8e690206c33ab374f1e1e294a84c5eaaeda2f8
sha256	93aac884e81fb8a3018e91661ba46228b4fb4a7563d34a8b46da85f344122d70
sha384	fb43adc174202f044e38467629260d090859b3693b40f526664c930c1ca4b3f6ef032015492b74fcb16b103c890dccb0
sha512	9949d5a14bdf24b1af9ec45675fcff9ac7e0d03568d007b42676c438bf210691b0f7ed798f0a93f3a777dc2602393c677482ce951ed4ce180548903ea1234f7

3. Change the phrase you typed in by removing one character and click "Calculate."

a. Is the checksum different from the previous computation? **yes**

b. Please take a Snip of results!

The screenshot shows a web interface with a title "File (5MB MAX)" and a "Calculate checksums..." button. Below the button, the results of the checksum calculation are displayed in a table. The table lists various checksum algorithms and their corresponding 32-character MD5, 40-character SHA1, and 128-character SHA512 hashes. The results are different from the previous screenshot, indicating that the checksums are sensitive to changes in the input text.

Algorithm	Checksum
md5	3d81497e7e3a6674434e202645c67b83
LM	df222ee06aee1a6e3695417d0cc8ee74
NTLM	66e8b3c683ff8137253a6bcb1cf1933c
sha1	3e70f345fc3b93da152d726e8c0ecf72b14af4e0
sha256	13289a98133a5794d8e5e7d29b3bbb37597749375a6cb6d94a9924bdf9f46466
sha384	3a12b1d5c9a00ce6570bb09ce0149b65a94680ec2621634e397f487b12d6fff678595568e84a1c2825041b6ca0f6c3af4
sha512	e4c40ff731fa109dc5d21bde25c851b689b746b2bf46a6e1dfb15a178e6150ed97b1ec2c5d775694a520a3aeb81cf1ecf196c4d53d1318909a4c39c148b5f5

4. Next, we going to explore [HMAC](http://beautifytools.com/hmac-generator.php) by opening up <http://beautifytools.com/hmac-generator.php>
5. Copy the same phase into the text box, then type a random string of text in the box "Key" that is displayed when you clicked on HMAC.
 - a. Be sure your key is different than your partners.
 - b. Is your HMAC checksum the same as your partners? Why or why not?
 - i. **No it is not because we both used different keys**
6. Both of you type in "SEC250" as the HMAC key.
 - a. Is the checksum the same for you and your partners? Why or Why not?
 - i. **Yes it is because we both used the same key**
7. Now, let's download & check an [ISO's](#) integrity, something you'll be doing in our program frequently.
8. First, download the CentOS-7 Minimal 1908 ISO here: http://ftp.linux.ncsu.edu/pub/CentOS/7/isos/x86_64/
 - a. FYI: This is a popular Linux OS we use in CNCS
9. Also, open the sha265.sum.txt file. This checksum is what we are going to check the download's checksum against.
10. Now, let's go to <https://md5file.com/calculator> and select the ISO you just downloaded.
11. Once finished calculating, you should see its SHA-256 checksum.
 - a. Do the both sets of checksums match? **yes**
 - b. Provide one Snip including both the md5file.com's checksum + the sha1sum.txt file's checksum, validating the ISO's integrity.

The image shows a file upload interface at the top and a browser window at the bottom. The upload interface displays the filename "CentOS-7-x86_64-Minimal-2207-02.iso" with a size of 1035993088 bytes. Below the filename, the calculated checksums are shown: MD5: 3e39d08511a014c16730650051a0dcca, SHA1: bf8284dad10fea431ad368269afc083a45a8a355, SHA256: d68f92f41ab008f94bd89ec4e2403920538c19a7b35b731e770ce24d66be129a, and SHA512: f005877b402436503e077e7c83529506c08dc36a872b5d2bc7d703ed2143f30c81918a4f63183af3b3ab441a78. The browser window shows a list of files with their corresponding SHA-256 checksums. The file "CentOS-7-x86_64-Minimal-2207-02.iso" is highlighted in blue, and its checksum "d68f92f41ab008f94bd89ec4e2403920538c19a7b35b731e770ce24d66be129a" is also highlighted in blue.

Choose Files No file chosen

CentOS-7-x86_64-Minimal-2207-02.iso - 1035993088 bytes

MD5: 3e39d08511a014c16730650051a0dcca
 SHA1: bf8284dad10fea431ad368269afc083a45a8a355
 SHA256: d68f92f41ab008f94bd89ec4e2403920538c19a7b35b731e770ce24d66be129a
 SHA512: f005877b402436503e077e7c83529506c08dc36a872b5d2bc7d703ed2143f30c81918a4f63183af3b3ab441a78

http://ftp.linux.ncsu.edu/pub/Cer x +

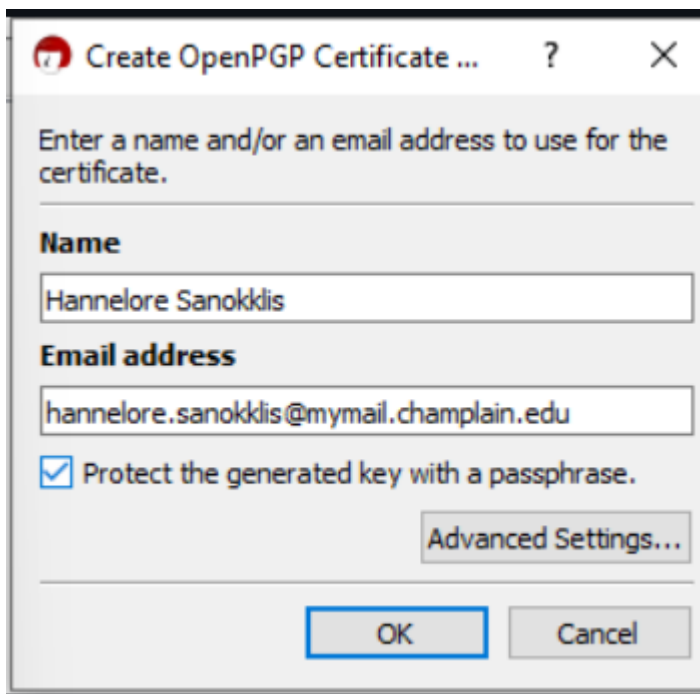
Not secure | http://ftp.linux.ncsu.edu/pub/CentOS/7/isos/x86_64/sha256sum.txt

Champlain My Drive - Google... calendar Typacer Canvas Minitab LC hack tools

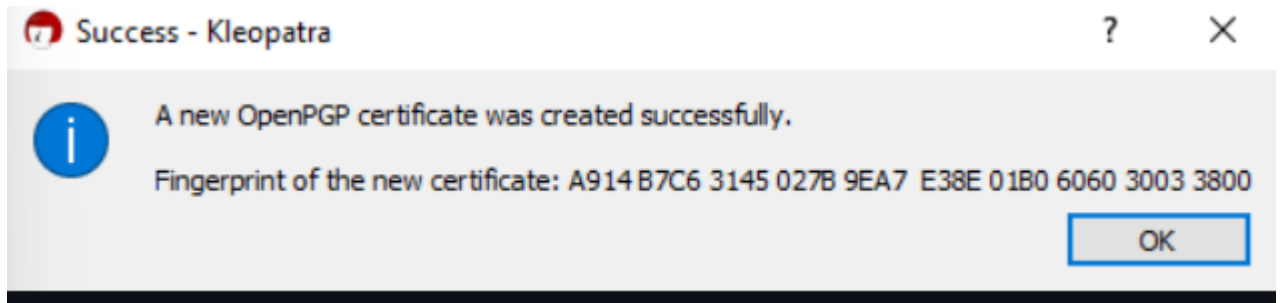
689531cce9cf484378481ae762fae362791a9be078fda10e4f6977bf8fa71350	CentOS-7-x86_64-Everything-2009.iso
b79079ad71cc3c5ceb3561fff348a1b67ee37f71f4cddfec09480d4589c191d6	CentOS-7-x86_64-NetInstall-2009.iso
07b94e6b1a0b0260b94c83d6bb76b26bf7a310dc78d7a9c7432809fb9bc6194a	CentOS-7-x86_64-Minimal-2009.iso
e33d7b1ea7a9e2f38c8f693215dd85254c3a4fe446f93f563279715b68d07987	CentOS-7-x86_64-DVD-2009.iso
4b257cb5418e2ba44064121020dfe457fadaff0d0c597bb2f4e7f7eec4aef58a	CentOS-7-x86_64-DVD-2207-02.iso
f3f83472a24c8ebc66c81b346a743f4000b6b6ddf8c0eb098422d41476873b3b	CentOS-7-x86_64-Everything-2207-02.iso
d68f92f41ab008f94bd89ec4e2403920538c19a7b35b731e770ce24d66be129a	CentOS-7-x86_64-Minimal-2207-02.iso

Fun with Public-Private Keys!

1. Download from pgp4win.org (select \$0 to download for free) on your Windows 10 VM.
 - a. There's an extensive product tech guide with screenshots on how to install & operate this tool <https://files.gpg4win.org/doc/gpg4win-compendium-en.pdf>
 - b. Of course, it's a bit out of date, so the screens nor items may not be exactly the same (because everything online is perfect, right?).
 - c. Your mission: Be curious, explore, test, and win!
 - d. FYI: This is a small taste of higher level courses.
2. Start the install once downloaded:
 - a. Achtung! During the install, please select **ALL** Components to install.
3. Creating a Key pair & Digital Certificate:
 - a. File > Key Pair > Create a personal OpenPGP key pair
 - b. Insert your First & Last name, along with an email address.
 - c. Show all details
 - i. Snip for your details.



- d. Create a passphrase for your private key; strong + something you will NEVER forget
 - i. Snip your successfully created key pair's Fingerprint



4.

5. File > Export your Secret Keys & name your output file your First_Last name, and then save it.
 - a. Just like your car keys, please do not share nor lose this!
6. Now, open up a new program on your desktop, GPA or GNU Privacy Assistant
7. Once opened, you get what's about to happen ... Key Management!
8. You should see your public & private key pair (gold + light blue-ish keys) with your name & email.
9. Download another key from <https://ssl.intevation.de/Intevation-Distribution-Key.asc> and save it to your Desktop.
 - a. In the key that you download, note that everything between and including the blocks

-----BEGIN PGP PUBLIC KEY BLOCK-----
-----END PGP PUBLIC KEY BLOCK-----

...pertain to the public key.

Everything else in the file is ignored. If the block heading "-----BEGIN PGP PUBLIC KEY BLOCK-----" and/or "-----END PGP PUBLIC KEY BLOCK-----" are missing, then the file will be ignored as not having a valid public key.

10. Open the file that you downloaded so you learn to recognize a valid public key.
11. Import the new key from your desktop, and after selecting it, you should get a message that 2 public keys are read & imported.
12. Right-click the keys, and now you can sign both which sets the trust for the keys after you've verified it is legit. (Here, we are assuming the verification process has occurred!)
 - a. There's a key created on 2010 & another on 2016. When selecting the Details tab ...
 - i. What are the Key Types? **1,024-bit DSA & 3,072-bit RSA**
 - ii. What are their precise expiration dates? **11/2/2021 & 3/16/2020**
 - iii. What level is the Owner Trust (that's you!)? **The trust for the key I created is "ultimate" and the trust for the downloaded key is just "full"**
13. Right-click on both keys, and Set Owners Trust to "ultimate"
 - a. This is part of that "Web of Trust" which makes online security a thing!
 - b. What level is the Owner Trust on the keys now? **You cannot change the level of trust in the newer version of this application**