ECE435: Network Engineering – Homework 3
encryption

Due: Friday, 11 February 2022, 5:00pm

For this homework short answers will suffice.

To submit, create a document with your answers (text, pdf, libreoffice, MS Office if you must) and e-mail them to *vincent.weaver@maine.edu* by the homework deadline. Title your e-mail "ECE435 Homework 3" and be sure your name is included in the document.

1. **Cryptographic Hash Functions**

   (a) **md5sum/sha256 (3pts)**

      i. Download the file `hw3_test.txt` from the website:
      `http://web.eece.maine.edu/~vweaver/classes/ece435/hw3_test.txt`
      and calculate the md5sum.
      On Linux you can run something like `md5sum test.txt`
      If you aren't running Linux, you can try using a website for this,
      `http://onlinemd5.com/` might work.

      Report the md5sum that you get.

      ii. Make a copy of the file, and then make a small change (for example change the homework #). Re-run the md5sum. What's the resulting md5sum? How does the result compare to the unmodified file?

      iii. Also generate (and report) the SHA-256 sum for the same file. On Linux you can use the `sha256sum` program for this. How is it different from the md5sum?

2. **PGP/GPG (5pts)**

   On Linux use the `gpg` program for these tasks (if not installed, you can install it, something like `apt-get install gpg` or equivalent). You can also download GPG software for Windows/OSX from `https://gnupg.org/download/`.

   (a) Validating Signature

      i. The file `hw3_test.txt.signed` is a file that has been PGP/GPG signed by me.
      Verify that it was actually me that signed it.
      First download the signed file:
      `http://web.eece.maine.edu/~vweaver/classes/ece435/hw3_test.txt.signed`

      Then download my public key:
      `http://web.eece.maine.edu/~vweaver/classes/ece435/weaver.public_key`

      You will have to add this key to your keystore:
      `gpg --import weaver.public_key`
      Validate the `hw3_test.txt.signed` file:
      `gpg --verify ./hw3_test.txt.signed`

Was it signed by me?

Now change something in the `hw3_test.txt.signed` file.
Reverify. Does it still pass?

ii. You have validated the document using the public key I linked to, but how can you know it was really *me* who signed things and not an imposter?
GPG might have complained about this.

Describe one technique used to authenticate that a public key belongs to who it says it does.

(b) Encrypt a message using gpg and using my public key.
You can use the public key you imported earlier.
Create a text file `secret_message.txt` with your message.
Then run something like this:

```
gpg --output secret_message.gpg --encrypt \
--recipient vincent.weaver@maine.edu secret_message.txt
```

Attach this `secret_message.gpg` when submitting your assignment.

3. **Short Answer Questions (2pts)**

(a) The git SCM tool used to use SHA-1 to uniquely identify files. They are now transitioning to using SHA-256 instead. Why?

(b) The https protocol encrypts http connections. Before any headers are exchanged, both sides need to negotiate encryption methods and keys. This has the downside of making virtual hosting (having more than one website served on one machine via the "host" header) more difficult. Why is that?