Assignment 8: Cryptography

2019-05-06 22:53
1a0f14a

10 May 2019

There are three parts to this assignment. Provide the requested answers and information on (or attached to) a GitLab wiki page called `A8`.

(1) Monoalphabetic cipher

Below are individualized links pieces of text encoded using a single-substitution (monoalphabetic) cipher. Your task is to **crack the code** and discover the secret poem. You should start by doing a **frequency analysis** of the letters in your text.

When finished, take a picture of your decrypted text, and attach it to your wiki page.

AG 5952	text08.crypt.pdf
AM 1455	text17.crypt.pdf
BM 8155	text16.crypt.pdf
CF 5354	text06.crypt.pdf
CT 0003	text21.crypt.pdf
DD 0521	text05.crypt.pdf
EC 4153	text04.crypt.pdf
JM 7397	text15.crypt.pdf
JM 8993	text14.crypt.pdf
KB 0792	text03.crypt.pdf
KK 9498	text10.crypt.pdf
KS 7370	text20.crypt.pdf
ML 5931	text11.crypt.pdf
SA 9088	text01.crypt.pdf
SB 2069	text02.crypt.pdf
SF 5271	text07.crypt.pdf
SK 9463	text09.crypt.pdf
SL 1483	text13.crypt.pdf
SM 9272	text18.crypt.pdf
SQ 0414	text19.crypt.pdf
ST 6641	text22.crypt.pdf
SW 4503	text01.crypt.pdf
XL 5030	text12.crypt.pdf

(2) Vigenère cipher

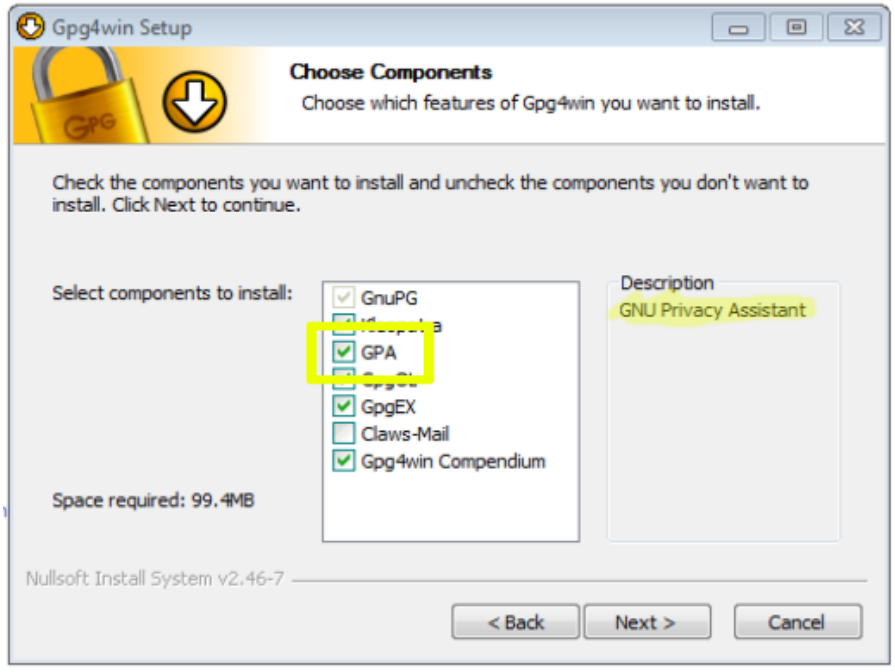
1. Choose a password that is 5–8 letters, and write it down.
2. Write down a sentence that is about 4–6 times the length of your password.

3. Use the polyalphabetic substitution table to encode the sentence using your password.
4. Type the encrypted sentence **and the password** directly into your wiki page (does not need to be an attachment).
5. You'll get full credit for this portion only if I can make sense of your sentence by decrypting using your password. So you may want to give that a test run with a friend: give them your encrypted sentence and password, and see if they get it right.

(3) Public key cryptography (GPG)

Use some variant of GNU Privacy Guard (GPG) or Pretty Good Privacy (PGP). Here are some options, including the software download links and a video illustrating their use.

- Windows:
  - Software: `http://www.gpg4win.org/` (free) **Note:** download the full version, and when you install, **select "GPA"** (GNU Privacy Assistant) on the **Choose Components screen**:



  - Video demonstration: `https://vimeo.com/113980848`
- Mac:
  - Software: `https://gpgtools.org/` (free)
  - Video demonstration: `https://vimeo.com/114185832`
- iPhone/iPad:

  - Software: `https://ipgmail.com/` ($2ish)
- Android phone/tablet:
  - Software: OpenKeychain (free)

Once you have one of the GPG apps installed, generate a new key pair using your email address and password. If using a lab computer, you should back up your key to a USB drive (ideally) or store it somewhere in the cloud. (In real life, you should not let your private key leave your control, but we can be more relaxed for this exercise.)

- Import my public key, which you can get at that link.
- Export your public key to a `.txt` file, and attach that file to the wiki page.
- Compose a short message to me, then sign it with your key and encrypt it with my key. Attach the encrypted version of the message to the wiki page. Its extension is usually either `.gpg` or `.gpg.asc`.