The combination of modern symmetric cryptography, asymmetric cryptography and hash functions form the basis of secure Internet, secure Intranet, secure system and service as well as Blockchain, etc. by assuring their **confidentiality, integrity, authenticity and nonrepudiation, which leads to availability.**

This lab is supposed to be done on a Windows 10 virtual machine.

1 Task 1: Git for Windows with TortoiseGit and GitHub %30

There are lots of open source projects hosted on Github. In this task, you will learn how to set up secure communication between you VM machine and Github.

1. Set up a Windows 10 virtual machine on any virtual machine managers you like such as VirtualBox, VMWare Workstation Pro, QEMU or Hyper-V, etc.
2. Download the latest git from `https://git-scm.com/` and TortoiseGit from `https://tortoisegit.org/` then install them on your Windows 10 VM.
3. Refer to the tutorial[23], setup and test your secure communication to Github from your Windows 10 VM using TortoiseGit.
4. If you want to learn more about Git and Github, here are some labs[24] provided by Github.

2 Task 2: Secure e-mails and files using GnuPG for Windows %70

In this task, you will use Gpg4Win[9] to manage your private/public keys, certificates and your friends' certificates. On which, you can secure e-mails, files and folders.

Gpg4win[5] consists of the following components:

- **GnuPG:** the core encryption tool
- **Certificate managers**
  - **Kleopatra**: certificate manager for OpenPGP and X.509
  - **GPA**: an alternate certificate manager (GNU) for OpenPGP and X.509
- **Plugins for email and file encryption**
  - **GpgOL**: a plugin for Microsoft Outlook to provide email encryption
  - **GpgEX**: a plugin for Windows Explorer to provide file encryption

- **Gpg4win Compendium**: introduction to encryption (OpenPGP and X.509) and user manual for Gpg4win

Find a classmate works as your communication partner to complete the subtasks:

1. Download 'gpg4win-3.1.4.exe' from Gpg4Win[9] then install it completely(select all its components) on your Windows 10 VM.
2. Run Kleopatra, from its menu **File –> New Key Pair...**, create
   - A personal OpenPGP key pair. Publish your OpenPGP public key to the 'PGP Global Directory'[28] key server[27]
3. Check the integrity of 'gpg4win-3.1.4.exe'(save all the downloaded files below in the same folder):
   - Right-click 'gpg4win-3.1.4.exe' then click property, in the popped up dialog box, check the digital signatures
   - Download the public keys `https://ssl.intevation.de/Intevation-Distribution-Key.asc` and `https://ssl.intevation.de/Intevation-Distribution-Key-2016.asc` from `https://www.gpg4win.org/package-integrity.html` then import them into Kleopatra, right-click the imported keys in Kleopatra and certify them
   - Download the signature file of 'gpg4win-3.1.4.exe.sig' from `https://files.gpg4win.org/gpg4win-3.1.4.exe.sig`. Right-click the signature file and use GpgEX to verify it.
4. Create a folder 'test' containing at least three sample files, Use your OpenPGP key and GpgEX to
   - Create then verify checksums of 'test'
   - Encrypt then decrypt 'test'
   - Sign then verify 'test'
   - Sign and encrypt then Decrypt and verify 'test'
5. If you want to learn more, the Gpg4Win Compendium[10] is a good resource.
6. Watch this video[32], using Mailvelope[18, 19] to import your partner's public PGP key that published on the PGP keyserver[28], send an encrypted and signed email to your partner, then decrypt and verify his encrypted and signed email that sent to you. Do you need to certify your partner's public key?

3 Report

Write a report about the process you complete the tasks in the description, key screen snapshots are needed as evidences.

Submit your report in Blackboard.

References

[1] Computer Security: A hands-on Approach, Wenliang Du

[2] Computer Security: Principles & Practice, Second Edition, William Stallings and Lawrie Brown

[3] Pretty Good Privacy. https://en.wikipedia.org/wiki/Pretty_Good_Privacy

[4] GNU Privacy Guard. https://en.wikipedia.org/wiki/GNU_Privacy_Guard

[5] Gpg4win. https://en.wikipedia.org/wiki/Gpg4win

[6] GnuPG. https://www.gnupg.org/

[7] PGP Tutorial. http://uncovering-cicada.wikia.com/wiki/PGP_TUTORIAL

[8] PGP tutorial. https://www.forte.net/devdocs/reference/pgp_tutorial.htm

[9] Gpg4win. https://www.gpg4win.org

[10] The Gpg4win Compendium. https://files.gpg4win.org/doc/gpg4win-compendium-en.pdf

[11] CAcert. http://www.cacert.org/

[12] CAcert Wiki. https://en.wikipedia.org/wiki/CAcert.org

[13] CrypTool. https://en.wikipedia.org/wiki/CrypTool

[14] CrypTool Portal. https://www.cryptool.org

[15] OpenPGP. https://www.openpgp.org/

[16] Seahorse. https://wiki.gnome.org/Apps/Seahorse

[17] FlowCrypt. https://flowcrypt.com/

[18] Mailvelope Wiki. https://en.wikipedia.org/wiki/Mailvelope

[19] Mailvelope official website. https://www.mailvelope.com

[20] Mailvelope source code. https://github.com/mailvelope/

[21] git. https://git-scm.com/

[22] TortoiseGit. https://tortoisegit.org/

[23] Git for Windows with TortoiseGit and GitHub . http://dancingmonkeysaccelerated.blogspot.com/2012/03/git-for-windows-with-tortoisegit-and.html

[24] GitHub Learning Lab. https://lab.github.com/

[25] Signing Git commits with GPG on Windows.https://jamesmckay.net/2016/02/signing-git-commits-with-gpg-on-windows/

[26] Using GPG in TortoiseGit. https://blog.rathena.cn/post/use-gpg-in-tortoisegit/

[27] Key server (cryptographic). https://en.wikipedia.org/wiki/Key_server_(cryptographic)

[28] PGP Global Directory. https://keyserver.pgp.com

[29] sks Key Servers. https://sks-keyservers.net/

[30] SKS OpenPGP Key server. https://keyserver.ubuntu.com/

[31] PGP Public Key Server. https://pgp.key-server.io/

[32] Encrypt Your Gmail/Yahoo/Outlook/iCloud and Other Webmail. https://www.youtube.com/watch?v=-Hz40_P6bVE

[33] SEED Lab. http://www.cis.syr.edu/~wedu/seed/index.html

[34] Resources from Google web search. https://www.google.com/