

# TP Cryptographie 2ème partie

Guillaume Bienkowski — Brincube

# TP

1. Fonctions de hachage
2. Signatures digitales
3. Certificats

# Récupération des sources

```
git clone https://github.com/masterind4/masterind4.github.io.git  
code masterind4.github.io/
```

# Méthodologie

Le TP se fera sur ordinateur avec un terminal et un navigateur.

Gardez les traces de vos commandes (ainsi que leur sortie dans le terminal) dans un document texte que vous m'enverrez à la fin de la cours sur mon email

*gbi — at — braincube.com*.

Il faudra aussi y joindre les fichiers des certificats pour MQTT que vous générerez en fin de session.

# Fonctions de hachage

## Exercice 1

Rendez-vous sur <https://prometheus.io/download/>

Téléchargez la version linux `amd64` de `pushgateway`

1. Vérifiez à l'aide de l'utilitaire `shasum` que la somme de contrôle est bonne.
2. Extrayez et lancez en ligne de commande l'utilitaire `pushgateway --help`

Fournir: les commandes lancées dans leur terminal ainsi que leur sortie

# Fonctions de hachage

## Exercice 2

Rendez-vous sur <https://masterind4.github.io/>

Téléchargez la version 1.0 de `Antivirus.exe`

### UTILISEZ LE MIROIR 1

1. Vérifiez à l'aide de l'utilitaire `md5sum` que la somme de contrôle est bonne
2. Lancez `Antivirus.exe`

# Fonctions de hachage

## On continue l'exercice

Rendez-vous sur <https://masterind4.github.io/>

Téléchargez la version **MIROIR 2** de `Antivirus.exe`

3. Vérifiez à l'aide de l'utilitaire `md5sum` que la somme de contrôle est bonne

Lancez `Antivirus.exe`

4. Que s'est-il passé?


5. Proposez vos idées pour que cela ne puisse plus se reproduire

# Signatures digitales

## Exercice 1

Rendez-vous sur <https://veracrypt.fr/en/Downloads.html>

1. Téléchargez la version debian 11 de veracrypt ainsi que sa signature PGP:

-  **Linux:**
  - Generic Installers: [veracrypt-1.25.4-setup.tar.bz2](#) (41.5 MB) ([PGP Signature](#))
  - Linux Legacy installer for 32-bit CPU with no SSE2: [veracrypt-1.25.4-x86-legacy-setup.tar.bz2](#) (13.8 MB) ([PGP Signature](#))
  - Debian/Ubuntu packages:
    - Debian 11:
      - GUI: [veracrypt-1.25.4-Debian-11-amd64.deb](#) ([PGP Signature](#))
      - Console: [veracrypt-console-1.25.4-Debian-11-amd64.deb](#) ([PGP Signature](#))

2. Profitez-en pour télécharger aussi la clé publique GPG de veracrypt (tout en haut)



## Vérification

Utilisez `gpg` pour:

3. **importer** ( `man gpg` ) la clé publique que vous venez de télécharger (vérifiez le fingerprint)

4. **vérifier** ( `man gpg verify` ) la signature du paquet deb que vous venez de télécharger

Garder les commandes et leur sortie dans votre document.

# Certificats

**Exercice 1: Utiliser `openssl s_client` pour se connecter de façon sécurisée à un serveur tiers.**

1. Tenter une connection sur `letsencrypt.org` sur le port `443`, et utiliser l'option `-showcerts` pour afficher les certificats renvoyés par le serveur.

Vérifier que la connection retourne bien `Verify return code: 0 (ok)`, qui signifie que la chaîne de certification est bien valide.

Utiliser `Ctrl + C` pour sortir.

Aide:

```
man s_client
```

Sauvegarder le **premier** certificat affiché par la commande précédente dans un fichier avec l'extension `.pem` et faire afficher avec `openssl x509` les détails de chaque certificats (utiliser l'option `-text` pour afficher les détails en format lisible.)

2. Récupérer la liste des DNS autorisés ( `Subject Alternative Name` ) par le certificat final.
3. Lister les contraintes basiques ( `Basic Constraints` ) sur le certificat, et expliquer ce que peut signifier cette contrainte.

## Exercice 2: Créer un certificat client

Rendez-vous sur <https://test.mosquitto.org>

Suivez les instructions pour créer une CSR d'un certificat à vous, et faites le signer par le rootCA de MQTT via leur interface (chercher "generate your own certificate" sur la page).

Pensez bien à récupérer le rootCA de mosquitto.

Fournissez dans votre email les certificats que vous aurez générés.

Téléchargez l'applimage ici: <https://mqtt-explorer.com/> et lancez-la sur votre ordinateur

Configurez la connexion suivant les instructions de MQTT et en spécifiant votre certificat & clé privée, et le root CA de Mosquitto.

Activez évidemment le TLS.

**Attention:** dans l'interface de MQTT Explorer, supprimez les souscriptions et ajoutez une souscription à `master4` sinon le trafic sera trop gros.

Chattez avec vos collègues. En tout bien tout honneur.