Εργαστήριο 3.1 – Κρυπτογράφηση, Υπολογισμός Hash και Υπογραφή Αρχείων με το GPG

1. Σύνοψη Εργαστηρίου 3
   1.1 Περιγραφή Εργαστηρίου 3
   1.2 Εκπαιδευτικοί Στόχοι 3
   1.3 Προαπαιτούμενα 3
   1.4 Εκτιμώμενος Χρόνος Ολοκλήρωσης 4
2. Ξεκινώντας 5
   2.1 Τι είναι το GPG; 5
   2.2 Γιατί να χρησιμοποιήσετε το GPG για Κρυπτογράφηση, Hash και Υπογραφή; 5
   2.3 Λίστα Ελέγχου Ρύθμισης Εργαστηρίου 5
3. Εγκατάσταση και ρύθμιση του GPG 7
   3.1 Εγκατάσταση GPG 7
   3.2 Δημιουργία του πρώτου σας ζεύγους κλειδιών 7
   3.3 Εξαγωγή και διαχείριση κλειδιών 8
   3.4 Ανακεφαλαίωση: Βασικά σημεία ρύθμισης GPG 8
4. Κρυπτογράφηση αρχείου 9
   4.1 Κρυπτογράφηση για παραλήπτη 9
   4.2 Κρυπτογράφηση για προσωπική χρήση 9
   4.3 Αποκρυπτογράφηση αρχείου 9
   4.4 Σύνοψη: Κρυπτογράφηση Αρχείων 10
5. Αποτύπωση και Επαλήθευση Αρχείων 11
   5.1 Δημιουργία SHA-256 Hash 11
   5.2 Επαλήθευση Ακεραιότητας Αρχείου 11
   5.3 Η σημασία του Hashing 11
   5.4 Σύνοψη: Hashing Αρχείων 12
6. Ψηφιακή Υπογραφή Αρχείων 13
   6.1 Δημιουργία Επισυναπτόμενης Υπογραφής 13
   6.2 Δημιουργία Αποσυνδεδεμένης Υπογραφής 13

6.3 Επαλήθευση Υπογραφής..... 13
6.4 Ανασκόπηση: Υπογραφή Αρχείου και Αυθεντικότητα..... 14
7. Δοκιμασία Εργαστηρίου..... 15
7.1 Άσκηση: Κρυπτογράφηση → Hash → Υπογραφή Αρχείου..... 15
7.2 Οδηγίες Βήμα-Βήμα..... 15
7.3 Ερωτήσεις Αναστοχασμού..... 16
8. Σύνοψη & Επόμενα Βήματα..... 17
8.1 Σημαντικά Σημεία..... 17
8.2 Δεξιότητες που Αποκτήσατε..... 17
8.3 Επόμενο Εργαστήριο: HTTPS και Πιστοποιητικά στην Πράξη..... 17
9. Παράρτημα..... 19
9.1 Αναφορά Εντολών GPG 19
9.2 Συνηθισμένες Εντολές Hashing..... 19
9.3 Συμβουλές Επίλυσης Προβλημάτων 20
9.4 Επιπλέον Πηγές 20

1. Επισκόπηση Εργαστηρίου

1.1 Περιγραφή Εργαστηρίου

Σε αυτό το εργαστήριο, θα εξασκηθείτε στη χρήση του **GNU Privacy Guard (GPG)** για την ασφαλή προστασία αρχείων με κρυπτογραφικές μεθόδους. Το GPG αποτελεί ένα ευρέως διαδεδομένο και ανοιχτού κώδικα εργαλείο για **κρυπτογράφηση, δημιουργία και έλεγχο ψηφιακών αποτυπωμάτων, καθώς και ψηφιακή υπογραφή**.

Θα μάθετε να:

- Κρυπτογραφήστε αρχεία για να διασφαλίσετε το απόρρητο.
- Δημιουργήστε και ελέγξτε κατακερματισμούς για να διατηρήσετε την ακεραιότητα των αρχείων.
- Υπογράψτε ψηφιακά αρχεία για να πιστοποιήσετε την αυθεντικότητα και να αποτρέψετε αλλοιώσεις.

Αυτές οι δεξιότητες εφαρμόζονται άμεσα σε ασφαλή κοινή χρήση αρχείων, δημιουργία αντιγράφων ασφαλείας και ακόμα και στη διανομή λογισμικού.

1.2 Εκπαιδευτικοί Στόχοι

Μετά την ολοκλήρωση αυτού του εργαστηρίου, θα μπορείτε να:

- Εγκαταστήστε και ρυθμίστε το GPG στο σύστημά σας.
- Δημιουργήστε και διαχειριστείτε ζεύγη δημοσίων/ιδιωτικών κλειδιών.
- Κρυπτογραφήστε αρχεία για εσάς και για άλλους.
- Χρησιμοποιήστε hashing για να επαληθεύσετε την ακεραιότητα των αρχείων.
- Υπογράψτε ψηφιακά αρχεία και επαληθεύστε τις υπογραφές.
- Εφαρμόστε ολόκληρη τη διαδικασία **Κρυπτογράφηση → Hash → Υπογραφή → Επαλήθευση**.

1.3 Προϋποθέσεις

Πριν ξεκινήσετε αυτό το εργαστήριο, θα πρέπει να έχετε:

- Έναν υπολογιστή με **Linux, macOS ή Windows**.
- Πρόσβαση σε τερματικό ή γραμμή εντολών.

- Βασικές γνώσεις στη χρήση εντολών του shell.
- (Μόνο για Windows) Ο **εγκαταστάτης Gpg4win**.
- (Προαιρετικό) Ένας επεξεργαστής κειμένου για τη δημιουργία δοκιμαστικών αρχείων.

1.4 Εκτιμώμενος Χρόνος Ολοκλήρωσης

Δραστηριότητα	**Εκτιμώμενος Χρόνος**
Εγκατάσταση και ρύθμιση του GPG	45 λεπτά
Κρυπτογράφηση και αποκρυπτογράφηση αρχείων	45 λεπτά
Δημιουργία κατακερματισμού και επαλήθευση ακεραιότητας αρχείων	30 λεπτά
Υπογραφή και επαλήθευση γνησιότητας αρχείων	45 λεπτά
Πρόκληση: Ροή Εργασίας Κρυπτογράφηση → Κατακερματισμός → Υπογραφή 60 λεπτά	
Αναστοχασμός και καταγραφή	15 λεπτά
Συνολικός εκτιμώμενος χρόνος	**~4 ώρες**

Σημείο ελέγχου

Πριν συνεχίσετε, βεβαιωθείτε ότι:

- Γνωρίζετε ότι αυτό το εργαστήριο διαρκεί περίπου **4 ώρες**.
- Διαθέτετε υπολογιστή με πρόσβαση στη γραμμή εντολών.
- Είστε έτοιμοι να εγκαταστήσετε το GPG (ή να επιβεβαιώσετε ότι είναι ήδη εγκατεστημένο).

2. Ξεκινώντας

2.1 Τι είναι το GPG;

GNU Privacy Guard (GPG) είναι μια δωρεάν και ανοιχτού κώδικα υλοποίηση του **προτύπου OpenPGP**. Προσφέρει εργαλεία κρυπτογράφησης για:

- **Κρυπτογράφηση** → Μετατρέπει τα αρχεία ώστε να είναι αναγνώσιμα μόνο με το σωστό ιδιωτικό κλειδί.
- **Δημιουργία αποτυπωμάτων (Hashing)** → Παράγει ένα ψηφιακό αποτύπωμα για να εντοπίζονται αλλαγές.
- **Υπογραφή** → Προσθέτει μια ψηφιακή υπογραφή που αποδεικνύει τον δημιουργό και την αυθεντικότητα.

Το GPG χρησιμοποιείται ευρέως από προγραμματιστές, διαχειριστές συστημάτων και ειδικούς ασφαλείας — από την προστασία προσωπικών email μέχρι τον έλεγχο γνησιότητας λογισμικού.

2.2 Γιατί να χρησιμοποιήσετε το GPG για κρυπτογράφηση, κατακερματισμό και υπογραφές;

Το GPG ξεχωρίζει επειδή συνδυάζει **εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα** σε ένα μόνο εργαλείο:

- **Εμπιστευτικότητα** → Κρυπτογράφηση αρχείων ώστε να είναι ορατά μόνο στον σωστό παραλήπτη.
- **Ακεραιότητα** → Εντοπισμός τυχόν τυχαίας αλλοίωσης ή κακόβουλης παρέμβασης μέσω κατακερματισμού.
- **Αυθεντικότητα** → Επιβεβαίωση της ταυτότητας του αποστολέα με ψηφιακές υπογραφές.

Παραδείγματα από την πράξη:

- Συνήθως οι λήψεις λογισμικού συνοδεύονται από **κατακερματισμούς και υπογραφές**.
- Οι ομάδες χρησιμοποιούν το GPG για να ανταλλάσσουν ευαίσθητα αρχεία με ασφάλεια.
- Τα αντίγραφα ασφαλείας μπορούν να κρυπτογραφηθούν για να αποφευχθεί διαρροή σε περίπτωση κλοπής.

2.3 Λίστα ελέγχου για την προετοιμασία του εργαστηρίου

Πριν ξεκινήσετε, βεβαιωθείτε ότι διαθέτετε:

Το GPG εγκατεστημένο

- Linux: Προεγκατεστημένο σε πολλές διανομές· σε διαφορετική περίπτωση:sudo apt install gnupg

- macOS: brew install gnupg

- Windows: Κατεβάστε και εγκαταστήστε το **Gpg4win** από την επίσημη ιστοσελίδα.

Έτοιμα αρχεία δοκιμής

- Δημιουργήστε ένα απλό αρχείο κειμένου (π.χ. secret.txt) για χρήση με κρυπτογράφηση, ψηφιακή υπογραφή και κατακερματισμό.

Διαθέσιμο ζεύγος κλειδιών

- Δημιουργήστε ένα αν χρειαστεί:
  gpg --full-generate-key

Πρόσβαση σε τερματικό/γραμμή εντολών

- Όλες οι εντολές αυτού του εργαστηρίου θα εκτελούνται μέσω τερματικού.

Σημείο ελέγχου

Πριν συνεχίσετε:

- Έχετε εγκαταστήσει το GPG στο σύστημά σας;
- Δημιουργήσατε ζεύγος κλειδιών με την εντολή gpg --full-generate-key;
- Έχετε έτοιμο τουλάχιστον ένα αρχείο κειμένου για δοκιμές;

3. Εγκατάσταση και Ρύθμιση του GPG

3.1 Εγκατάσταση GPG

Το GPG διατίθεται δωρεάν και λειτουργεί σε όλα τα βασικά λειτουργικά συστήματα:

- **Linux**
  - Συνήθως είναι προεγκατεστημένο. Αν λείπει, εγκαταστήστε το ως εξής:

```
sudo apt update
sudo apt install gnupg
```

- **macOS**
  - Εγκατάσταση μέσω Homebrew: brew install gnupg

- **Windows**
  - Κατεβάστε το **Gpg4win** από: https://gpg4win.org
  - Εκτελέστε το αρχείο εγκατάστασης και ακολουθήστε τον οδηγό ρυθμίσεων.

Συμβουλή: Επιβεβαιώστε την εγκατάσταση με:

```
gpg --version
```

3.2 Δημιουργία του πρώτου ζεύγους κλειδιών

Το GPG χρησιμοποιεί ένα **ζεύγος δημόσιου/ιδιωτικού κλειδιού**:

- Το **δημόσιο κλειδί** κοινοποιείται σε άλλους ώστε να μπορούν να κρυπτογραφούν αρχεία για εσάς.
- Το **ιδιωτικό κλειδί** παραμένει απόρρητο και χρησιμοποιείται για την αποκρυπτογράφηση και την υπογραφή αρχείων.

Για να δημιουργήσετε ένα ζεύγος κλειδιών:

```
gpg --full-generate-key
```

Βήματα:

1. Επιλέξτε **RSA και RSA** (προεπιλογή).
2. Ορίστε μέγεθος κλειδιού → **4096 bits** συνιστάται.
3. Βάλτε ημερομηνία λήξης → **2 χρόνια** (ανανεώνεται αργότερα).

4. Πληκτρολογήστε το όνομά σας και το email σας (χρησιμεύει ως αναγνωριστικό κλειδιού).

5. Ορίστε έναν ισχυρό κωδικό πρόσβασης.

3.3 Εξαγωγή και Διαχείριση Κλειδιών

Αφού δημιουργήσετε τα κλειδιά σας, μπορείτε να τα διαχειριστείτε:

- **Εμφάνιση των κλειδιών σας** gpg --list-keys

- **Εξαγωγή δημόσιου κλειδιού (για κοινή χρήση)** gpg --armor --export your@email.com > publickey.asc

- **Εξάγετε το ιδιωτικό σας κλειδί (μόνο για αντίγραφο ασφαλείας – διατηρήστε το ασφαλές!)** gpg --armor --export-secret-keys your@email.com > privatekey.asc

Μην κοινοποιείτε ποτέ το ιδιωτικό σας κλειδί. Μόνο το **δημόσιο κλειδί** είναι για διαμοιρασμό.

3.4 Ανακεφαλαίωση: Βασικά βήματα ρύθμισης GPG

Ενέργεια	**Εντολή/Δράση**
Εγκατάσταση GPG	sudo apt install gnupg (Linux) brew install gnupg (macOS) Gpg4win (Windows)
Δημιουργία ζεύγους κλειδιών	`gpg --full-generate-key`
Εμφάνιση κλειδιών	`gpg --list-keys`
Εξαγωγή δημόσιου κλειδιού	`gpg --armor --export you@example.com > publickey.asc`
Εξαγωγή ιδιωτικού κλειδιού	`gpg --armor --export-secret-keys \ you@example.com > privatekey.asc`

Σημείο ελέγχου

Πριν συνεχίσετε:

- Έχετε εγκαταστήσει το GPG με επιτυχία;
- Δημιουργήσατε ζεύγος κλειδιών με gpg --full-generate-key;
- Μπορείτε να εμφανίσετε τα κλειδιά σας και να εξαγάγετε το δημόσιο κλειδί σας;

4. Κρυπτογράφηση Αρχείου

4.1 Κρυπτογράφηση για Παραλήπτη

Για να στείλετε ένα αρχείο με ασφάλεια, χρειάζεστε το **δημόσιο κλειδί του παραλήπτη**. Αφού το εισαγάγετε στο GPG, εκτελέστε:

```
gpg -e -r recipient@example.com secret.txt
```

- -e → Κρυπτογράφηση
- -r → Email παραλήπτη (ID κλειδιού)
- secret.txt → Αρχείο προς κρυπτογράφηση

Αυτό θα δημιουργήσει ένα κρυπτογραφημένο αρχείο με όνομα secret.txt.gpg.

Μόνο ο παραλήπτης με το δικό του ιδιωτικό κλειδί μπορεί να το αποκρυπτογραφήσει.

4.2 Κρυπτογράφηση για προσωπική χρήση

Αν θέλεις να διασφαλίσεις τα δικά σου αρχεία, αρκεί να τα κρυπτογραφήσεις στη **δική σου διεύθυνση email**:

```
gpg -e -r you@example.com notes.txt
```

Αυτό είναι ιδιαίτερα χρήσιμο για **αντίγραφα ασφαλείας** ή ευαίσθητα αρχεία που θέλεις να παραμείνουν αποκλειστικά για εσένα.

4.3 Αποκρυπτογράφηση αρχείου

Για να αποκρυπτογραφήσετε ένα κρυπτογραφημένο αρχείο, εκτελέστε:

```
gpg -d secret.txt.gpg
```

- Αν το αρχείο έχει κρυπτογραφηθεί για εσάς, το GPG θα ζητήσει τον **κωδικό πρόσβασης του ιδιωτικού σας κλειδιού**.
- Μπορείτε να αποθηκεύσετε το απλό κείμενο σε αρχείο με: gpg -d secret.txt.gpg > secret_decrypted.txt

Πάντα να ελέγχετε την κρυπτογράφηση, αποκρυπτογραφώντας τα δικά σας αρχεία, για να βεβαιωθείτε ότι τα κλειδιά και ο κωδικός σας λειτουργούν σωστά.

Εργασία **Εντολή**

Κρυπτογράφηση για παραλήπτη gpg -e -r recipient@example.com file.txt

Κρυπτογράφηση για προσωπική χρήση gpg -e -r you@example.com file.txt

Αποκρυπτογράφηση αρχείου

```
gpg -d file.txt.gpg
```

Σημείο Ελέγχου

Πριν προχωρήσετε:

- Καταφέρατε να κρυπτογραφήσετε με επιτυχία ένα δοκιμαστικό αρχείο;
- Το αποκρυπτογραφήσατε ξανά στη αρχική του μορφή;
- Έχετε κατανοήσει τη διαφορά και το ρόλο των **δημόσιων και ιδιωτικών κλειδιών** στην κρυπτογράφηση;

5. Κατακερματισμός και Επαλήθευση Αρχείων

5.1 Δημιουργία κατακερματισμού SHA-256

Μια **συνάρτηση κατακερματισμού** δημιουργεί ένα μοναδικό ψηφιακό αποτύπωμα για κάθε αρχείο. Ακόμη και η παραμικρή αλλαγή στο αρχείο οδηγεί σε εντελώς διαφορετικό κατακερματισμό.

Για να δημιουργήσετε έναν κατακερματισμό SHA-256:

```
sha256sum important.zip
```

Παράδειγμα αποτελέσματος:

```
d2d2c3f3b4a5e6c7d8f9a0b1c2d3e4f56789abcdeffedcba9876543210fedcba  important.zip
```

Τα hashes συνήθως δημοσιεύονται μαζί με τα αρχεία λογισμικού, ώστε οι χρήστες να μπορούν να ελέγξουν την αυθεντικότητα των αρχείων.

5.2 Έλεγχος Ακεραιότητας Αρχείων

Αργότερα, μπορείτε να υπολογίσετε ξανά το hash και να το συγκρίνετε:

```
sha256sum important.zip
```

- Αν το hash είναι το ίδιο → το αρχείο παραμένει αμετάβλητο.
- Αν διαφέρει → το αρχείο έχει αλλαχθεί ή καταστραφεί.

5.3 Γιατί το Hashing έχει σημασία

Το Hashing βρίσκει εφαρμογή σε πολλές καθημερινές περιπτώσεις:

- **Ακεραιότητα λογισμικού** → Βεβαιωθείτε ότι τα αρχεία που κατεβάζετε δεν έχουν τροποποιηθεί.
- **Αντίγραφα ασφαλείας** → Εξασφαλίστε ότι τα αποθηκευμένα αρχεία παραμένουν ίδια.
- **Ψηφιακή εγκληματολογία** → Εντοπίστε αν έχει αλλοιωθεί κάποιο αποδεικτικό στοιχείο.
- **Blockchain & πρωτόκολλα ασφαλείας** → Τα hashes αποτελούν τη βάση για ψηφιακές υπογραφές και proof-of-work.

Άσκηση	**Εντολή**
Δημιουργία αποτυπώματος SHA-256	sha256sum όνομα_αρχείου
Επαλήθευση αποτυπώματος	Σύγκρινε τα αποτελέσματα σε διαφορετικές χρονικές στιγμές

Σημείο Ελέγχου

Πριν συνεχίσετε:

- Δημιουργήσατε SHA-256 hash για κάποιο αρχείο σας;
- Ελέγξατε ότι το hash παρέμεινε το ίδιο όταν το αρχείο δεν άλλαξε;
- Κατανοείτε πώς τα hashes αποκαλύπτουν αλλοίωση ή φθορά;

6. Ψηφιακή Υπογραφή Αρχείων

6.1 Δημιουργία Ενσωματωμένης Υπογραφής

Μια **ενσωματωμένη υπογραφή** συνδυάζει την υπογραφή με το ίδιο το αρχείο.

Για να υπογράψετε ένα αρχείο:

```
gpg --sign report.txt
```

- Με αυτή την εντολή δημιουργείται ένα νέο αρχείο report.txt.gpg.
- Περιλαμβάνει τόσο το αρχικό αρχείο όσο και την υπογραφή.

Επιλέξτε ενσωματωμένες υπογραφές όταν θέλετε να μοιραστείτε το αρχείο μαζί με την απόδειξη της αυθεντικότητάς του.

6.2 Δημιουργία Αποσυνδεδεμένης Υπογραφής

Κάποιες φορές δεν θέλετε να τροποποιήσετε το αρχείο — σε αυτή την περίπτωση μπορείτε να δημιουργήσετε μια **αποσυνδεδεμένη υπογραφή**.

```
gpg --detach-sign report.txt
```

- Αυτό δημιουργεί το αρχείο report.txt.sig (ή .asc).
- Το αρχείο της υπογραφής είναι ξεχωριστό από το αρχικό.

Οι αποσυνδεδεμένες υπογραφές χρησιμοποιούνται συχνά στη διανομή λογισμικού (π.χ. αρχείο .tar.gz με συνοδευτικό .sig για έλεγχο γνησιότητας).

6.3 Έλεγχος εγκυρότητας υπογραφής

Για να ελέγξετε αν η υπογραφή ενός αρχείου είναι έγκυρη:

- Για επισυναπτόμενη υπογραφή: gpg --verify report.txt.gpg

- Για αποσυνδεδεμένη υπογραφή:

  ```
  gpg --verify report.txt.sig report.txt
  ```

Εάν το αρχείο έχει τροποποιηθεί ή χρησιμοποιηθεί λάθος δημόσιο κλειδί, το GPG θα ειδοποιήσει ότι η υπογραφή δεν είναι έγκυρη.

6.4 Ανακεφαλαίωση: Υπογραφή Αρχείων και Αυθεντικότητα

Εργασία	**Εντολή**
Δημιουργία ενσωματωμένης υπογραφής	`gpg --sign file.txt`
Δημιουργία αποσυνδεδεμένης υπογραφής gpg	`--detach-sign file.txt`
Επαλήθευση ενσωματωμένης υπογραφής	`gpg --verify file.txt.gpg`
Επαλήθευση αποσυνδεδεμένης υπογραφής	`gpg --verify file.txt.sig file.txt`

Σημείο ελέγχου

Πριν συνεχίσετε:

- Υπογράψατε κάποιο αρχείο με επισυναπτόμενη υπογραφή;
- Δημιουργήσατε και αποσυνδεδεμένη υπογραφή;
- Επαληθεύσατε με επιτυχία και τις δύο υπογραφές;

7. Πρόκληση Εργαστηρίου

Ήρθε η σειρά σου να συνδυάσεις και τις τρεις κρυπτογραφικές τεχνικές: **κρυπτογράφηση, κατακερματισμός και ψηφιακή υπογραφή**.

7.1 Εργασία: Κρυπτογράφησε → Κάνε Hash → Υπόγραψε ένα αρχείο

1. **Δημιούργησε ένα αρχείο δοκιμής**

```
echo "Αυτό είναι το μυστικό μου αρχείο για το εργαστήριο." > labfile.txt
```

2. **Κρυπτογράφησέ το με το δημόσιο κλειδί σου**

```
# Δημιουργεί το labfile.txt.gpg:
gpg -e -r you@example.com labfile.txt
```

3. **Δημιούργησε κατακερματισμό του αρχικού αρχείου**

```
sha256sum labfile.txt > labfile.txt.sha256
```

4. **Υπογράψτε το αρχείο με το προσωπικό σας κλειδί**

```
# Δημιουργεί το labfile.txt.sig.
gpg --detach-sign labfile.txt
```

5. **Επαληθεύστε την υπογραφή και το hash**

```
gpg --verify labfile.txt.sig labfile.txt
sha256sum -c labfile.txt.sha256
```

7.2 Οδηγίες βήμα-βήμα

Βήμα	Εντολή	Αναμενόμενο αποτέλεσμα
Δημιουργία αρχείου	`echo "κείμενο" > labfile.txt`	Το αρχείο δημιουργήθηκε
Κρυπτογράφηση αρχείου	`gpg -e -r you@example.com labfile.txt`	Δημιουργήθηκε το labfile.txt.gpg
Υπολογισμός hash αρχείου	`sha256sum labfile.txt > labfile.txt.sha256`	Αποθηκεύτηκε ο έλεγχος SHA-256

Βήμα	Εντολή	Αναμενόμενο αποτέλεσμα
Υπογραφή αρχείου	`gpg --detach-sign labfile.txt`	Δημιουργήθηκε το labfile.txt.sig
Επαλήθευση αρχείων	`gpg --verify labfile.txt.sig labfile.txt`	Το μήνυμα υπογραφής είναι έγκυρο
Επαλήθευση κατακερματισμού	sha256sum -c labfile.txt.sha256	Ο έλεγχος ακεραιότητας ήταν επιτυχής

7.3 Ερωτήσεις αναστοχασμού

Καταγράψτε τις απαντήσεις σας στο εργαστηριακό σας σημειωματάριο ή στην εργασία σας:

1. Ποια είναι η διαφορά ανάμεσα στην κρυπτογράφηση και την υπογραφή;
2. Γιατί να δημοσιεύσει κάποιος το **hash** ενός αρχείου μαζί με την **υπογραφή**;
3. Ποιο βήμα διασφαλίζει το **απόρρητο**;
4. Ποιο βήμα διασφαλίζει την **ακεραιότητα**;
5. Ποιο βήμα διασφαλίζει τη **γνησιότητα**;
6. Πώς θα εξηγούσατε αυτή τη διαδικασία σε έναν συνάδελφο χωρίς τεχνικές γνώσεις;

Η δοκιμασία ολοκληρώθηκε!

Ολοκληρώσατε με επιτυχία τον κύκλο **Κρυπτογράφηση → Hash → Υπογραφή → Επαλήθευση** . Έτσι ακριβώς γίνεται η ασφαλής διανομή αρχείων στην πράξη.

8. Σύνοψη και Επόμενα Βήματα

8.1 Βασικά Σημεία

Σε αυτό το εργαστήριο, εφαρμόσατε πρακτικές κρυπτογραφίας με **GPG** και συναφή εργαλεία. Συγκεκριμένα:

Εγκαταστήσατε και ρυθμίσατε το GPG στο σύστημά σας.

Δημιουργήσατε ζεύγος δημόσιου/ιδιωτικού κλειδιού.

Κρυπτογραφήσατε αρχεία είτε για εσάς είτε για κάποιον παραλήπτη.

Επαληθεύσατε την ακεραιότητα των αρχείων με **SHA-256 hash**.

Υπογράψατε ηλεκτρονικά αρχεία (με επισυναπτόμενη ή ξεχωριστή υπογραφή).
Επαληθεύσατε την αυθεντικότητα και την ακεραιότητα των υπογεγραμμένων αρχείων.
Ολοκληρώσατε ολόκληρη τη διαδικασία **Κρυπτογράφηση → Hash → Υπογραφή → Επαλήθευση** .

Αυτές είναι οι **ίδιες τεχνικές που εφαρμόζονται στη βιομηχανία** για διανομή λογισμικού, δημιουργία αντιγράφων ασφαλείας, ασφαλή επικοινωνία και ψηφιακή ανάλυση.

8.2 Δεξιότητες που αποκτήσατε

Με την ολοκλήρωση αυτού του εργαστηρίου, πλέον μπορείτε να:

- Διακρίνετε τη διαφορά ανάμεσα σε **κρυπτογράφηση, κατακερματισμό και ψηφιακή υπογραφή**.
- Διασφαλίζετε το απόρρητο των αρχείων μέσω κρυπτογράφησης.
- Ανιχνεύετε αλλοίωση ή φθορά με κατακερματισμό.
- Επιβεβαιώνετε την ταυτότητα και τη γνησιότητα με ψηφιακές υπογραφές.
- Εφαρμόζετε συνδυαστική κρυπτογραφική προστασία σε πραγματικές διαδικασίες.

Αυτές οι δεξιότητες αποτελούν τη βάση για να κατανοήσετε πώς λειτουργούν τα πρωτόκολλα ασφαλούς επικοινωνίας και τα συστήματα εμπιστοσύνης.

8.3 Επόμενο Εργαστήριο: HTTPS και Πιστοποιητικά στην Πράξη

Στη συνέχεια, θα δείτε πώς οι έννοιες αυτές επεκτείνονται πέρα από τα αρχεία στο **περιβάλλον του διαδικτύου**.

Στο **Εργαστήριο 3.2: HTTPS και Πιστοποιητικά στην Πράξη**, θα:

- Εξερευνήστε τις συνδέσεις HTTPS στον περιηγητή σας.
- Κατανοήστε πώς τα **πιστοποιητικά** δημιουργούν εμπιστοσύνη στο διαδίκτυο.
- Ανακαλύψτε το σύστημα της **Αρχής Πιστοποιητικών (CA)** και δείτε πώς η κρυπτογράφηση και η υπογραφή προστατεύουν τις ιστοσελίδες, όπως προστάτεψαν και τα αρχεία σας.

Επόμενα Βήματα

- Αποθηκεύστε τα αρχεία σας .gpg, .sig, και .sha256 ως υλικό του εργαστηρίου.
- Καταγράψτε τις απαντήσεις της αναστοχαστικής σας διαδικασίας.
- Επαναλάβετε τις εντολές σας ώστε να τις εκτελείτε με σιγουριά.
- Ετοιμαστείτε για **Lab 3.2 – HTTPS και Πιστοποιητικά στην Πράξη**.

Τώρα έχετε περάσει από την κρυπτογράφηση προσωπικών αρχείων στην προετοιμασία για κρυπτογράφηση και μοντέλα εμπιστοσύνης σε διαδικτυακή κλίμακα.

9. Παράρτημα

9.1 Αναφορά εντολών GPG

Εργασία	Εντολή
Δημιουργία νέου ζεύγους κλειδιών	gpg --full-generate-key
Λίστα κλειδιών	gpg --list-keys
Εξαγωγή δημόσιου κλειδιού	gpg --armor --export you@example.com > publickey.asc
Εξαγωγή ιδιωτικού κλειδιού (μόνο για δημιουργία αντιγράφου ασφαλείας)	gpg --armor --export-secret-keys you@example.com > privatekey.asc
Κρυπτογράφηση αρχείου για παραλήπτη	gpg -e -r recipient@example.com file.txt
Κρυπτογράφηση αρχείου για προσωπική χρήση	gpg -e -r you@example.com file.txt
Αποκρυπτογράφηση αρχείου	gpg -d file.txt.gpg
Υπογραφή αρχείου (συνημμένη)	gpg --sign file.txt
Υπογραφή αρχείου (ξεχωριστή)	gpg --detach-sign file.txt
Επαλήθευση συνημμένης υπογραφής	gpg --verify file.txt.gpg
Επαλήθευση ξεχωριστής υπογραφής	gpg --verify file.txt.sig file.txt

9.2 Συχνές εντολές κατακερματισμού

Εργασία	Εντολή
Δημιουργία hash SHA-256	sha256sum όνομα_αρχείου
Επαλήθευση hash (με το αρχείο)	sha256sum -c όνομα_αρχείου.sha256

9.3 Συμβουλές για την Επίλυση Προβλημάτων

Πρόβλημα	Πιθανή Αιτία	Λύση
Το GPG δεν βρέθηκε	Δεν έχει εγκατασταθεί	Εγκαταστήστε το μέσω διαχειριστή πακέτων ή Gpg4win
Αποτυχία δημιουργίας κλειδιού	Ασθενής τυχαιότητα (Linux)	Κινήστε το ποντίκι, πληκτρολογήστε ή εκτελέστε διεργασίες στο παρασκήνιο για να αυξήσετε την τυχαιότητα
Σφάλμα "Δεν βρέθηκε δημόσιο κλειδί" κατά την κρυπτογράφηση	Δεν έχει εισαχθεί το δημόσιο κλειδί του παραλήπτη	Εισάγετε το κλειδί τους με την εντολή gpg --import key.asc
Λάθος κωδικός κατά την αποκρυπτογράφηση	Λανθασμένο ιδιωτικό κλειδί ή συνθηματικό	Δοκιμάστε ξανά με το σωστό κωδικό
Ασυμφωνία κατατεμαχισμού (hash mismatch)	Το αρχείο έχει τροποποιηθεί ή καταστραφεί	Κατεβάστε ξανά το αρχικό αρχείο και συγκρίνετε το αποτέλεσμα

9.4 Πρόσθετοι Πόροι

- **Επίσημη Τεκμηρίωση GnuPG**: https://gnupg.org/documentation/
- **Gpg4win (Εγκατάσταση για Windows)**: https://gpg4win.org
- **Οδηγός SHA256SUM (Linux/Unix)**: https://linux.die.net/man/1/sha256sum
- **Πρακτική Κρυπτογράφηση με GPG (Βιβλίο/Οδηγός)**: https://www.debian.org/doc/manuals/securing-debian-manual/ch-crypto.en.html#gpg