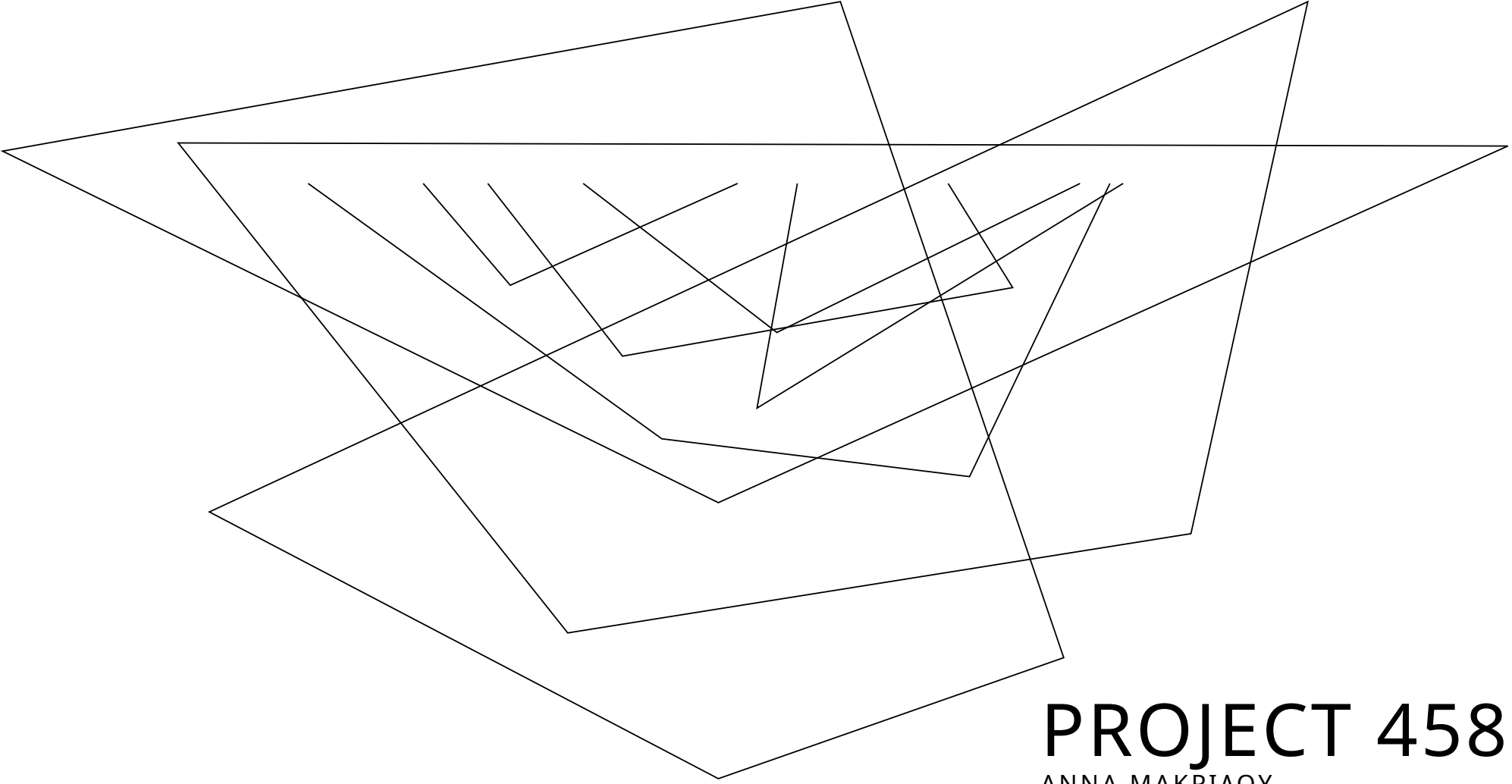
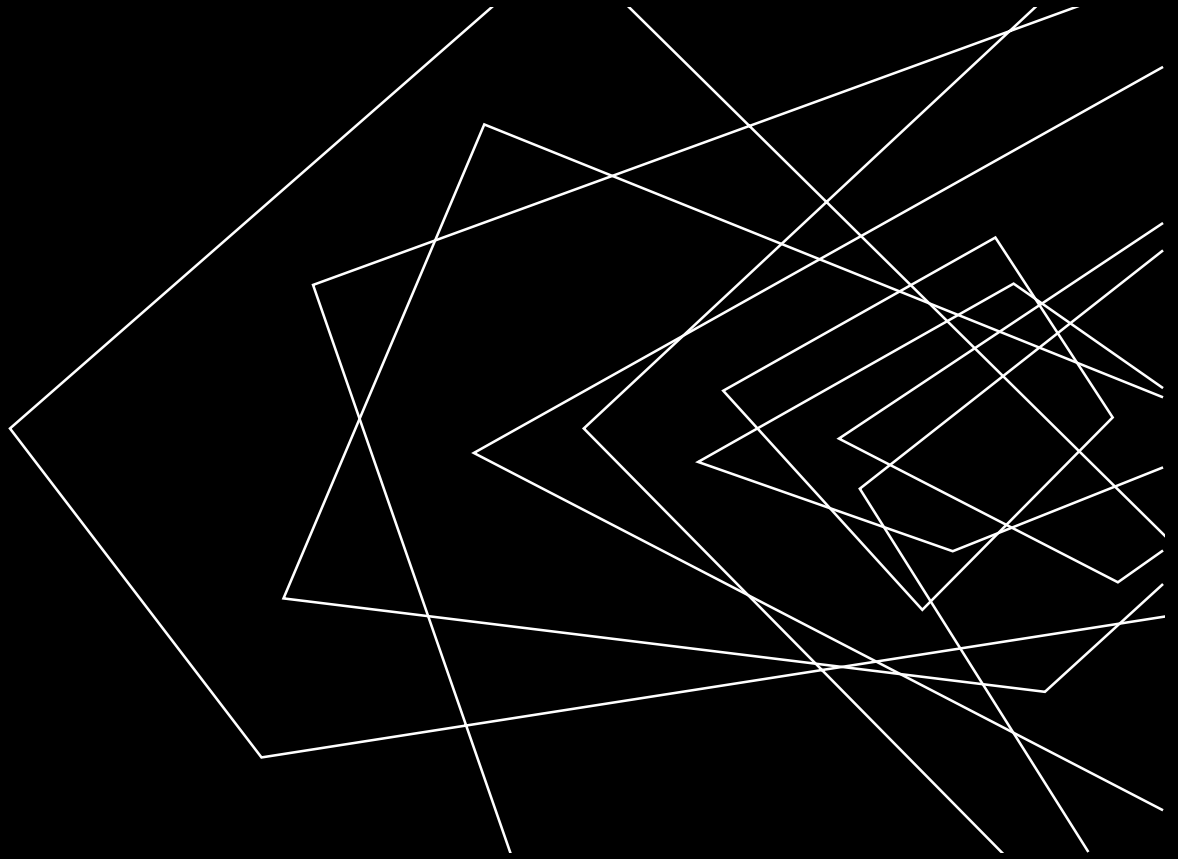


PROJECT 458

ΑΝΝΑ ΜΑΚΡΙΔΟΥ
ΑΛΕΞΑΝΔΡΟΣ ΦΟΥΡΤΟΥΝΗΣ
ΓΕΩΡΓΙΟΣ ΞΗΡΟΥΔΑΚΗΣ
ΠΑΝΤΕΛΕΗΜΩΝ ΤΣΑΓΚΑΡΑΚΗΣ

CRYPTO AGILITY FRAMEWORK FOR WEAK CRYPTOGRAPHY AND PQC TRANSITION



Chapter 1: Introduction

Chapter 2: Cryptography Inventory tool

Chapter 3: Crypto agility and migration planning

Chapter 4: Crypto-Agility simulator tool

Chapter 5: Conclusions

CHAPTER 1

- Ανάγκη για μετάβαση σε Post-Quantum Cryptography (PQC) λόγω απειλής κβαντικών υπολογιστών.
- **Στόχος**: Αναγνώριση ευπαθειών και αντικατάσταση παρωχημένων κρυπτογραφικών αλγορίθμων.

CHAPTER 2

Custom Parser

Χρησιμοποιήθηκε για την ανίχνευση αδυναμιών στον κώδικα.

Κατηγοριοποίηση αδυναμιών:

- **HIGH**: Σοβαρές ευπάθειες (MD5, DES, 3DES, μικρά RSA κλειδιά).
- **MEDIUM**: Μέτριας σοβαρότητας (SHA-1, CBC mode χωρίς integrity checks).
- **LOW**: Μακροπρόθεσμες συστάσεις (SHA-256, IDEA).

CHAPTER 2

Αρχεία που εξετάστηκαν:

- **Java:** 4/4 ευπαθή.
- **C:** 5/5 ευπαθή.
- **Python:** 5/5 ευπαθή.

CHAPTER 3

Στρατηγική Μετάβασης

- **Καταγραφή υπαρχόντων κρυπτογραφικών μηχανισμών**.
- **Ανίχνευση ευπαθειών με Semgrep**.
- **Αντικατάσταση παρωχημένων αλγορίθμων:**
  - SHA-256 / SHA-3 αντί για MD5 και SHA-1.
  - AES-GCM αντί για DES / 3DES.
  - RSA 2048+ με OAEP padding αντί για απλό RSA.
  - ECDSA αντί για DSA.
- **Υιοθέτηση Post-Quantum λύσεων**.

Χρήση PQC σε Μικρομεσαίες Επιχειρήσεις

- Προκλήσεις: Περιορισμένοι πόροι, legacy συστήματα, συνεχής λειτουργία.
- Σταδιακή μετάβαση για διασφάλιση επιχειρησιακής συνέχειας.
- Εκπαίδευση προσωπικού.

- Εξασφαλίζει μια ομαλή μετάβαση σε ανθεκτικούς PQC αλγορίθμους με ελάχιστες επιπτώσεις στη λειτουργία των συστημάτων.

CHAPTER 4

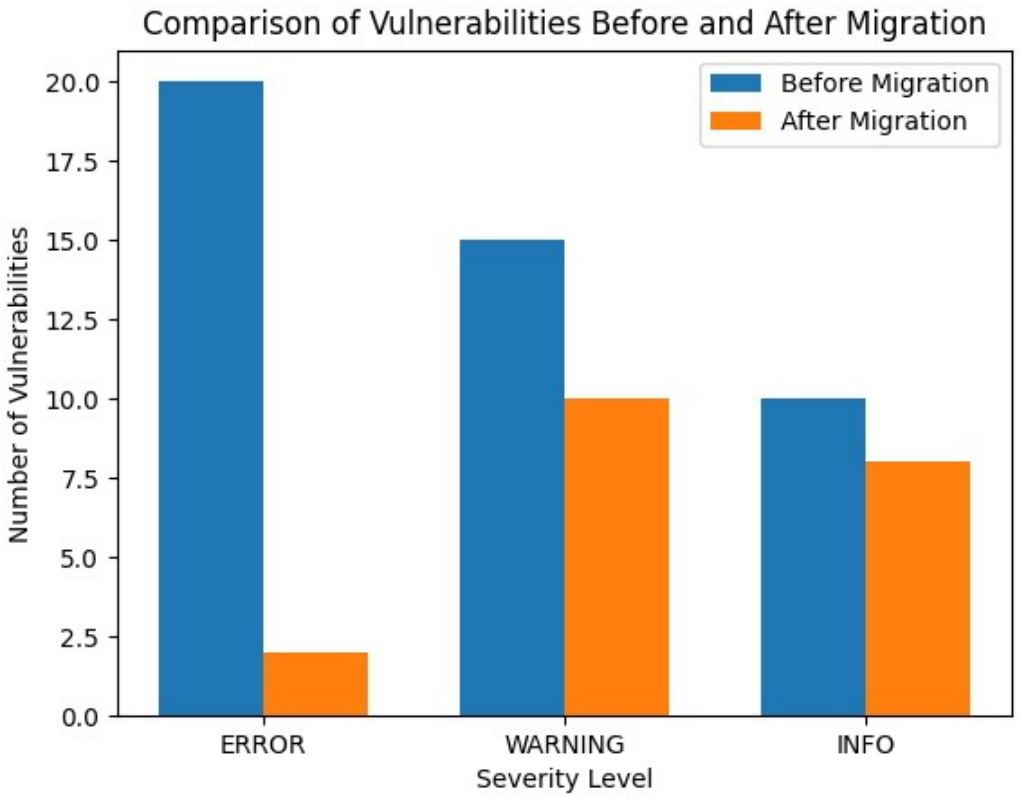
Προσομοιωτής Κρυπτογραφικής Ευελιξίας

- **Στόχος:** Αναγνώριση αδύναμων κρυπτογραφικών μηχανισμών και προσομοίωση μετάβασης σε ασφαλέστερους αλγόριθμους.
- **Βασικές Λειτουργίες:**
  - **Ανίχνευση αδύναμων κρυπτογραφικών μηχανισμών** μέσω του Cryptographic Inventory Tool.
  - **Αυτόματη πρόταση ισχυρότερων αλγορίθμων** για κάθε ευπαθή μηχανισμό.
  - **Δοκιμαστική αντικατάσταση αλγορίθμων** σε προσομοιωμένο περιβάλλον.
  - **Παρακολούθηση συμμόρφωσης** με διεθνή κρυπτογραφικά πρότυπα.
  - **Στατιστική ανάλυση των αλλαγών** και του επιπέδου ασφαλείας μετά την αντικατάσταση.

BONUS

- **Recursive Scanning:** Αναδρομική ανάλυση φακέλων & υποφακέλων.
- **Case Management:** Δημιουργία, αποθήκευση & φόρτωση σαρώσεων.

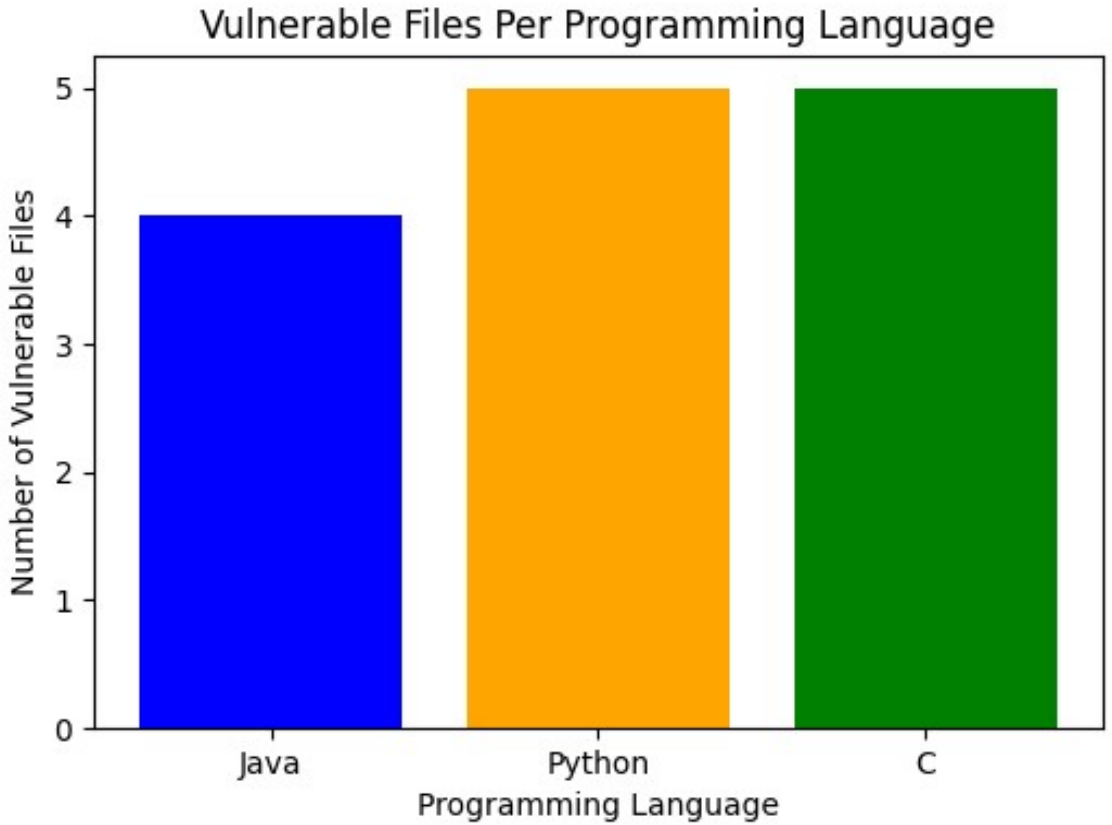
- **Βάσεις δεδομένων:** Εισαγωγή, εξαγωγή & διαγραφή δεδομένων.
- **Stress Test:** Έλεγχος απόδοσης της βάσης δεδομένων.
- **Οπτικοποιήσεις:** Διαδραστικά γραφήματα ευρημάτων.



ΣΎΓΚΡΙΣΗ ΕΥΠΑΘΕΙΏΝ ΠΡΙΝ ΚΑΙ ΜΕΤΆ ΤΗ ΜΕΤΆΒΑΣΗ

- **Στόχος:** Αξιολόγηση της αποτελεσματικότητας της μετάβασης σε ασφαλέστερους αλγορίθμους.
- **HIGH:** Σημαντική μείωση από 20 σε λιγότερο από 5.
- **MEDIUM:** Πτώση από 15 σε 10.
- **LOW:** Μικρή μείωση από 10 σε 8.

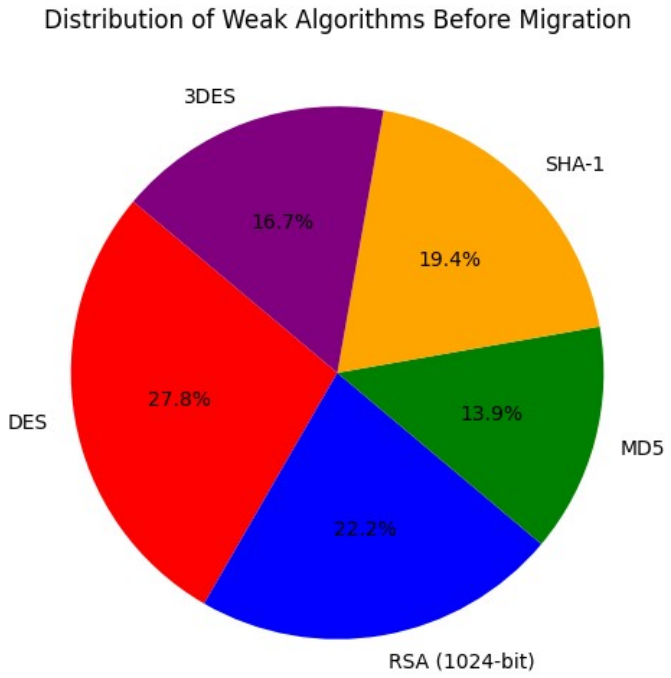
Η μετάβαση βελτίωσε την ασφάλεια, μειώνοντας τις σοβαρές ευπάθειες, αλλά απαιτείται περαιτέρω βελτίωση για τις μέτριες και ελάσσονες ευπάθειες.



VULNERABLE FILES

- **Java:** 4 ευπαθή αρχεία.
- **Python:** 5 ευπαθή αρχεία.
- **C:** 5 ευπαθή αρχεία.

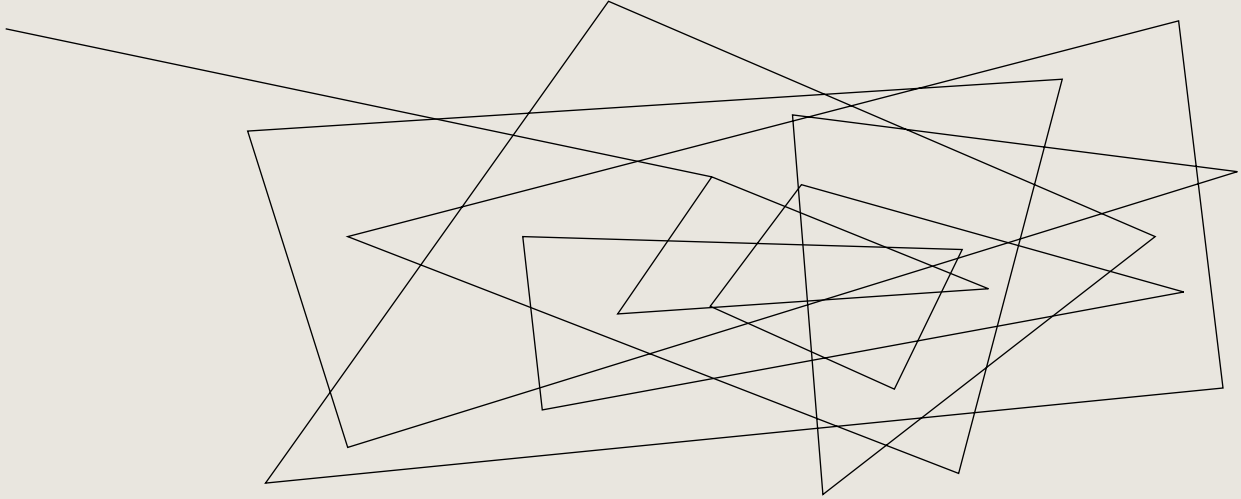
Συμπέρασμα:
- Οι περισσότερες ευπάθειες εντοπίζονται σε Python και C.
- Όλες οι γλώσσες εμφανίζουν σημαντικό αριθμό ευπαθών αρχείων.
- Η ασφάλεια του κώδικα απαιτεί προσαρμοσμένα μέτρα για κάθε γλώσσα.



WEAK ALGORITHM DISTRIBUTION

Αυτοί οι αλγόριθμοι έπρεπε να αντικατασταθούν με πιο ασφαλείς επιλογές (π.χ. AES-GCM, SHA-3, RSA 2048+).

CONCLUSION



- **Ανάλυση & ανίχνευση ευπαθειών με custon parser.**
- **Όλα τα αρχεία περιείχαν τουλάχιστον μία σοβαρή αδυναμία.**
- **Πλάνο μετάβασης:** Αντικατάσταση MD5, DES με ασφαλέστερες επιλογές.
- **PQC:** Σταδιακή υιοθέτηση για μελλοντική ασφάλεια.
- **Ενίσχυση προστασίας απέναντι στις κβαντικές επιθέσεις.**

THANK YOU