



CRYPTOGRAPHY PROJECT

CONCLUSION ANALYSIS

George Krasakis
AP23012

ΠΕΡΙΕΧΟΜΕΝΑ

1. Project A.1	2
1.1 CryptoFile_content	2
1.2 Fernet encrypted_txt	2
1.3 ChaCha20Poly1305 encrypted_txt.....	2
1.4 ES-GCM encrypted_txt	2
1.5 Επεξήγηση και σύγκριση των διαφόρων μεθόδων κρυπτογράφησης (Fernet, ChaCha20Poly1305, ES-GCM)	3
2. Project A.2	4
2.1 CMAC (Cipher-based Message Authentication Code).....	4
2.2 HMAC (Hash-based Message Authentication Code)	4
2.3 Poly1305	4
2.4 Σύγκριση CMAC, HMAC και Poly1305.....	4
3. Project A.3	5
3.1 DSA (Digital Signature Algorithm).....	5
3.2 RSA (Rivest-Shamir-Adleman).....	5
3.3 Ed25519.....	6
3.4 Σύγκριση μεγεθών και χαρακτηριστικών υπογραφής.....	6
4. Project B.1	7
4.1 Doc validation.....	7
4.2 Verifying the validation of signature	8

Το έγγραφο συνολικά παρέχει γενικές πληροφορίες για κάθε διαφορετική περίπτωση με σκοπό την εκμάθηση των περιπτώσεων που αναλύθηκαν.

Σημαντικά στοιχεία για την εργασία αποτελούν οι ενότητες:

- [Επεξήγηση και σύγκριση των διαφόρων μεθόδων κρυπτογράφησης \(Fernet, ChaCha20Poly1305, ES-GCM\)](#)
- [Σύγκριση CMAC, HMAC και Poly1305](#)
- [Σύγκριση μεγεθών και χαρακτηριστικών υπογραφής](#)
- [Project B.1](#)

Project A.1

1.1 CryptoFile_content

Το πραγματικό μέγεθος αρχείου PDF πριν την κρυπτογράφηση είναι: **201675 bytes**

1.2 Fernet encrypted_txt

Το μέγεθος του κρυπτογραφημένου με Fernet αρχείου είναι: **268984 bytes**.

Όπως φαίνεται το μέγεθος σε bytes του κρυπτογραφημένου κειμένου είναι μεγαλύτερο από το μέγεθος του αρχικού. Η αύξηση αυτή οφείλεται κυρίως στην προσθήκη κάποιων ετικετών ελέγχου ταυτότητας και άλλων μεταδεδομένων που απαιτούνται για την ασφαλή κρυπτογράφηση και αποκρυπτογράφηση αντίστοιχα. Το Fernet χρησιμοποιεί έναν αλγόριθμο AES 128 bit σε λειτουργία CBC με ένα SHA256 HMAC για έλεγχο ταυτότητας, το οποίο συμβάλλει στο μέγεθος του κρυπτογραφημένου κειμένου.

1.3 ChaCha20Poly1305 encrypted_txt

Το μέγεθος του κρυπτογραφήματος ChaCha20Poly1305 είναι: **201691 bytes**.

Το αποτέλεσμα έχει μια μικρή αύξηση σε μέγεθος σε σχέση με το αρχικό. Το ChaCha20Poly1305 αποτελεί μια μέθοδο κρυπτογράφησης AEAD που παρέχει προστασία τόσο εμπιστευτικότητας όσο και ακεραιότητας. Είναι γενικά πιο συμπαγές σε σύγκριση με το Fernet επειδή χρησιμοποιεί ένα μικρότερο nonce (12 bytes) και δεν απαιτεί ξεχωριστές ετικέτες για την αυθεντικοποίηση, ενσωματώνοντας τη στο ίδιο το κρυπτογράφημα.

1.4 ES-GCM encrypted_txt

Το μέγεθος του κρυπτογραφήματος ES-GCM είναι: **201691 bytes**.

Το AES-GCM παράγει επίσης ένα μέγεθος κρυπτογραφημένου κειμένου ελαφρώς μεγαλύτερο από το αρχικό μέγεθος του αρχείου. Το AES-GCM είναι ακόμη μία μέθοδος κρυπτογράφησης AEAD που συνδυάζει την κρυπτογράφηση AES σε λειτουργία Galois/Counter Mode (GCM) με έλεγχο ταυτότητας για προστασία της ακεραιότητας. Όπως και το ChaCha20Poly1305, ενσωματώνει τα δεδομένα

αυθεντικοποίησης στο κρυπτογράφημα, συμβάλλοντας σε ένα σχετικά μικρό μέγεθος κρυπτογραφήματος.

1.5 Επεξήγηση και σύγκριση των διαφόρων μεθόδων κρυπτογράφησης (Fernet, ChaCha20Poly1305, ES-GCM)

- **Fernet:** Το μεγαλύτερο μέγεθος (268984 bytes) οφείλεται κυρίως στην πρόσθετη πληροφορία που προστίθεται από το σχήμα κρυπτογράφησης, συμπεριλαμβανομένου του IV (Initialization Vector), της ετικέτας αυθεντικοποίησης και πιθανώς του padding. Η χρήση της λειτουργίας CBC και του HMAC για τον έλεγχο ταυτότητας από το Fernet καθιστά αναγκαία αυτά τα πρόσθετα δεδομένα.
- **ChaCha20Poly1305 & AES-GCM :** Τόσο το ChaCha20Poly1305 όσο και το AES-GCM έχουν μέγεθος κρυπτογραφημένου κειμένου κοντά στο αρχικό μέγεθος του αρχείου (201691 bytes). Η μικρή αυτή αύξηση επιτυγχάνεται ενσωματώνοντας την αυθεντικοποίηση και την κρυπτογράφηση σε μία μόνο διαδικασία. Με τον τρόπο αυτό μειώνεται η πρόσθετη πληροφορία σε σύγκριση με το Fernet. Το ChaCha20Poly1305, ειδικότερα, χρησιμοποιεί ένα μικρότερο nonce και δεν απαιτεί ξεχωριστή ετικέτα αυθεντικοποίησης επειδή αυθεντικοποιεί τα δεδομένα μέσα στο κρυπτογράφημα.

Ασφάλεια έναντι μεγέθους: Ενώ το Fernet παρέχει ισχυρή ασφάλεια με τη χρήση του AES και του HMAC, έχει ως κόστος το αυξημένο μέγεθος του κρυπτογραφημένου κειμένου. Από την άλλη πλευρά, το ChaCha20Poly1305 και το AES-GCM προσφέρουν συγκρίσιμη ασφάλεια με πιο συμπαγή μεγέθη κρυπτογραφημένου κειμένου, καθιστώντας τις κατάλληλες επιλογές στην περίπτωση που ελαχιστοποίηση του μεγέθους του κειμένου αποτελεί προτεραιότητα.

Project A.2

Οι CMAC, HMAC και Poly1305 αποτελούν τύπους κωδικών αυθεντικοποίησης μηνυμάτων (MAC) που χρησιμοποιούνται για την επαλήθευση της ακεραιότητας και της αυθεντικότητας των δεδομένων και χρησιμοποιείται συνήθως σε συστήματα IoT.

2.1 CMAC (Cipher-based Message Authentication Code)

Ο CMAC βασίζεται σε έναν αλγόριθμο κρυπτογράφησης, συνήθως AES (Advanced Encryption Standard). Επιπρόσθετα, ο CMAC χρησιμοποιεί ένα συμμετρικό κλειδί και εφαρμόζει την κρυπτογράφηση μπλοκ στα δεδομένα με δομημένο τρόπο για την παραγωγή μιας ετικέτας σταθερού μεγέθους.

- Το μέγεθος της ετικέτας εξόδου για CMAC είναι 16 bytes (128 bits) όταν χρησιμοποιείται AES.
- Το σταθερό μέγεθος ετικέτας των 16 bytes μπορεί να θεωρηθεί μικρό για ορισμένες εφαρμογές υψηλής ασφάλειας.

2.2 HMAC (Hash-based Message Authentication Code)

2.3 Poly1305

Ο Poly1305 παράγει μια ετικέτα με τον υπολογισμό ενός πολυωνύμου κατακερματισμού των δεδομένων σε συνδυασμό με ένα nonce και ένα μυστικό κλειδί.

- Το μέγεθος της ετικέτας εξόδου για το Poly1305 είναι 16 bytes (128 bits).
- Ο Poly1305 χρησιμοποιείται συχνά σε συνδυασμό με άλλους αλγορίθμους (π.χ. ChaCha20) για συστήματα κρυπτογράφησης με έλεγχο ταυτότητας

2.4 Σύγκριση CMAC, HMAC και Poly1305

Όταν συγκρίνουμε τα μεγέθη των ετικετών CMAC, HMAC και Poly1305, παρατηρούμε ότι τόσο η CMAC όσο και η Poly1305 παράγουν σχετικά συμπαγείς ετικέτες ελέγχου ταυτότητας των 16 bytes (128 bits), καθιστώντας τις κατάλληλες για εφαρμογές όπου η ελαχιστοποίηση της επιβάρυνσης είναι κρίσιμη. Αντίθετα, η HMAC παράγει μεγαλύτερη ετικέτα 32 bytes (256 bits) λόγω της εξάρτησής της από κρυπτογραφικές συναρτήσεις κατακερματισμού όπως η SHA-256, οι οποίες παράγουν εγγενώς

μεγαλύτερες εξόδους. Αυτό το μεγαλύτερο μέγεθος ετικέτας του HMAC παρέχει υψηλότερο επίπεδο ασφάλειας, καθιστώντας το μια ισχυρή επιλογή για πρωτόκολλα ασφαλείας που απαιτούν ακεραιότητα και ελέγχου ταυτότητας. Έτσι, η επιλογή μεταξύ αυτών των αλγορίθμων MAC εξαρτάται συχνά από την ισορροπία μεταξύ του απαιτούμενου επιπέδου ασφάλειας και της επιτρεπόμενης επιβάρυνσης δεδομένων για τη συγκεκριμένη εφαρμογή.

- CMAC value size: 16 bytes
- HMAC value size: 32 bytes
- Poly1305 tag size: 16 bytes

Project A.3

3.1 DSA (Digital Signature Algorithm)

Ο DSA είναι ένας αλγόριθμος δημόσιου κλειδιού που έχει σχεδιαστεί ειδικά για ψηφιακές υπογραφές. Δημιουργεί μια ψηφιακή υπογραφή χρησιμοποιώντας ένα ζεύγος αριθμών που προκύπτουν από την κατακερματισμένη μορφή των δεδομένων και ένα ιδιωτικό κλειδί. Με μέγεθος κλειδιού 2048 bit, το μέγεθος της υπογραφής DSA που προκύπτει είναι συνήθως 70 bytes. Το DSA είναι γνωστό για την αποτελεσματικότητά του τόσο στη δημιουργία κλειδιών όσο και στην επαλήθευση υπογραφών, καθιστώντας το ευνοϊκή επιλογή για κυβερνητικές και οικονομικές εφαρμογές που απαιτούν ασφαλείς και επαληθεύσιμες ψηφιακές υπογραφές. Ωστόσο, το μέγεθος της υπογραφής μπορεί να διαφέρει ανάλογα με το κλειδί και τη συνάρτηση κατακερματισμού που χρησιμοποιείται.

3.2 RSA (Rivest-Shamir-Adleman)

Ο RSA είναι ένας από τους πιο ευρέως αναγνωρισμένους και χρησιμοποιούμενους κρυπτογραφικούς αλγορίθμους, ικανός τόσο για κρυπτογράφηση όσο και για ψηφιακές υπογραφές. Λειτουργεί με βάση την αρχή της παραγοντοποίησης ακεραίων και χρησιμοποιεί ένα ιδιωτικό κλειδί για την κρυπτογράφηση του κατακερματισμού των δεδομένων για τη δημιουργία μιας υπογραφής. Για ένα κλειδί 2048 bit, το μέγεθος της υπογραφής RSA είναι 256 bytes, αντικατοπτρίζοντας τον σχεδιασμό του για ισχυρή ασφάλεια μέσω μεγάλων μεγεθών κλειδιών. Επίσης, η ευελιξία του RSA και η ευρεία υιοθέτησή του στις ασφαλείς επικοινωνίες και τα ψηφιακά πιστοποιητικά το καθιστούν

ακρογωνιαίο λίθο πολλών κρυπτογραφικών συστημάτων. Το μεγαλύτερο μέγεθος υπογραφής μπορεί να αποτελέσει μειονέκτημα.

3.3 Ed25519

Το Ed25519 είναι ένα σύγχρονο σύστημα υπογραφής δημόσιου κλειδιού που βασίζεται στον αλγόριθμο ψηφιακής υπογραφής Edwards-curve (EdDSA). Έχει σχεδιαστεί για να παρέχει υψηλή ασφάλεια και απόδοση, εξαλείφοντας την ανάγκη για παραγωγή τυχαίων αριθμών κατά την υπογραφή. Οι υπογραφές Ed25519 είναι συμπαγείς, με σταθερό μέγεθος 64 bytes, γεγονός που τις καθιστά ιδιαίτερα αποδοτικές τόσο για την υπογραφή όσο και για την επαλήθευση. Αυτός ο αλγόριθμος είναι κατάλληλος για εφαρμογές σε μηνύματα, ενημερώσεις λογισμικού και κρυπτογραφικά πρωτόκολλα, όπου η απόδοση και η ασφάλεια είναι υψίστης σημασίας. Αν και νεότερος και λιγότερο διαδεδομένος από τον RSA, η αποδοτικότητα και η ευρωστία του Ed25519 οδηγούν στην αυξανόμενη δημοτικότητά του στις σύγχρονες κρυπτογραφικές εφαρμογές.

3.4 Σύγκριση μεγεθών και χαρακτηριστικών υπογραφής

Κατά τη σύγκριση των μεγεθών υπογραφής των DSA, RSA και Ed25519, προκύπτουν σαφείς διαφορές. Το DSA, με μέγεθος κλειδιού 2048 bit, παράγει υπογραφή **70 byte**, η οποία είναι σχετικά συμπαγής και κατάλληλη για περιβάλλοντα που χρειάζονται αποτελεσματικές διαδικασίες επαλήθευσης. Ο RSA, από την άλλη πλευρά, παράγει μια σημαντικά μεγαλύτερη υπογραφή **256 byte** για το ίδιο μέγεθος κλειδιού, προσφέροντας ισχυρή ασφάλεια με κόστος την αυξημένη επιβάρυνση δεδομένων και τις αυξημένες υπολογιστικές απαιτήσεις. Αντίθετα, το Ed25519 παράγει μια σταθερή υπογραφή **64 byte**, εξισορροπώντας υψηλή ασφάλεια και απόδοση με ελάχιστη επιβάρυνση δεδομένων.

Project B.1

4.1 Doc validation

- **Issuer of the Certificate**

APED Qualified eSignature Issuing CA

- **Signature Algorithm and Key Size**

RSA/SHA256

- **Public Key**

RSA (2048 bits)

- **Key owner**

Issued by: APED Qualified eSignature Issuing CA

- **Certificate Serial Number**

09 8B 48 F6 A8 97 DA 4D DE 89 26 6F 2F 08 EE 3B

- **Issuing and Expiration Date of the Certificate**

Valid from: 01/04/2022

Valid to: 31/03/2025

4.2 Verifying the validation of signature

- Αρχικά παρατηρώ το Signing time (Timestamp), δηλαδή την ημερομηνία και την ώρα που υπεγράφη το ΦΕΚ.

Στο ΦΕΚ που χρησιμοποίησα ως παράδειγμα:

Signing Time: 21/06/2024 23:51:26 + 03:00

- Έπειτα θα πρέπει να παρατηρήσω το διάστημα που είναι έγκυρο το πιστοποιητικό

Valid from: 01/04/2022 14:12:17 + 03:00


Valid to: 31/03/2025 14:12:16 + 03:00

- Διακρίνω ότι η ημερομηνία που υπεγράφη το ΦΕΚ είναι εντός των ορίων του πιστοποιητικού χρονικά, επομένως είναι έγκυρη.
- Επιπλέον, επιβεβαιώνω ότι η χρήση του πιστοποιητικού προορίζεται για ψηφιακή υπογραφή

Digital Signature, Non-Repudiation

- Παρατηρώ εάν έχει αλλάξει κάτι στο ψηφιακό πιστοποιητικό δηλαδή τη ψηφιακή υπογραφή αυτού που έχει εκδώσει.
- Τέλος, παρατηρώ εάν αυτός που έχει υπογράψει το έγγραφο είναι στο trusted CA.

Trust services results (1)

 **HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY** QCert for ESig QTimestamp Cert for ESig

APED Qualified eSignature Issuing CA CA/QC Granted