

Κρυπτογραφία και Ηλεκτρονικοί Υπολογιστές

ΣΥΝΤΕΛΕΣΤΕΣ:

- *Κραβαρίτης Αλέξανδρος*
- *Μαργώνη Αγγελική*
- *Χαλιμούρδα Κων/να*

Ορισμός κρυπτογραφίας

Με τον όρο κρυπτογραφία, αναφερόμαστε στη μελέτη μαθηματικών τεχνικών που στοχεύουν στην εξασφάλιση θεμάτων που άπτονται της ασφάλειας μετάδοσης πληροφοριών

Στόχοι κρυπτογραφίας

- ❖ η παράδοση των κρυπτογραφημένων πληροφοριών στους σωστούς / επιλεγμένους παραλήπτες
- ❖ η άμεση και πλήρης παράδοση των στοιχείων χωρίς να έχουν υποστεί κάποια μορφή αλλοίωσης
- ❖ η πιστοποίηση της ταυτότητας του αποστολέα

Τομείς εφαρμογών κρυπτογραφίας

- Οικονομικός
- Επαγγελματικός

- Κοινωνικός
- Ασφάλειας



Βασικοί όροι σύγχρονης κρυπτογραφίας

- ❖ Αλγόριθμος κρυπτογράφησης (encryption)
- ❖ Αλγόριθμος αποκρυπτογράφησης (decryption)
- ❖ **Κρυπτογραφικό κλειδί:** χρησιμοποιώντας ένα κλειδί, η σύγχρονη κρυπτογραφία, μπορεί να χρησιμοποιηθεί εξίσου για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση, καθώς επίσης και για τη δημιουργία ή επαλήθευση ψηφιακής υπογραφής. Τέτοιου είδους κλειδιά χρησιμοποιούνται από συμμετρικούς ή μη συμμετρικούς (δημόσιου κλειδιού) κρυπτογραφικούς αλγόριθμους.
- ❖ **Οικονομολογική κρυπτογραφία**

Ορισμός και ανάλυση κρυπτοσυστημάτων

Κρυπτόςστημα είναι το σύνολο των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης.

Κατηγορίες

- ❖ Αναδιάταξης
- ❖ Αντικατάστασης
- ❖ Σημειωματαρία μιας χρήσης
- ❖ Ρότορες
- ❖ Συμμετρικά κρυπτοσυστήματα
- ❖ Ασύμμετρα συστήματα

Κρυπτοσυστήματα

ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

ΚΛΑΣΣΙΚΑ

πολυσταδιακές

1. αναδιάταξης



μονοσταδιακές

2. αντικατάστασης



πολυαλφαβητικής



μονοαλφαβητικής



ομοφωνικής

→ πολυγραμματικής

3. σημειωματάριο μιας χρήσης

4. ρότορες

ΜΟΝΤΕΡΝΑ

συναρτήσεις κατακερματισμού

1. συμμετρικά



συμμετρικοί
αλγόριθμοι



ψευδοτυχαίες
ακολουθίες



ψηφιακές
υπογραφές

2. ασύμμετρα



Ασύμμετροι
κρυπταλγόριθμοι



ψηφιακές υπογραφές

Αλγόριθμοι βασισμένοι σε κλειδιά

- ❖ **Αλγόριθμοι συμμετρικού κλειδιού:** χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση
- ❖ **Αλγόριθμοι ασύμμετρου κλειδιού:** χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί κρυπτογράφησης δε μπορεί να εξαχθεί από το κλειδί αποκρυπτογράφησης.

Συμμετρικά και ασύμμετρα κρυπτοσυστήματα

- ❖ **Συμμετρικό κρυπτόςστημα:** είναι το σύστημα εκείνο που κατά τη διαδικασία της αποκρυπτογράφησης χρησιμοποιεί ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού.
- ❖ **Ασύμμετρο κρυπτόςστημα:** Κύριο χαρακτηριστικό είναι η ύπαρξη δύο κλειδιών: ενός δημοσίου που είναι διαθέσιμο σε όλους και ένα ιδιωτικό το οποίο είναι μυστικό, τα οποία έχουν ακριβώς την ίδια αντίστροφη δράση.

Ψηφιακή Υπογραφή

Αποτελείται από τρεις (3) αλγόριθμους:

1. Δημιουργίας δημόσιου και ιδιωτικού κλειδιού
2. Προσθήκης ψηφιακής υπογραφής σε μηνύματα και έγγραφα
3. Ελέγχου ψηφιακής υπογραφής μηνύματος ή εγγράφου

Χρήση ψηφιακής υπογραφής

Η ψηφιακή υπογραφή χρησιμοποιείται και στα πλαίσια του σχολικού περιβάλλοντος. Χαρακτηριστικό παράδειγμα χρήσης της είναι η αξιοποίηση της κατά την υποβολή της απογραφής του ηλεκτρονικού εξοπλισμού της σχολικής μονάδας ώστε να πιστοποιηθεί η εγκυρότητα της αναφοράς που στάλθηκε από τον Διευθυντή του σχολείου στο Υπουργείο Παιδείας.



Σύστημα Πανελλήνιων εξετάσεων

Οι πανελλαδικές εξετάσεις είναι ένα σύστημα αξιολόγησης χιλιάδων μαθητών της Γ' τάξης του Λυκείου σε όλη την Ελλάδα κάθε χρόνο που αφορά στην πρόσβαση τους στην τριτοβάθμια εκπαίδευση. Γι' αυτό η αλλοίωση ή παραποίηση πληροφοριών ή θεμάτων είναι ανεπίτρεπτη. Στα πλαίσια του μαθήματος της ερευνητικής μας εργασίας με θέμα την «κρυπτογραφία» και κατόπιν υποδείξεως της καθηγήτριας μας, ζητήσαμε τη βοήθεια του διευθυντή του σχολείου μας, ώστε να ενημερωθούμε για το προαναφερόμενο σύστημα.



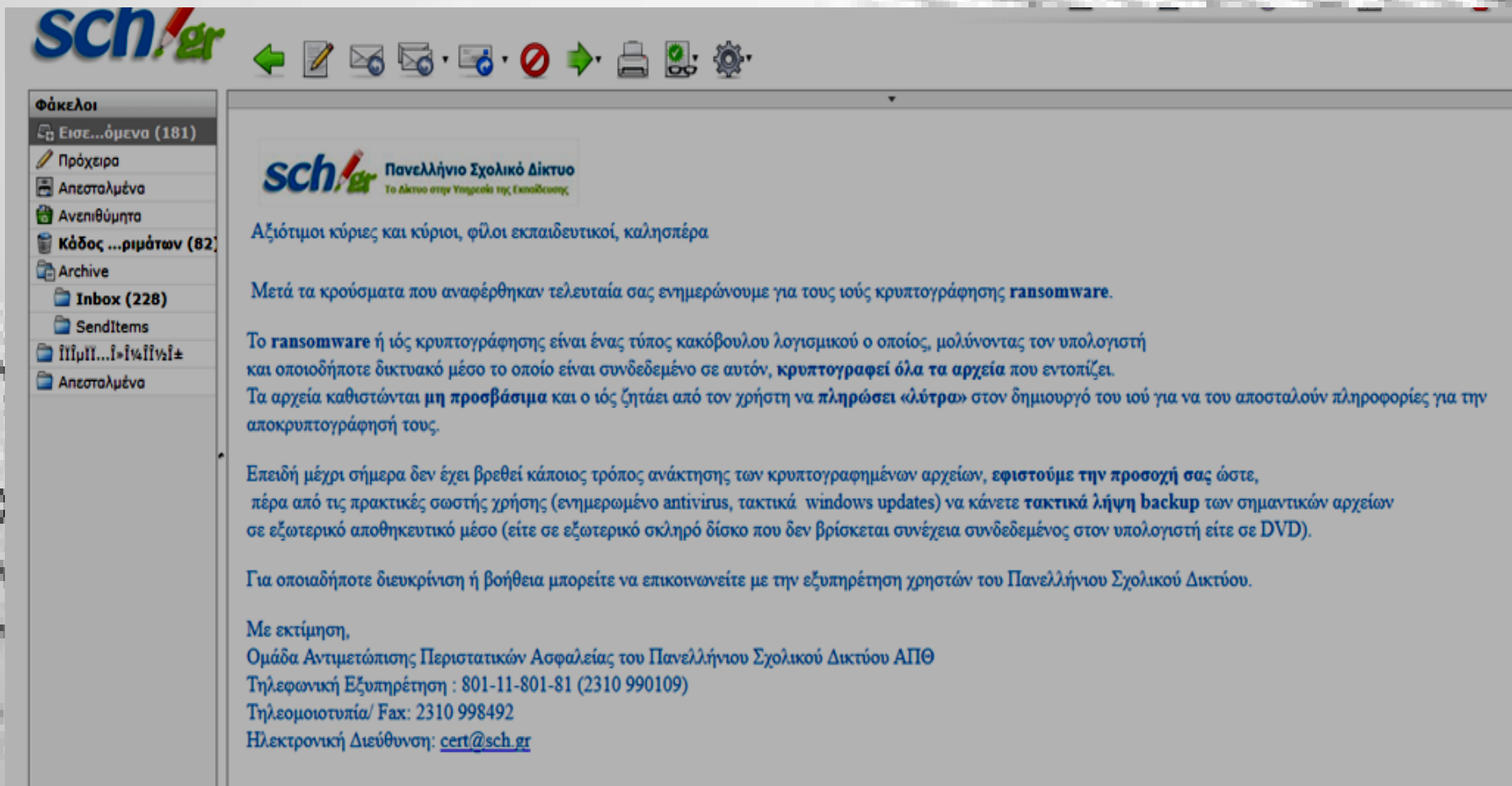
Το Υπουργείο Παιδείας, για την κάλυψη των προαναφερόμενων αναγκών, υιοθέτησε μια νέα μέθοδο μετάδοσης δεδομένων που είναι γνωστή ως "Μετάδοση VBI« η οποία βασίζεται στην κρυπτογραφημένη μετάδοση των θεμάτων.

Κατά την διάρκεια των εξετάσεων το σύστημα τίθεται σε λειτουργία αρκετές ώρες νωρίτερα από την ώρα έναρξης. Τα θέματα λαμβάνονται κρυπτογραφημένα και η αποκρυπτογράφηση τους γίνεται με ειδικό λογισμικό που έχει εγκατασταθεί λίγες μέρες νωρίτερα στον υπολογιστή που γίνεται η λήψη σε συνδυασμό με το κλειδί που έχει συνδεθεί στον ίδιο υπολογιστή. Μετά την λήψη σε καθορισμένη ώρα, των θεμάτων, την αποκρυπτογράφηση και τον έλεγχο της ορθής εκτύπωσης τα θέματα διαγέρονται στους μαθητές και οι εξετάσεις ξεκινάνε.

Το σύστημα αυτό εξασφαλίζει την ακεραιότητα των δεδομένων και τη 'δίκαιη' διεξαγωγή των εξετάσεων.

Κρυπτογραφία και κακόβουλο λογισμικό

Η κρυπτογραφία μπορεί να χρησιμοποιηθεί και σε κακόβουλο λογισμικό. Παρακάτω παρατίθεται μήνυμα προειδοποίησης του ΠΣΔ προς όλους τους χρήστες του για την ύπαρξη ιού που κρυπτογραφεί τα αρχεία του υπολογιστή του χρήστη και καταστεί αδύνατη την χρήση τους. Συνήθως ζητείται ένα χρηματικό ποσό για την επαναφορά των αρχείων στην αρχική τους μορφή



The screenshot shows an email interface with the 'sch.gr' logo in the top left. The email content is in Greek and discusses a ransomware virus. The text is as follows:

sch.gr Πανελλήνιο Σχολικό Δίκτυο
Το Δίκτυο στην Υπηρεσία της Εκπαίδευσης

Αξιότιμοι κύριες και κύριοι, φίλοι εκπαιδευτικοί, καλησπέρα

Μετά τα κρούσματα που αναφέρθηκαν τελευταία σας ενημερώνουμε για τους ιούς κρυπτογράφησης **ransomware**.

Το **ransomware** ή ιός κρυπτογράφησης είναι ένας τύπος κακόβουλου λογισμικού ο οποίος, μολύνοντας τον υπολογιστή και οποιοδήποτε δικτυακό μέσο το οποίο είναι συνδεδεμένο σε αυτόν, **κρυπτογραφεί όλα τα αρχεία** που εντοπίζει. Τα αρχεία καθιστώνται **μη προσβάσιμα** και ο ιός ζητάει από τον χρήστη να **πληρώσει «λύτρα»** στον δημιουργό του ιού για να του αποσταλούν πληροφορίες για την αποκρυπτογράφησή τους.

Επειδή μέχρι σήμερα δεν έχει βρεθεί κάποιος τρόπος ανάκτησης των κρυπτογραφημένων αρχείων, **επιστούμε την προσοχή σας** ώστε, πέρα από τις πρακτικές σωστής χρήσης (ενημερωμένο αντιϊνίγος, τακτικά windows updates) να κάνετε **τακτικά λήψη backup** των σημαντικών αρχείων σε εξωτερικό αποθηκευτικό μέσο (είτε σε εξωτερικό σκληρό δίσκο που δεν βρίσκεται συνέχεια συνδεδεμένος στον υπολογιστή είτε σε DVD).

Για οποιαδήποτε διευκρίνιση ή βοήθεια μπορείτε να επικοινωνείτε με την εξυπηρέτηση χρηστών του Πανελληνίου Σχολικού Δικτύου.

Με εκτίμηση,
Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας του Πανελληνίου Σχολικού Δικτύου ΑΠΘ
Τηλεφωνική Εξυπηρέτηση : 801-11-801-81 (2310 990109)
Τηλεομοιοτυπία/ Fax: 2310 998492
Ηλεκτρονική Διεύθυνση: cert@sch.gr

*Ευχαριστούμε για την
προσοχή σας....!!!*