Κρυπτογραφία και Ηλεκτρονικοί Υπολογιστές

ΣΥΝΤΕΛΕΣΤΕΣ:

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

Ορισμός κρυπτογραφίας

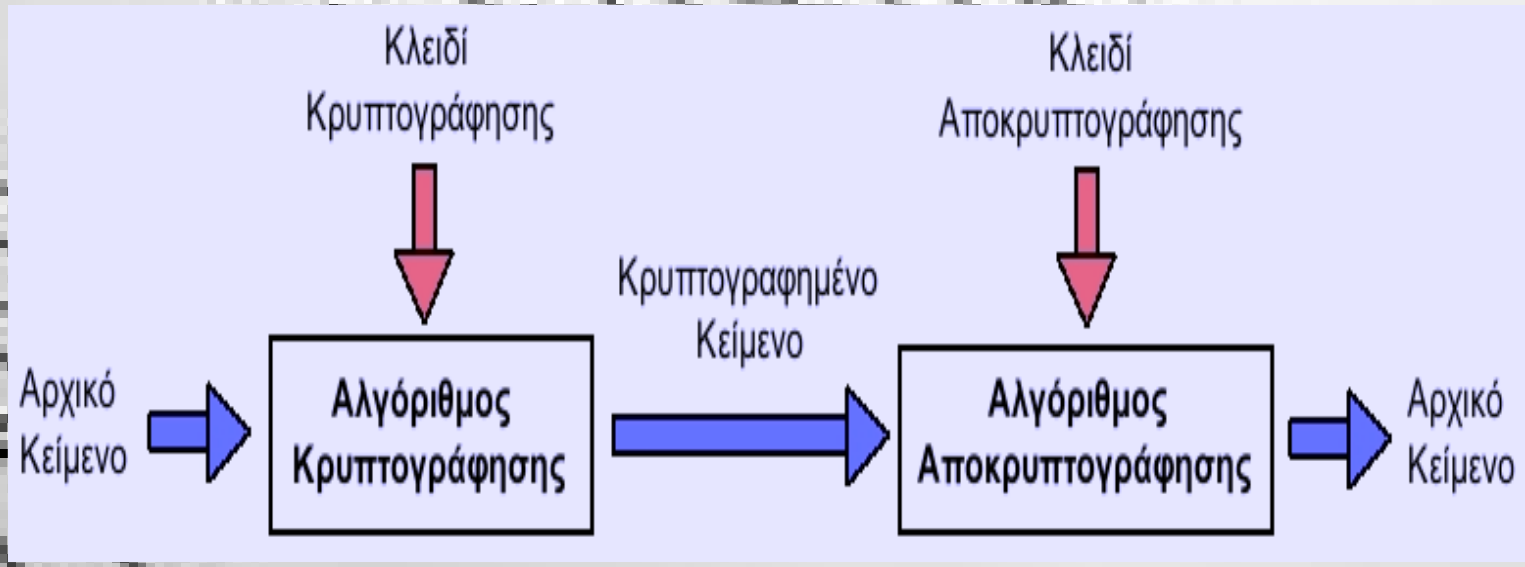
Με τον όρο κρυπτογραφία, αναφερόμαστε στη μελέτη μαθηματικών τεχνικών που στοχεύουν στην εξασφάλιση θεμάτων που άπτονται της ασφάλειας μετάδοσης πληροφοριών

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 σύγχρονής 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 αλγορίθμους.
- **Οικονομολογική κρυπτογραφία**

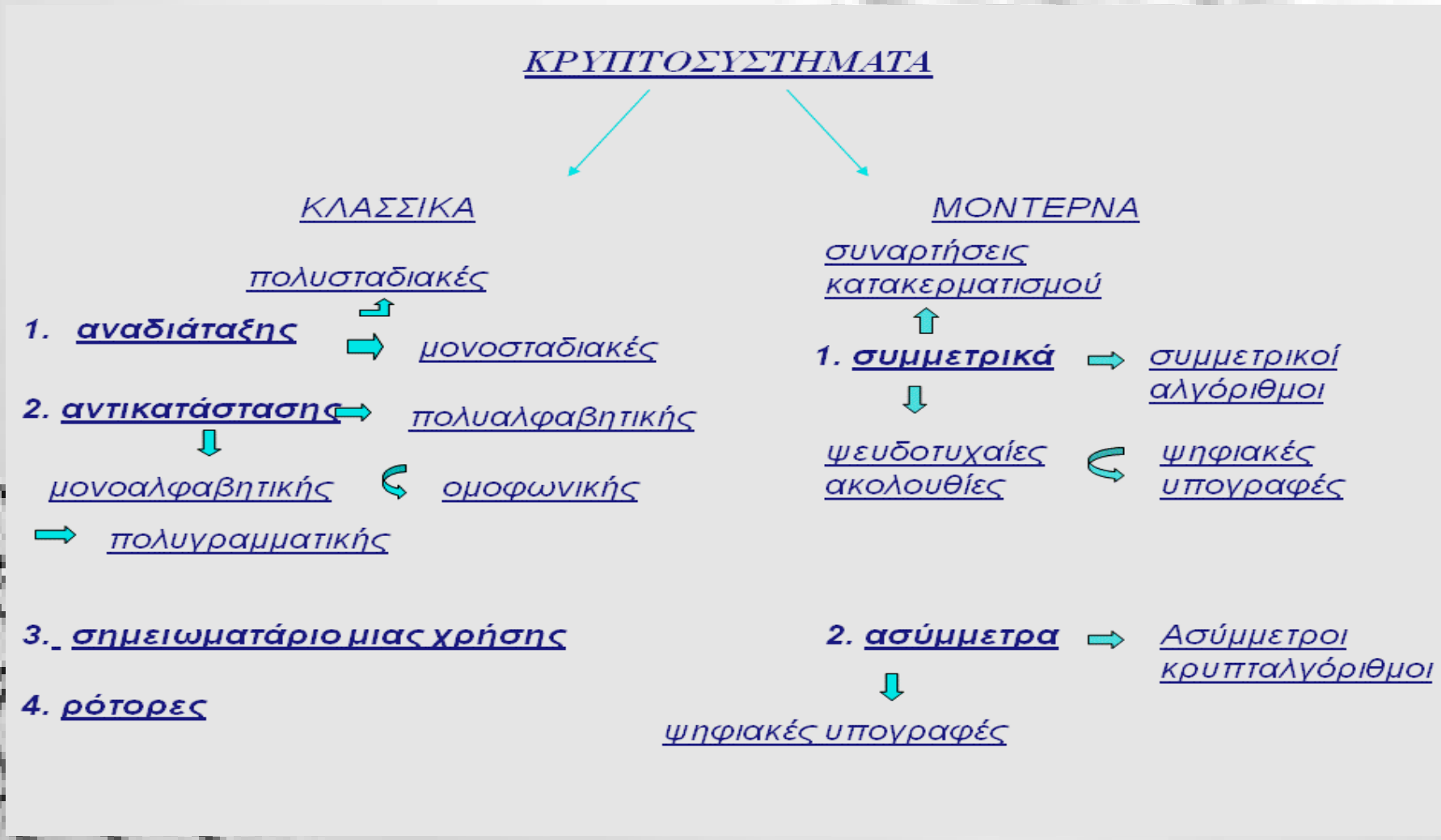
Ορισμός και ανάλυση κρυπτοσυστημάτων

Κρυπτοσύστημα είναι το σύνολο των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης.

Κατηγορίες

- Αναδιάταξης
- Αντικατάστασης
- Σημειωματάριο μιας χρήσης
- Ρότορες
- Συμμετρικά κρυπτοσυστήματα
- Ασύμμετρα συστήματα

Κρυπτοσυστήματα



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 κρυπτοσύστημα:** 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 κρυπτοσύστημα:** 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 αξιοποίησης 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 υπόδειξεως της καθηγήτριας μας, ζητήσαμε τη βοήθεια του διευθυντή του σχολείου μας, ώστε να ενημερωθούμε για το προαναφερόμενο σύστημα.

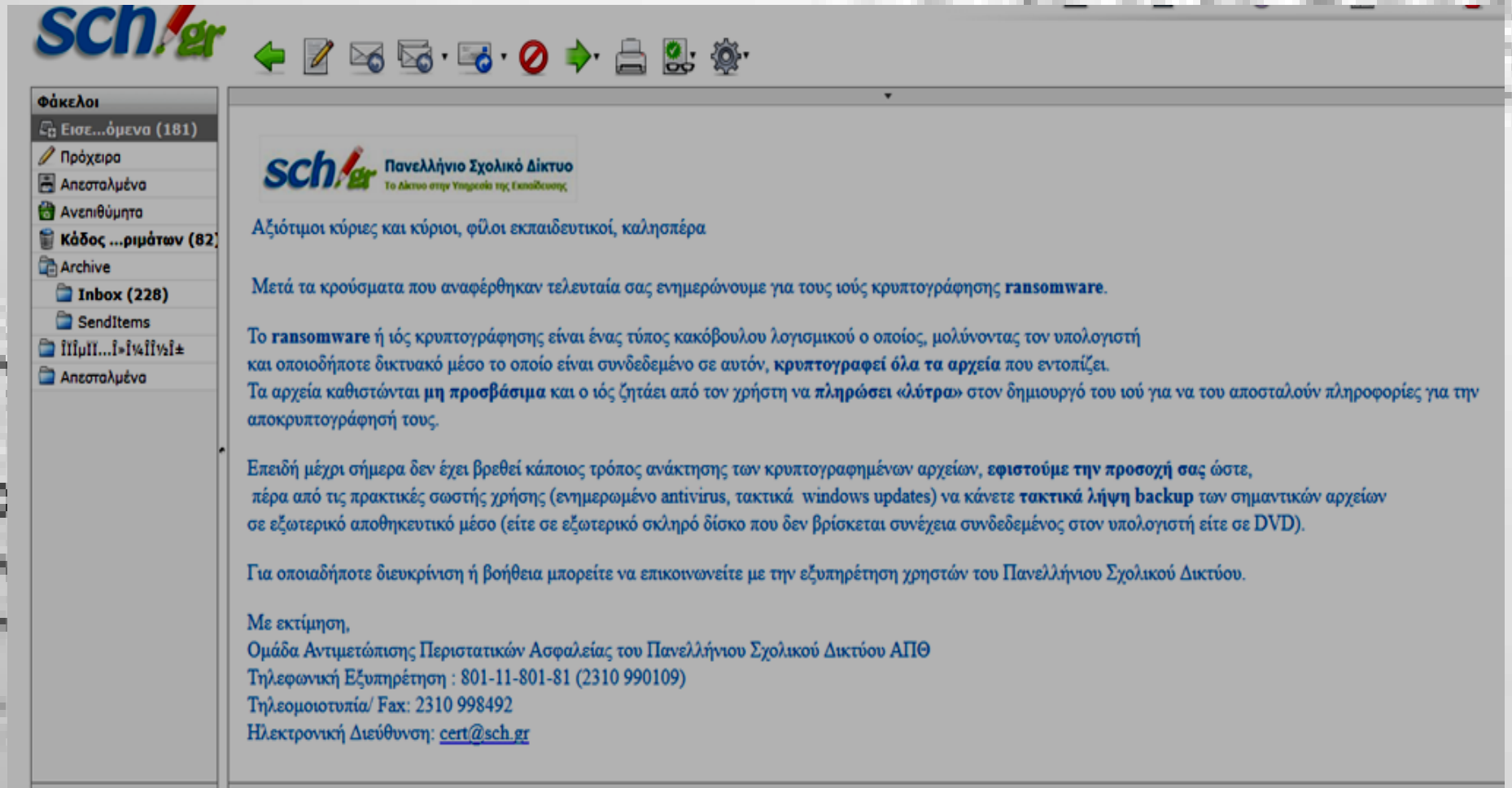
Το Υπουργείο Παιδείας, για την κάλυψη των προαναφερόμενων αναγκών, υιοθέτησε μια νέα μέθοδο μετάδοσης δεδομένων που είναι γνωστή ως "Μετάδοση VBI« η οποία βασίζεται στην κρυπτογραφημένη μετάδοση των θεμάτων.

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 διανέμονται 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




Ευχαριστούμε για την προσοχή σας...!!!