Ελληνική Δημοκρατία
Τεχνολογικό Εκπαιδευτικό
Ίδρυμα Ηπείρου

Πληροφορική Ι

Ενότητα 10 : **Ασφάλεια**

Δρ. Γκόγκος Χρήστος

Τμήμα Χρηματοοικονομικής & Ελεγκτικής (Παράρτημα Πρέβεζας)

Πληροφορική Ι

Ενότητα 10 : Ασφάλεια

Δρ. Γκόγκος Χρήστος
Επίκουρος Καθηγητής

Άρτα, 2015

Άδειες Χρήσης

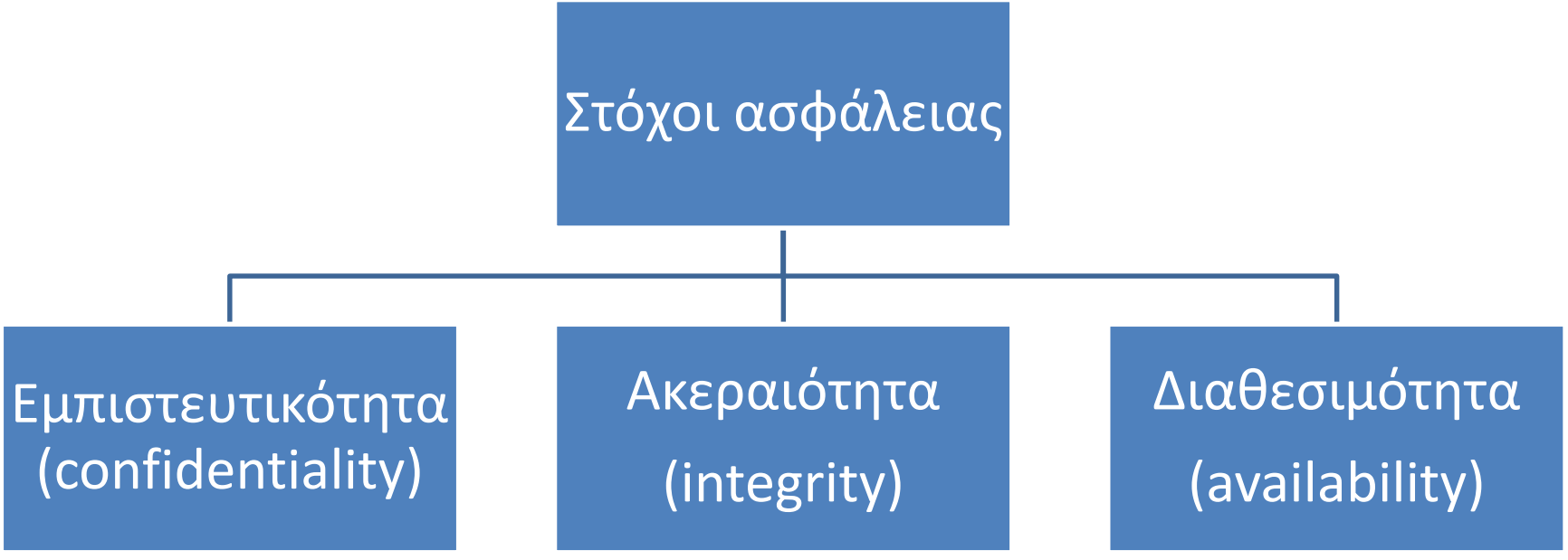
- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «**Εκπαίδευση και Δια Βίου Μάθηση**» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Ηπείρου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Στόχοι ασφάλειας



Εμπιστευτικότητα

- Επιθέσεις με στόχο την εμπιστευτικότητα

- Η εμπιστευτικότητα αφορά την διατήρηση του απορρήτου των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση

- **Κατασκόπευση** (στόχος η υποκλοπή εμπιστευτικών πληροφοριών κατά την μετάδοσή τους)
- **Ανάλυση κυκλοφορίας** (παρακολούθηση κυκλοφορίας με στόχο την εξαγωγή συμπερασμάτων)

Ακεραιότητα

- Επιθέσεις με στόχο την ακεραιότητα

- Οι αλλαγές θα πρέπει να γίνονται μόνο από εξουσιοδοτημένους χρήστες και μόνο μέσω εξουσιοδοτημένων μηχανισμών

- **Τροποποίηση** (ο επιτιθέμενος τροποποιεί τις πληροφορίες προς όφελός του)
- **Μεταμφίεση** (ο επιτιθέμενος χρησιμοποιεί την ταυτότητα κάποιου άλλου)
- **Αναπαραγωγή** (ο επιτιθέμενος αντιγράφει ένα μήνυμα με σκοπό την επανάληψή του)
- **Απάρνηση** (ο αποστολέας ή ο παραλήπτης αρνείται ότι έλαβε μέρος σε μια συναλλαγή)

Διαθεσιμότητα

- Επιθέσεις με στόχο την διαθεσιμότητα

- Οι πληροφορίες που παράγονται και αποθηκεύονται θα πρέπει να είναι συνεχώς διαθέσιμες στους εξουσιοδοτημένους χρήστες
- **Άρνηση υπηρεσιών** (στόχος είναι διακοπή των υπηρεσιών προς τους έγκυρους χρήστες)

Υπηρεσίες ασφάλειας

Η πιστοποίηση αυθεντικότητας ταυτοποιεί τα εμπλεκόμενα μέλη σε μια συναλαγή

Τεχνικές

- Στεγανογραφία
- Κρυπτογραφία
  - Κρυπτογραφία συμμετρικού κλειδιού
  - Κρυπτογραφία ασύμμετρου κλειδιού

Στεγανογραφία

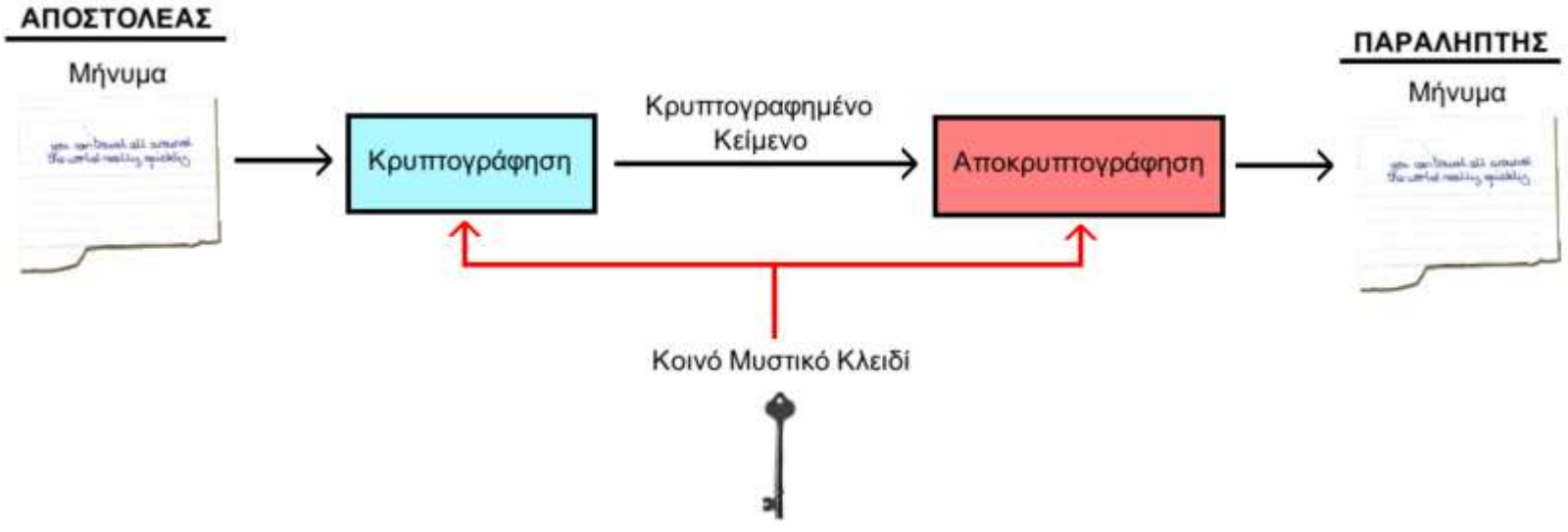
- Τα δεδομένα ενός μηνύματος αποκρύπτονται καθώς βρίσκονται κρυμμένα σε κάτι άλλο
- Οι κρυμμένες πληροφορίες δεν χρησιμοποιούνται αποκλειστικά για λόγους μυστικότητας. Μπορούν να χρησιμοποιηθούν για:
  - Προστασία πνευματικών δικαιωμάτων
  - Αποτροπή αλλαγών στα δεδομένα
  - Πρόσθετες πληροφορίες

Λογισμικά στεγανογραφίας

- Hide in Picture (απόκρυψη πληροφοριών μέσα σε αρχεία εικόνας)
- wbStego (απόκρυψη πληροφοριών μέσα σε pdf αρχεία)
- mp3Stego (απόκρυψη πληροφοριών μέσα σε mp3 αρχεία)
- Stegomagic

ΚΕΙΜΕΝΟ

Κρυπτογραφία συμμετρικού κλειδιού



Κρυπτογραφία συμμετρικού κλειδιού

- Στόχος είναι η μετάδοση μηνυμάτων μέσω ενός μη ασφαλούς καναλιού επικοινωνίας
- Αρχή του Kerckhoff: Είναι προτιμότερο να είναι γνωστή η μέθοδος κρυπτογράφησης (The enemy knows the system)
- Ορολογία
  - Απλό κείμενο (plaintext)
  - Κρυπτοκείμενο (ciphertext)
  - Κρυπταλγόριθμος (ciphers)
  - Μυστικό κλειδί (key)
- Οι δύο συμμετέχοντες στην επικοινωνία χρησιμοποιούν ένα γνωστό μόνο σε αυτούς κλειδί για να γίνεται η κρυπτογράφηση και η αποκρυπτογράφηση των μηνυμάτων
- Προβλήματα:
  - Κλοπή κλειδιού
  - Αριθμός κλειδιών

Κλασικοί κρυπταλγόριθμοι

- **Κρυπταλγόριθμοι αντικατάστασης**: ένα σύμβολο αντικαθίσταται από ένα άλλο
- **Κρυπταλγόριθμοι αναδιάταξης**: αλλάζει την θέση των συμβόλων

- Σπάσιμο κρυπταλγορίθμων
  - Επίθεση κατά μέτωπο
  - Επίθεση ανάλυσης συχνότητας

Σύγχρονοι κρυπταλγόριθμοι

- Βασίζονται σε σειρές από bits αντί για κείμενο
- Χρησιμοποιούν συνδυασμό από αναδιατάξεις, αντικαταστάσεις και άλλους μετασχηματισμούς

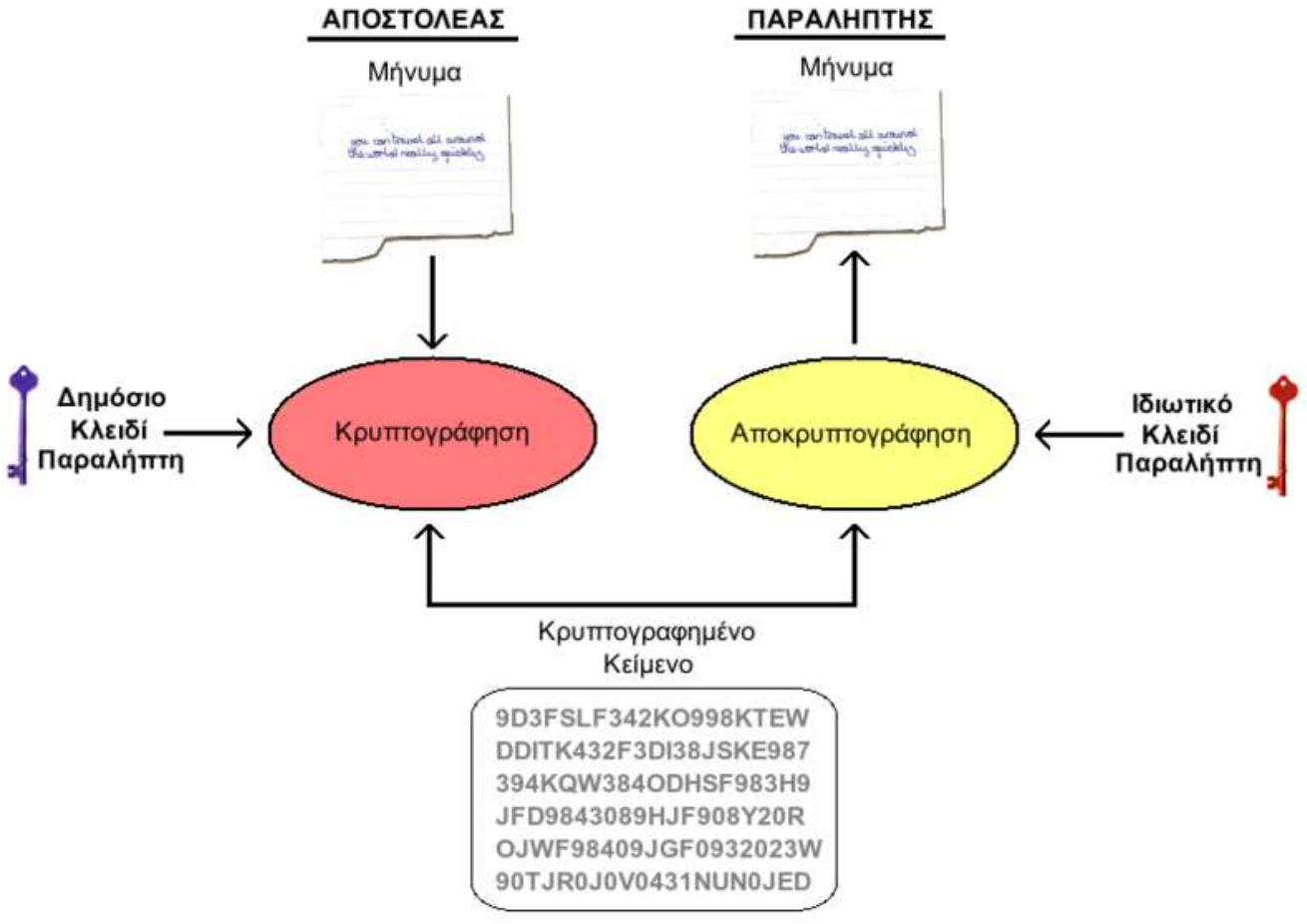
Ο AES είναι ισχυρότερος από τον DES

- **DES (Data Encryption Standard):** Δέχεται κείμενο 64bit και το κρυπτογραφεί σε κείμενο 64bit χρησιμοποιώντας κλειδί 56bit.
- **AES (Advanced Encryption Standard):** Δέχεται κείμενο 128bit και το κρυπτογραφεί σε κείμενο 128bit χρησιμοποιώντας κλειδί 128, 192 ή 256bit.

Κρυπτογραφία ασύμμετρου κλειδιού

- Η κρυπτογραφία ασύμμετρου κλειδιού χρησιμοποιείται σε μικρές ποσότητες πληροφοριών
- Χρησιμοποιούνται διαφορετικά κλειδιά: ένα ιδιωτικό και ένα δημόσιο
- Ένα μήνυμα κωδικοποιείται ως μια σειρά από ακεραίους αριθμούς
- Σε μια επικοινωνία ανάμεσα στο Α και στον Β που ο Α στέλνει ένα μήνυμα στον Β
  - Και οι δύο διαθέτουν τα δικά τους δημόσια και ιδιωτικά κλειδιά
  - Ο Α κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του Β
  - Ο Β λαμβάνει το μήνυμα και το αποκρυπτογραφεί με το ιδιωτικό κλειδί του

Κρυπτογραφία ασύμμετρου κλειδιού



Ο αλγόριθμος RSA

- Πρώτος είναι ένας αριθμός που διαιρείται μόνον με τον εαυτό του και την μονάδα
- Ο αλγόριθμος RSA βασίζεται στην δυσκολία παραγοντοποίησης ενός μεγάλου πρώτου αριθμού ως γινόμενο 2 πρώτων αριθμών

Σύγκριση ασύμμετρης και συμμετρικής κρυπτογραφίας

- Οι δύο μέθοδοι κρυπτογραφίας συμπληρώνονται η μια από την άλλη
- Η κρυπτογραφία συμμετρικού κλειδιού βασίζεται στη διαμοιραζόμενη μυστικότητα ενώ η κρυπτογραφία ασύμμετρου κλειδιού βασίζεται στην «προσωπική» μυστικότητα

Βιβλιογραφία

1. Forouzan B., Mosharaf F. Εισαγωγή στην επιστήμη των υπολογιστών. Εκδόσεις Κλειδάριθμος (2010)
2. Καρολίδης Δ., Ξαρχάκος Κ.. Εισαγωγή στην πληροφορική και στο διαδίκτυο. Εκδόσεις Άβακας (2008).
3. Σφακιανάκης Μ. Εισαγωγή στην πληροφορική σκέψη. Εκδόσεις Κλειδάριθμος (2003).
4. Τσιτμηδέλης Σ., Τικτοπούλου Ε. Εισαγωγή στην πληροφορική. Πανεπιστημιακές εκδόσεις Αράκυνθος (2009).
5. Γιαγλής Γ. Εισαγωγή στην πληροφορική. Γκιούρδας εκδοτική (2009).
6. Αβούρης Ν., Κουφοπαύλου Ο., Σερπάνος Δ. Εισαγωγή στους υπολογιστές. Εκδόσεις typorama (2004).
7. Biermann A. Σπουδαίες ιδέες στην επιστήμη των υπολογιστών. Πανεπιστημιακές εκδόσεις Κρήτης (2008).
8. Brookshear J.G. Η επιστήμη των υπολογιστών, μια ολοκληρωμένη παρουσίαση. Εκδόσεις Κλειδάριθμος (2009).
9. Ceruzzi P.E. Ιστορία της υπολογιστικής τεχνολογίας. Από τον ENIAC μέχρι το διαδίκτυο. Εκδόσεις Κάτοπτρο (2006).

Σημείωμα Αναφοράς

Έκδοση: 1.0 Άρτα, 2015. Διαθέσιμο από τη δικτυακή διεύθυνση:
http://eclass.teiep.gr/OpenClass/courses/ACC136/

Σημείωμα Αδειοδότησης

[1] http://creativecommons.org/licenses/by-nc-nd/4.0/deed.el

Τέλος Ενότητας

Επεξεργασία: Ευάγγελος Καρβούνης

Άρτα, 2015

Ευρωπαϊκή Ένωση
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΕΣΠΑ 2007-2013
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Τέλος Ενότητας

Ασφάλεια