Ασφάλεια Συστημάτων

Τζέριες Μπεσαράτ, PhD

20 Μαΐου 2022, Άρτα

Στο προηγούμενο μάθημα αναπτύξαμε

- Παράγοντες Ασφάλειας
- Παράγοντες Επιθέσεων
  - Μεθοδολογία επίθεσης
  - Απειλές
- Ασφαλής Σχεδιασμός Διαδικτυακών Εφαρμογών
  - Επικύρωση δεδομένων εισόδου
  - Αυθεντικοποίηση
  - Εξουσιοδότηση
  - Διαχείριση ρυθμίσεων
  - Προστασία ευαίσθητων δεδομένων
  - Διαχείριση συνόδου
  - Χρήση κρυπτογραφίας
  - Αλλοίωση παραμέτρων
  - Διαχείριση εξαιρέσεων
  - Έλεγχος και καταγραφή

Εισαγωγή στην κρυπτολογία

Ο όρος κρυπτολογία (cryptology) είναι ετυμολογικά μια σύνθετη λέξη που αποτελείται από τα λήμματα «κρυπτός» και «λόγος» και δηλώνει τη μυστικότητα του λόγου που μπορεί να είναι προφορικός ή με τη μορφή ενός γραπτού κειμένου.

Η μυστικότητα των περιεχομένων αφορά την προστασία της εμπιστευτικότητας (confidentiality) της πληροφορίας που περιέχεται σε αυτά. Σήμερα, με τον όρο κρυπτολογία ορίζεται η επιστημονική περιοχή που περιλαμβάνει την κρυπτογραφία (cryptography) και την κρυπτανάλυση (cryptanalysis).

Θα δούμε

- Κρυπτογραφία
  - Κρυπτογραφικό Σύστημα
  - Κρυπτανάλυση
  - Κλειδί
  - Αλγόριθμοι Κρυπτογράφησης
- Στεγανογραφία
- Χρήσιμες Έννοιες
- Μελέτη κλασσικών κρυπτογραφικών αλγορίθμων
  - Αλγόριθμος του Καίσαρα
  - Αλγόριθμος Vigenere

Εισαγωγή

Η πρώτη εμφάνιση τεχνικών κρυπτογραφίας συναντάται περίπου 4.000 χρόνια πριν, στα πρώιμα στάδια του Αιγυπτιακού πολιτισμού, όταν οι συγγραφείς της εποχής περιέγραφαν τη ζωή των βασιλιάδων με ασυνήθιστες ιερογλυφικές αναπαραστάσεις.

Ως αποτέλεσμα αυτής της ενέργειας, η ανάγνωση των ιερογλυφικών ήταν δυνατή μόνο από όσους γνώριζαν τον μυστικό κώδικα που είχε χρησιμοποιηθεί κατά τη συγγραφή τους, ενώ για όλους τους άλλους οι παραστάσεις ήταν ακατανόητες. Η διεργασία μετασχηματισμού ενός αρχικού κειμένου (plaintext) σε μια ακατάληπτη μορφή με τη χρήση ενός κρυπτογραφικού αλγορίθμου ονομάζεται κρυπτογράφηση.

Σχετική με την κρυπτογραφία είναι η περιοχή της στεγανογραφίας (steganography)

Η λέξη προέρχεται από τις λέξεις «στεγανός» και «γραφή» και δηλώνει την προσπάθεια απόκρυψης της ύπαρξης ενός μηνύματος που είναι κρυμμένο μέσα στα μηνύματα μιας φανερής (φαινομενικά απροστάτευτης) επικοινωνίας μεταξύ δύο οντοτήτων.

Η κύρια διαφορά με την κρυπτογραφία είναι ότι η στεγανογραφία στοχεύει στην απόκρυψη της ύπαρξης του κρίσιμου μηνύματος, το οποίο δεν είναι απαραίτητο να είναι κρυπτογραφημένο.

Κρυπτογραφικός Αλγόριθμος

Ένας κρυπτογραφικός αλγόριθμος (Cipher/Encryption algorithm) περιγράφει τη μέθοδο μετασχηματισμού μηνυμάτων σε μια μορφή τέτοια που να μην επιτρέπεται σε μη εξουσιοδοτημένα μέρη η αποκάλυψη του περιεχομένου τους. Οι αρχαίοι Σπαρτιάτες χρησιμοποίησαν την κρυπτογραφία και εκμεταλλεύτηκαν τις τεχνικές της για στρατιωτικούς σκοπούς.

Αναφέρεται χαρακτηριστικά η χρήση της «σκυτάλης», η οποία ήταν μια ξύλινη ράβδος πάνω στην οποία περιτυλίγονταν ένας πάπυρος σε μορφή ταινίας.

Το μήνυμα αποτυπωνόταν στον τυλιγμένο γύρω από την σκυτάλη πάπυρο, κατά μήκος της ράβδου, οπότε όταν ο πάπυρος ξετυλίγονταν, η ανάγνωση του κειμένου κατά μήκος του πάπυρου κατέληγε να μην αποδίδει ένα καταληπτό νόημα. Το αρχικό μήνυμα ήταν δυνατό να διαβαστεί μόνο από κάποιον ο οποίος διέθετε σκυτάλη ίδιας διαμέτρου, ώστε να προσαρμόσει πάνω της εκ νέου τον πάπυρο και να αποκρυπτογραφήσει το μήνυμα.

Σε αυτή την περίπτωση, η διάμετρος της σκυτάλης αποτελεί το κλειδί (key) κρυπτογράφησης, το οποίο μαζί με τον κρυπτογραφικό αλγόριθμο αποτελεί το μέσο για το μετασχηματισμό του αρχικού μηνύματος σεκρυπτοκείμενο (cipher text).

Λειτουργία Σπαρτιατικής σκυτάλης

Κρυπτογραφία

Στόχος της κρυπτογραφίας είναι να παρέχει υπηρεσίες ασφάλειας, όπως:

- Εμπιστευτικότητα (confidentiality).
- Ακεραιότητα (integrity).
- Αυθεντικοποίηση (authentication).
- Αδυναμία αποποίησης (non-repudiation).

Επιπλέον, είναι επιθυμητές οι παρακάτω ιδιότητες για ένα κρυπτοσύστημα και τα συστατικά μέρη του:

- Πρέπει να χρησιμοποιούνται αποδοτικοί αλγόριθμοι για τις λειτουργίες της κρυπτογράφησης και αποκρυπτογράφησης.
- Το σύστημα πρέπει να είναι εύχρηστο και να μην προκαλεί σύγχυση στον χρήστη.
- Η προστασία που παρέχει το σύστημα πρέπει να προϋποθέτει μόνο τη μυστικότητα των κλειδιών και όχι των αλγορίθμων που χρησιμοποιούνται

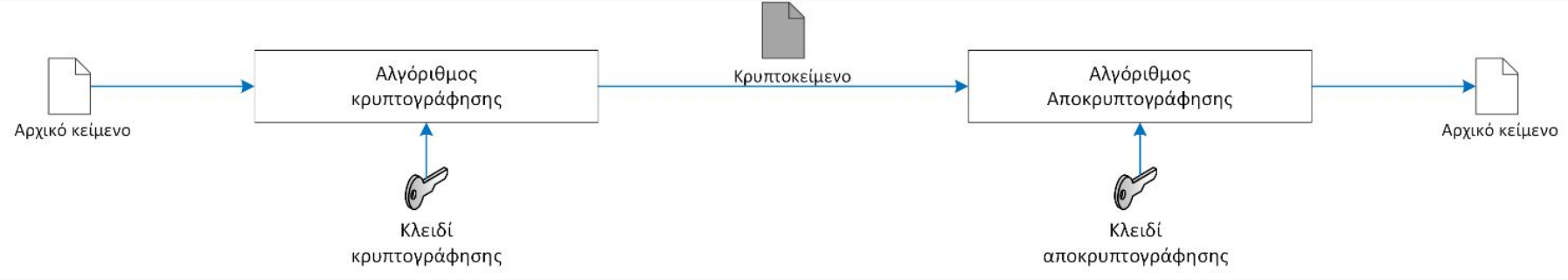
Κρυπτογραφικό σύστημα

Σε ένα κρυπτογραφικό σύστημα, τα δεδομένα που περιέχονται σε ένα μήνυμα με τη μορφή ενός αρχικού κειμένου (plaintext), κρυπτογραφούνται και το παραγόμενο μήνυμα αποτελεί το κρυπτοκείμενο (ciphertext).

Στη συνέχεια, το κρυπτοκείμενο αποστέλλεται στον παραλήπτη, όπου αποκρυπτογραφείται για να αναπαραχθεί το αρχικό κείμενο.

Η κρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης που χρησιμοποιεί ένα κλειδί κρυπτογράφησης.

Τυπικό κρυπτοσύστημα



Πότε είναι ασφαλές ένα κρυπτογραφικό σύστημα;

- Το κόστος της παραβίασης του κρυπτομηνύματος, δηλαδή της ανάκτησης του κλειδιού αποκρυπτογράφησης, υπερβαίνει την αξία των πληροφοριών που τελικά λαμβάνονται ως αποτέλεσμα της κρυπτανάλυσης.
- Ο χρόνος που απαιτείται για τη διαδικασία της κρυπτανάλυσης υπερβαίνει την ωφέλιμη διάρκεια ζωής των λαμβανομένων πληροφοριών.

Κρυπτανάλυση

Στόχος της κρυπτανάλυσης είναι η εύρεση του κλειδιού αποκρυπτογράφησης που χρησιμοποιήθηκε για την ασφαλή ανταλλαγή μηνυμάτων με τη χρήση ενός κρυπτοσυστήματος.

Ο ρόλος του κρυπταναλυτή, επομένως, έρχεται σε πλήρη αντίθεση με το ρόλο του κρυπτογράφου, καθώς ο πρώτος προσπαθεί να παραβιάσει ένα κρυπτοσύστημα το οποίο χρησιμοποιεί ο δεύτερος.

Για την εύρεση του κλειδιού αποκρυπτογράφησης

Ο κρυπταναλυτής μπορεί να χρησιμοποιήσει τεχνικές όπως:

- **Επίθεση Ωμής Βίας (Brute-Force Attack):** Ο επιτιθέμενος, μέσω εξαντλητικής αναζήτησης, προσπαθεί να αποκαλύψει το κλειδί αποκρυπτογράφησης, δοκιμάζοντας όλους τους πιθανούς συνδυασμούς στοιχείων του αλφαβήτου που χρησιμοποιήθηκε κατά τον ορισμό του.
- **Επίθεση Στατιστικής Ανάλυσης (Statistical Analysis Attack):** Ο κρυπταναλυτής προσπαθεί να εκμεταλλευτεί, προς όφελός του, εγγενή χαρακτηριστικά της γλώσσας στην οποία έχει γραφτεί το αρχικό κείμενο.

Επιθέσεις Κρυπτανάλυσης

Μπορούμε να διακρίνουμε τις επιθέσεις κρυπτανάλυσης, με βάση την πληροφορία που διαθέτει ο κρυπταναλυτής, ως εξής:

- Μόνο κρυπτοκειμένου (ciphertext only)
- Γνωστού αρχικού κειμένου (known plaintext)
- Επιλεγμένου αρχικού κειμένου (chosen plaintext)
- Επιλεγμένου κρυπτοκειμένου (chosen ciphertext)
- Επιλεγμένου κειμένου (chosen text)

Κλειδί

Σε ένα κρυπτογραφικό σύστημα, η ανάκτηση του αρχικού κειμένου, το οποίο πρέπει να παραμείνει μυστικό από τρίτους, προϋποθέτει την ανάκτηση του κλειδιού αποκρυπτογράφησης.

Ένα κλειδί αποτελείται από μια σειρά bit. Για την αποφυγή του εντοπισμού του κλειδιού μέσω της εξαντλητικής αναζήτησης (brute force attack), το πλήθος των πιθανών τιμών (συνδυασμών από bit) που μπορεί να πάρει ένα κλειδί, πρέπει να είναι τεράστιο προκειμένου να αντιμετωπίζονται οι επιθέσεις αυτές στη βάση των κριτηρίων κόστους και χρόνου που αναφέρθηκαν προηγουμένως. Έτσι, για μήκος κλειδιού της τάξης των 64bit, οι πιθανές τιμές κλειδιού είναι 256, δηλαδή μπορούν να παραχθούν περισσότερα από 7x1016 διαφορετικά κλειδιά.

ενδεικτικά η αύξηση του χρόνου αναζήτησης σε σχέση με το μήκος του κλειδιού και τον αριθμό η των επεξεργαστικών μονάδων

Μήκος κλειδιού	**Χώρος αναζήτησης**	**Απαιτούμενος χρόνος με $6x10^7$ κλειδιά ανά sec**
56	$7,2x10^{16}$	38 έτη / n
64	$1,8x10^{19}$	9749 έτη / n
128	$3,4x10^{38}$	$1,8x10^{23}$ έτη / n
256	$1,16x10^{77}$	$6,1x10^{61}$ έτη / n
512	$1,36x10^{154}$	$7,1x10^{138}$ έτη / n

Αλγόριθμοι κρυπτογράφησης

Οι κρυπτογραφικοί αλγόριθμοι διακρίνονται ως προς:

- το είδος των κλειδιών που χρησιμοποιούν και
- τον τρόπο επεξεργασίας του αρχικού και του κρυπτογραφημένου κειμένου.

Είδος κλειδιών

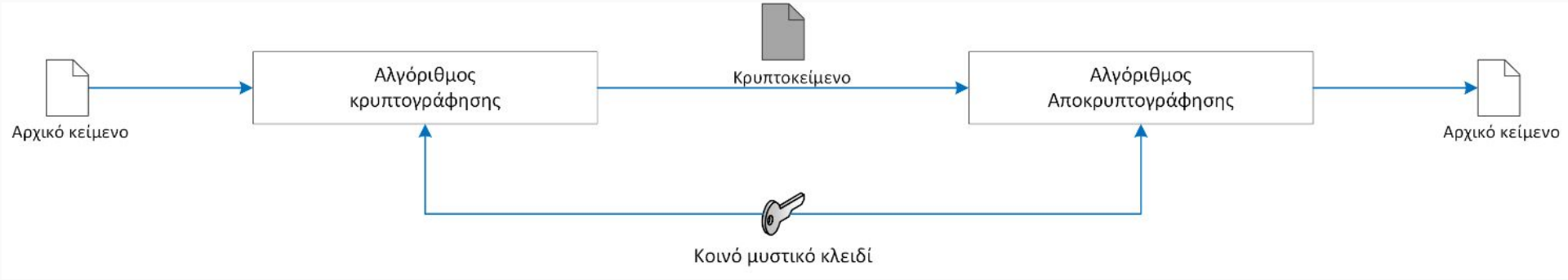
Κατηγοριοποιώντας τους αλγορίθμους κρυπτογράφησης ως προς το είδος των κλειδιών, διακρίνουμε τους συμμετρικούς (symmetric) αλγορίθμους και τους ασύμμετρους (asymmetric) ή δημοσίου κλειδιού (public key).

Συμμετρικοί Αλγόριθμοι

Στους συμμετρικούς κρυπτογραφικούς αλγορίθμους, η κρυπτογράφηση και η αποκρυπτογράφηση γίνεται χρησιμοποιώντας (συμμετρικά) το ίδιο κλειδί, αλλά με αντίστροφες λειτουργίες. Η οντότητα Α κρυπτογραφεί το αρχικό κείμενο με το κλειδί Κ και αποστέλλει το κρυπτοκείμενο, ενώ η οντότητα Β παραλαμβάνει το κρυπτοκείμενο και χρησιμοποιεί το ίδιο κλειδί Κ για να το αποκρυπτογραφήσει και να ανακτήσει το αρχικό κείμενο.

Η συμμετρική κρυπτογραφία ονομάζεται και κρυπτογραφία μυστικού κλειδιού.

Συμμετρική κρυπτογραφία



Ασύμμετροι αλγόριθμοι

Οι ασύμμετροι αλγόριθμοι χρησιμοποιούν διαφορετικό κλειδί για την κρυπτογράφηση (π.χ. το δημόσιο κλειδί του παραλήπτη) και διαφορετικό για την αποκρυπτογράφηση (π.χ. το ιδιωτικό κλειδί του παραλήπτη).

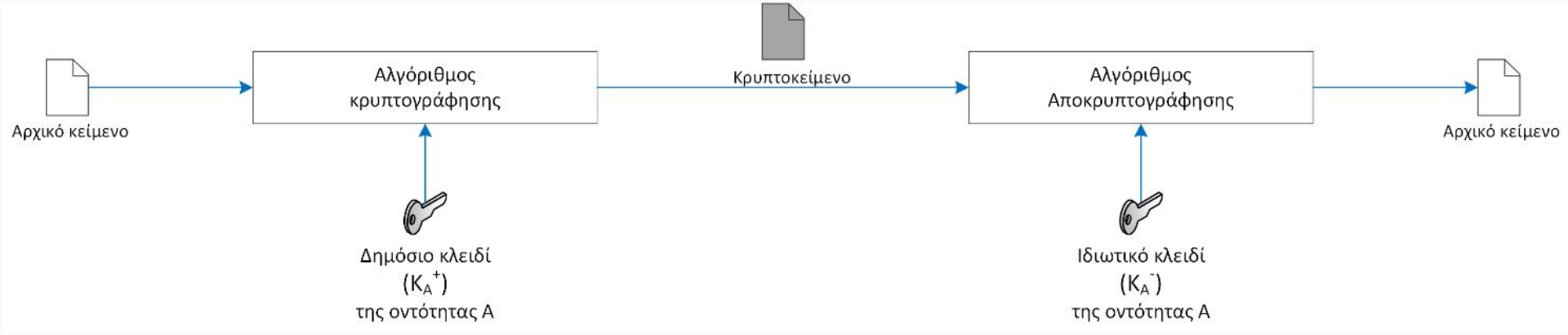
Κάθε οντότητα που συμμετέχει σε ένα κρυπτοσύστημα δημοσίου κλειδιού, διαθέτει ένα δικό της ζεύγος κλειδιών, με μεγάλη διάρκεια ισχύος που εξαρτάται από το σκοπό χρήσης του (π.χ. για κρυπτογράφηση ή για υπογραφή).

Οι ασύμμετροι αλγόριθμοι λειτουργούν ικανοποιώντας δυο (2) βασικές απαιτήσεις:

- **Είναι υπολογιστικά ανέφικτο να υπολογιστεί το ένα κλειδί γνωρίζοντας το άλλο κλειδί του ίδιου κατόχου.** Η ιδιότητα αυτή επιτρέπει να δημοσιοποιηθεί το ένα κλειδί (δημόσιο κλειδί) και να διατηρηθεί το άλλο πραγματικό μυστικό, ώστε να το γνωρίζει μόνον ο ιδιοκτήτης του (ιδιωτικό κλειδί). Λόγω αυτού του σχήματος λειτουργίας, οι αλγόριθμοι αυτοί ονομάζονται αλγόριθμοι δημοσίου κλειδιού, οπότε:
  - Το δημόσιο κλειδί (K+) κάθε οντότητας είναι διαθέσιμο σε όλες τις άλλες οντότητες
  - Το ιδιωτικό κλειδί (K-) είναι αυστηρά γνωστό μόνο στη μια οντότητα που κατέχει το ζεύγος των κλειδιών στο οποίο ανήκει.

- **Κάθε αρχικό κείμενο που κρυπτογραφείται με το ένα κλειδί, αποκρυπτογραφείται μόνο με το άλλο κλειδί του ίδιου ζεύγους.** Έτσι, μια οντότητα Α μπορεί να κρυπτογραφήσει ένα μήνυμα το οποίο προορίζεται για την οντότητα Β, χρησιμοποιώντας το δημόσιο κλειδί της οντότητας Β. Στη συνέχεια, το κρυπτοκείμενο που παράγεται αποστέλλεται στον παραλήπτη (Β), όπου μόνον αυτός μπορεί να το αποκρυπτογραφήσει χρησιμοποιώντας το ιδιωτικό κλειδί του. Με τον τρόπο αυτό εξασφαλίζεται η εμπιστευτικότητα του μηνύματος.

Εφαρμογή κρυπτογραφίας δημοσίου κλειδιού για προστασία της εμπιστευτικότητας



Τρόπος επεξεργασίας

Κατηγοριοποιώντας τους αλγόριθμους κρυπτογράφησης ως προς τον τρόπο επεξεργασίας, διακρίνουμε τις περιπτώσεις αλγορίθμων

- **Δέσμης (block)** : Οι αλγόριθμοι δέσμης μετατρέπουν το αρχικό κείμενο (μήνυμα) σε δέσμες σταθερού μήκους, π.χ. των 64 bit, τις οποίες στη συνέχεια κρυπτογραφούν. Σε μια σύνοδο κρυπτογράφησης, όλες οι δέσμες δεδομένων ενός μηνύματος κρυπτογραφούνται με το ίδιο κλειδί.
- **Ροής (stream)**: Οι αλγόριθμοι ροής κρυπτογραφούν το αρχικό κείμενο, το οποίο θεωρείται ότι έχει τη μορφή μιας ροής από bit, εφαρμόζοντας την πράξη XOR μεταξύ κάθε bit της ροής του μηνύματος και μιας άλλης ροής, γνωστής ως κλειδοροής (key stream).

Ανθεκτικότητα

Με βάση τις υποθέσεις για την χειρότερη περίπτωση, γίνονται δοκιμές με σκοπό να βρεθούν τρόποι για να «σπάσει» το κρυπτογραφημένο κείμενο, δηλαδή να βρεθεί το μυστικό κλειδί αποκρυπτογράφησής του.

Σε αυτή την περίπτωση, ο σχεδιαστής ή ο χρήστης που προτίθεται να χρησιμοποιήσει ένα προϊόν κρυπτογράφησης παίζει το ρόλο του κρυπταναλυτή.

Στεγανογραφία

Η στεγανογραφία, αποτελεί έναν κλάδο της κρυπτολογίας όπου, σε αντίθεση με την κρυπτογραφία, στόχος δεν είναι η μετατροπή του μηνύματος σε ακατανόητη μορφή αλλά η απόκρυψη της ύπαρξής του.
Οι στεγανογραφικές τεχνικές μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς, όπως:

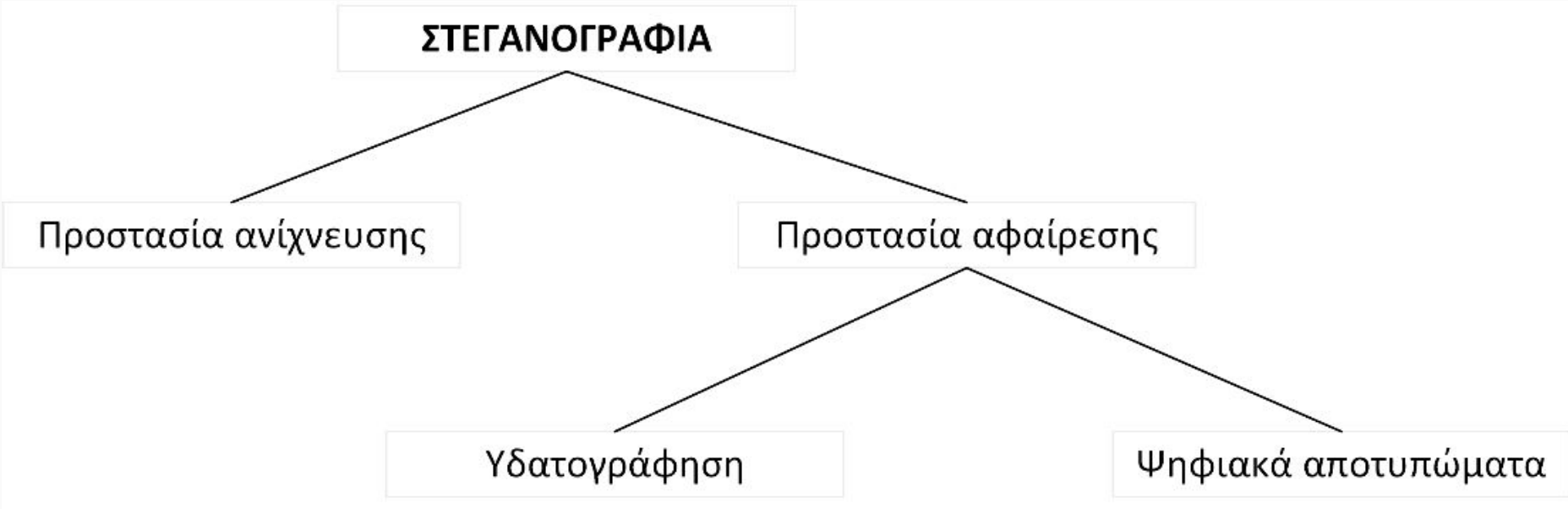
- Διαφύλαξη της εμπιστευτικότητας ενός μηνύματος.
- Προστασία πληροφορίας από μη εξουσιοδοτημένη τροποποίηση.
- Έλεγχος πρόσβασης κατά τη διανομή ηλεκτρονικού περιεχομένου.

Ψηφιακή Υδατογράφηση και τα Ψηφιακά Αποτυπώματα

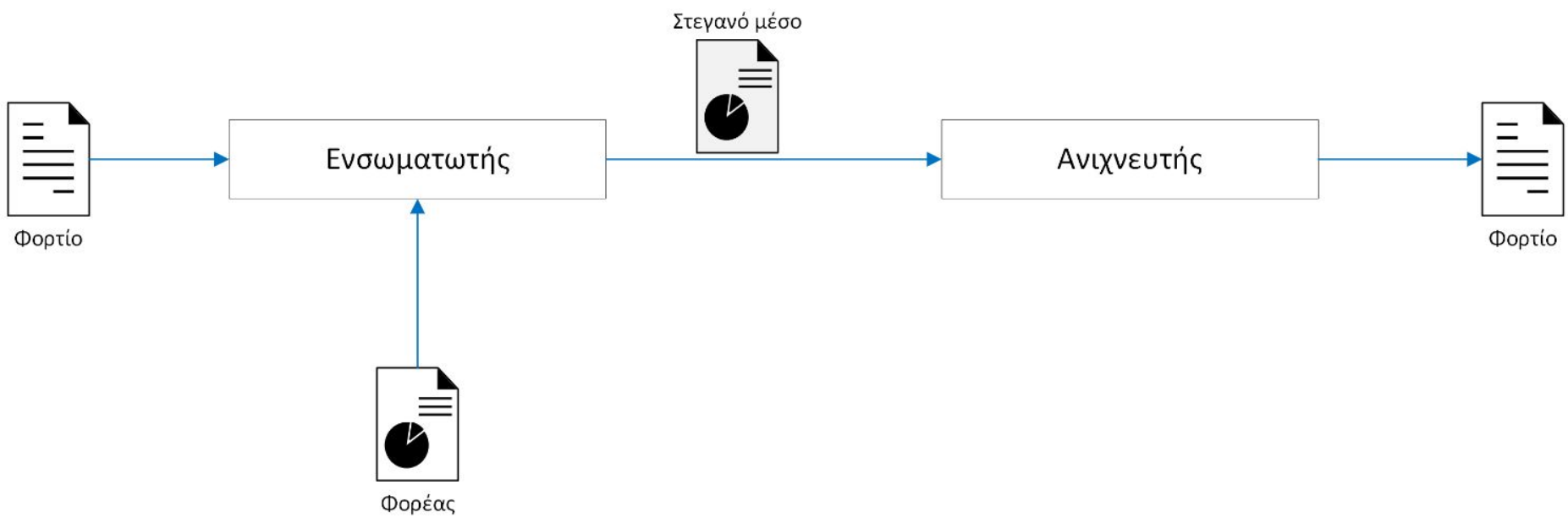
Μια ακόμη χρήση της στεγανογραφίας στις μέρες μας, είναι η προστασία των πνευματικών δικαιωμάτων ηλεκτρονικού περιεχομένου, όπου το κρυφό μήνυμα επιβεβαιώνει την ταυτότητα του νόμιμου ιδιοκτήτη του.

Η Ψηφιακή Υδατογράφηση (Digital Watermarking) και τα Ψηφιακά Αποτυπώματα (Digital Fingerprinting) είναι δύο κατηγορίες στις οποίες διαχωρίζεται η τεχνική του ηλεκτρονικού «σημαδέματος» ενός ηλεκτρονικού αρχείου με τεχνικές στεγανογραφίας.

Κατηγοριοποίηση σύγχρονων στεγανογραφικών τεχνικών



Διαδικασία ψηφιακής υδατογράφησης



3 κύριες αρχές

Η στεγανογραφία βασίζεται σε τρεις κύριες αρχές, οι οποίες αποτελούν και ένα μέτρο της αποδοτικότητας μιας στεγανογραφικής τεχνικής:

- **Ποσότητα Πληροφορίας:** Όσο περισσότερη πληροφορία (μεγαλύτερο φορτίο) μπορούμε να αποκρύψουμε, τόσο πιο αποδοτική είναι η στεγανογραφική τεχνική.
- **Δυσκολία Ανίχνευσης:** Μια στεγανογραφική τεχνική θα πρέπει να είναι ανθεκτική σε προσπάθειες ανίχνευσης. Υπάρχει οπωσδήποτε μια άμεση σχέση μεταξύ της ποσότητας πληροφορίας που μπορούμε να κρύψουμε και της δυσκολίας ανίχνευσης που προσφέρει η μέθοδος που χρησιμοποιούμε. Όσο περισσότερη πληροφορία, για παράδειγμα, προσπαθούμε να κρύψουμε ενσωματώνοντάς την στο στεγανό μέσο, τόσο πιο εύκολη γίνεται η ανίχνευση της κρυμμένης πληροφορίας.
- **Δυσκολία Αφαίρεσης Πληροφορίας:** Πρέπει να είναι πολύ δύσκολη, αν όχι αδύνατη, η αφαίρεση του κρυμμένου μηνύματος (φορτίου) από το στεγανό μέσο, χωρίς αυτό να γίνεται αντιληπτό από το νόμιμο παραλήπτη.

Επικοινωνιακό σύστημα

Η Θεωρία Πληροφορίας εστιάζει στην επικοινωνία μεταξύ των οντοτήτων, οι οποίες συμμετέχουν σε ένα επικοινωνιακό σύστημα

Αλγόριθμος του Καίσαρα

Ο αλγόριθμος του Καίσαρα ανήκει στην κατηγορία κρυπτογραφικών αλγορίθμων μονοαλφαβητικής αντικατάστασης, όπου το κλειδί είναι ένας χαρακτήρας του οποίου ο αύξων αριθμός θέσης στο αλφάβητο προκαλεί μια μετάθεση όλων των χαρακτήρων στο αλφάβητο. Ο Ιούλιος Καίσαρας στο βιβλίο «The Gallic Wars» περιγράφει έναν αλγόριθμο όπου κάθε γράμμα της αλφαβήτου μετατίθεται τρεις θέσεις δεξιότερα στο αλφάβητο. Η κρυπτογράφηση υλοποιείται με αντικατάσταση κάθε γράμματος του αρχικού κειμένου με το γράμμα που προκύπτει μετά τη μετάθεση. Αντίστοιχα, η αποκρυπτογράφηση γίνεται με αντικατάσταση του κάθε χαρακτήρα σύμφωνα με την αντίστροφη μετάθεση του αρχικού αλφαβήτου.

Αλγόριθμος Vigenere

Ο αλγόριθμος Vigenere ανήκει στην κατηγορία των κρυπτογραφικών αλγορίθμων πολυαλφαβητικής αντικατάστασης, όπου το κλειδί είναι μια μικρή ακολουθία γραμμάτων (π.χ. μια λέξη). Λειτουργεί όπως ο αλγόριθμος του Καίσαρα, αλλά χρησιμοποιεί τόσα διαφορετικά νέα αλφάβητα (μετά τις μεταθέσεις) όσα και τα διαφορετικά γράμματα της λέξης που χρησιμοποιείται ως κλειδί.