Ηλεκτρονική Διακυβέρνηση

Παπανικολάου Γεώργιος

Κρυπτογράφηση

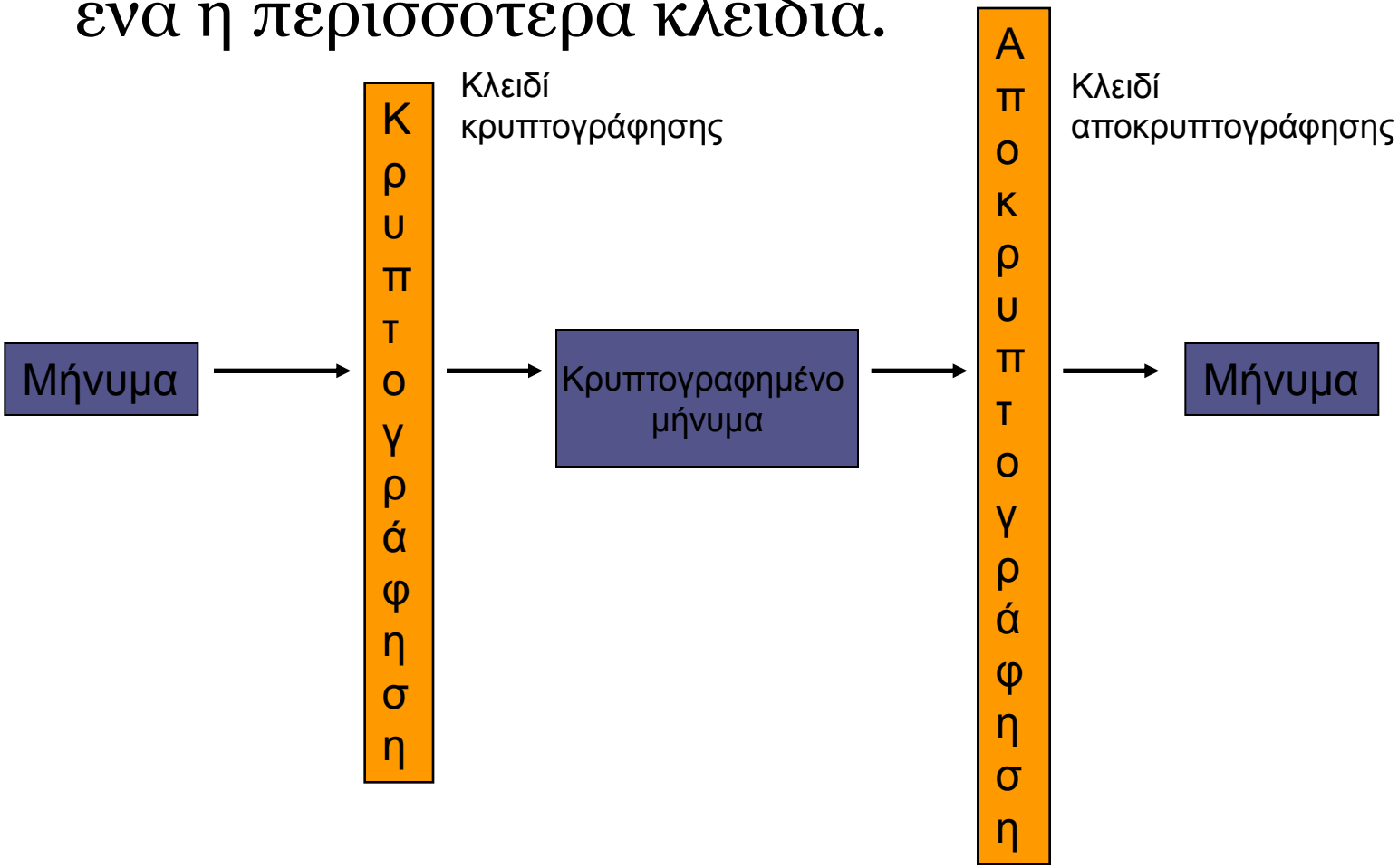
- Έννοιες κρυπτογράφησης

Απλό κείμενο
Κρυπτοκείμενο
Κλειδιά

Αλγόριθμοι κρυπτογράφησης
Αλγόριθμοι αποκρυπτογράφησης
Διαδικασίες κρυπτογράφησης

Κρυπτογράφηση

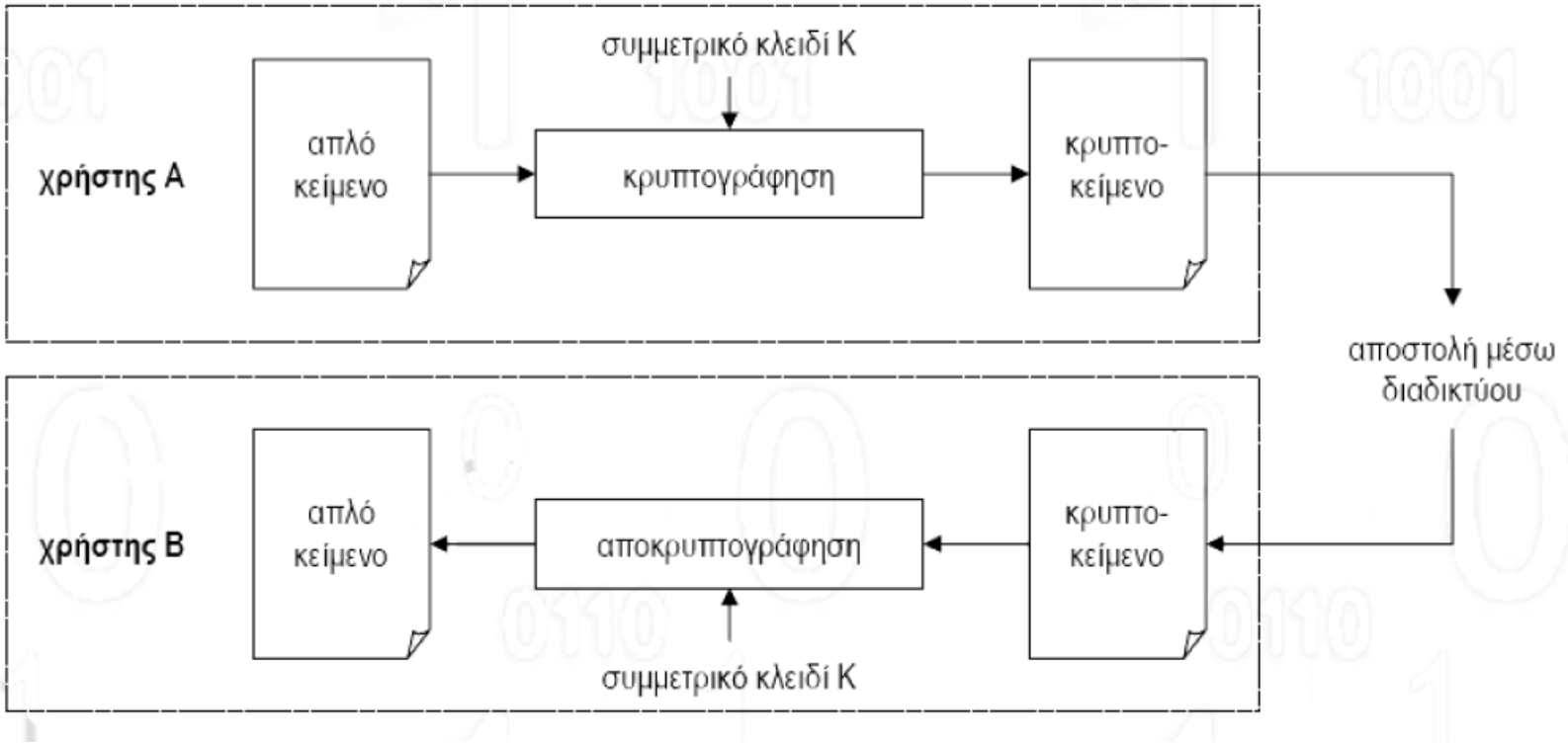
- Οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν ένα η περισσότερα κλειδιά.



Κρυπτογράφηση

- Η ασφάλεια έγκειται στο ότι δεν είναι γνωστό το κλειδί.
- Η αλγόριθμοι κρυπτογράφησης – αποκρυπτογράφησης είναι ευρέως γνωστοί.
- Αλγόριθμοι συμμετρικής κρυπτογράφησης
  AES, DES, IDEA, RC2, RC4, RC5, E0, A5/1
- Αλγόριθμοι ασύμμετρης κρυπτογραφίας
  RSA, DSA, ECC, Knapsack, ElGamal

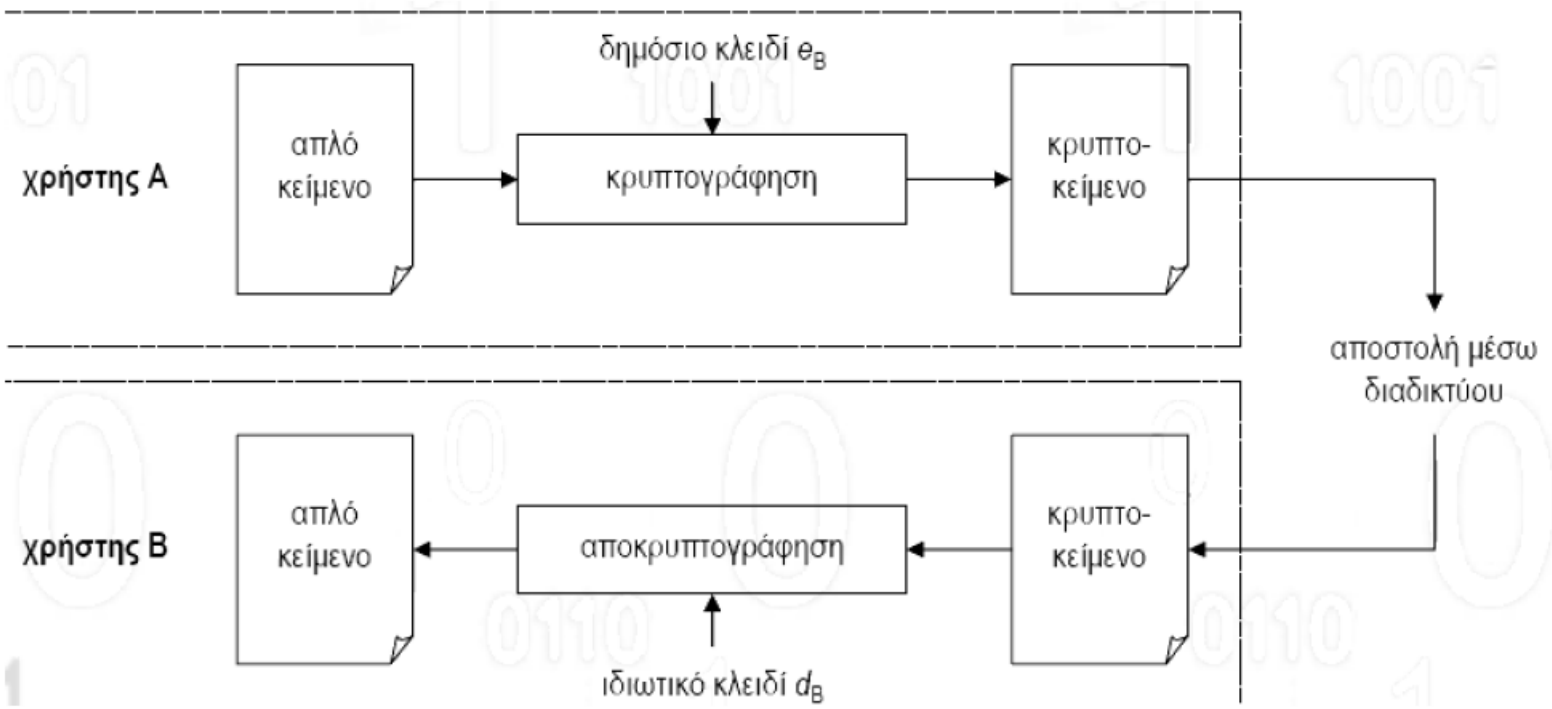
Συμμετρική κρυπτογραφία



Συμμετρική κρυπτογραφία

- Το ίδιο κρυφό κλειδί χρησιμοποιείται για την κρυπτογράφηση και για την αποκρυπτογράφηση.
- Το βασικότερο πρόβλημα στην συμμετρική κρυπτογραφία είναι ότι το κλειδί διανέμεται πάνω σε ανοικτά δίκτυα υπολογιστών κάτι που δεν είναι ασφαλής.
- Τα κλειδιά έχουν πεπερασμένο χρόνο ζωής.

Ασύμμετρη Κρυπτογραφία



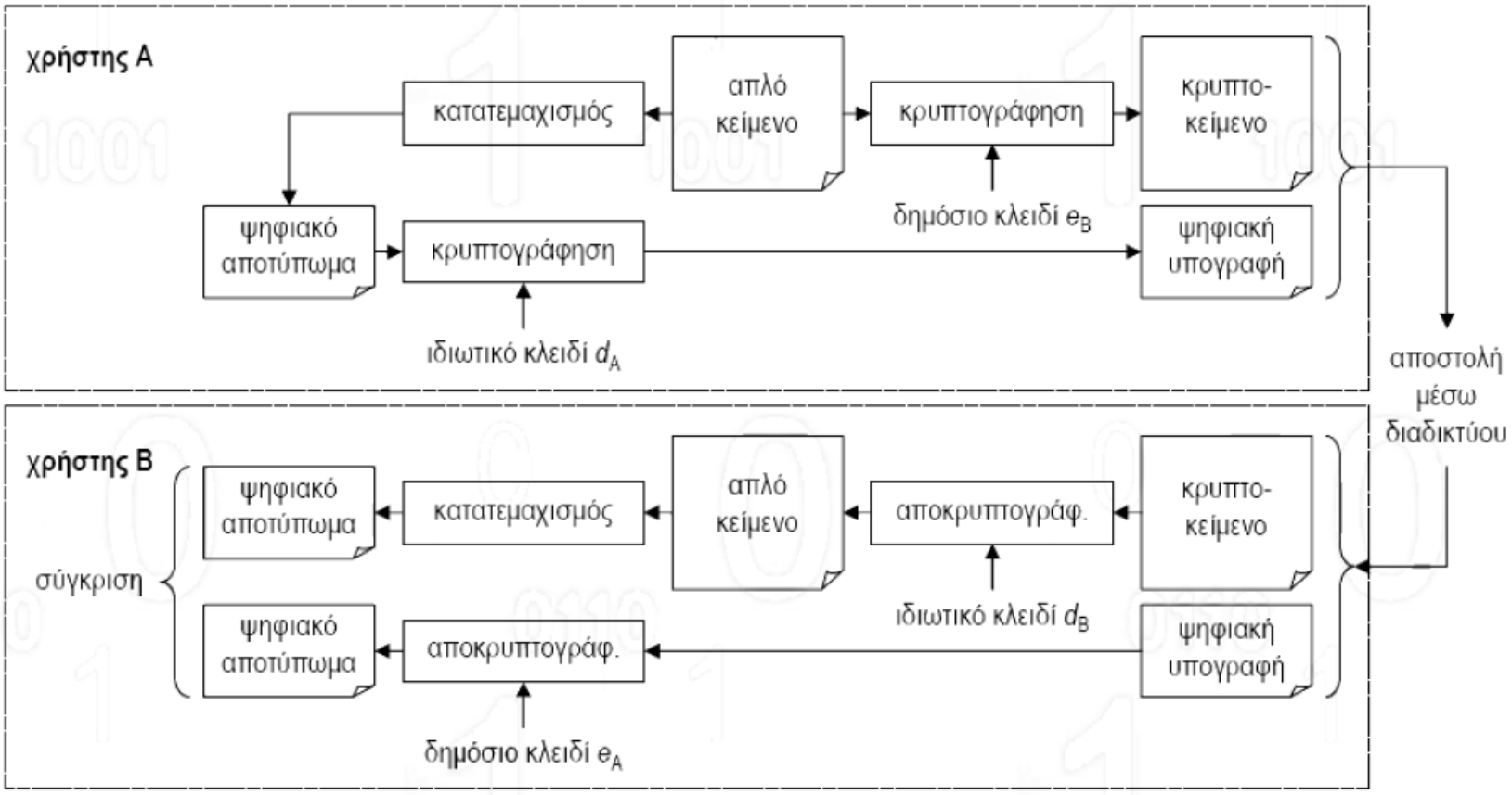
Ασύμμετρη Κρυπτογραφία

- Ένα μήνυμα που κρυπτογραφείται με το δημόσιο κλειδί αποκρυπτογραφείται με το αντίστοιχο ιδιωτικό κλειδί.
- Το ένα κλειδί συνδέεται με το άλλο με απλό τρόπο. Το ένα προκύπτει από το άλλο.
- Το δημόσιο κλειδί γνωστοποιείται σε δημόσιες βάσης δεδομένων (δημόσιος κατάλογος).
- Το ιδιωτικό κλειδί κρατείται απόρρητο αφού είναι προσωπικό του κάθε χρήστη.
- Το ζεύγος ιδιωτικό κλειδί – δημόσιο κλειδί μπορεί να μείνει το ίδιο για μεγάλα χρονικά διαστήματα.

Ασύμμετρη κρυπτογραφία

- Επειδή στην ασύμμετρη κρυπτογραφία μπορεί να γίνει επίθεση από τρίτο άτομο και να αποσταλεί μήνυμα που να μην γνωρίζει ο παραλήπτης ότι προέρχεται από τρίτο άτομο, χρησιμοποιείται η ψηφιακή υπογραφή του αποστολέα.
- Η επιθέσεις αυτές είναι γνωστές ως επιθέσεις ενδιάμεσου ατόμου (man in the middle).

Ασύμμετρη κρυπτογραφία



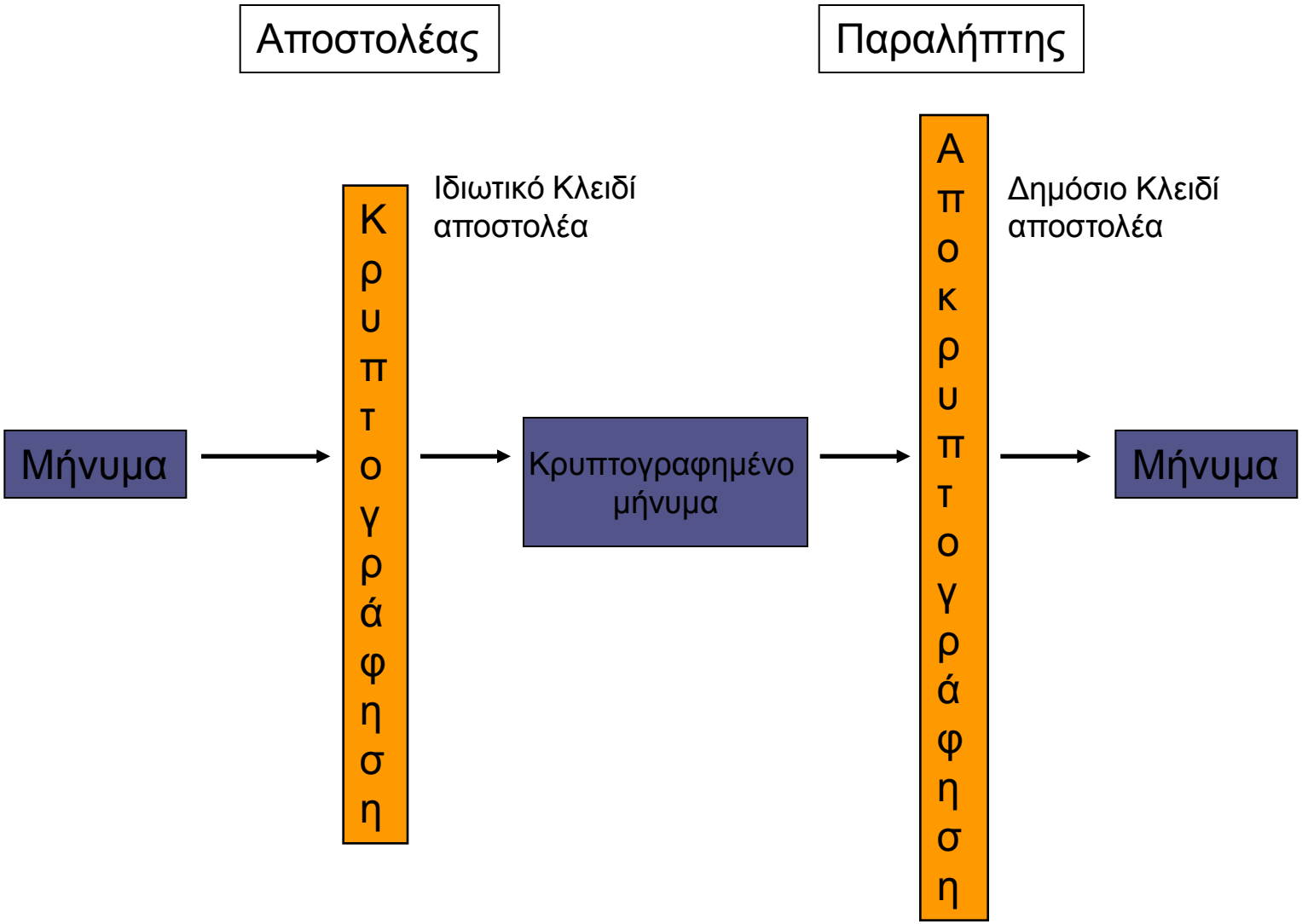
Ασύμμετρη κρυπτογραφία

- Πιστοποίηση ταυτότητας
  -Επιβεβαίωση ότι το μήνυμα που αποκρυπτογραφείται είναι αυθεντικό (data integrity).
  -Επιβεβαίωση ότι ο αποστολέας είναι αυτός που ισχυρίζεται. (identification)

Ασυμμετρη κρυπτογραφια

- Η ασύμμετρη κρυπτογραφία χρησιμοποιείται για την
  α) επιβεβαίωση της ταυτότητας του αποστολέα
  β) Ανταλλαγή εμπιστευτικών μηνυμάτων

Ασύμμετρη κρυπτογραφία για επιβεβαίωση ταυτότητας αποστολέα



Ασύμμετρη κρυπτογραφία για εμπιστευτικά μηνύματα