ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΙΚΑ ΜΑΘΗΜΑΤΑ

Ειδικά Θέματα Βάσεων Δεδομένων

Ενότητα 9: Κρυπτογράφηση δεδομένων

Δρ. Τσιμπίρης Αλκιβιάδης

Τμήμα Μηχανικών Πληροφορικής ΤΕ

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
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

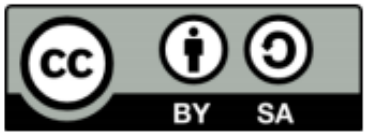
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

CC BY SA

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 παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Κεντρικής Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- 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.

Ενότητα 9

Κρυπτογράφηση δεδομένων

Δρ. Τσιμπίρης Αλκιβιάδης

Περιεχόμενα ενότητας

- Ασφάλεια δεδομένων -Αρχές αυθεντικοποίησης
- Ταυτοποίηση
- Αυθεντικοποίηση
- Ηλεκτρονικές υπογραφές
- Ψηφιακές υπογραφές
- Κρυπτογράφηση δεδομένων
- Παραδείγματα κρυπτογράφησης δεδομένων
- Πρότυπο Des
- Κρυπτογράφηση με δημόσιο κλειδί
- Μηχανισμός κρυπτογράφησης RSA
- Παράδειγμα με RSA
- Παράδειγμα κρυπτογράφησης με δημόσιο κλειδί

Σκοποί ενότητας

Σε αυτήν την ενότητα θα γίνει ανάλυση της κρυπτογράφησης των δεδομένων η οποία ορίζεται ως η αποθήκευση ή η μετάδοση των εμπιστευτικών δεδομένων σε κωδικοποιημένη μορφή. Τέλος παρουσιάζονται οι μηχανισμοί κρυπτογράφησης, υποκατάστασης μετάθεσης, δημόσιου κλειδιού και γίνεται μια εξοικείωση με τις ψηφιακές υπογραφές.

Ασφάλεια δεδομένων -Αρχές αυθεντικοποίησης

Στις ηλεκτρονικές συναλλαγές πρώτιστο ρόλο παίζει η προστασία των προσωπικών δεδομένων και της ασφάλειας. Για επιτυχημένες λύσεις ΗΔ απαιτείται να υπάρχει η **αυθεντικοποίηση** των συναλλασσόμενων μερών εξασφαλίζοντας:

- Εμπιστευτικότητα
- Ακεραιότητα
- Ταυτοποίηση
- Αυθεντικότητα
- Μη αποποίηση ευθύνης

Ασφάλεια δεδομένων-Ταυτοποίηση

Ως **ταυτοποίηση** ορίζεται ο προσδιορισμός των πληροφοριών/δεδομένων που μπορούν να ταυτοποιήσουν μια οντότητα (πολίτες/ επιχειρήσεις). Στο πλαίσιο αυτό εντάσσονται οι εξής παράμετροι:

- Η προστασία της ιδιωτικότητας και η προστασία των προσωπικών δεδομένων εφαρμόζοντας το Ν. 2742/1997 και την Κοινοτική Οδηγία 95/46/ΕΚ
- Η εγκυρότητα μητρώων που αφορά τις ιδιότητες με τις οποίες ο πολίτης συναλλάσσεται με τη δημόσια διοίκηση
- Ο μοναδικός αριθμός ταυτοποίησης

Ασφάλεια δεδομένων- Αυθεντικοποίηση

Ως **αυθεντικοποίηση** ορίζεται η δυνατότητα παροχής αδιαμφισβήτητων στοιχείων για την επαλήθευση της ταυτότητας μιας οντότητας. Συγκεκριμένα αφορά:

- Έλεγχος αυθεντικότητας κι επίπεδα εμπιστοσύνης, δηλαδή ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι
- Αναγνωριστικά & ψηφιακά πιστοποιητικά, δηλαδή η ηλεκτρονική επιβεβαίωση της ταυτότητας μιας οντότητας

Ηλεκτρονικές υπογραφές

Έρχονται να καλύψουν το θέμα της ασφάλειας των συναλλαγών επιτρέποντας στον λήπτη των δεδομένων να διαπιστώνει την προέλευσή τους (αυθεντικότητα), να ελέγχει κατά πόσο τα πρωτότυπα δεδομένα είναι πλήρη και αναλοίωτα (ακεραιότητα), αλλά και μέσω των «παρεχόντων υπηρεσιών πιστοποίησης» να είναι βέβαιος για την ταυτότητα του υπογράφοντος (ταυτοποίηση). Χωρίζονται σε 2 κατηγορίες:

- τις **ψηφιακές υπογραφές** που χρησιμοποιούν την κρυπτογραφία με τη χρήση αλγοριθμικών κλειδιών
- Τις **ηλεκτρονικές υπογραφές** που υποστηρίζονται από μεθόδους όπως η βιομετρική, η αναγνώριση φωνής κ.ά.

Ψηφιακές υπογραφές

Υποστηρίζονται από την ασύμμετρη κρυπτογραφία και πρέπει να ικανοποιούν τις ακόλουθες απαιτήσεις για να θεωρούνται αξιόπιστες και έγκυρες:

- Να συνδέεται μονοσήμαντα με τον υπογράφοντα
- Να ταυτοποιεί τον υπογράφοντα
- Να δημιουργείται με μέσα τα οποία ο υπογράφων διατηρεί υπό αποκλειστικό του έλεγχο
- Να εντοπίζεται οποιαδήποτε αλλοίωση των δεδομένων με τα οποία συνδέεται

Κρυπτογράφηση δεδομένων

Η διαδικασία της **Κρυπτογράφησης δεδομένων(Data encryption)** είναι η εξής:

- Απλό κείμενο → Κρυπτογράφηση κειμένου (αλγόριθμος κρυπτογράφησης + κλειδί κρυπτογράφησης)
- Κρυπτογράφηση κειμένου → Κρυπτογραφικό κείμενο

- Κρυπτογράφηση του ΚΑΙΣΑΡΑ

Σχόλιο! Οι λεπτομέρειες του αλγορίθμου γνωστοποιούνται το κλειδί μυστικό

Κρυπτογράφηση δεδομένων

Η κρυπτογράφηση αποτελεί μια μέθοδο διασφάλισης των ηλεκτρονικών συναλλαγών, προστασίας των διακινούμενων δεδομένων και των οντοτήτων που συναλλάσσονται.

Η **κρυπτογράφηση δημόσιου κλειδιού** εξασφαλίζει την ιδιωτικότητα, την ακεραιότητα και την εμπιστευτικότητα. Υπάρχουν 2 τεχνικές κρυπτογράφησης η *συμμετρική κρυπτογραφία* (κοινό κλειδί για κρυπτογράφηση κι αποκρυπτογράφηση) και η *ασύμμετρη κρυπτογραφία* (δημόσιο κλειδί για την κρυπτογράφηση και ιδιωτικό κλειδί για την αποκρυπτογράφηση)

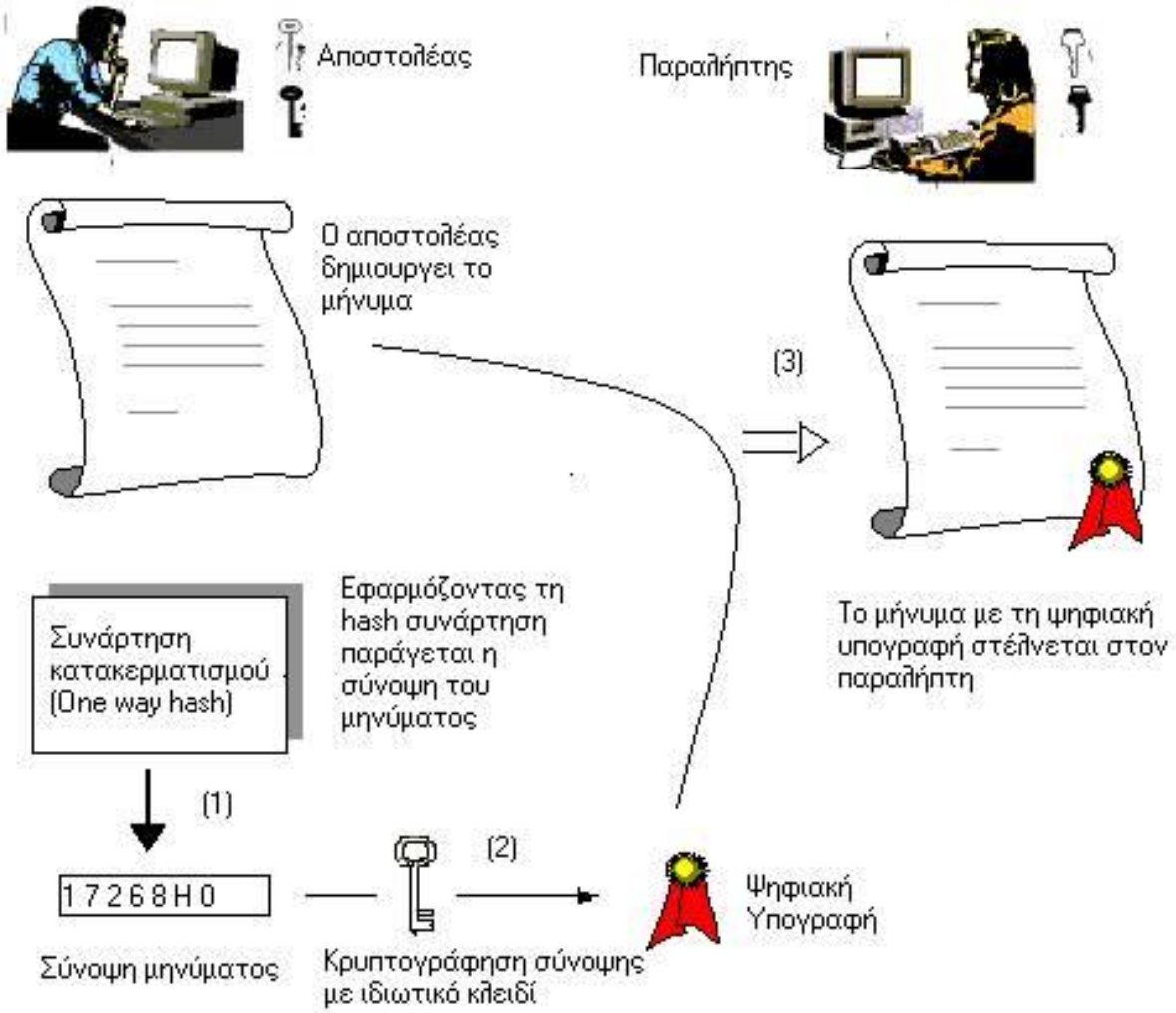
Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI)

Είναι ο μηχανισμός επαλήθευσης των ταυτοτήτων των προσώπων που διαθέτουν δημόσιο κλειδί. Πρόκειται για ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών που πιστοποιεί την εγκυρότητα του κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο και παράλληλα προστατεύει την ασφάλεια της συναλλαγής.

Ο οργανισμός που εκδίδει πιστοποιητικά ονομάζεται Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) ή Αρχή Πιστοποίησης.

Στην Ελλάδα οι ΠΥΠ ελέγχονται από την Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (Ε.Ε.Τ.Τ)

Χρήση κρυπτογράφησης και ψηφιακής υπογραφής



Παράδειγμα κρυπτογράφησης δεδομένων

PlainText = ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

Κλειδί= Test

Για την κρυπτογράφηση του κειμένου η διαδικασία είναι η εξής:

- Χωρίστε το σε ίσα μέρη σύμφωνα με το κλειδί (ΤΕΙ+ ΚΕΝΤ ΡΙΚΗ Σ+ΜΑΚ ΕΔΟΝ ΙΑΣ+)
- Αντικαταστήστε τους χαρακτήρες με αριθμούς από το 00-26 (κενό=00 Α=01….).
- Αποτέλεσμα

Σχόλιο! Στα κενά τοποθετείται +

A	1
B	2
C	3
D	4
E	5
F	6
G	7
H	8
I	9
J	10
K	11
L	12
M	13
N	14
O	15
P	16
Q	17
R	18
S	19
T	20
U	21
V	22
W	23
X	24
Y	25
Z	26

Παράδειγμα κρυπτογράφησης δεδομένων

- Άθροιση των προηγούμενων αποτελεσμάτων και διαίρεση τους με το 27
- Κρατήστε το υπόλοιπο της διαίρεσης
- Αντικατάστασή κάθε αριθμού του υπολοίπου με τον χαρακτήρα που του αντιστοιχεί

Παράδειγμα2 κρυπτογράφησης δεδομένων

PlainText = ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕ

Κλειδί= Test

Για την κρυπτογράφηση του κειμένου η διαδικασία είναι η εξής:

- Χωρίστε το σε ίσα μέρη σύμφωνα με το κλειδί (ΤΜΗΜ Α+ΜΗ ΧΑΝΙ ΚΩΝ+ ΠΛΗΡ ΟΦΟΡ ΙΚΗΣ +ΤΕ+)
- Αντικαταστήστε τους χαρακτήρες με αριθμούς από το 00-26 (κενό=00 Α=01….).
- Αποτέλεσμα 20130801001308240114091……

Σχόλιο! Στα κενά τοποθετείται +

A	1
B	2
C	3
D	4
E	5
F	6
G	7
H	8
I	9
J	10
K	11
L	12
M	13
N	14
O	15
P	16
Q	17
R	18
S	19
T	20
U	21
V	22
W	23
X	24
Y	25
Z	26

Πρότυπο Des

Πρότυπο DES:

- **Υποκατάσταση** (SUBSTITUTION) :χρησιμοποιεί ένα κλειδί κρυπτογράφησης έτσι ώστε να προσδιοριστεί για τον κάθε χαρακτήρα απλού κειμένου ένας χαρακτήρας κρυπτογραφικού κειμένου με τον οποίο θα υποκατασταθεί αυτός ο χαρακτήρας

- **Μετάθεση** (PERMUTATION) οι χαρακτήρες απλού κειμένου απλώς αναδιατάσσονται με κάποια διαφορετική σειρά.

Καμία από τις δύο αυτές προσεγγίσεις δεν είναι ιδιαίτερα ασφαλής. Ο συνδυασμός όμως αυτών των δύο παρέχουν έναν πολύ υψηλό βαθμό ασφάλειας. Ο συνδυασμός αυτών των δύο δημιούργησε το πρότυπο **DES** (Data Encryption Standard — Πρότυπο Κρυπτογράφησης Δεδομένων), που υιοθετήθηκε για πρώτη φορά ως ομοσπονδιακό πρότυπο των ΗΠΑ το 1977.

Πρότυπο Des

Χαρακτηριστικά του προτύπου DES:

- Το απλό κείμενο υποδιαιρείται σε τμήματα των 64 bit και το κάθε τμήμα κρυπτογραφείται με ένα κλειδί των 64 bit

- Το κλειδί αποτελείται από 56 bit δεδομένων + 8 bit ισοτιμίας, και επομένως δεν υπάρχουν 2^{64} αλλά μόνο 2^{56} πιθανά κλειδιά).

- Για την κρυπτογράφηση ενός τμήματος, πρώτα εκτελείται μια αρχική μετάθεση πάνω σε αυτό, έπειτα το τμήμα που προκύπτει από τη μετάθεση υποβάλλεται σε μια ακολουθία 16 βημάτων σύνθετης υποκατάστασης, και τέλος εφαρμόζεται άλλη μία μετάθεση, η αντίστροφη της αρχικής στο αποτέλεσμα του προηγούμενου βήματος.

Πρότυπο Des

- Η υποκατάσταση στο βήμα i δεν ελέγχεται άμεσα από το αρχικό κλειδί κρυπτογράφησης Κ, αλλά από ένα κλειδί Κi που υπολογίζεται από τις τιμές Κ και i.
- Το DES έχει την ιδιότητα-χαρακτηριστικό ότι ο αλγόριθμος αποκρυπτογράφησης είναι ο ίδιος με τον αλγόριθμο κρυπτογράφησης, με μία διαφορά όμως τα κλειδιά Κi εφαρμόζονται με αντίστροφη σειρά.

Κρυπτογράφηση με δημόσιο κλειδί

- Σε ένα μηχανισμό με δημόσιο κλειδί (public-key), τόσο ο αλγόριθμος κρυπτογράφησης όσο και 'το κλειδί κρυπτογράφησης είναι διαθέσιμα σε όλους ώστε να μπορεί ο καθένας να μετατρέψει κάποιο απλό κείμενο σε κρυπτογραφικό κείμενο.

- Το αντίστοιχο κλειδί αποκρυπτογράφησης διατηρείται μυστικό (οι μηχανισμοί με δημόσιο κλειδί έχουν δύο κλειδιά, ένα για την κρυπτογράφηση και ένα για την αποκρυπτογράφηση).

- Το κλειδί αποκρυπτογράφησης δεν είναι δυνατό να προκύψει από το κλειδί κρυπτογράφησης έτσι, ακόμα και το άτομο που κάνει την αρχική κρυπτογράφηση δεν μπορεί να κάνει την αντίστοιχη αποκρυπτογράφηση αν δεν έχει την εξουσιοδότηση να το κάνει.

Μηχανισμός κρυπτογράφησης RSA

Ο μηχανισμός κρυπτογράφησης με δημόσιο κλειδί RSA βασίζεται στα εξής δύο γεγονότα:

- Υπάρχει ένας γνωστός γρήγορος αλγόριθμος με τον οποίο μπορεί να προσδιοριστεί αν ένας δεδομένος αριθμός είναι πρώτος αριθμός.

- Δεν υπάρχει κανένας γνωστός γρήγορος αλγόριθμος για την εύρεση των πρώτων παραγόντων ενός δεδομένου παραγώγου (δηλαδή, όχι πρώτου) αριθμού.

Σχόλιο! Το όνομα RSA του μηχανισμού κρυπτογράφησης προέκυψε από τα αρχικά του ονόματος των εμπνευστών του(Rivest, Shamir, Adleman).

Μηχανισμός κρυπτογράφησης RSA

Η λειτουργία του μηχανισμού κρυπτογράφησης RSA έχει ως εξής:

- Επιλέγονται τυχαία δύο διαφορετικοί μεγάλοι πρώτοι αριθμοί, p και q, και υπολογίζεται το γινόμενο r = p * q.
- Επιλέγεται τυχαία ένας μεγάλος ακέραιος e που είναι σχετικά πρώτος (relatively prime) ως προς το γινόμενο (p — 1) * (q — 1). Ο ακέραιος e είναι το κλειδί της κρυπτογράφησης. Έστω ότι παίρνετε ως κλειδί αποκρυπτογράφησης d το μοναδικό "πολλαπλασιαστικό αντίστροφο" του ακεραίου υπολοίπου της διαίρεσης του e με το (p - 1) * (q - 1), δηλαδή:
  - d * e = 1 modulo (p - 1) * (q - 1)
  - Ο αλγόριθμος για τον υπολογισμό του d με δεδομένα τα e, p, και q είναι απλός
  - Γνωστοποιούνται οι ακέραιοι r και e, όχι όμως ο d.

Σχόλιο! Η επιλογή του e είναι εύκολη. Οποιοσδήποτε πρώτος αριθμός, μεγαλύτερος και από τον p και από τον q, είναι κατάλληλος.

Μηχανισμός κρυπτογράφησης RSA

Η λειτουργία του μηχανισμού κρυπτογράφησης RSA έχει ως εξής (Συνέχεια):

- Για να κρυπτογραφηθεί ένα απόσπασμα απλού κειμένου P (που θεωρούμε για λόγους απλότητας ότι είναι ένας ακέραιος μικρότερος από τον r), αντικαθίσταται από το κρυπτογραφικό κείμενο C που υπολογίζεται με τον εξής τρόπο: $C = P^e$ modulo

- Για να αποκρυπτογραφηθεί ένα απόσπασμα κρυπτογραφικού κειμένου C, αντικαθίσταται από το απλό κείμενο P που υπολογίζεται με τον εξής τρόπο:$P = C^d$ modulo r

Η αποκρυπτογράφηση του C με χρήση του d **αποκαθιστά** το αρχικό P. Όμως, ο υπολογισμός του d με γνωστά μόνο τα r και e (και όχι τα ρ και q) είναι **ανέφικτος.**

Παράδειγμα με RSA

Έστω **p= 3** και **q = 5**, τότε **r = 15**, και το γινόμενο **(p -1) * (q -1) =8** και το **e = 11**. Επίσης ένας πρώτος αριθμός μεγαλύτερος και από το p και από το q. Για να υπολογιστεί το d κάνετε τα εξής:

- **d * 11 = 1 modulo 8** από το οποίο προκύπτει **d = 3.**

Έστω τώρα ότι το απλό κείμενο P αποτελείται από τον ακέραιο 13. Τότε, το κρυπτογραφικό κείμενο C προκύπτει από τις πράξεις:

- **C = P^e modulo r** = 13^{11} modulo 15 = 1.792.160.394.037 modulo 15 = **7**

Παράδειγμα με RSA

Το αρχικό απλό κείμενο P προκύπτει από τις πράξεις :

P	**=**	**C^d modulo r**
	=	7^3 modulo 15
	=	343 modulo 15
	=	**13**

Παράδειγμα κρυπτογράφησης με δημόσιο κλειδί

Μηχανισμοί κρυπτογράφησης με Δημόσιο Κλειδί :Επιτρέπουν τα κρυπτογραφημένα μηνύματα να είναι "υπογεγραμμένα", ώστε ο παραλήπτης να μπορεί να είναι βέβαιος ότι το μήνυμα προέρχεται από το άτομο που υποτίθεται ότι προέρχεται (δηλαδή, οι "υπογραφές" δεν μπορούν να πλαστογραφηθούν).

Παράδειγμα

- Έστω ότι οι αλγόριθμοι κρυπτογράφησης είναι οι ECA και ECB (για την κρυπτογράφηση των μηνυμάτων που θα στέλνονται στον Α και στον Β, αντίστοιχα).
- Έστω ότι οι αντίστοιχοι αλγόριθμοι αποκρυπτογράφησης είναι οι DCA και DCB, αντίστοιχα.
- Οι αλγόριθμοι ECA και DCA είναι αντίστροφοι μεταξύ τους, όπως και οι ECB και DCB.

Παράδειγμα κρυπτογράφησης με δημόσιο κλειδί

Παράδειγμα συνέχεια

- ο Α εφαρμόζει πρώτα τον αλγόριθμο αποκρυπτογράφησης DCA στο P, και στη συνέχεια κρυπτογραφεί το αποτέλεσμα και το μεταδίδει ως κρυπτογραφικό κείμενο :C = ECB (DCA (P)).

- Μόλις πάρει το C, ο χρήστης Β εφαρμόζει τον αλγόριθμο αποκρυπτογράφησης DCB και στη συνέχεια τον αλγόριθμο κρυπτογράφησης ECA, ώστε να προκύψει το τελικό αποτέλεσμα P:

ECA (DCB (C))
= ECA (DCB (ECB (DCA (P))))
= ECA (DCA (P)) επειδή τα DCB και ECB αναιρούνται.
= P επειδή τα ECA και DCA αναιρούνται.

Παράδειγμα κρυπτογράφησης με δημόσιο κλειδί

Μετά την διαδικασία αυτή ο Β ξέρει ότι το μήνυμα προέρχεται από τον Α, επειδή ο αλγόριθμος ECA θα δώσει το P μόνο αν χρησιμοποιήθηκε ο αλγόριθμος DCA στη διαδικασία κρυπτογράφησης και αυτός ο αλγόριθμος είναι γνωστός μόνο στον Α. Κανένας, ούτε ακόμα και ο Β δεν μπορεί να πλαστογραφήσει την υπογραφή του Α.