Εισαγωγη

Τεχνολογιες Διαχειρισης Ασφαλειας (ΤεΔΑ) - ΠΜΣ Προηγμενα Συστηματα Πληροφορικης

Δρ. Καραντζιας Θανος

Περιεχόμενα

ΑΣΦΑΛΕΙΑ

- Γενικές Απαιτήσεις Ασφάλειας
- Τομείς των Μέτρων Ασφάλειας
- Σύστημα Ασφάλειας Πληροφοριών Οργανισμού

ΚΡΥΠΤΟΓΡΑΦΙΑ

- Συμμετρική Κρυπτογραφία
- Κρυπτογραφία Δημοσίου Κλειδιού
- Βασικοί μηχανισμοί και διαδικασίες Κρυπτογραφίας

Γενικές Απαιτήσεις Ασφάλειας

- Αυθεντικοποίηση (authentication)
- Ακεραιότητα (Integrity)
- Εμπιστευτικότητα (Confidentiality)
- Εξουσιοδότηση (Authorization)
- Μη-άρνηση της ευθύνης (Non-Repudiation)
- Διαθεσιμότητα (Availability)

Καθορισμός Απαιτήσεων Ασφάλειας

Υπάρχουν 3-είς κύριες πηγές καθορισμού των Απαιτήσεων Ασφάλειας

- ***Αξιολόγηση των κινδύνων που αφορούν την οργάνωση*** (με βάση τη συνολική επιχειρηματική στρατηγική και στόχους οργανισμού)
  - Risk Assessment
  - Αναγνώριση κινδύνων των πόρων
  - Αναγνώριση της πιθανότητας εμφάνισης των κινδύνων
  - Αναγνώριση αξίας και σημαντικότητας
- ***Νομικό – Κανονιστικό - Συμβατικό Πλαίσιο***
- ***Σύνολο αρχών – στόχων – απαιτήσεων του οργανισμού για την επεξεργασία των πληροφοριών (***με βάση τις δραστηριότητές του οργανισμού)

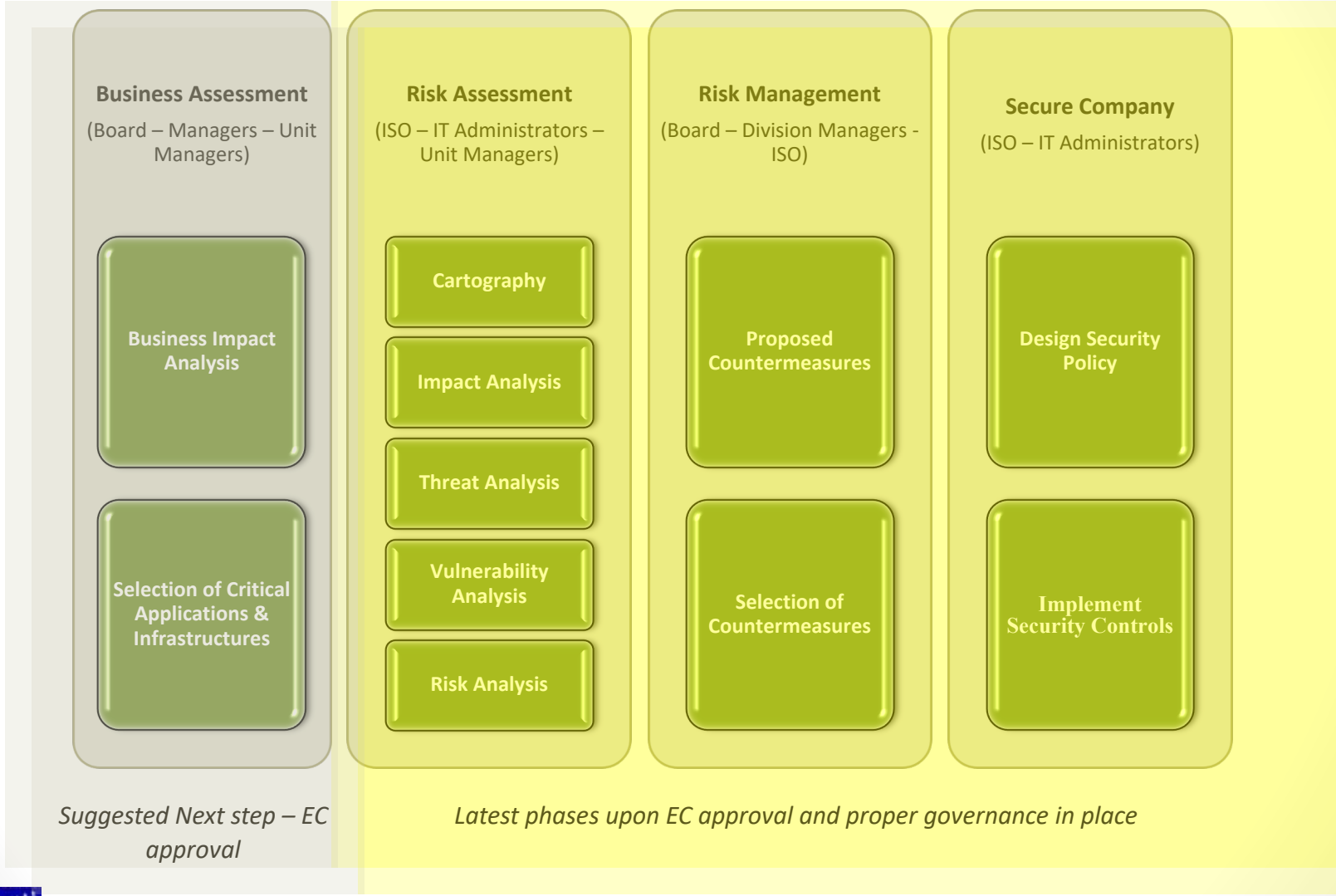
Κύριοι Τομείς Μέτρων Ασφάλειας

- Πολιτική Ασφάλειας
- Οργάνωση Ασφάλειας Πληροφοριών
- Διαχείριση Πόρων
- Ασφάλεια Ανθρωπίνων Πόρων
- Φυσική & Περιβαλλοντική Ασφάλεια
- Διαχείριση Επικοινωνιών και Λειτουργιών
- Έλεγχος Πρόσβασης
- Απόκτηση, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων
- Διαχείριση Περιστατικών Ασφάλειας Πληροφοριών
- Σχέδιο Επιχειρησιακής Συνέχειας
- Συμμόρφωση

Δομή Τομέων των Μέτρων Ασφάλειας

- Κάθε Τομέας Μέτρων Ασφάλειας περιλαμβάνει μία ή περισσότερες κατηγορίες Ασφάλειας
- Κάθε κατηγορία Ασφάλειας περιέχει:
  - Έναν αντικειμενικό στόχο που πρέπει να επιτευχθεί
  - Ένα ή περισσότερα μέτρα ασφάλειας που πρέπει να υλοποιηθούν για να επιτευχθεί ο παραπάνω στόχος
- Ένα μηχανισμός Ασφάλειας περιλαμβάνει:
  - Μία λύση η οποία ικανοποιεί τον αντικειμενικό στόχο για τον οποίο προορίζεται
  - Οδηγίες υλοποίησης της λύσης
  - Άλλες πληροφορίες (πχ. Νομικές θεωρήσεις ή αναφορές σε πρότυπα)

Διαδικασία Εφαρμογής Ασφάλειας



Εμπλεκόμενα Τμήματα

	Διοίκηση	Developers	IT	Business Unit	Project Managers	Physical Security	Presales	HR	Legal
Πολιτική Ασφάλειας	✓	✓	✓	✓	✓	✓	✓	✓	✓
Οργάνωση Ασφάλειας Πληροφοριών	✓			✓	✓				
Διαχείριση Πόρων	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ασφάλεια Ανθρωπίνων Πόρων	✓							✓	
Φυσική και Περιβαλλοντική Ασφάλεια		✓	✓			✓			
Διαχείριση Επικοινωνιών & Εργασιών									
Έλεγχος Πρόσβασης	✓	✓	✓	✓	✓	✓	✓	✓	✓
Προμήθεια – Ανάπτυξη – Συντήρηση ΠΣ		✓	✓		✓				
Διαχείριση Περιστατικών Ασφάλειας	✓	✓	✓	✓	✓	✓	✓	✓	✓
Διαχείριση Επιχειρησιακής Συνέχειας	✓	✓	✓	✓	✓	✓	✓	✓	✓
Συμμόρφωση	✓								✓

Υλοποίηση Συστήματος Ασφάλειας Πληροφοριών

- Καθορισμός Ορίων Εφαρμογής Ασφάλειας
- Καταγραφή Υπάρχουσας Κατάστασης
- Δημιουργία νέων διαδικασιών
- Εκτίμηση κινδύνων Ασφάλειας
- Οριοθέτηση Κατωφλιού Επικινδυνότητας
- Υλοποίηση Βελτιωτικών Μέτρων
- Καταγραφή Διαδικασιών και Έγκρισή τους
- Λειτουργία Συστήματος Ασφάλειας

Απαιτούμενη Μεθοδολογία

Καθορισμός Έργου	Αξιολόγηση Αδυναμιών Α.Π.	Υιοθέτηση νέου Πλαισίου Α.Π.	Υλοποίηση Συστήματος Α.Π.	Εκπαίδευση Εφαρμογής	Δοκιμαστική Εφαρμογή & Εσωτερικές Επιθεωρήσεις	Πιστοποίηση
1. Επιλογή Εμπλεκομένων 2. Εισαγωγή στο πρότυπο ISO27001:2005 3. Παρουσίαση Βασικών απαιτήσεων του Έργου 4. Ανάθεση Ρόλων στο Σύστημα	1. Καθορισμός Δεδομένων και Πληροφοριών 2. Ανάλυση Πληροφοριακών Υποδομών 3. Αξιολόγηση και διαβάθμιση κινδύνων Ασφάλειας 4. Υποβολή προτάσεων αντιμετώπισης των σημαντικών κινδύνων 5. Εντοπισμός απαιτούμενης τεκμηρίωσης	1. Δημιουργία Πολιτικής Ασφάλειας Πληροφοριών 2. Ορισμός Δεικτών και στόχων Ασφάλειας Πληροφοριών 3. Δημιουργία Πλάνου Ενεργειών	1. Υλοποίηση και εφαρμογή νέων πολιτικών και διαδικασιών Ασφάλειας 2. Υλοποίηση των τεχνολογικών λύσεων και υποδομών Ασφάλειας 3. Σύνταξη Διαδικασιών Συστήματος 4. Ανάπτυξη και καθιέρωση Μεθοδολογίας Εκτίμησης Κινδύνων	1. Εκπαίδευση στις απαιτήσεις ISO27001:2005 2. Εκπαίδευση στις νέες διαδικασίες Ασφάλειας 3. Εκπαίδευση στη μεθοδολογία Εσωτερικών Επιθεωρήσεων	1. Εφαρμογή των νέων διαδικασιών 2. Επιθεωρήσεις όλου του προσωπικού για την εφαρμογή των νέων διαδικασιών 3. Διενέργεια Συμβουλίου Ανασκόπησης για την αξιολόγηση εφαρμογής του Συστήματος 4. Εφαρμογή διορθωτικών Ενεργειών (εφόσον υπάρχουν)	1. Συνεννόηση με τον Φορέα Πιστοποίησης 2. Υποβολή φακέλου Πιστοποίησης 3. Εφαρμογή διορθωτικών Ενεργειών (εφόσον υπάρχουν)

Κρυπτογραφία

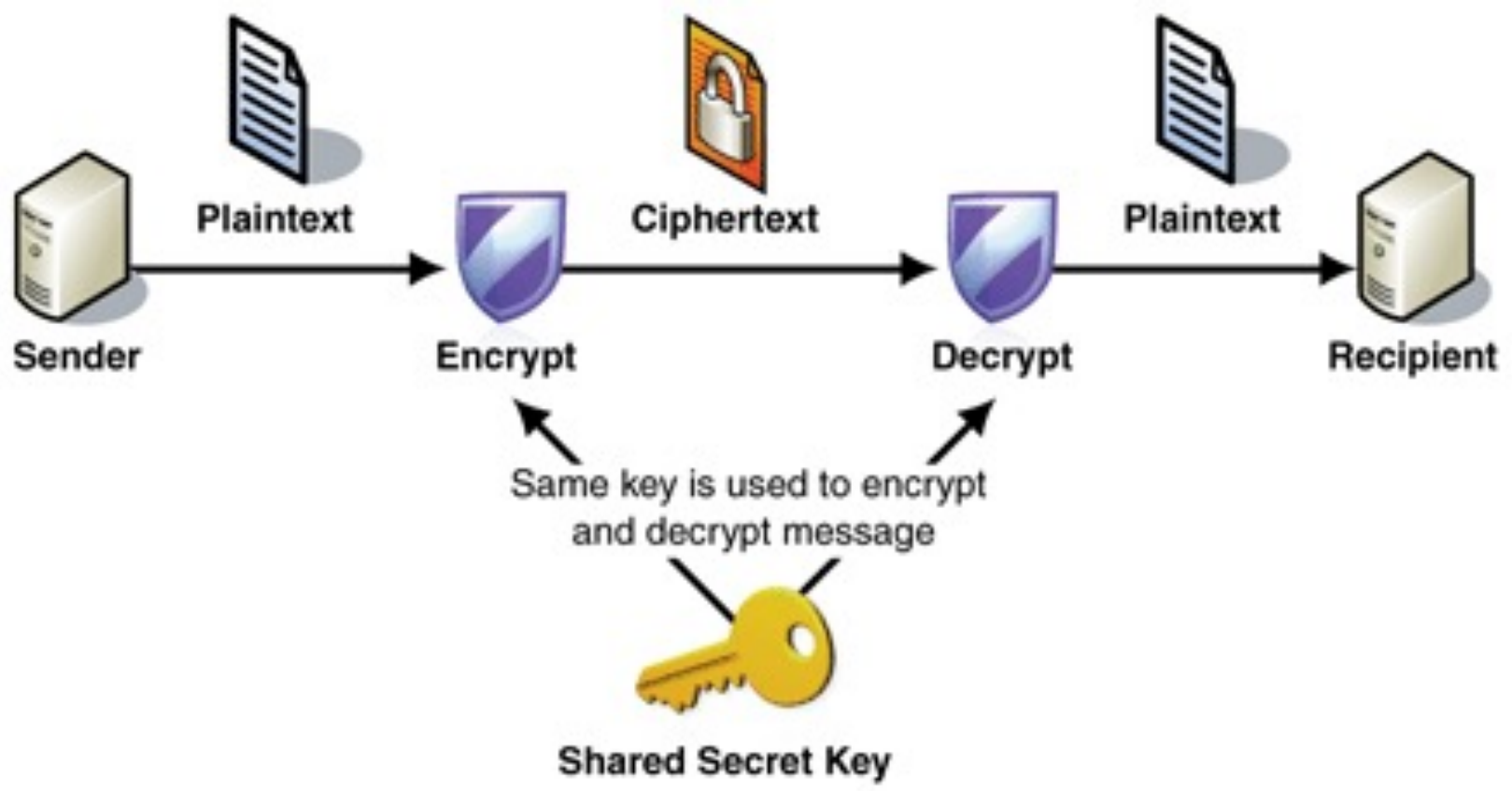
- ***Κρυπτογραφία*** (cryptography): η μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα, με σκοπό την εξασφάλιση της ασφάλειας των δεδομένων.
- Ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να αναγνωσθεί χωρίς την γνώση της σωστής ακολουθίας ψηφιακών δεδομένων (bits)
- Εφαρμογές της κρυπτογραφίας:
  - Κρυπτογράφηση
  - Αποκρυπτογράφηση

Συμμετρική Κρυπτογραφία

Κύρια χαρακτηριστικά:

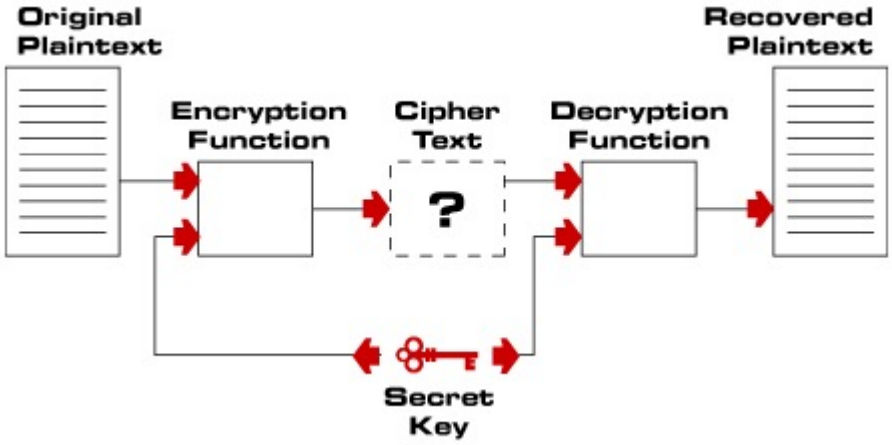
- Ίδιο κρυπτογραφικό κλειδί κρυπτογράφησης
- Ίδιο κρυπτογραφικό κλειδί αποκρυπτογράφησης
- *Μυστικό Κλειδί (secret key – private key – shared key)*
- Το *Μυστικό Κλειδί έχει διανεμηθεί με ασφαλή τρόπο μεταξύ των οντοτήτων*

Σενάριο Συμμετρικής Κρυπτογραφίας



Μειονεκτήματα / Πλεονεκτήματα

- Μειονεκτήματα
  - Όσο μεγαλώνει ο αριθμός των οντοτήτων, η διαχείριση των κοινών κλειδιών γίνεται όλο και πιο δύσκολη
  - Εφόσον οι οντότητες χρησιμοποιούν το ίδιο κλειδί δεν μπορεί κάποιος να αποδείξει από που ξεκίνησε το κρυπτογραφημένο μήνυμα
- Πλεονεκτήματα
  - Γρήγορη
  - Ιδιαίτερα Αποτελεσματική



Γνωστοί Αλγόριθμοι Συμμετρικής Κρυπτογραφίας

- DES (Data Encryption Standard:
  - Αναπτύχθηκε από την IBM, την NSA και το National Institute of Standards and Technology (NIST)
  - Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας
  - Ο DES (εκτός από κρυπτογράφηση) χρησιμοποιείται στην παραγωγή MACs (σε CBC mode)
  - Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος
- Triple-DES:
  - Παραλλαγή του DES – Το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου:
    - DES-EEE3 *(Encrypt-Encrypt-Encrypt)*: Τρεις συνεχόμενες κρυπτογραφήσεις με τρία διαφορετικά κλειδιά
    - DES-EDE3 *(Encrypt-Decrypt-Encrypt)*: Κρυπτογραφείται - Αποκρυπτογραφείται και Κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.
    - DES-EEE2: Ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά
    - DES-EDE2: Ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο κλειδιά
  - Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο.

Γνωστοί Αλγόριθμοι Συμμετρικής Κρυπτογραφίας

- DESX:
  - Παραλλαγή του DES
  - Η είσοδος στο DESX περνάει από μια XOR πράξη με ένα κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης
  - Παρουσιάζει δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις
- AES (Advanced Encryption Standard):
  - Αλγόριθμος κρυπτογράφησης τμημάτων που προορίζεται να γίνει τυποποίηση του FIPS και να αντικαταστήσει τον DES.
- IDEA (International Data Encryption Algorithm):
  - Αλγόριθμος κρυπτογράφησης τμημάτων (Lai και Massey) μεγέθους 64 bits και κλειδιά 128 bits
  - Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις
  - Εφαρμόσιμος τόσο σε υλικό (hardware) όσο και σε λογισμικό (software)
  - Πολλές φορές παρουσιάζει μειονεκτήματα στην απόδοση

Γνωστοί Αλγόριθμοι Συμμετρικής Κρυπτογραφίας

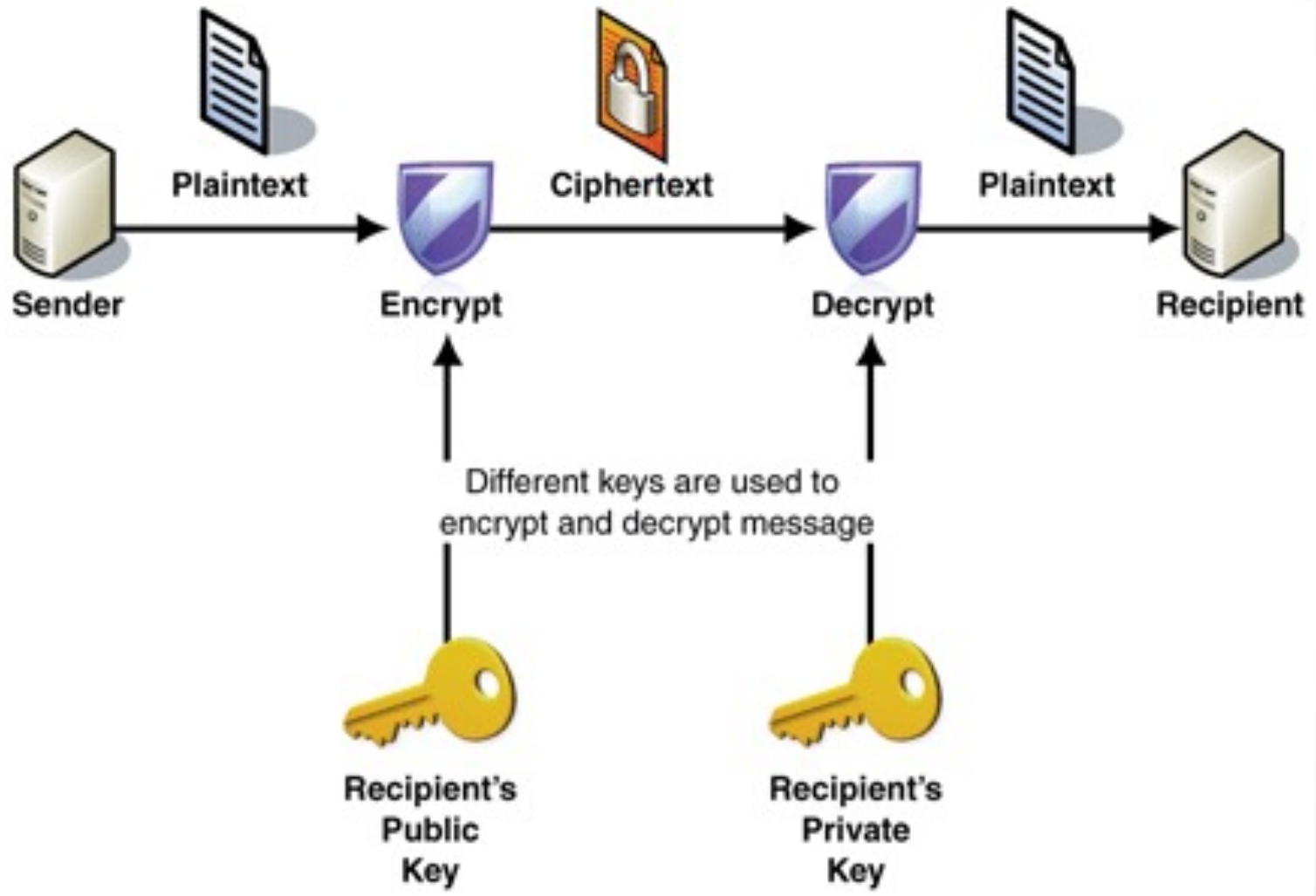
- RC2, RC4, RC5:
  - RC2: Αλγόριθμος κρυπτογράφησης τμημάτων με κλειδί μεταβλητού μήκους
  - RC2: Έχει μέγεθος block ίσο με 64 bits
  - RC2: Γρηγορότερος από τον DES (3-5 φορές)
  - RC4: Αλγόριθμος κρυπτογράφησης ροών
  - RC4: Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte
  - RC4: Χρησιμοποιείται στο πρωτόκολλο SSL
  - RC5: Αλγόριθμος κρυπτογράφησης τμημάτων με κλειδί μεταβλητού μήκους
  - RC5: Έχει μέγεθος block ίσο με 32/64/128 bits
  - RC5: Ο αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255
- Blowfish:
  - Αλγόριθμος κρυπτογράφησης τμημάτων (Schneier)
  - Μέγεθος τμήματος 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits
  - Οι διεργασίες βασίζονται σε πράξεις XOR και προσθέσεις λέξεων των 32 bits
  - Σημαντικά ταχύτερος από τον DES

Κρυπτογραφία Δημοσίου Κλειδιού

Κύρια χαρακτηριστικά:

- Κρυπτογραφία Δημοσίου Κλειδιού == Ασύμμετρη Κρυπτογραφία
- Δύο διαφορετικά **αλλά μαθηματικά συσχετιζόμενα** κλειδιά:
  - Το δημόσιο κλειδί (public key) – Με αυτό γίνεται η κρυπτογράφηση
  - Το ιδιωτικό κλειδί (private key) – Με αυτό γίνεται η αποκρυπτογράφηση
- Με τη χρησιμοποίηση του ενός κλειδιού δεν είναι δυνατή η εύρεση του άλλου

Σενάριο Κρυπτογραφίας Δημοσίου Κλειδιού



Μειονεκτήματα / Πλεονεκτήματα

- Μειονεκτήματα
  - Πολύπλοκοι Υπολογισμοί -> Αυξημένο Υπολογιστικό Κόστος (1000 φορές πιο αργή από την συμμετρική)
  - Κρυπτογράφηση Περιορισμένου Μεγέθους Πληροφορίας
  - Ανάγκη ισχυρής προστασίας του ιδιωτικού κλειδιού
- Πλεονεκτήματα
  - Αποδεικνύεται εύκολα από που ξεκίνησε το κάθε κρυπτογραφημένο μήνυμα
  - Δεν χρειάζεται ασφαλές κανάλι επικοινωνίας για την ανταλλαγή των δημοσίων κλειδιών
  - Μπορεί να εφαρμοστεί ευκολότερα σε μεγάλα frameworks

Γνωστοί Αλγόριθμοι Ασύμμετρης Κρυπτογραφίας

- RSA:
  - Λαμβάνουμε δύο μεγάλους πρώτους αριθμούς p, q
  - Υπολογίζουμε το γινόμενο τους (modulus) n = p x q
  - Διαλέγουμε ένα αριθμό e μικρότερο του n και τέτοιο, ώστε e και (p-1) x (q-1) να μην έχουν κοινούς διαιρέτες εκτός του 1
  - Βρίσκουμε έναν άλλο αριθμό d, ώστε (e x d - 1) να διαιρείται από το (p-1) x (q-1)
  - Τα ζευγάρια (n, e) και (n, d) καλούνται δημόσιο κλειδί και ιδιωτικό κλειδί, αντίστοιχα
- DSA (Digital Signature Algorithm):
  - Δημιουργήθηκε από το National Institute of Standards and Technology (NIST) που δημοσιοποίησε το Digital Signature Algorithm
  - Στον DSA η παραγωγή των υπογραφών είναι πιο γρήγορη από την επιβεβαίωση τους (αντίθετα με τον RSA)
  - Έλλειψη ευελιξίας
  - Αργή επαλήθευση των υπογραφών,
  - Αδυναμία συνεργασίας με άλλα πρωτόκολλα πιστοποίησης ταυτότητας

Βασικοί μηχανισμοί και διαδικασίες Κρυπτογραφίας

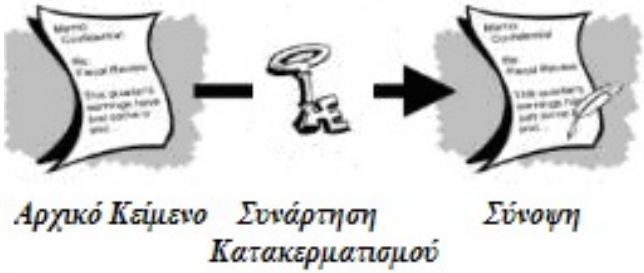
- Συμφωνία κλειδιών
- Συναρτήσεις κατακερματισμού
- Αλγόριθμοι κρυπτογράφησης τμημάτων
- Αλγόριθμοι κρυπτογράφησης ροών
- Ψηφιακές υπογραφές
- Κώδικες Αυθεντικοποίησης Μηνυμάτων

Συμφωνία κλειδιών

- Η διαδικασία επίτευξης συμφωνίας στην πληροφορία κρυπτογραφικών κλειδιών μυστικά πάνω από ένα ανοιχτό κατανεμημένο δίκτυο
- Χρησιμοποιούνται πρωτόκολλα (key agreement protocols) με τα ακόλουθα χαρακτηριστικά:
  - Γνωστά κλειδιά συνόδου (ακόμα κι αν έχουν υποκλαπεί)
  - (Τέλεια) πρόσθια μυστικότητα (perfect forward secrecy) – (δεν επηρεάζεται η μυστικότητα του συνόλου των κλειδιών)
  - Άγνωστο μοίρασμα κλειδιού (μία οντότητα γνωρίζει πάντα που δίνει το κλειδί της)
  - Απομίμηση με υποκλοπή κλειδιού (ακόμα και σε υποκλοπή να μην μπορεί να χρησιμοποιηθεί το κλειδί)
  - Απώλεια πληροφορίας (η υποκλοπή πληροφορίας δεν επηρεάζει την λειτουργία του πρωτοκόλλου)
  - Ανεξαρτησία μηνυμάτων

Συναρτήσεις Κατακερματισμού

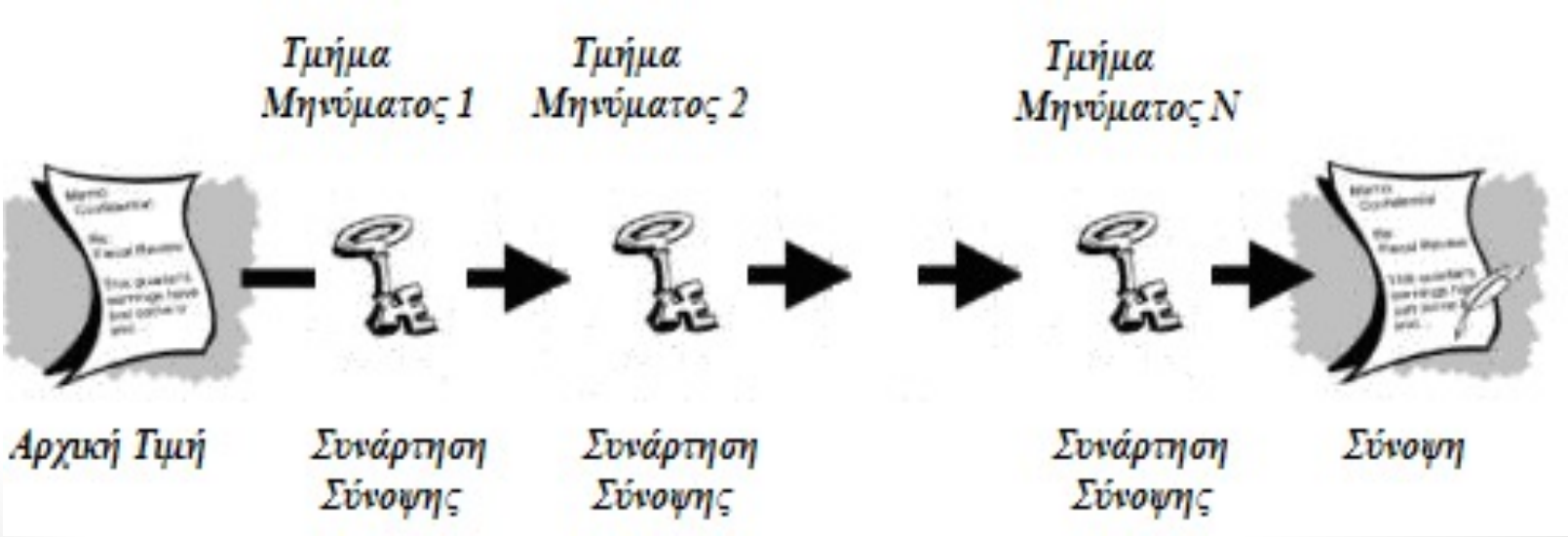
- Μια συνάρτηση κατακερματισμού (hash function) H είναι ένας μετασχηματισμός που λαμβάνει μια είσοδο μεταβλητού μήκους m και επιστρέφει μια συμβολο-ακολουθία σταθερού μήκους, που ονομάζεται τιμή της συνάρτησης h, δηλαδή h = H(m).
- Η τιμή της συνάρτησης κατακερματισμού αναπαριστά με συνέπεια το μήνυμα ή έγγραφο από το οποίο υπολογίστηκε.



- Βασικές Απαιτήσεις:
  - Η είσοδος να είναι οποιουδήποτε μήκους.
  - Η έξοδος να έχει σταθερό μέγεθος.
  - Η H(x) να είναι εύκολο να υπολογιστεί για οποιοδήποτε δεδομένο x.
  - Η H(x) είναι μονόδρομη (one-way).
  - Η H(x) είναι ανθεκτική σε συγκρούσεις (collision-free).

Συναρτήσεις Συμπίεσης

- Παίρνουν είσοδο καθορισμένου μήκους και δίνουν έξοδο μικρότερου, περιορισμένου μήκους
- Βήματα Συναρτήσεων Συμπίεσης:
  - Το μήνυμα τεμαχίζεται σε τμήματα (blocks), των οποίων το μέγεθος εξαρτάται από την συνάρτηση σύνοψης
  - Αυτό συμπληρώνεται (padded) για λόγους ασφαλείας, ώστε το μήκος του μηνύματος να είναι πολλαπλάσιο του μήκους του block



Γνωστοί Αλγόριθμοι Συναρτήσεων Κατακερματισμού

- SHA και SHA-1 (Secure Hash Algorithm)
  - Οι SHA και SHA-1 αναπτύχθηκαν από το NIST.
  - Ο SHA-1 αποτελεί επανέκδοση του SHA που διόρθωνε μια ατέλεια του τελευταίου.
  - Ο SHA-1 παίρνει είσοδο μήνυμα μήκους μικρότερο από 264 bits και παράγει σύνοψη 160 bits
- MD2, MD4, MD5 (Message Digest)
  - Παίρνουν στην είσοδο μήνυμα αυθαίρετου μήκους και δίνουν στην έξοδο μια σύνοψη 128 bits
  - Ο MD2 είχε σχεδιαστεί για μηχανές 8 bit, σε αντίθεση με τους MD4 και MD5 που προορίζονται για μηχανές 32 bits

Αλγόριθμοι κρυπτογράφησης τμημάτων

- Οι αλγόριθμοι κρυπτογράφησης τμημάτων (block ciphers) είναι ένας τύπος αλγορίθμων συμμετρικής κρυπτογράφησης που μετατρέπει ένα τμήμα μη κρυπτογραφημένου κειμένου, καθορισμένου μεγέθους (plaintext), σε ίδιου μεγέθους τμήμα κρυπτογραφημένου κειμένου (ciphertext)
- Το καθορισμένο μήκος καλείται *μέγεθος τμήματος (block size)*
- Οι αλγόριθμοι τμημάτων λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα τμήμα διαδοχικά αρκετές φορές
- Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υπό-κλειδί.
- Το σύνολο των υπό-κλειδιών προέρχεται από το μυστικό κλειδί που χορήγησε ο χρήστης, με ειδική συνάρτηση.

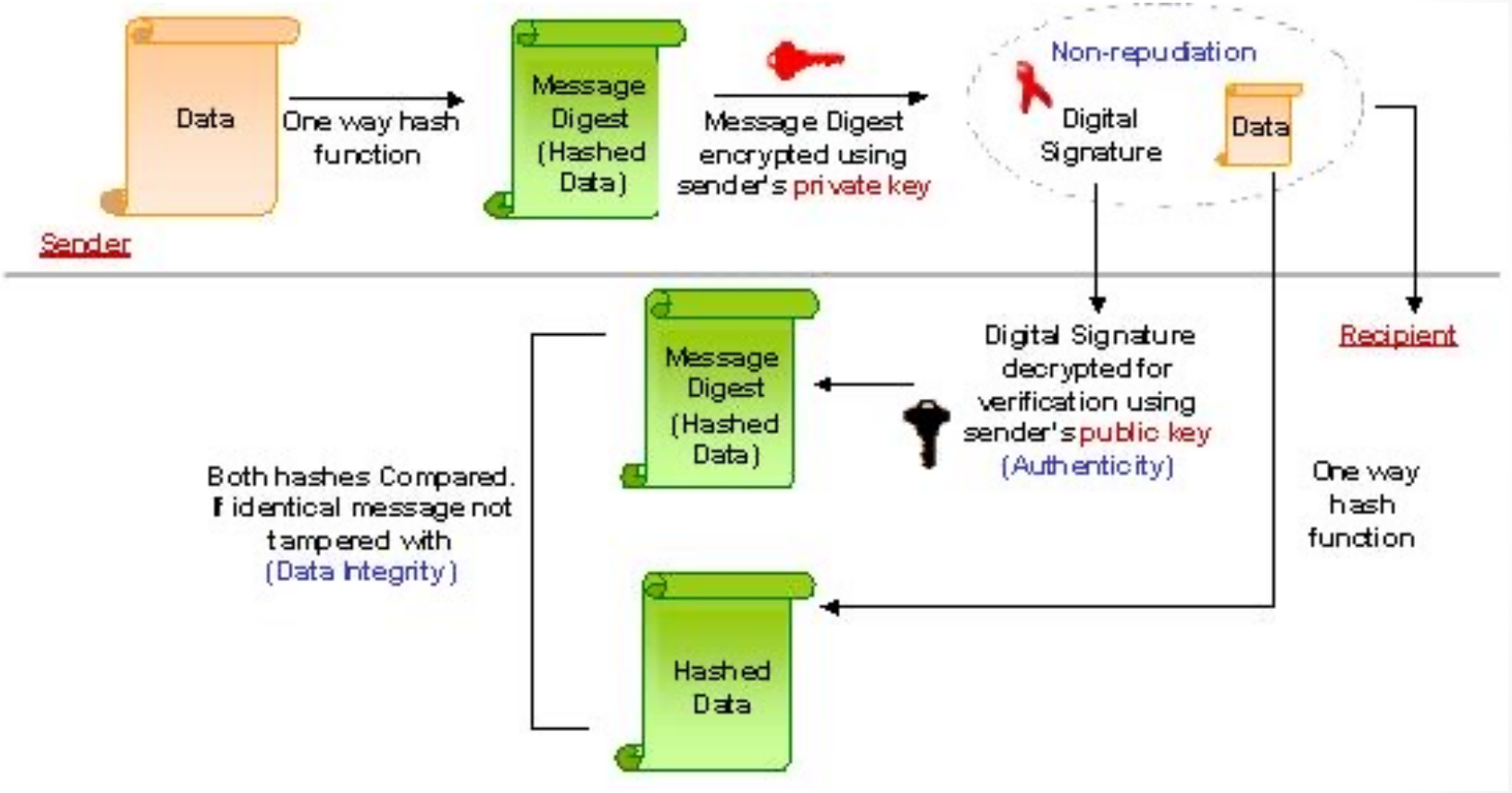
Αλγόριθμοι Feistel

- Το κείμενο χωρίζεται στο μισό.
- Η συνάρτηση f εφαρμόζεται στο ένα μισό με χρήση ενός υπό-κλειδιού και η έξοδος της f περνάει από λογική πράξη X-OR με το άλλο μισό.
- Το αποτέλεσμα της λογικής πράξης γίνεται είσοδος της f (με νέο υπό-κλειδί) και το προηγούμενο μισό το οποίο μετασχηματίστηκε γίνεται μία από τις εισόδους της επόμενης X-OR.
- Ο αλγόριθμος συνεχίζεται με τον ίδιο τρόπο και στο τέλος της τελευταίας επανάληψης, τα δύο κρυπτογραφημένα μισά συνενώνονται.

Αλγόριθμοι κρυπτογράφησης ροών

- Ένας αλγόριθμος κρυπτογράφησης ροών (Stream cipher) είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης
- Εξαιρετικά ταχείς αλγόριθμοι (πολύ ταχύτεροι από τους αλγόριθμους τμημάτων)
- Οι αλγόριθμοι ροών λειτουργούν με μικρότερες μονάδες απλού κειμένου (συνήθως με bits)
- Ένας αλγόριθμος ροών παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται κλειδοροή (keystream) - Παράγεται τελείως στην τύχη.
- Η κρυπτογράφηση επιτυγχάνεται με το συνδυασμό της κλειδο-ροής με το plaintext, συνήθως μέσω πράξης X-OR

Ψηφιακές υπογραφές



Κώδικες Αυθεντικοποίησης Μηνυμάτων

- Ένας Κώδικας Αυθεντικοποίησης Μηνύματος ΚΑΜ (Message Authentication Code – MAC) αποτελεί ένα κομμάτι πληροφορίας που χρησιμοποιείται για την αυθεντικοποίηση ενός μηνύματος
- Ένας αλγόριθμος ΚΑΜ δέχεται ως είσοδο ένα μυστικό κλειδί και ένα μήνυμα τυχαίου μεγέθους (το οποίο θέλουμε να αυθεντικοποιήσουμε) και έχει ως έξοδο το ΜΑΚ (ετικέτα – tag)
- Οι συναρτήσεις που παράγουν ΜΑΚ είναι παρόμοιες με τις συναρτήσεις κατακερματισμού, αλλά έχουν διαφορετικές απαιτήσεις ασφάλειας.
- Οι ΚΑΜ μπορούν να κατηγοριοποιηθούν ως:
  - Ασφαλείς χωρίς συνθήκες
  - Βασισμένοι σε συναρτήσεις κατακερματισμού
  - Βασισμένοι σε αλγορίθμους ροών (stream ciphers)
  - Βασισμένοι σε αλγορίθμους τμημάτων (block ciphers)

Ευχαριστώ
για την προσοχή σας!!

Επικοινωνία: karant@unipi.gr

Ενημέρωση: http://gunet2.cs.unipi.gr/eclass/