# Ηλεκτρονική Διακυβέρνηση

## **Ενότητα 7**: Μάθημα 7

Βράνα Βασιλική
Τμήμα Διοίκησης Επιχειρήσεων

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

# 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.

# Κρυπτογραφία (1)

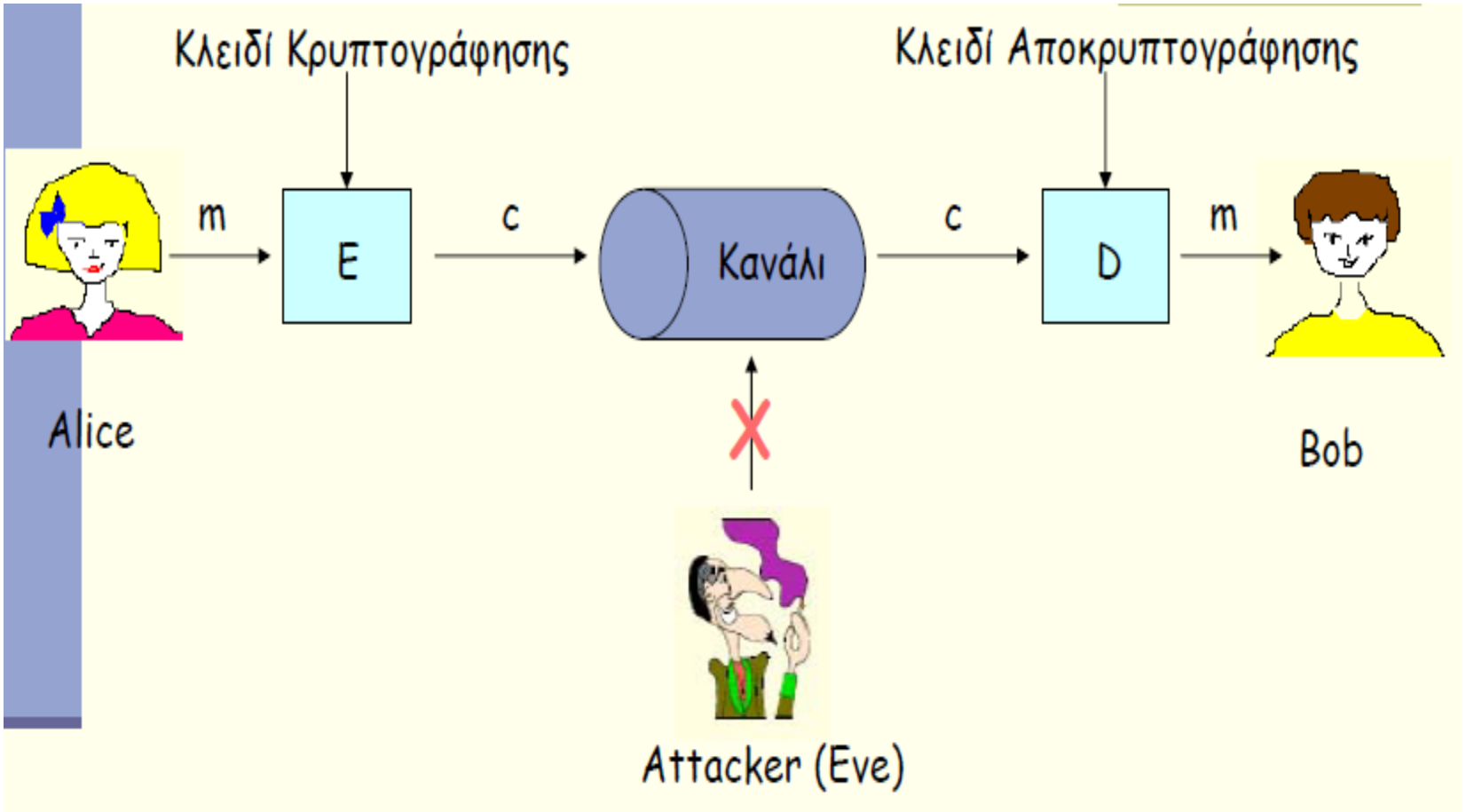
- Η κρυπτογραφία χρησιμοποιείται σήμερα ως ένα χρήσιμο εργαλείο στην ασφάλεια πληροφοριών, δηλαδή την προστασία των δεδομένων ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους

- Επιστήμη που μελετά τρόπους κωδικοποίησης μηνυμάτων.

# Κρυπτογραφία (2)

- Η κρυπτογραφία δεν αποτελεί το μόνο μέσο για την επίτευξη της Ασφάλειας Πληροφορίας, ωστόσο προσφέρει ένα σύνολο από τεχνικές (κρυπτογραφικά εργαλεία – cryptographic tools) προς αυτήν την κατεύθυνση…

# Κρυπτογραφία (3)



# Ορισμοί για την Κρυπτογραφία (1)

- **Αρχικό κείμενο** (plaintext), ονομάζεται το αρχικό μήνυμα που θέλουμε να κρυπτογραφήσουμε.

  Ονομάζεται και απλό ή καθαρό.
- **Κρυπτογραφημένο κείμενο** ή κρυπτογράφημα (ciphertext), ονομάζεται η μυστική-κρυπτογραφημένη μορφή του κειμένου.
- **Αλγόριθμος κρυπτογράφησης** (encyption algorithm) ή μέθοδος κρυπτογράφησης (ciphering), ονομάζεται η μέθοδος που ακολουθείται για τη μετατροπή του αρχικού κειμένου σε μυστική μορφή.

# Ορισμοί για την Κρυπτογραφία (2)

- **Κρυπτογράφηση** (encryption), ονομάζεται η διαδικασίας μετατροπής του αρχικού κειμένου σε κρυπτογράφημα.

- **Αποκρυπτογράφηση** (decryption, deciphering) ονομάζεται η αντίστροφη διαδικασία της κρυπτογράφησης, δηλαδή η μετατροπή του κρυπτογραφήματος σε αρχικό κείμενο.

# Ορισμοί για την Κρυπτογραφία (2)

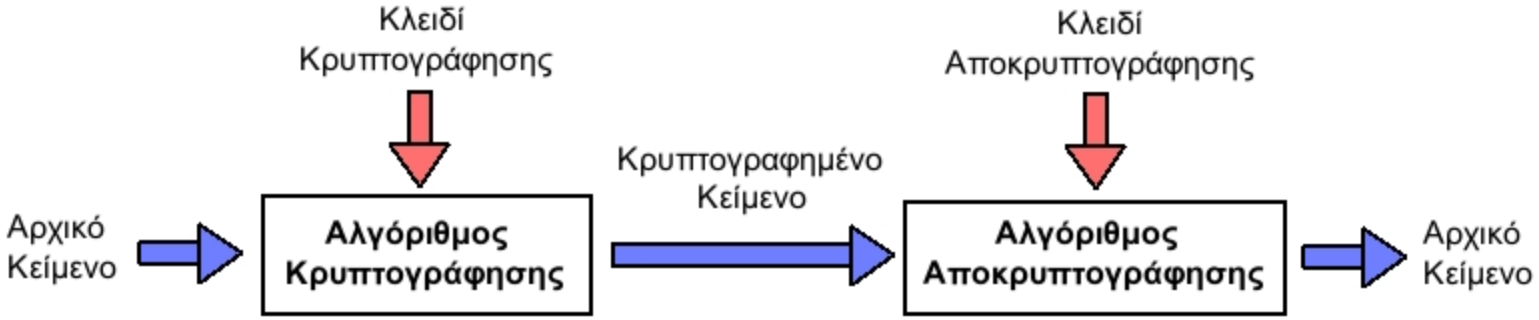
- **Κλειδί (key) κρυπτογράφησης**, ονομάζεται η αναλυτική περιγραφή της μεθόδου κρυπτογράφησης. Το κλειδί για παράδειγμα μπορεί να είναι η αντιστοιχία γραμμάτων του αρχικού κειμένου και του κρυπτογραφήματος.
- **Κάλυμμα** ενός μηνύματος (padding), ονομάζεται το επιπρόσθετο κείμενο το οποίο πρέπει να προσθέσουμε στο κείμενο προκειμένου το αρχικό κείμενο να αποκτήσει ένα συγκεκριμένο αρχικό μήκος που απαιτεί κάποιος αλγόριθμος κρυπτογράφησης

# Ορισμοί για την Κρυπτογραφία (2)

- **Κλειδί (key) κρυπτογράφησης**, ονομάζεται η αναλυτική περιγραφή της μεθόδου κρυπτογράφησης. Το κλειδί για παράδειγμα μπορεί να είναι η αντιστοιχία γραμμάτων του αρχικού κειμένου και του κρυπτογραφήματος.
- **Κάλυμμα** ενός μηνύματος (padding), ονομάζεται το επιπρόσθετο κείμενο το οποίο πρέπει να προσθέσουμε στο κείμενο προκειμένου το αρχικό κείμενο να αποκτήσει ένα συγκεκριμένο αρχικό μήκος που απαιτεί κάποιος αλγόριθμος κρυπτογράφησης

# Αλγόριθμοι βασισμένοι σε κλειδιά

- Οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν ένα ή περισσότερα κλειδιά.




  - Η ασφάλεια έγκειται στο **ότι δεν είναι γνωστό το κλειδί** - οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι ευρέως γνωστοί (**Αρχή Kerchoff**)

# Πόσο ασφαλές είναι ένα σύστημα;

– Όσο μεγαλύτερο είναι το πλήθος των κλειδιών τόσο μεγαλύτερη είναι η ασφάλεια

(… εκτός και αν ο αλγόριθμος δεν είναι ασφαλής)

– Ένα σύστημα με μικρό αριθμό κλειδιών, μπορεί να είναι ασφαλές, για μικρό χρονικό διάστημα !

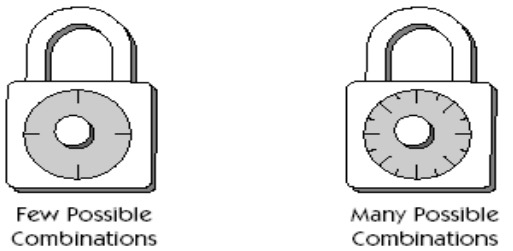



**Figure 1-2** Some locks have very few possible combinations; others have many possible combinations.

Mel, H. & Baker, D. (2001). *Cryptography Decrypted*. Addison-Wesley,

# Κώδικες αντικατάστασης

- Κάθε γράμμα ή ομάδα γραμμάτων αντικαθίσταται από ένα άλλο γράμμα ή ομάδα γραμμάτων

- Κώδικας του Καίσαρα.
  - Αποδίδεται στον Ιούλιο Καίσαρα
  - Κάθε γράμμα μετατοπίζεται κατά k χαρακτήρες
  - Το k είναι το κλειδί του κώδικα

# Αλγόριθμος του Καίσαρα

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Το κλειδί είναι: k=3

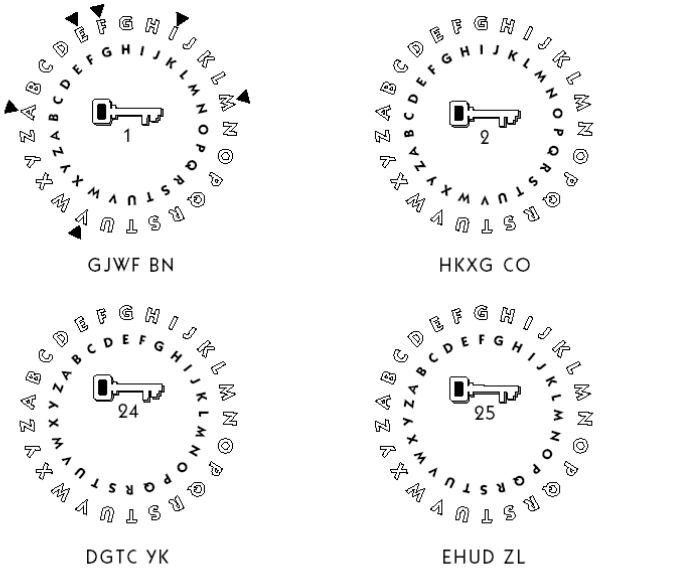



**Figure 2-4** Four Caesar cipher keys—1, 2, 24, and 25—encrypting `FIVE AM`.

- Αριθμός διαθέσιμων κλειδιών στο Αγγλικό αλφάβητο : 25

Mel, H. & Baker, D. (2001). *Cryptography Decrypted*. Addison-Wesley,

# Αλγόριθμος του Καίσαρα

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Το κλειδί είναι: k=3

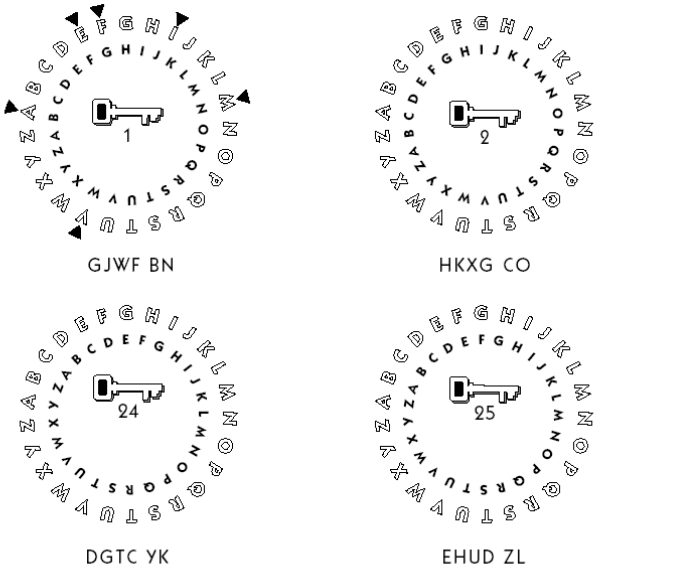



**Figure 2-4** Four Caesar cipher keys—1, 2, 24, and 25—encrypting `FIVE AM`.

- Αριθμός διαθέσιμων κλειδιών στο Αγγλικό αλφάβητο : 25

Mel, H. & Baker, D. (2001). *Cryptography Decrypted*. Addison-Wesley,

# Αλγόριθμος Μονο-αλφαβητικής αντικατάστασης

| P | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | Q | R | Z | V | E | H | P | N | X | T | O | B | Y | C | G | I | U | L | A | J | M | W | D | F | S | K |

- Μονοαλφαβητικός: Χρήση ενός κρυπτο-αλφάβητου
- Το κρυπτο-αλφάβητο αποτελεί το κλειδί του αλγορίθμου

- Αριθμός πιθανών κλειδιών στο Αγγλικό αλφάβητο : **25! $=1,5*10^{25}$**

# Το ‘σπάσιμο’ ενός κώδικα…..

- Συχνότητα εμφάνισης γραμμάτων: e, t, o, a, n, i …….
- Συχνότητα εμφάνισης δι-γραμμάτων:  th, in, er,…….
- Συχνότητα εμφάνισης τρι-γραμμάτων: the, ing, and,…..
- Τακτική:
  - εύρεση συχνότητας γραμμάτων, δι-γραμματων, τρι-γραμμάτων
  - τα  πιο συχνά κωδικά γράμματα μάλλον αντιστοιχούν στα e  και t
- Μια άλλη τακτική είναι να εντοπιστεί μια συχνά χρησιμοποιούμενη λέξη ή φράση

# Κατηγορίες αλγόριθμων ως προς το είδος του κλειδιού

- Αλγόριθμοι συμμετρικού κλειδιού
- Αλγόριθμοι ασύμμετρου κλειδιού

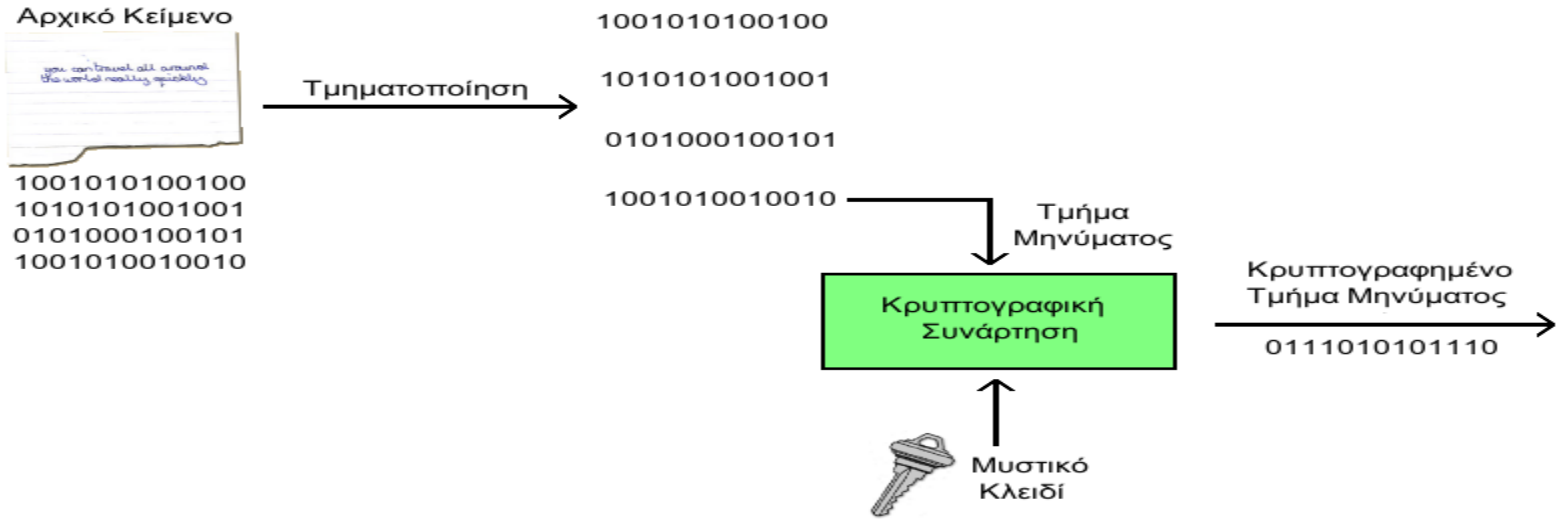
# Αλγόριθμοι συμμετρικού κλειδιού

- Αλγόριθμοι συμμετρικού κλειδιού: Χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση

- **Πρόβλημα:** Πώς ανταλλάσουν το μυστικό κλειδί δυο χρήστες;

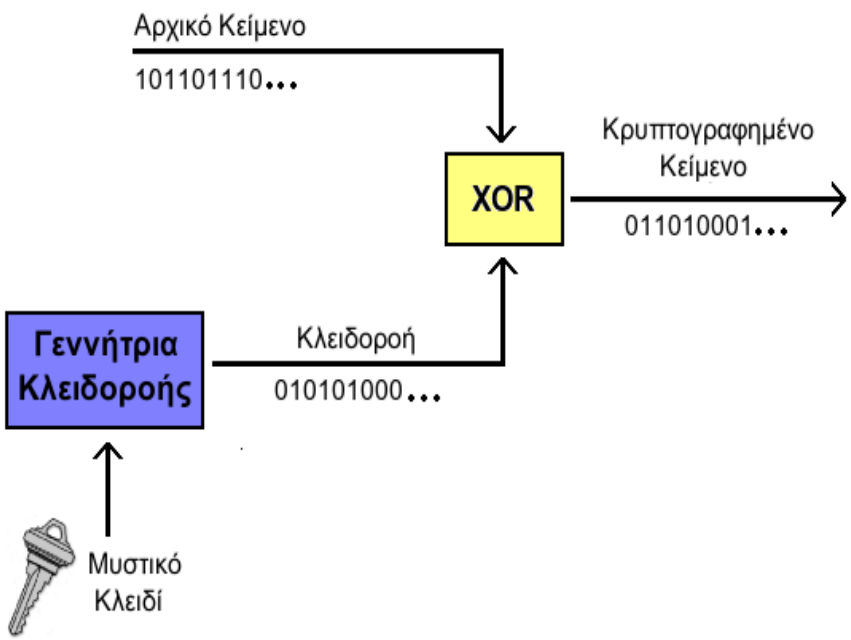
✓ Το κανάλι μέσω του οποίου ανταλλάσσεται το K πρέπει να είναι ασφαλές

# Κρυπτογραφικοί αλγόριθμοι δέσμης (block ciphers)




Τεμαχίζουν σε τμήματα (blocks) το αρχικό κείμενο που πρόκειται να κρυπτογραφηθεί και κρυπτογραφούν κάθε τμήμα ξεχωριστά. Η κρυπτογράφηση κάθε ενός τμήματος γίνεται χρησιμοποιώντας μία μαθηματική συνάρτηση κρυπτο-γράφησης και το μυστικό κλειδί

# Κρυπτογραφικοί αλγόριθμοι ροής (stream ciphers)




επιλέγεται αρχικά μία γεννήτρια κλειδοροής (keystream generator), η οποία δέχεται ως είσοδο το μυστικό κλειδί και παράγει στην έξοδό της μία ψευδοτυχαία ακολουθία bits, η οποία ονομάζεται κλειδοροή (keystream).

Στην συνέχεια εφαρμόζεται η συνάρτηση XOR ανάμεσα στο αρχικό κείμενο και στην κλειδοροή και το αποτέλεσμα της συνάρτησης είναι η τελική κρυπτογραφημένη ροή δεδομένων

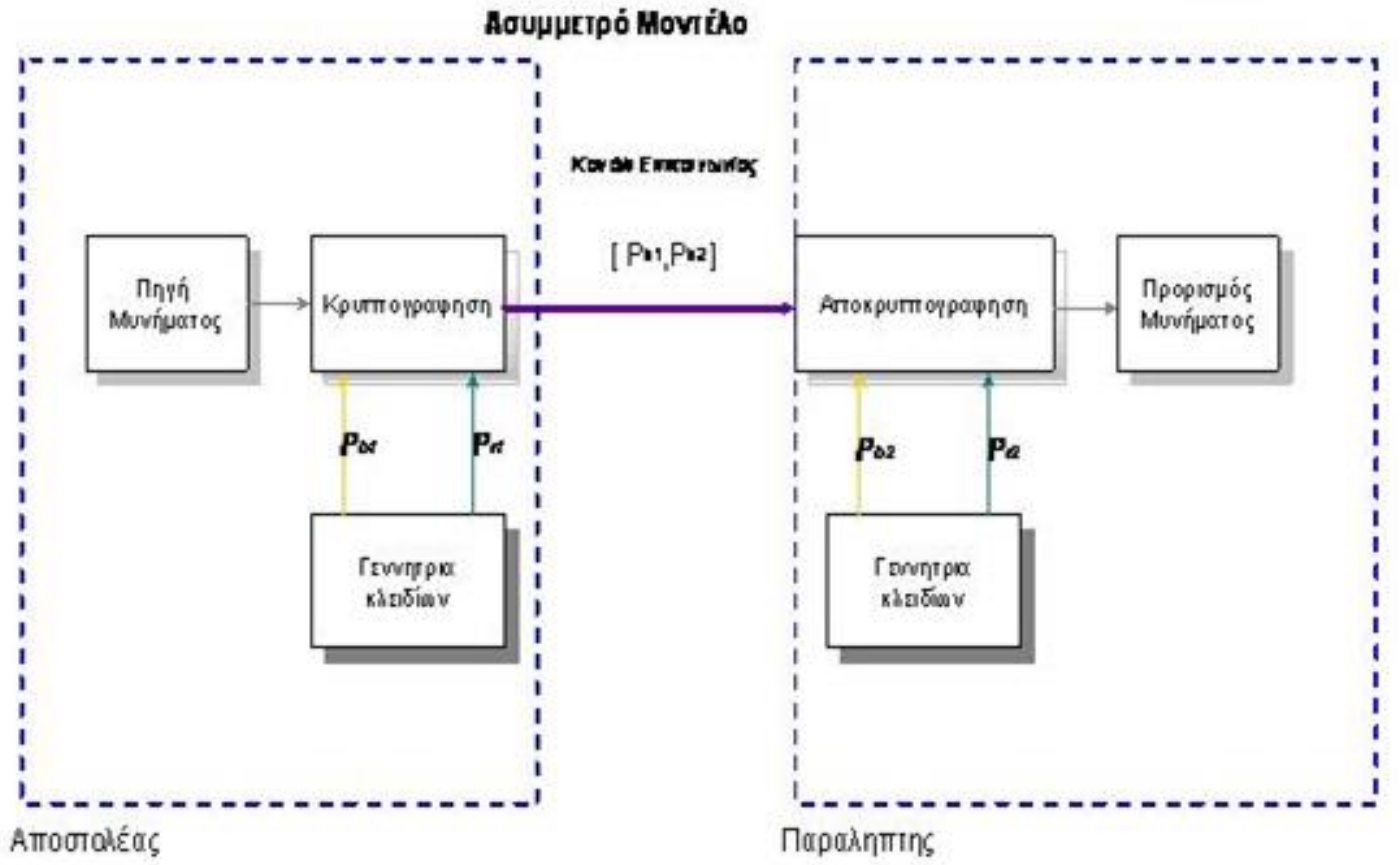
# Αλγόριθμοι ασύμμετρου κλειδιού (1)

- Αλγόριθμοι ασύμμετρου κλειδιού: Χρησιμοποιούν διαφορετικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση.
- Τα κλειδιά αυτά αποτελούν ένα μαθηματικά συνδεδεμένο ζεύγος.
- Το κλειδί κρυπτογράφησης δεν μπορεί να εξαχθεί από το κλειδί αποκρυπτογράφησης

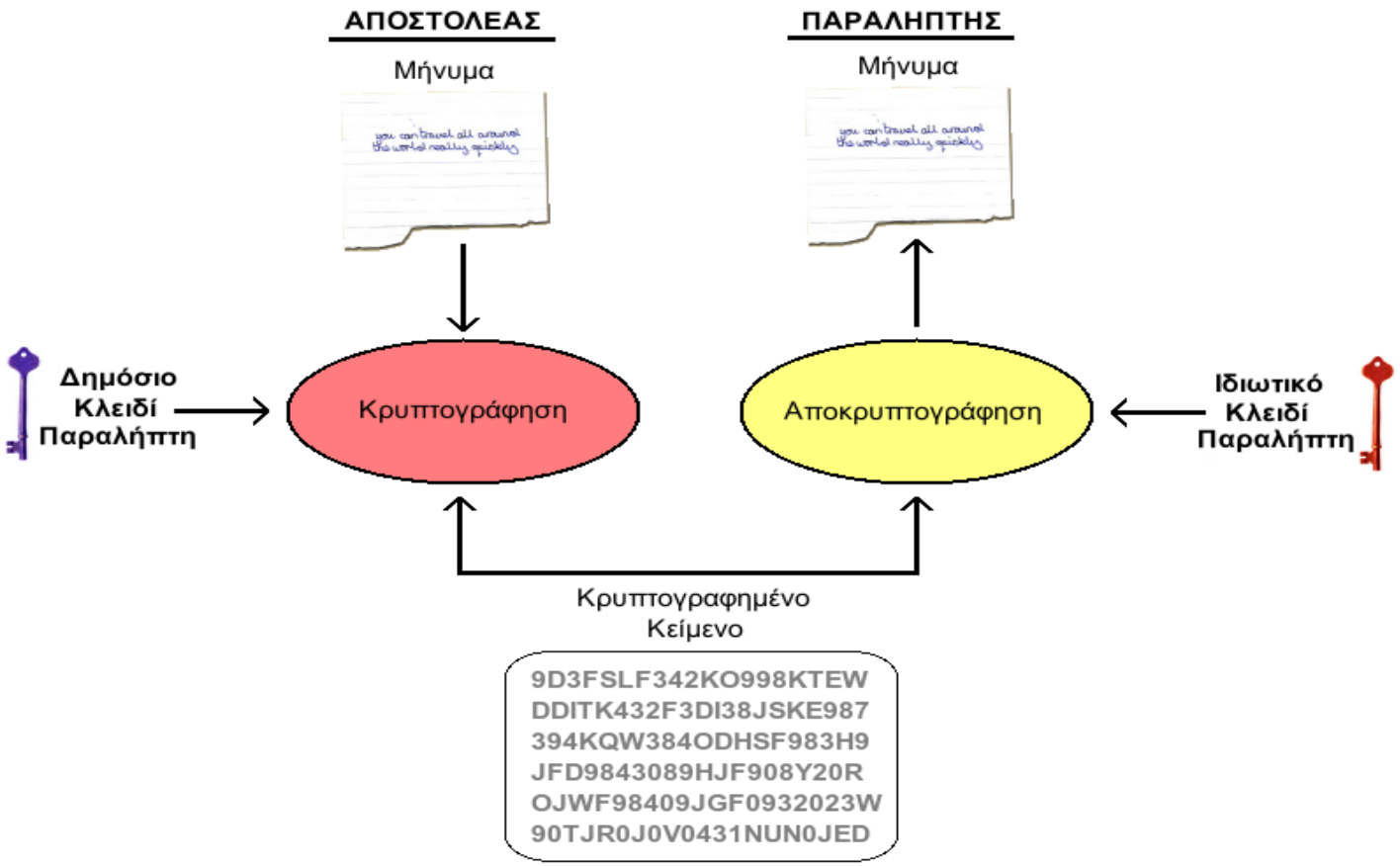
# Αλγόριθμοι ασύμμετρου κλειδιού (2)

- Το κλειδί κρυπτογράφησης γνωστοποιείται (συνήθως μέσω ψηφιακού πιστοποιητικού) σε τρίτους και λέγεται δημόσιο κλειδί
- Το κλειδί αποκρυπτογράφησης είναι γνωστό μόνο στον κάτοχό του και λέγεται ιδιωτικό ή μυστικό κλειδί.
- **Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό**
- Η κρυπτογράφηση Δημοσίου Κλειδιού μπορεί να χρησιμοποιηθεί και για τη δημιουργία και επαλήθευση ψηφιακής υπογραφής.

# Αλγόριθμοι ασύμμετρου κλειδιού (3)



# Αλγόριθμοι Δημόσιου κλειδιού – κρυπτογράφηση(1)



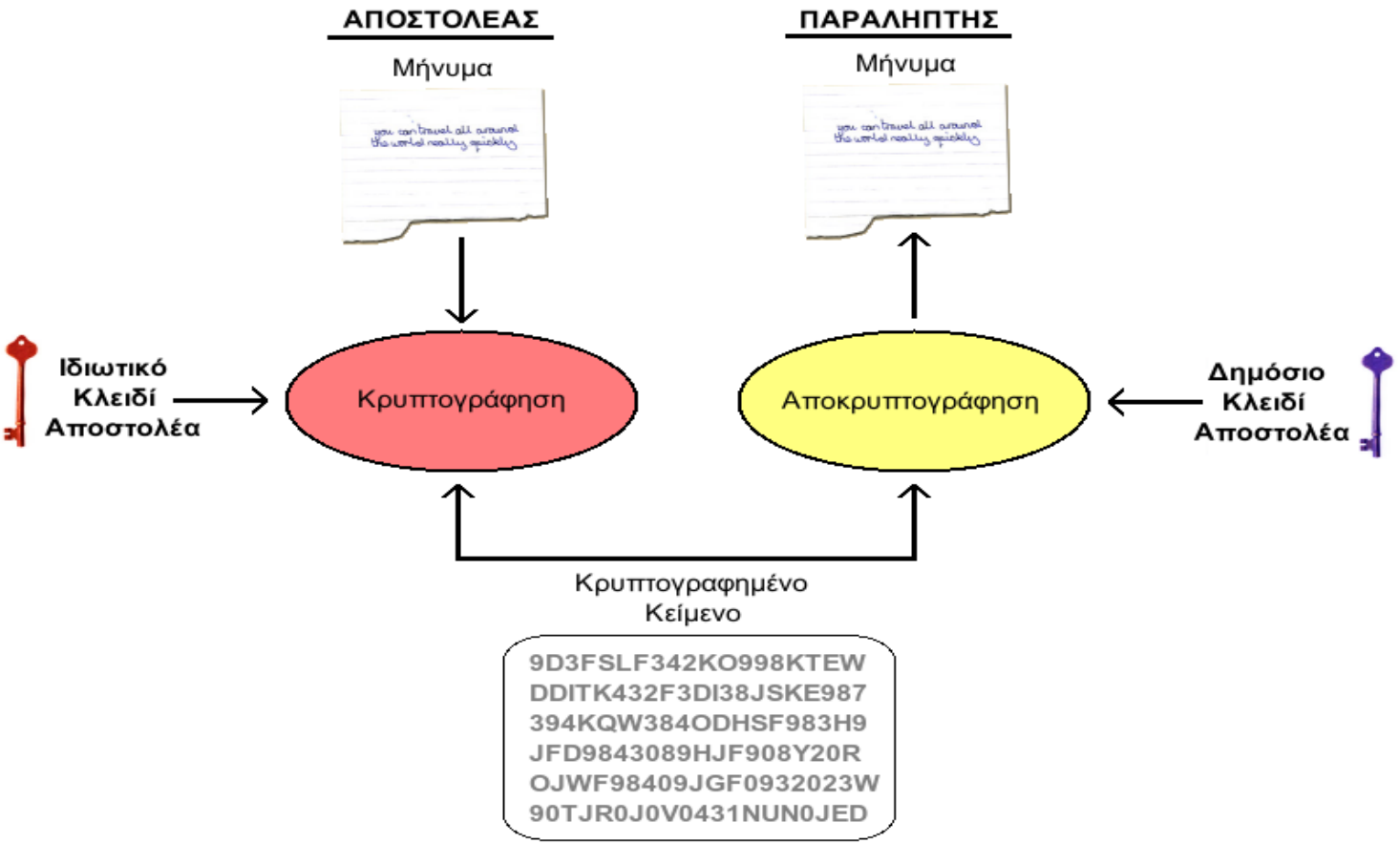
# Αλγόριθμοι Δημόσιου κλειδιού-κρυπτογράφηση(2)

- Ο αποστολέας χρησιμοποιεί το Δημόσιο Κλειδί $e_B$ του παραλήπτη για να κρυπτογραφήσει το M. $C= E_{e_B}(M)$
- Ο παραλήπτης χρησιμοποιεί το Ιδιωτικό Κλειδί του $d_B$ για να αποκρυπτογραφήσει το μήνυμα: $M= D_{d_B}(C)$
- Εγγυώνται την εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημένο μήνυμα που θα στείλει ο αποστολέας μέσω του διαδικτύου στον παραλήπτη θα είναι αναγνώσιμο από αυτόν και μόνο

# Ψηφιακή υπογραφή

- **Ψηφιακή Υπογραφή:** μία συμβολοσειρά η οποία συνοδεύει ηλεκτρονικά δεδομένα ή αρχεία και μπορεί να χρησιμοποιηθεί για την επαλήθευση της ακεραιότητάς τους, καθώς και τη αποποίηση ευθύνης.
- Για τη δημιουργία/επαλήθευση ψηφιακών υπογραφών χρησιμοποιείται κρυπτογράφηση δημόσιου κλειδιού. Το ιδιωτικό κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το δημόσιο κλειδί για την επαλήθευση της υπογραφής.

# Αλγόριθμοι Δημόσιου κλειδιού -ψηφιακή υπογραφή(1)



# Αλγόριθμοι Δημόσιου κλειδιού -ψηφιακή υπογραφή(2)

- Ο αποστολέας χρησιμοποιεί το Ιδιωτικό του κλειδί $d_B$ για υπογράψει ψηφιακά το μήνυμα $C= E_{d_B} (M)$

- Ο παραλήπτης χρησιμοποιεί το Δημόσιο Κλειδί του αποστολέας για να επαληθεύσει την υπογραφή

- **Ταυτοποίηση**, δηλαδή ο παραλήπτης γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα

# Ψηφιακά πιστοποιητικά (1)

- **Ψηφιακό Πιστοποιητικό**: είναι ένα ψηφιακό έγγραφο το οποίο χρησιμοποιείται στην κρυπτογραφία Δημόσιου Κλειδιού, για να πιστοποιήσει την αυθεντικότητα των δημόσιων κλειδιών των χρηστών.
- Ένα ψηφιακό πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί ενός χρήστη, το όνομα του κατόχου του, τους χρησιμοποιούμενους αλγόριθμους και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του κλειδιού.

# Ψηφιακά πιστοποιητικά (2)

- Για να είναι έγκυρο ένα ψηφιακό πιστοποιητικό, είναι υπογεγραμμένο από κάποια Αρχή Πιστοποίησης και περιλαμβάνει μια ημερομηνία λήξης
- Η έκδοση ενός ψηφιακού πιστοποιητικού γίνεται μετά από αίτηση του ενδιαφερομένου σε μία Αρχή Πιστοποίησης
- http://www.yap.gov.gr/index.php/themata-enimerosis-politi/lista-syxnon-erotiseon-apantiseon.html?view=category&id=104

# SSL Certificates

- SSL - Secure Socket Layers. Αλλιώς γνωστό και ως Ηλεκτρονικό Πιστοποιητικό.
- Το πρωτόκολλο SSL δημιουργεί μια ασφαλή σύνδεση μεταξύ του εκάστοτε ιστοσελίδας και του φυλλομετρητή του χρήστη.
- Τα SSL πιστοποιητικά εξασφαλίζουν την ασφαλή ανταλλαγή δεδομένων ανάμεσα στις δύο πλευρές, αποτρέποντας κακόβουλους χρήστες από την υποκλοπή δεδομένων.

# Διαδικασίες των SSL Certificates

- Ασφαλή μεταφορά δεδομένων μεταξύ ενός εξυπηρετητή και ενός υπολογιστή.

- Πιστοποίηση και ταυτοποίηση, βοηθώντας τον χρήστη να επιβεβαιώσει την ταυτότητα της ιστοσελίδας με την οποία συναλλάσσεται.

# Πως λειτουργούν τα SSL Certificates (1)

- Ο φυλλομετρητής  ελέγχει το SSL Certificate, για να διαπιστώσει αν είναι έγκυρο και να πιστοποιήσει την ταυτότητα της ιστοσελίδας.

- Ο εξυπηρετητής επικοινωνεί με τον φυλλομετρητή, και ενεργοποιείται η κρυπτογράφηση δεδομένων σε συγκεκριμένα bit (συνήθως 128bit ή 256bit).

# Πως λειτουργούν τα SSL Certificates (2)

- Ο εξυπηρετητής και ο φυλλομετρητής ανταλλάσσουν μοναδικούς κωδικούς αποκρυπτογράφησης, ώστε να τους χρησιμοποιήσουν στην αποκρυπτογράφηση που πραγματοποιείται με την ολοκλήρωση της ανταλλαγής δεδομένων.
- Η διαδικασία ανταλλαγής δεδομένων ξεκινάει, το εικονίδιο ασφαλούς μεταφοράς δεδομένων SSL εμφανίζεται δίπλα από την γραμμή διεύθυνσης της ιστοσελίδας και η συναλλαγή είναι πλέον ασφαλής.

# SET

- Το SET (Secure Electronic Transaction) είναι ένα πρωτόκολλο εμπορικών συναλλαγών με τη χρήση καρτών σε ανοικτά δίκτυα, το οποίο αναπτύχθηκε από την MasterCard και την Visa ως μια μέθοδος εξασφάλισης των συναλλαγών με τη χρήση καρτών διαμέσου του Internet.
- Η διαδικασία περιλαμβάνει ένα αριθμό ελέγχων ασφαλείας που πραγματοποιείται με τη χρήση ψηφιακών πιστοποιητικών που χορηγούνται στους εμπλεκόμενους αγοραστές, εμπόρους και τράπεζες.

# Προδιαγραφές του SET (1)

- Παροχή προστασίας των οικονομικών δεδομένων ή και άλλων που διακινούνται μαζί τους από υποκλοπή.
- Διασφάλιση της ακεραιότητας των δεδομένων.
- Παροχή διαδικασιών πιστοποίησης ταυτότητας του κατόχου κάρτας.
- Παροχή υπηρεσιών πιστοποίησης των εμπόρων που μπορούν να δεχθούν την πληρωμή με τη χρήση τέτοιας μεθόδου, που προκύπτει από τη σχέση τους με κάποιο οικονομικό ίδρυμα παροχής καρτών.

# Προδιαγραφές του SET (2)

- Διασφάλιση της χρήσης των καλύτερων τεχνικών ασφάλειας και σχεδίασης συστημάτων για την προστασία όλων των νόμιμα εμπλεκομένων πλευρών.
- Η δημιουργία ενός πρωτοκόλλου το οποίο να είναι ανεξάρτητο από τους μηχανισμούς ασφάλειας του επιπέδου μεταφοράς χωρίς όμως και να αποτρέπει τη χρήση τους.

# Προδιαγραφές του SET (3)

- Να είναι διαλειτουργικό (όλοι οι φυλλομετρητές να δουλεύουν με όλους τους κύριους servers και οι τελευταίοι με τη σειρά τους δεν θα έχουν πρόβλημα συμβατότητας με τους Payment Gateway Servers).

# Συστατικά στοιχεία του SET - Cardholder Wallet

**Cardholder Wallet (Πορτοφόλι Χρήστη Κάρτας)**

- Είναι ένα προϊόν που χρησιμοποιεί ο καταναλωτής που βρίσκεται on-line και που επιτρέπει την πραγματοποίηση ασφαλών συναλλαγών σε ένα δίκτυο.
- Το Wallet πρέπει να δημιουργεί μηνύματα που τα αντιλαμβάνονται τα άλλα τρία προϊόντα που απαρτίζουν το SET (Merchant, Payment Gateway, Certificate Authority).

# Συστατικά στοιχεία του SET - Merchant Server

## Merchant Server (Server - Έμπορος)

- Είναι ένα προϊόν το οποίο τρέχει κάποιος on-line έμπορος για την επεξεργασία των στοιχείων των συναλλαγών και τη διεκπεραίωσή τους. Επικοινωνεί και αυτό με τα άλλα τρία μέρη του SET.

# Συστατικά στοιχεία του SET - Payment Gateway

## Payment Gateway (Πύλη Πληρωμών)

- Είναι το προϊόν που τρέχει κάποιος τρίτος ο οποίος και επεξεργάζεται την πιστοποίηση των εμπόρων και των συναλλαγών (συμπεριλαμβανομένων οδηγιών πληρωμών από κατόχους καρτών). Επιπλέον αλληλεπιδρά και με ιδιωτικά εμπορικά δίκτυα.

# Συστατικά στοιχεία του SET - Certificate Authority

## Certificate Authority (Υπηρεσία Πιστοποιητικών)

- Είναι το τελευταίο από τα συστατικά στοιχεία του SET το οποίο τρέχει μια αρμόδια υπηρεσία έκδοσης και πιστοποίησης ψηφιακών πιστοποιητικών για το σκοπό αυτό και όποτε ζητείται από τα Wallet, Merchant και Payment Gateway πάνω από δημόσια ή ιδιωτικά δίκτυα.


Τέλος

# Τέλος Ενότητας