ΕΠΛ 674: Εργαστήριο 1
Ασφάλεια Επικοινωνιακών Συστημάτων - Κρυπτογραφία

University of Cyprus
Department of Computer Science

NETRworks Research Laboratory

Παύλος Αντωνίου

Γραφείο: ΘΕΕ 02 Β176

Εαρινό Εξάμηνο 2011

Ασφάλεια - Απειλές

University of Cyprus

Αντίπαλος	Στόχος
Φοιτητής	Να διασκεδάσει κρυφοκοιτάζοντας το ηλεκτρονικό ταχυδρομείο των άλλων
Κράκερ	Να δοκιμάσει το σύστημα ασφαλείας κάποιου, να κλέψει δεδομένα
Εμπορικός αντιπρόσωπος	Να υποστηρίξει ότι αντιπροσωπεύει όλη την Ευρώπη, και όχι μόνο την Ανδόρα
Επιχειρηματίας	Να ανακαλύψει τη στρατηγική μάρκετινγκ ενός ανταγωνιστή
Πρώην υπάλληλος	Να εκδικηθεί επειδή τον απέλυσαν
Λογιστής	Να καταχραστεί χρήματα από μια εταιρεία
Χρηματιστής	Να αρνηθεί μια υπόσχεση που έδωσε σε έναν πελάτη μέσω ηλεκτρονικού ταχυδρομείου
Απατεώνας	Να κλέψει και να πουλήσει αριθμούς πιστωτικών καρτών
Κατάσκοπος	Να μάθει τα στρατιωτικά ή βιομηχανικά μυστικά του εχθρού
Τρομοκράτης	Να κλέψει μυστικά στοιχεία για τον βιολογικό πόλεμο

Ασφάλεια – Γενικά (I)

University of Cyprus

- Τα δίκτυα υπολογιστών και ειδικότερα το Διαδίκτυο (Internet) αποτελούν τη βάση ανάπτυξης της Κοινωνίας της Πληροφορίας
  - Ταχύτατη ανάπτυξη
  - Μεγάλη διεισδυτικότητα
- Όλο και περισσότεροι οργανισμοί και πολίτες-χρήστες χρησιμοποιούν όλο και περισσότερες τηλεματικές εφαρμογές
- Η «φύση» του Διαδικτύου γεννά «ανασφάλεια» αφού χαρακτηρίζεται από:
  - Χαλαρή διοίκηση/συντονισμό
  - Τεχνολογική ετερογένεια
  - «Ανοικτά» περιβάλλοντα
  - Πολιτιστική ποικιλία

Ασφάλεια – Γενικά (ΙΙ)

University of Cyprus

- Το πρόβλημα της ασφαλείας γίνεται ένας καθοριστικός παράγοντας επιτυχούς ανάπτυξης και λειτουργίας των σύγχρονων πληροφοριακών περιβαλλόντων:
  - Υποδομές
  - Επικοινωνιακές υπηρεσίες
  - Υπηρεσίες προστιθέμενης αξίας
- Η αυτοματοποίηση των επικοινωνιακών διαδικασιών αποτελεί και την μεγάλη αδυναμία των διασυνδεδεμένων πληροφοριακών συστημάτων
  - Αυτοματοποίηση → γρήγορες αλλά όχι ασφαλείς υπηρεσίες
- Συμπέρασμα → Το «τίμημα» της «Πληροφορικής» επανάστασης είναι η ανάγκη για συνεχή επαγρύπνηση σε θέματα ασφαλείας…

Ασφάλεια – Γενικά (III)

University of Cyprus

- Δεν υπάρχει λύση που να αντιμετωπίζει αποτελεσματικά θέματα ασφαλείας

- Η πιο διαδεδομένη λύση σε θέματα ασφαλείας → Κρυπτογραφία

Κρυπτογραφία - Βασικοί Ορισμοί (Ι)

University of Cyprus

Η Κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας η οποία ασχολείται με την μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για 2 ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη

Κρυπτογραφία - Βασικοί Ορισμοί (ΙΙ)

University of Cyprus

Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες (αντικειμενικοί σκοποί):

- ***Εμπιστευτικότητα*** *(Confidentiality)*: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- ***Ακεραιότητα*** *(Integrity)*: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- ***Μη απάρνηση*** *(Non repudiation)*: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- ***Πιστοποίηση*** *(Authentication)*: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Κρυπτογραφία - Βασικοί Ορισμοί (III)

University of Cyprus

- **Κρυπτογράφηση** (*encryption*) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με την χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.
- **Αρχικό κείμενο** (*plaintext*) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.
- **Κρυπτογραφημένο κείμενο** (*ciphertext*) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.
- **Κλειδί** (*key*) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης.

Κρυπτογραφία - Βασικοί Ορισμοί (IV)

University of Cyprus

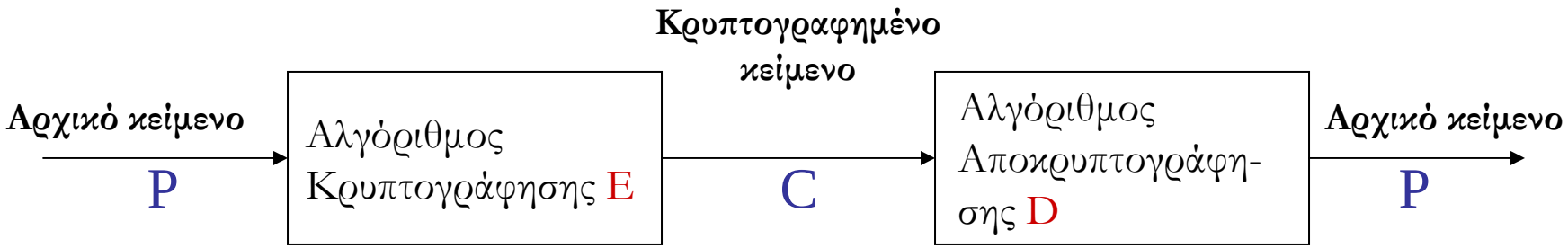
- **Κρυπτογραφικός αλγόριθμος** (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.
- Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση** (*decryption*).
- **Κρυπτανάλυση** (*cryptanalysis*) είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

Κρυπτογραφία - Μειονεκτήματα

University of Cyprus

1. Δεν μπορεί να αποτρέψει τη διαγραφή δεδομένων από έναν εισβολέα.
2. Το μεταδιδόμενο μήνυμα μπορεί να μεταβληθεί και να χρησιμοποιείται διαφορετικό κλειδί από αυτό που έχει ήδη καθοριστεί ή να καταγραφούν όλα τα κλειδιά για μελλοντική χρήση.
3. Μπορεί να βρεθεί ένας εύκολος και όχι ευρέως γνωστός τρόπος για την αποκρυπτογράφηση.
4. Ένα αρχείο μπορεί να προσπελασθεί πριν ή μετά την κρυπτογράφησή του.

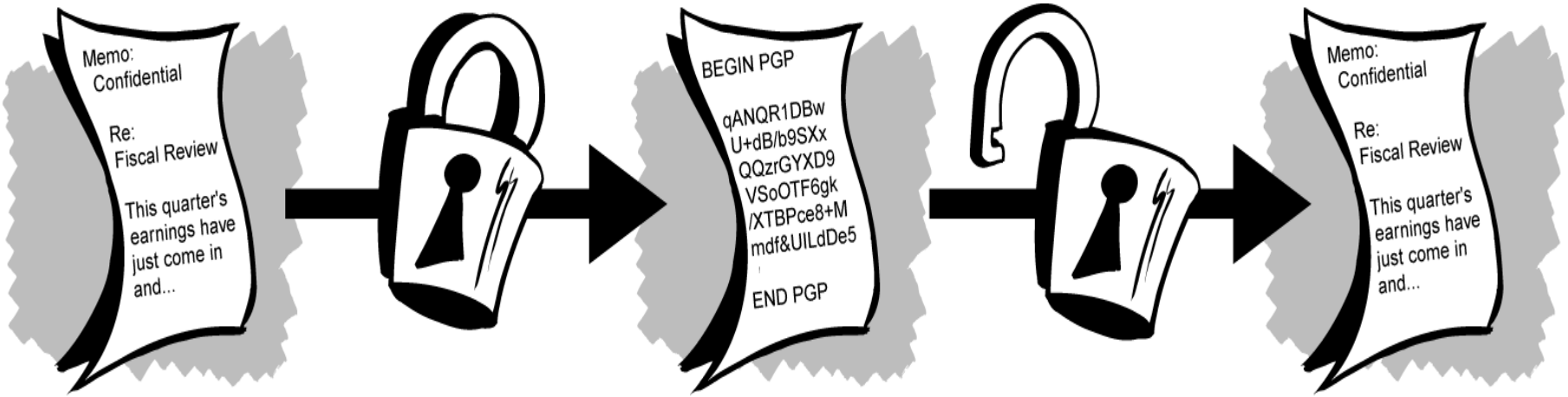
Τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης



Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P, C, k, E, D):

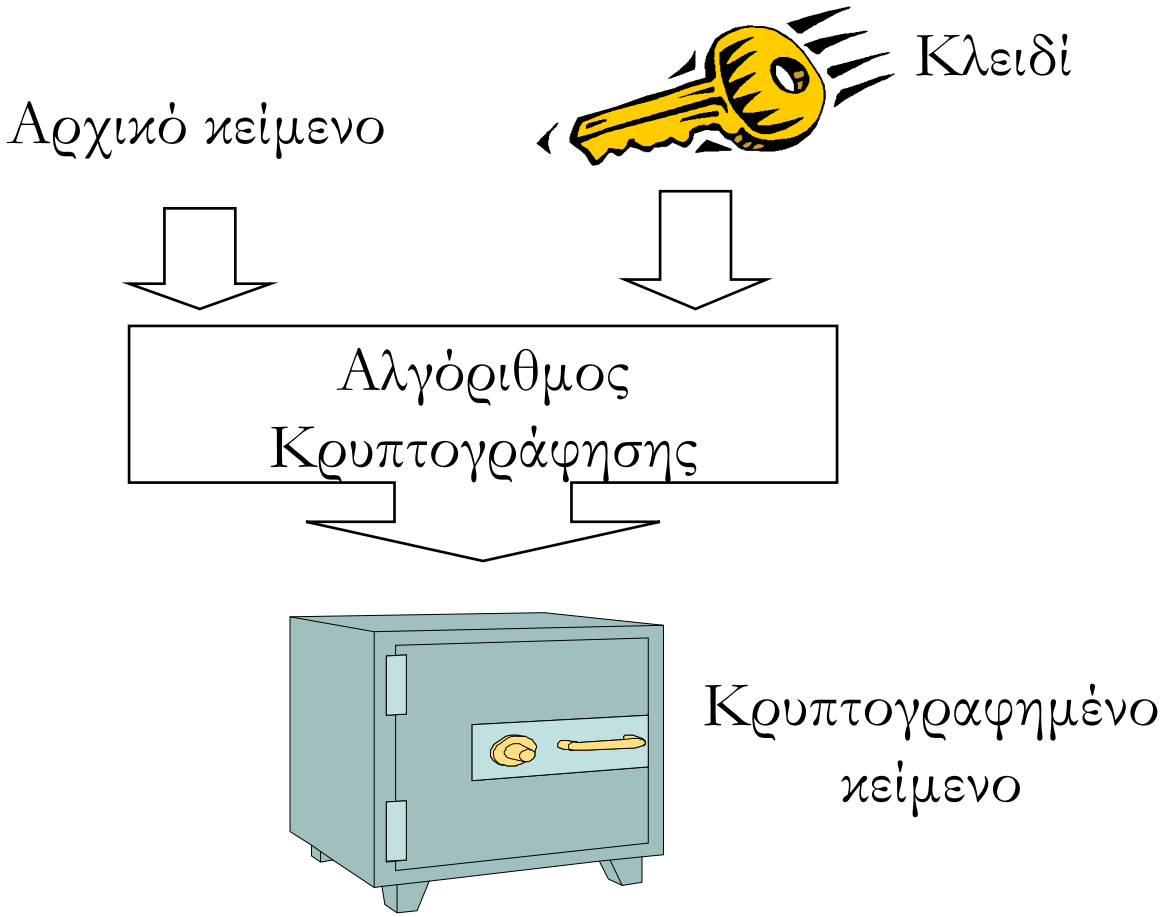
- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης

Κρυπτοσύστημα

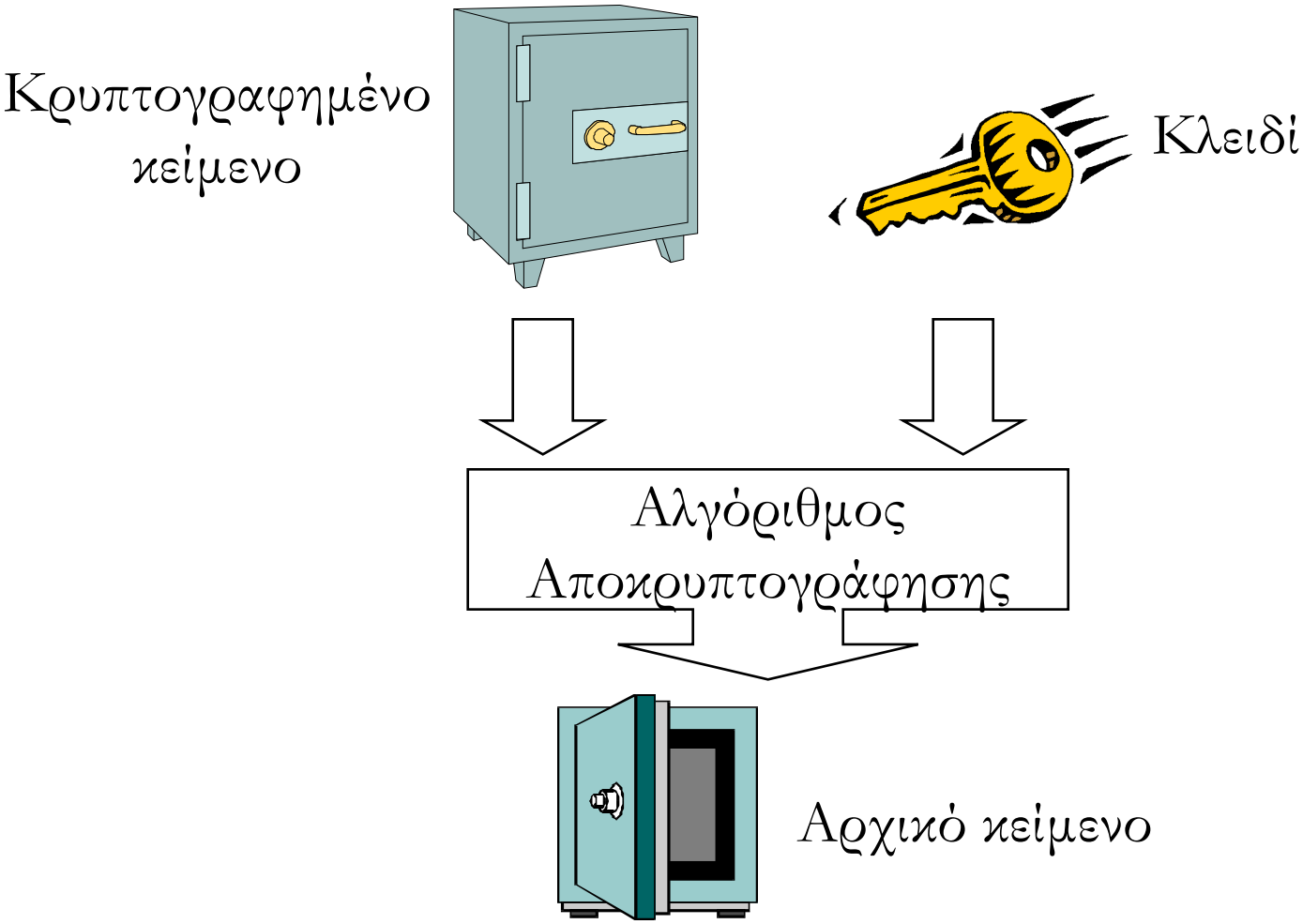


Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει την δυνατότητα σε 2 πρόσωπα να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας επιτιθέμενος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Κρυπτογράφηση



Αποκρυπτογράφηση



Κρυπτογραφία - Αλγόριθμοι

University of Cyprus

Υπάρχουν 2 είδη αλγορίθμων κρυπτογράφησης:

- Συμμετρικοί αλγόριθμοι ή αλγόριθμοι ιδιωτικού κλειδιού

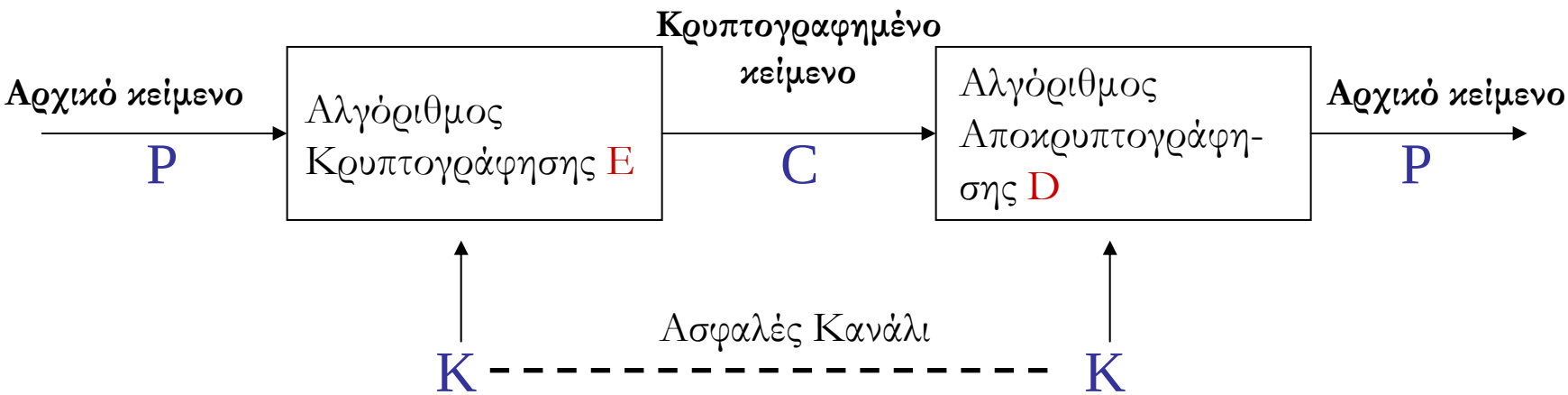
  (symmetric ή secret key).
- Ασύμμετροι αλγόριθμοι ή αλγόριθμοι δημόσιου κλειδιού

  (asymmetric ή public key).

Συμμετρικά Κρυπτοσυστήματα (Ι)

Συμμετρικό κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά την διαδικασία της κρυπτογράφησης-αποκρυπτογράφησης ένα κοινό κλειδί K. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Αλγόριθμοι: Data Encryption Standard (DES), Advanced Encryption Standard (AES)



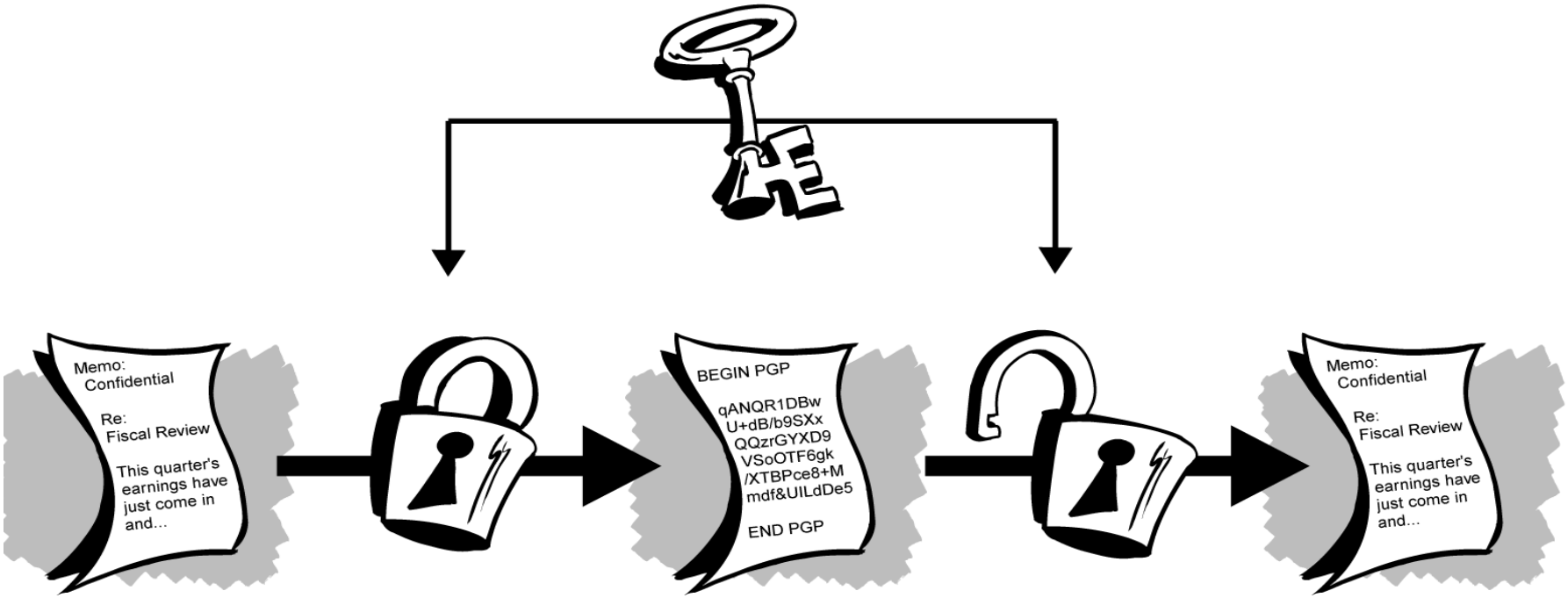
Συμμετρικά Κρυπτοσυστήματα (ΙΙ)

University of Cyprus

Τα στάδια της επικοινωνίας σε ένα Συμμετρικό κρυπτοσύστημα είναι τα ακόλουθα:

1. Ο Bob ή η Alice αποφασίζει για ένα κλειδί το οποίο το επιλέγει τυχαία μέσα από τον κλειδοχώρο.
2. Η Alice αποστέλει το κλειδί στον Bob μέσα από ένα ασφαλές κανάλι.
3. Ο Bob δημιουργεί ένα μήνυμα.
4. Κρυπτογραφεί το μήνυμα με το κλειδί που έλαβε από την Alice και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται.
5. Η Alice λαμβάνει την κρυπτοσυμβολοσειρά και στην συνέχεια με το ίδιο κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

Συμμετρικά Κρυπτοσυστήματα (III)



Ασύμμετρα Κρυπτοσυστήματα (Ι)

University of Cyprus

Ασύμμετρο κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά τη διαδικασία της κρυπτογράφησης-αποκρυπτογράφησης ένα ζεύγος κλειδιού (ιδιωτικό-δημόσιο). Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του Ιδιωτικού μόνο κλειδιού.

Αλγόριθμοι:

RSA (Ron **R**ivest, Adi **S**hamir and Len **A**dleman),

DSA (Digital Signature Algorithm), Diffie-Hellman

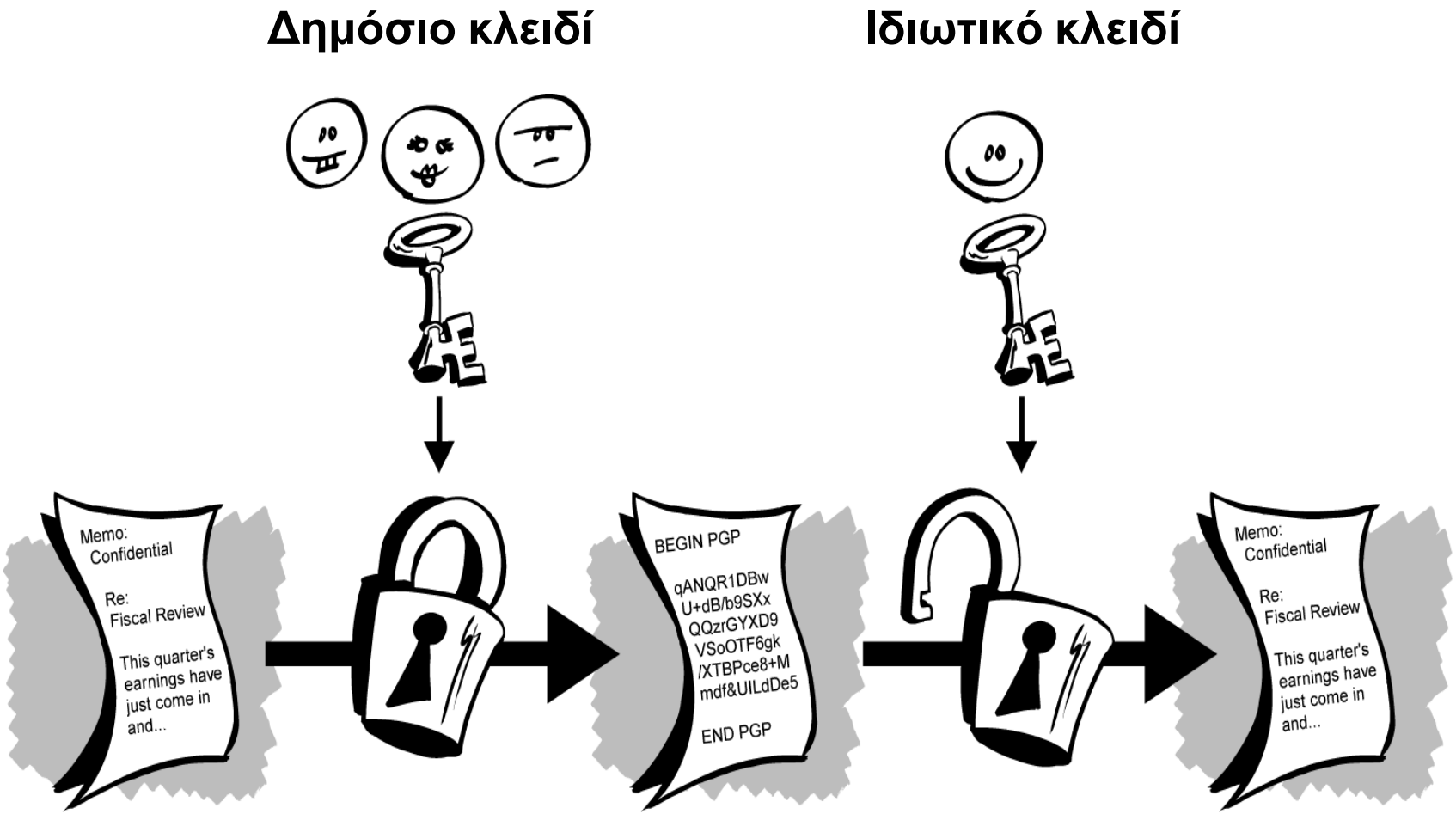
Ασύμμετρα Κρυπτοσυστήματα (ΙΙ)

University of Cyprus

Τα στάδια της επικοινωνίας σε ένα Ασύμμετρο κρυπτοσύστημα είναι τα ακόλουθα:

1. Η γεννήτρια κλειδιών του Bob παράγει 2 ζεύγη κλειδιών,
2. Η γεννήτρια κλειδιών της Alice παράγει 2 ζεύγη κλειδιών
3. Η Alice και ο Bob ανταλλάσσουν τα δημόσια ζεύγη
4. Ο Bob δημιουργεί ένα μήνυμα.
5. Κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί της Alice και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλεται
6. Η Alice λαμβάνει την κρυπτοσυμβολοσειρά και στην συνέχεια με το ιδιωτικό της κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

Ασύμμετρα Κρυπτοσυστήματα (III)



Σύγκριση (I)

University of Cyprus

Πλεονεκτήματα συμμετρικών αλγορίθμων:

- Χαμηλό υπολογιστικό κόστος
- Εύκολη υλοποίηση (hardware)

Μειονεκτήματα συμμετρικών αλγορίθμων:

- Γνωστοποίηση κλειδιού
- Κλιμάκωση

Σύγκριση (ΙΙ)

University of Cyprus

Πλεονεκτήματα ασύμμετρων αλγορίθμων:

- Υψηλή ασφάλεια. Δε χρειάζεται ποτέ να μεταδοθεί ή να αποκαλυφθεί το ιδιωτικό κλειδί
- Αποτελεί μέθοδο για ψηφιακές υπογραφές. Κάποιος μπορεί να επιβεβαιώσει την ταυτότητά του μόνο με το ιδιωτικό του κλειδί → αντιστοιχεί ένα ιδιωτικό κλειδί σε κάθε μοναδικό χρήστη → ένα σύστημα πιστοποίησης ταυτότητας παρέχει «ψηφιακή» εμπιστοσύνη στον κάτοχό του.

Μειονέκτημα ασύμμετρων αλγορίθμων :

- Ταχύτητα κρυπτογράφησης.

Υβριδικά Κρυπτοσυστήματα (Ι)

University of Cyprus

- Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης είναι πιο γρήγοροι από τους ασύμετρους αλγορίθμους

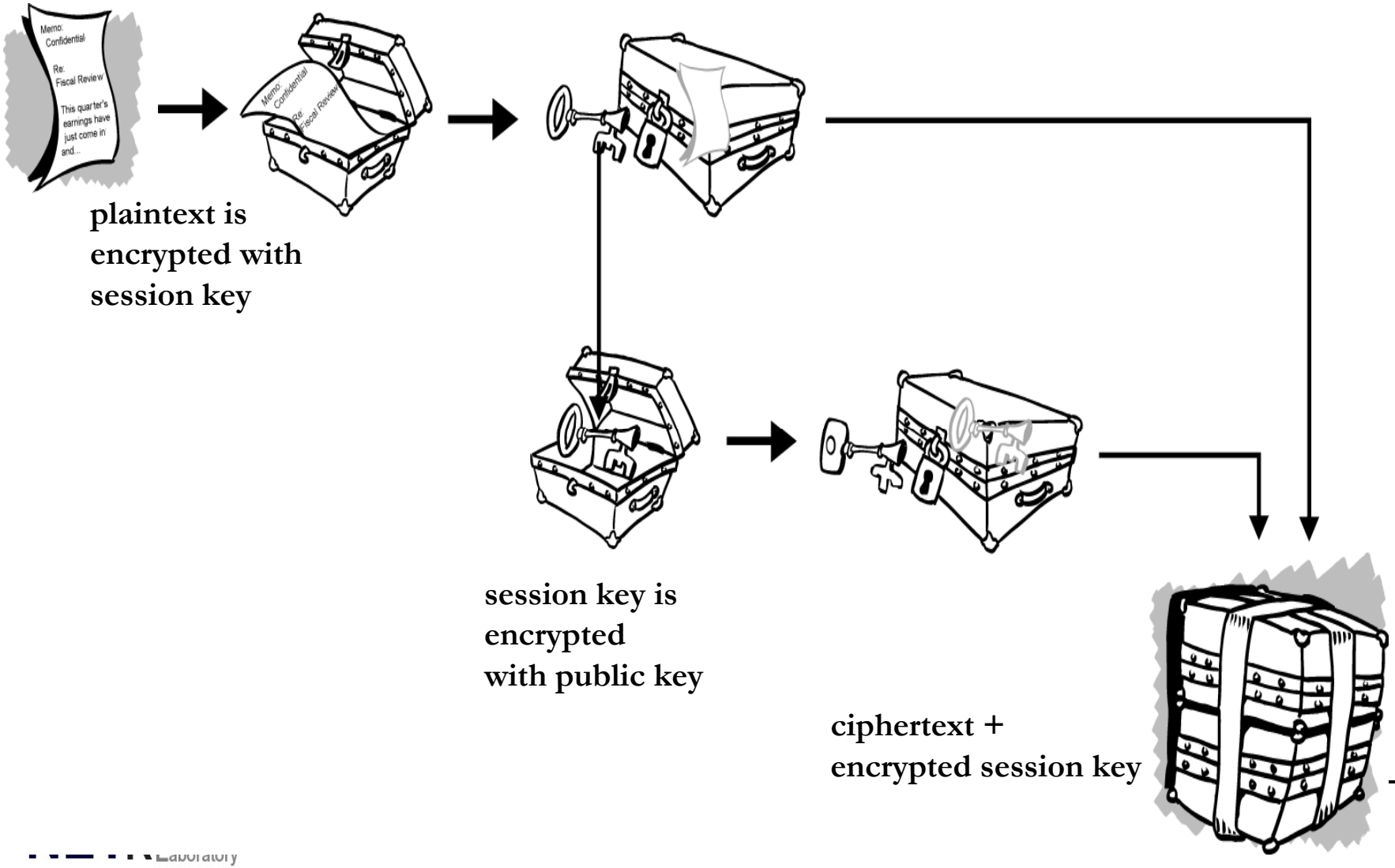
- Σε ένα υβριδικό σύστημα, η Alice χρησιμοποιεί το δημόσιο κλειδί του Bob προκειμένου να του στείλει το μυστικό κλειδί της συνόδου (*session key*)

- Η Alice και ο Bob χρησιμοποιούν το κλειδί της συνόδου για την ανταλλαγή μηνυμάτων

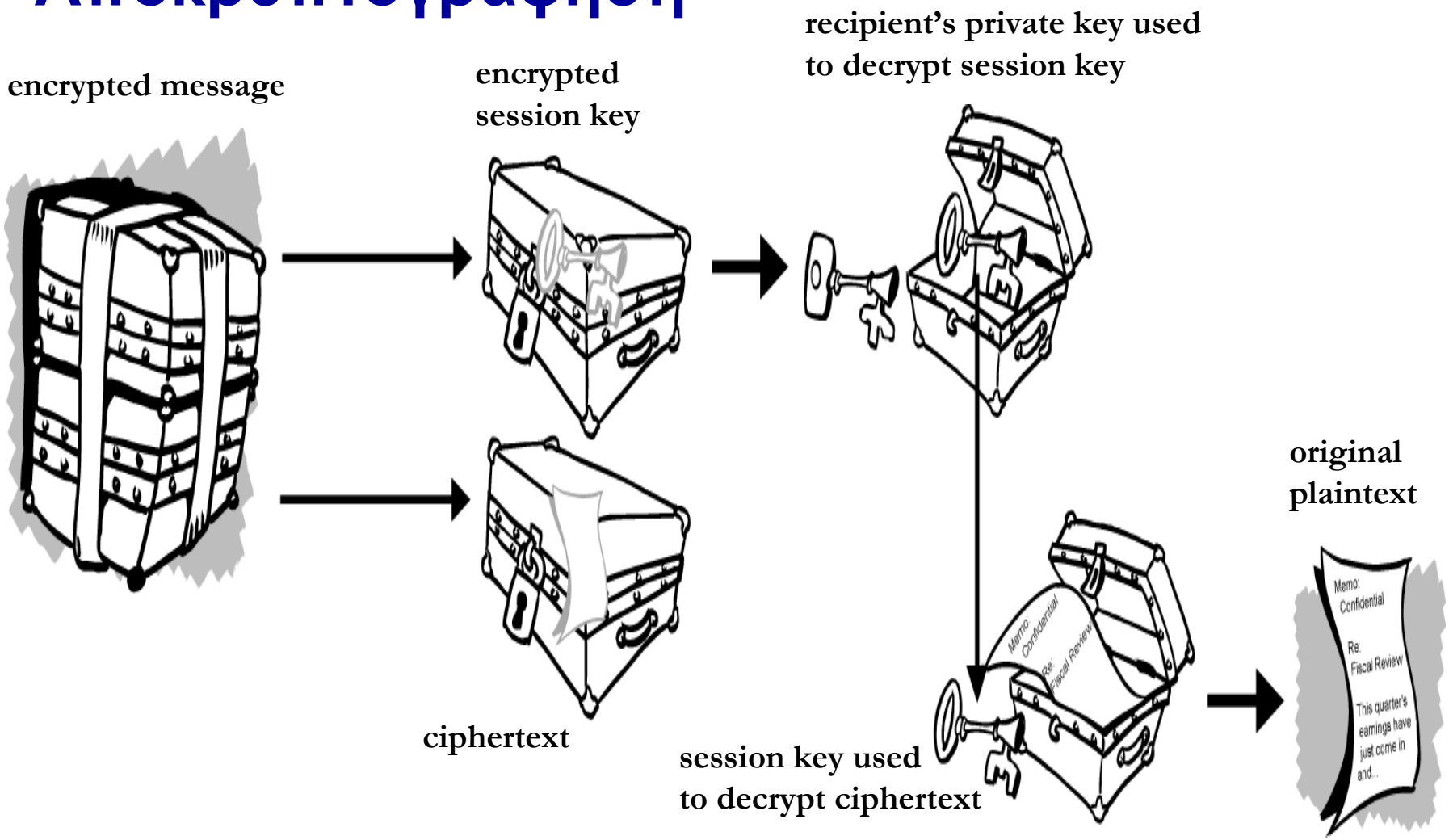
Υβριδικά Κρυπτοσυστήματα (ΙΙ)

1. Ο Bob θέλει να επικοινωνήσει με την Alice διατηρώντας μυστική την επικοινωνία αυτή
2. Η Alice δημιουργεί ένα κλειδί συνόδου, το κρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του Bob και του το αποστέλλει
3. Ο Bob χρησιμοποιεί το ιδιωτικό του κλειδί προκειμένου να ανακτήσει το κλειδί συνόδου, το οποίο και χρησιμοποιεί για την ανταλλαγή μηνυμάτων με την Alice

Παράδειγμα Υβριδικού Κρυπτοσυστήματος - Κρυπτογράφηση



Παράδειγμα Υβριδικού Κρυπτοσυστήματος - Αποκρυπτογράφηση



Αλγοριθμική Ισχύς (I)

- Η αντίσταση των αλγορίθμων κρυπτογράφησης σε παραβιάσεις κάθε μορφής εκφράζεται από την κρυπτογραφική ισχύ (cryptographic strength).
- Θεωρητικά κάθε συμμετρική κρυπτογραφική μέθοδος μπορεί να παραβιαστεί → υπολογίζοντας διαδοχικά όλα τα πιθανά ιδιωτικά κλειδιά → μέθοδος της «βίαιης δύναμης» (brutal force).
- Η υπολογιστική ισχύς που απαιτείται για να υπολογισθούν όλα τα πιθανά κλειδιά αυξάνεται εκθετικά με το μήκος του κλειδιού.

Αλγοριθμική Ισχύς (ΙΙ)

University of Cyprus

- Για να παραβιαστεί ένα σύστημα με κλειδί των 32 bits → συνδυασμός 2^{32} διαφορετικών υποψηφίων κλειδιών → υλοποιείται από ερασιτέχνη.
- Για να παραβιαστεί ένα σύστημα με κλειδί των 40 bits → συνδυασμός 2^{40} διαφορετικών υποψηφίων κλειδιών → υλοποιείται από πανεπιστήμια ή μικρές επιχειρήσεις.
- Για να παραβιαστεί ένα σύστημα με κλειδί των 56 bits → συνδυασμός 2^{56} διαφορετικών υποψηφίων κλειδιών → υλοποιείται από μεγάλες εταιρείες και κυβερνήσεις κρατών.
- Για να παραβιαστεί ένα σύστημα με κλειδί των 64 bits → συνδυασμός 2^{64} διαφορετικών υποψηφίων κλειδιών → υλοποιείται από ισχυρές χώρες.
- Για να παραβιαστεί ένα σύστημα με κλειδί των 80 bits → συνδυασμός 2^{80} διαφορετικών υποψηφίων κλειδιών → υλοποιήσιμο στο άμεσο μέλλον.
- Για να παραβιαστεί ένα σύστημα με κλειδί των 128 bits → συνδυασμός 2^{128} διαφορετικών υποψηφίων κλειδιών → απαραβίαστο στο προβλέψιμο μέλλον.

Αλγοριθμική Ισχύς (III)

University of Cyprus

- Ένας αλγόριθμος που έχει ιδιωτικό κλειδί με μεγάλο μήκος δεν είναι άτρωτος.
- Το μήκος του κλειδιού (δημόσιου και ιδιωτικού) που χρησιμοποιείται στην ασύμμετρη κρυπτογραφία είναι συνήθως πιο μεγάλο από αυτό της συμμετρικής. Παραδείγματα ισχύος:
  - Δημόσιο κλειδί με 384 bits μπορεί να παραβιαστεί από πανεπιστήμια, ερευνητικές ομάδες και εταιρίες.
  - Δημόσιο κλειδί με 512 bits μπορεί να παραβιαστεί από ισχυρές χώρες.
  - Δημόσια κλειδιά με 768 bits είναι προς το παρόν ασφαλή (αλλά προβλέπεται να παραβιαστούν στο άμεσο μέλλον.
  - Συστήματα των 1024 bits είναι στις μέρες μας απαραβίαστα.
  - Συστήματα των 2048 bits είναι στις μέρες μας αλλά και στις επόμενες δεκαετίες απαραβίαστα.

Εφαρμογές Κρυπτογραφίας

University of Cyprus

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία
3. Σταθερή τηλεφωνία (cryptophones)
4. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
5. Διπλωματικά δίκτυα (Τηλεγραφήματα)
6. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
7. Ηλεκτρονική ψηφοφορία
8. Ηλεκτρονική δημοπρασία
9. Ηλεκτρονικό γραμματοκιβώτιο
10. Word Wide Web
11. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
12. Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)
13. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
14. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)