Ασφάλεια Υπολογιστικών Συστημάτων
7ο Εξάμηνο

Εισαγωγή- Βασικές Έννοιες

Διδάσκων : Δρ. Παρασκευάς Κίτσος

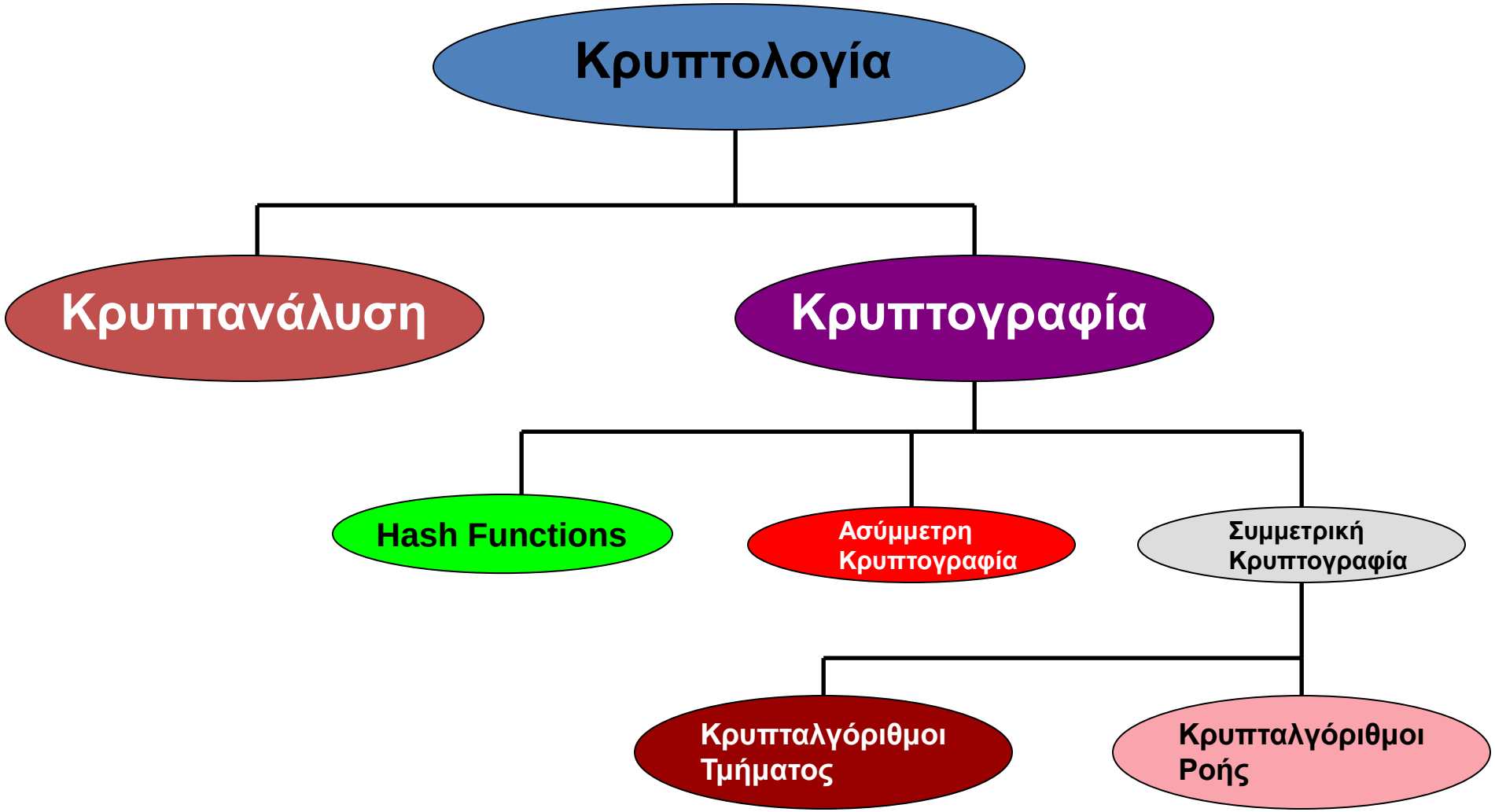
https://ecsalab.ece.uop.gr/

Καθηγητής

Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab.)

e-mail: kitsos@uop.gr

ΤΙ ΕΙΝΑΙ Η ΚΡΥΠΤΟΛΟΓΙΑ? (1/2)



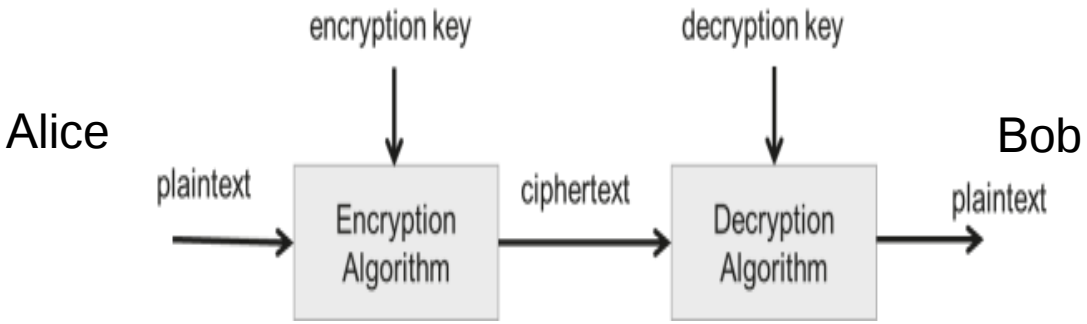
ΤΙ ΕΙΝΑΙ Η ΚΡΥΠΤΟΛΟΓΙΑ? (2/2)

- ***Κρυπτογραφία*** **(*Cryptography*)** είναι η μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα δύσκολο να λυθούν. Ουσιαστικά είναι η επιστήμη που έχει σαν αντικείμενο μελέτης το σύνολο των τεχνικών που αποσκοπούν στην ασφαλή (secure) μετάδοση (transmission) ενός μηνύματος.
- ***Κρυπτανάλυση*** **(*Cryptanalysis*)** είναι η επίλυση αυτών των προβλημάτων.
- ***Κρυπτολογία*** **(*Cryptology*)** είναι ο συνδυασμός της κρυπτογραφίας και κρυπτανάλυσης σε ένα ενιαίο επιστημονικό κλάδο.

ΒΑΣΙΚΟΙ ΟΡΙΣΜΟΙ

- ***Απλό κείμενο*** (***plaintext***) ονομάζεται η αρχική μορφή ενός κειμένου ενώ το κρυπτογραφημένο κείμενο ονομάζεται ***κρυπτοκείμενο*** (***ciphertext***) ή ***κρυπτογράφημα***.
- Ο μετασχηματισμός του απλού κειμένου σε κρυπτοκείμενο ονομάζεται ***κρυπτογράφηση*** (***encryption***) ενώ ο μετασχηματισμός του κρυπτοκειμένου σε απλό κείμενο ονομάζεται ***αποκρυπτογράφηση*** (***decryption***).
- Οι μαθηματικές συναρτήσεις που υλοποιούν τους παραπάνω μετασχηματισμούς ονομάζονται ***αλγόριθμοι κρυπτογράφησης*** και ***αποκρυπτογράφησης*** αντίστοιχα.
- Το ***κλειδί*** (***key***) αποτελεί επιπλέον πληροφορία και χρησιμοποιείται κατά στους παραπάνω μετασχηματισμούς

ΤΥΠΙΚΟ ΚΡΥΠΟΓΡΑΦΙΚΟ ΔΙΑΓΡΑΜΜΑ



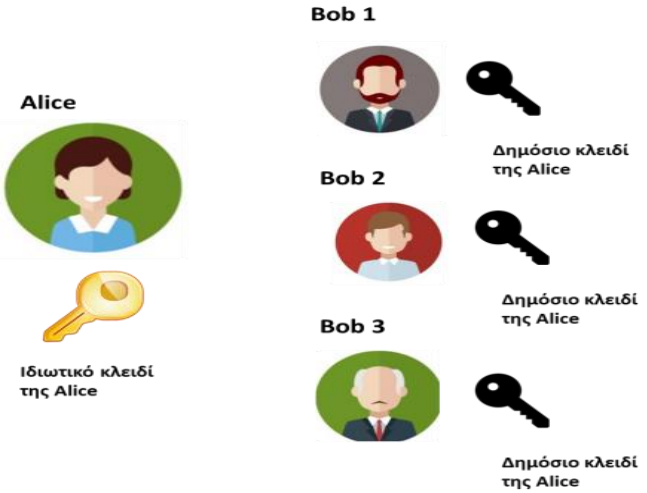
Ο αποστολέας (Alice) επιθυμεί να στείλει μήνυμα σε έναν αποδέκτη (Bob) μέσω ενός προσβάσιμου σε τρίτους καναλιού μετάδοσης (π.χ. Internet) διασφαλίζοντας την εμπιστευτικότητα της μεταδιδόμενης πληροφορίας

- Plaintext: Αρχικό, μη κρυπτογραφημένο κείμενο
- Encryption algorithm: Αλγόριθμος κρυπτογράφησης
- Ciphertext: Κρυπτοκείμενο (η έξοδος τους αλγορίθμου – ακατάληπτο μήνυμα)
- Decryption algorithm: Αλγόριθμος αποκρυπτογράφησης
- Encryption/Decryption key: Κλειδί κρυπτογράφησης/αποκρυπτογράφησης
- Η έξοδος του αλγορίθμου αποκρυπτογράφησης, για δοθέν κρυπτοκείμενο εισόδου και για το σωστό κλειδί αποκρυπτογράφησης, παράγει το αρχικό κείμενο

ΠΟΙΑ Η ΣΧΕΣΗ ΜΕΤΑΞΥ ΤΩΝ ΚΛΕΙΔΙΩΝ?

- Αν ταυτίζονται, αναφερόμαστε σε συμμετρικό αλγόριθμο κρυπτογράφησης
- Αν διαφέρουν, αναφερόμαστε σε ασύμμετρο αλγόριθμο κρυπτογράφησης (ή αλγόριθμο δημοσίου κλειδιού)

Συμμετρική κρυπτογράφηση: Μόνο η Alice και ο Bob γνωρίζουν το κοινό μυστικό κλειδί

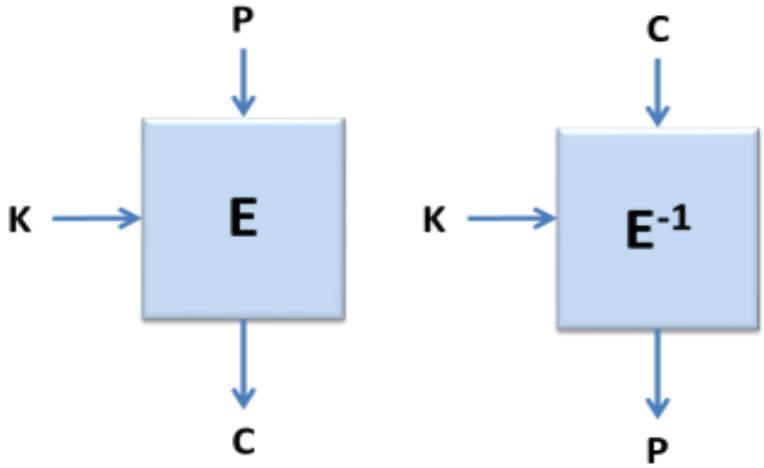


Ασύμμετρη κρυπτογράφηση: Όλοι γνωρίζουν το κλειδί κρυπτογράφησης για την Alice (δημόσιο), αλλά μόνο η Alice γνωρίζει το κλειδί αποκρυπτογράφησης (ιδιωτικό)

ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ

ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΣ ΤΜΗΜΑΤΟΣ (BLOCK CIPHER)

- Ο κρυπτογραφικός αλγόριθμος επενεργεί σε τμήματα (blocks) του μηνύματος, σταθερού μεγέθους (που καθορίζεται από τον αλγόριθμο)
- Κάθε τμήμα (block) μηνύματος εισόδου μετασχηματίζεται, μέσω του αλγόριθμου κρυπτογράφησης Ε, σε ένα τμήμα (block) κρυπτοκειμένου. Ο αντίστροφος μετασχηματισμός γίνεται στην αποκρυπτογράφηση
- Ουσιαστικά, συνιστά μία οικογένεια αντικαταστάσεων blocks από άλλα blocks
  - Το κλειδί k καθορίζει κάθε φορά την αντικατάσταση
  - Η σχέση εισόδων και εξόδων είναι ένα-προς-ένα και επί



ΠΡΟΤΥΠΟΙ ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΙ ΤΜΗΜΑΤΟΣ

- Οργανισμός NIST (National Institute of Standards and Technology): Έκδοση καθολικά αποδεκτών προτύπων κρυπτογραφικών δομικών στοιχείων
- Για κρυπταλγόριθμο τμήματος:
  - Αλγόριθμος DES (Data Encryption Standard): Αποτέλεσε πρότυπο από το 1976 και για περίπου δύο δεκαετίες
    - Αποσύρθηκε επίσημα το 2004 (μη ασφαλής σήμερα)
  - Αλγόριθμος AES (Advanced Encryption Standard): Πρότυπο κρυπταλγόριθμου τμήματος από το 2001 μέχρι και σήμερα
    - Τρία πιθανά μεγέθη κλειδιών: 128, 192 και 256 bits
    - Μέγεθος block: 128 bits

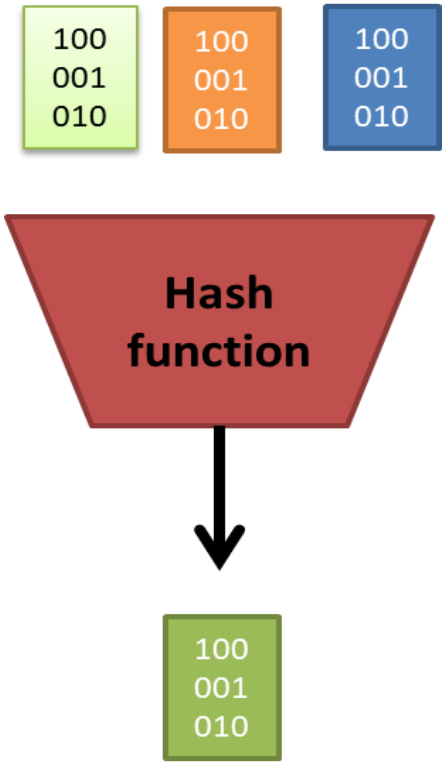
ΓΝΩΣΤΟΙ ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΙ ΤΜΗΜΑΤΟΣ

Κρυπταλγόριθμος τμήματος	Χρήση σήμερα	Χρήση στο μέλλον
AES	✓	✓
Camellia	✓	✓
3-DES (3 keys)	✓	✓
3-DES (2 keys)	✓	✗
Kasumi	✓	✗
RIPEMD-160	✓	✗
Blowfish	✓	✗
DES	✗	✗

Πηγή: Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ENISA)

Ο πίνακας αυτός επικαιροποιείται – για παράδειγμα, ο οργανισμός NIST θεωρεί ήδη ότι ο 3-DES με δύο κλειδιά (2 x 56 = 112 bits) δεν πρέπει να χρησιμοποιείται, ενώ δεν δίνει μεγάλη διάρκεια ζωής ούτε για τον 3-DES με τρία κλειδιά

ΚΡΥΠΤΟΓΡΑΦΙΚΗ ΣΥΝΑΡΤΗΣΗ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ (HASH FUNCTION)



- Δεδομένα αυθαίρετου μεγέθους στην είσοδο μετασχηματίζονται σε σταθερού μεγέθους δεδομένα στην έξοδο
  - Η έξοδος (τιμή κατακερματισμού) ονομάζεται και «αποτύπωμα» ή «σύνοψη» του μηνύματος
  - Τυπικά μεγέθη: εξόδου 128 bits, 256 bits
- Συνάρτηση μίας κατεύθυνσης (one-way): Δεδομένης της εξόδου, δεν μπορεί να υπολογιστεί η είσοδος
- Το μόνο κρυπτογραφικό δομικό στοιχείο που δεν χρειάζεται κλειδί (key) για τη λειτουργία του
  - Η ίδια είσοδος έχει πάντα το ίδιο αποτύπωμα (ίδια έξοδο)

ΠΡΟΤΥΠΑ ΣΥΝΑΡΤΗΣΕΩΝ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ

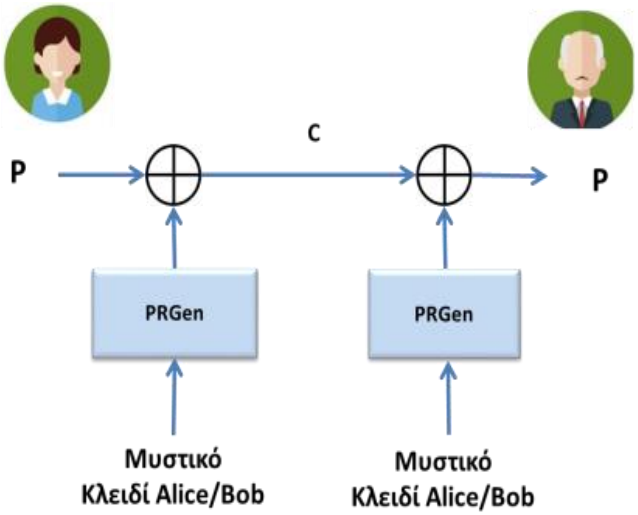
- Secure Hash Algorithm – 1 (SHA-1): Αποτέλεσε πρότυπο από το 1995 και για περίπου δύο δεκαετίες
  - Από το 2015 ο NIST ανακοίνωσε την επικείμενη απόσυρσή του. Πρακτικά, έπαψε να θεωρείται ασφαλής, λόγω επιθέσεων που επετεύχθηκαν, το 2017
- Secure Hash Algorithm – 2 (SHA-2): Πρόκειται για οικογένεια συναρτήσεων, με διάφορα μεγέθη εξόδου, που αποτελεί πρότυπο από το 2002
  - Ασφαλής μέχρι σήμερα
- Secure Hash Algorithm – 3 (SHA-3): Πρόκειται για οικογένεια συναρτήσεων, με διάφορα μεγέθη εξόδου, που αποτελεί το πιο πρόσφατο πρότυπο από το 2012

ΓΝΩΣΤΕΣ ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ

Συνάρτηση κατακερματισμού	Μέγεθος Εξόδου	Χρήση σήμερα	Χρήση στο μέλλον
SHA-2	256, 384, 512	✓	✓
SHA-3	256, 384, 512	✓	✓
Whirlpool	512	✓	✓
SHA-2	224	✓	✗
SHA-3	224	✓	✗
RIPEMD-160	160	✓	✗
SHA-1	160	✗	✗
MD-5	128	✗	✗
RIPEMD-128	128	✗	✗

Πηγή: Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ENISA)

ΓΕΝΝΗΤΡΙΕΣ ΨΕΥΔΟΤΥΧΑΙΩΝ ΑΚΟΛΟΥΘΙΩΝ (PSEUDORANDOM SEQUENCE GENERATORS)



- Παραγωγή ακολουθιών από bits που προσομοιάζουν μία γνήσια τυχαία ακολουθία
  - Αν και παράγονται από ντετερμινιστικά συστήματα
- Βασική χρήση: Κρυπταλγόριθμοι ροής (stream ciphers)
  - Η κρυπτογράφηση/αποκρυπτογράφηση προκύπτει με δυαδική (XOR) πρόσθεση, bit προς bit, του μηνύματος/κρυπτοκειμένου με την ψευδοτυχαία ακολουθία
  - Μυστικό (συμμετρικό) κλειδί χρησιμοποιείται για την αρχικοποίηση της γεννήτριας

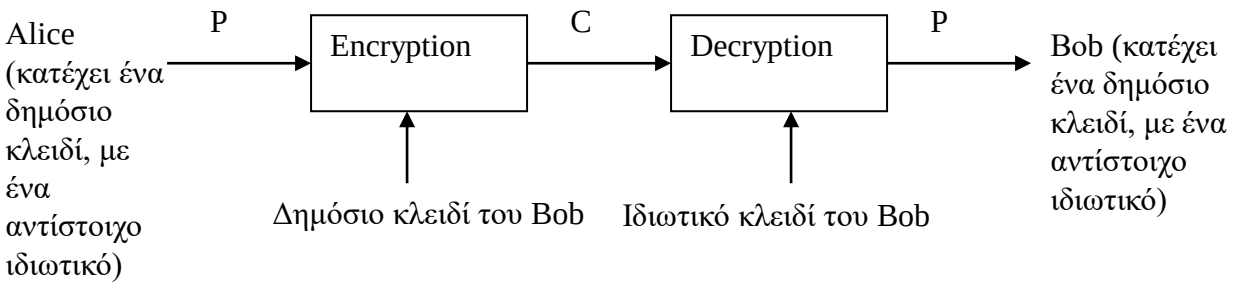
ΓΝΩΣΤΟΙ ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΙ ΡΟΗΣ

Γεννήτρια ψευδοτυχαίων αριθμών	Χρήση σήμερα	Χρήση στο μέλλον
HC-128	✓	✓
Cha Cha	✓	✓
Salsa20/20	✓	✓
SNOW 3G, 2.0	✓	✓
SOSEMANUK	✓	✓
Grain	✓	✗
Trivium	✓	✗
Mickey 2.0	✓	✗
A5/1, A5/2	✗	✗
RC4	✗	✗
Moustique	✗	✗

Πηγή: Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ENISA)

Ο πίνακας αυτός επικαιροποιείται, ενώ πολλοί κρυπταλγόριθμοι προσαρμόζονται – για παράδειγμα, ο Grain έχει ήδη αναπροσαρμοστεί και εξετάζεται το ενδεχόμενο προτυποποίησης της νέας του έκδοσης, από το NIST, ως lightweight κρυπταλγόριθμο

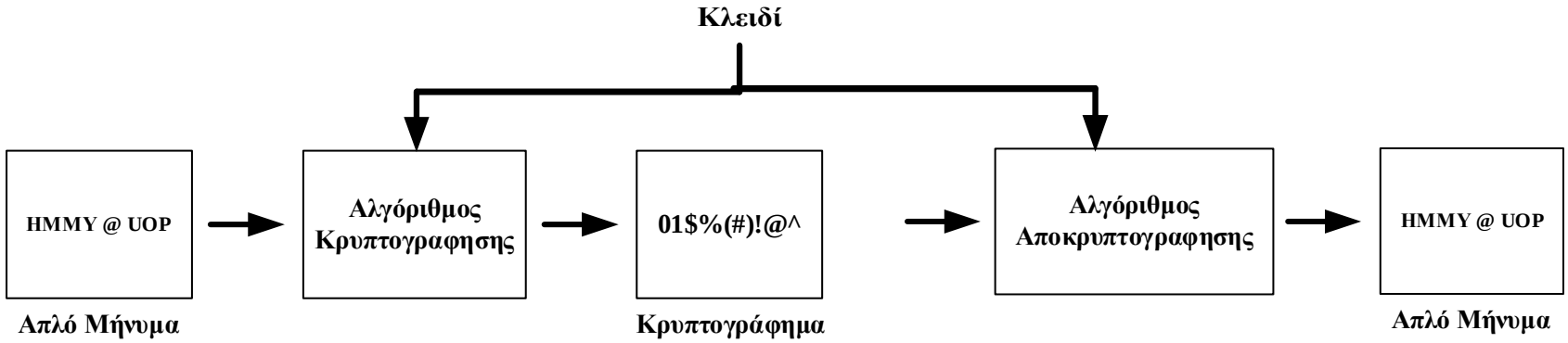
ΑΛΓΟΡΙΘΜΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ



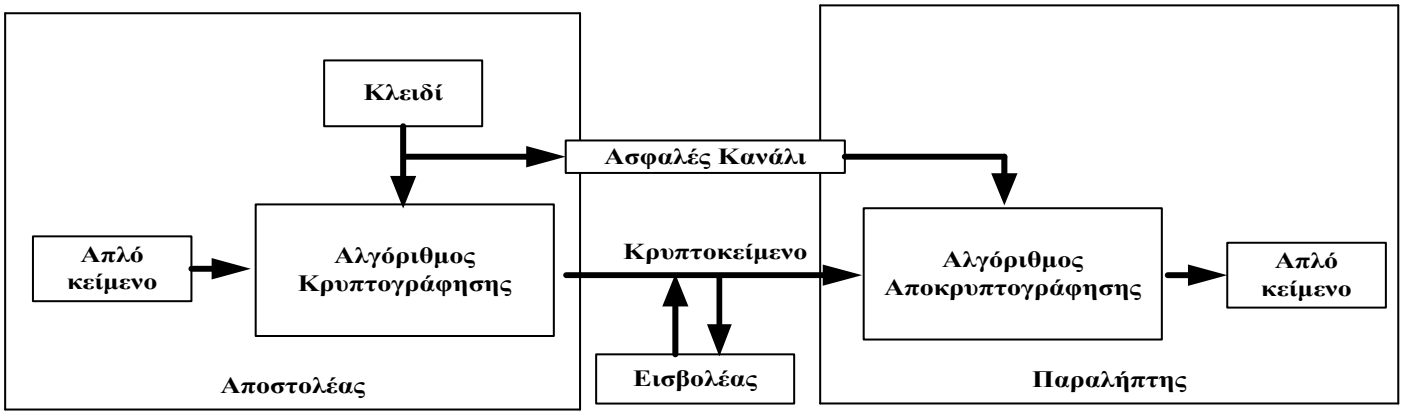
- Η ασφάλειά τους βασίζεται στην εγγενή δυσκολία γνωστών μαθηματικών προβλημάτων
- Προτάθηκαν πρώτη φορά από τους Diffie και Hellman το 1976
  - Ο αλγόριθμος των Diffie-Hellman βασίζει την ασφάλειά του στο λεγόμενο πρόβλημα διακριτού λογαρίθμου (Discrete Logarithm Problem – DLP)
  - Η επέκταση του προβλήματος αυτού στις ελλειπτικές καμπύλες (Elliptic Curve Discrete Logarithm Problem - ECDLP) δημιουργεί μία νέα οικογένεια αλγορίθμων, με το όνομα αλγόριθμοι ελλειπτικής καμπύλης
  - Ο πολύ γνωστός αλγόριθμος RSA βασίζει την ασφάλειά του στο λεγόμενο πρόβλημα παραγοντοποίησης (Factorisation Problem)

ΑΛΓΟΡΙΘΜΟΙ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ

- Οι ***αλγόριθμοι ιδιωτικού κλειδιού*** (***secret key algorithms***) χρησιμοποιούν το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση. Ονομάζονται και ***συμμετρικοί αλγόριθμοι (symmetric algorithms).***



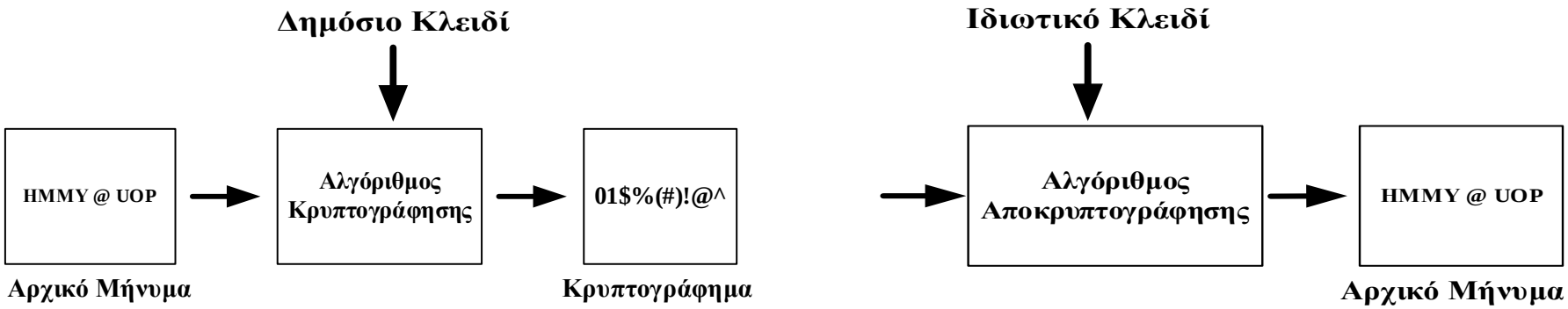
ΜΟΝΤΕΛΟ ΕΠΙΚΟΙΝΩΝΙΑΣ



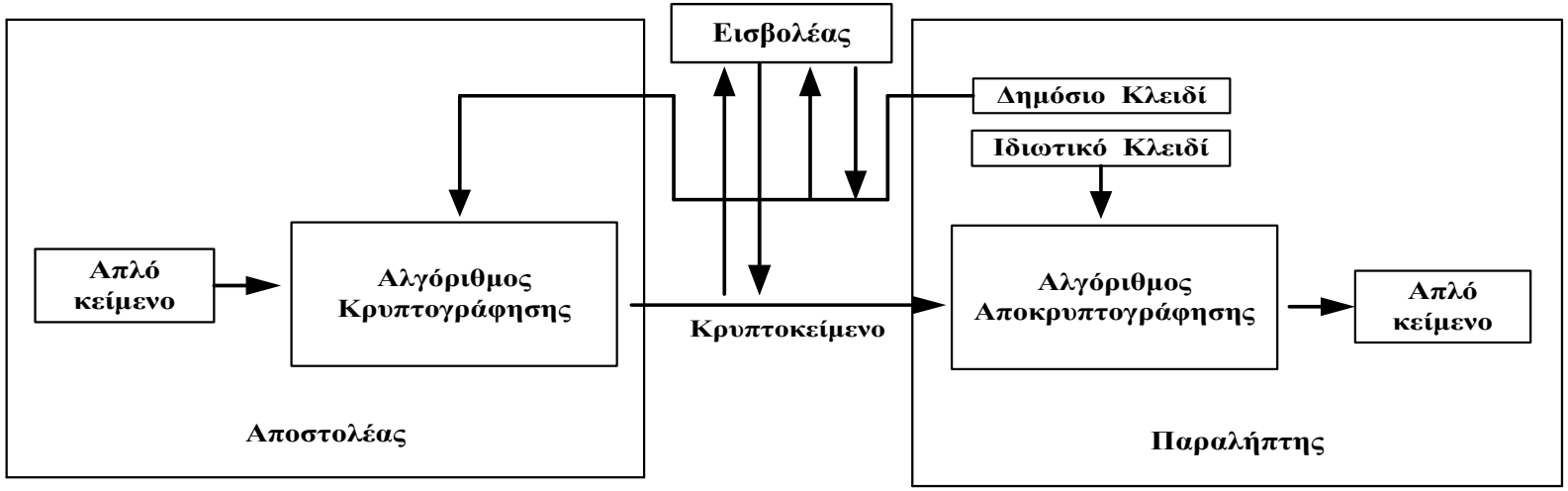
- Ασφάλεια στην μετάδοση του κλειδιού
- Ύπαρξη ασφαλούς καναλιού

ΑΛΓΟΡΙΘΜΟΙ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

- Οι ***αλγόριθμοι δημοσίου κλειδιού*** (***public key algorithms***) χρησιμοποιούν το ***δημόσιο κλειδί*** (***public key***) για την κρυπτογράφηση και το ιδιωτικό κλειδί (***private key***) για την αποκρυπτογραφηση. Ονομάζονται και ***ασύμμετροι αλγόριθμοι (asymmetric algorithms).***



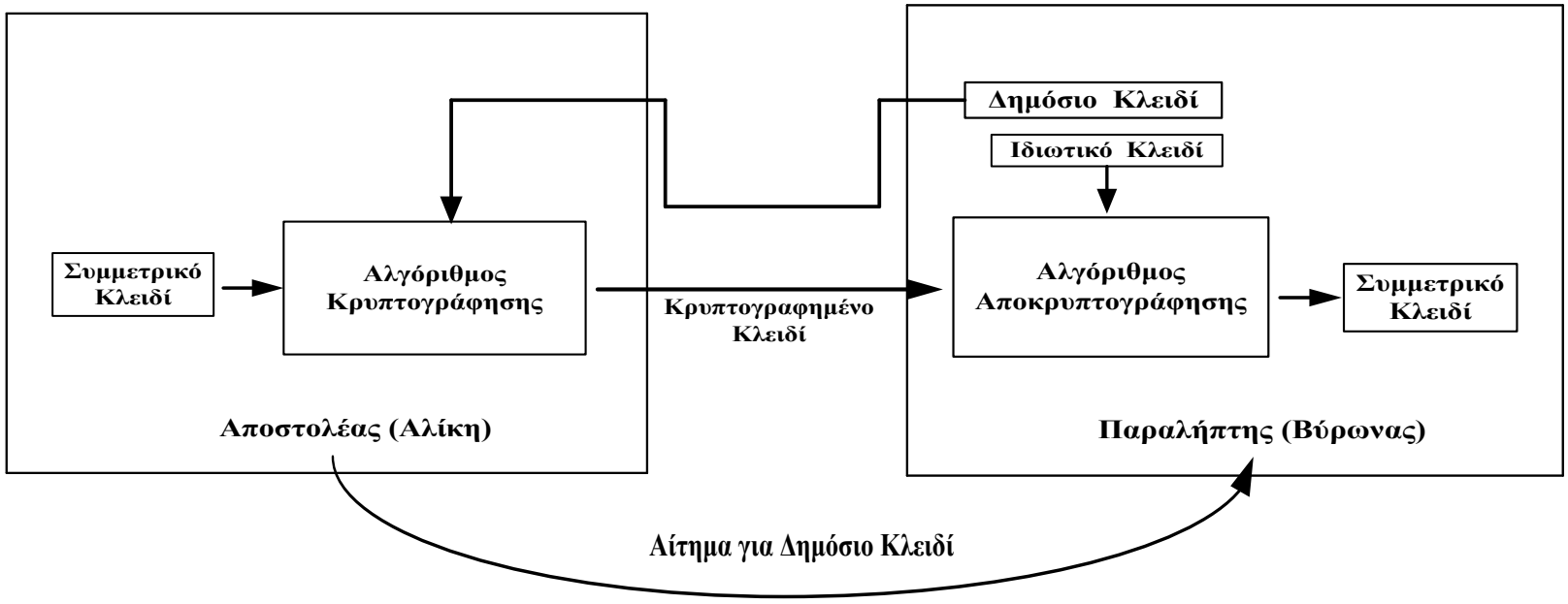
ΜΟΝΤΕΛΟ ΕΠΙΚΟΙΝΩΝΙΑΣ



- Τα δύο κλειδιά παράγονται από τον παραλήπτη
- Δεν απαιτείται ασφαλές κανάλι

ΚΡΥΠΤΟΓΡΑΦΙΚΟ ΠΡΩΤΟΚΟΛΛΟ

Είναι μια πλήρως καθορισμένη και αποσαφηνισμένη διαδικασία που πρέπει να ακολουθήσουν τα μέλη που επικοινωνούν έτσι ώστε να επιτύχουν μια συγκεκριμένη κρυπτογραφική υπηρεσία.



ΕΠΙΘΕΣΕΙΣ, ΜΗΧΑΝΙΣΜΟΙ & ΥΠΗΡΕΣΙΕΣ

- **Security Attack (Επίθεση Ασφάλειας)**

  Οποιαδήποτε ενέργεια η οποία υπονομεύει (στοχεύει) να πλήξει την ασφάλεια της πληροφορίας

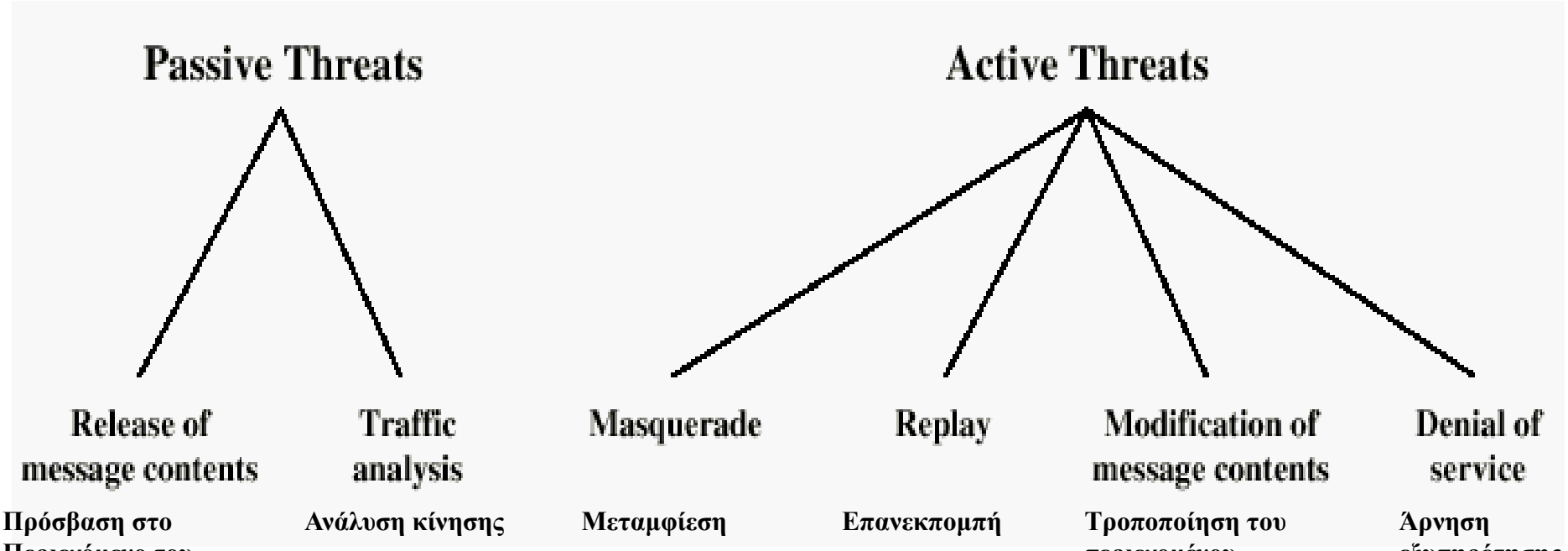
- **Security Mechanism (Μηχανισμός Ασφάλειας)**

  Μηχανισμός που έχει σχεδιαστεί για ανίχνευση (detect), προστασία (prevent) ή επαναφορά (recover) στην ομαλή λειτουργία ενός συστήματος μετά από κάποια επίθεση

- **Security Service (Υπηρεσία Ασφάλειας)**
  - Μία υπηρεσία που βελτιώνει την ασφάλεια των συστημάτων επεξεργασίας δεδομένων, καθώς και των μεταδιδόμενων πληροφοριών
  - Μια υπηρεσία ασφαλείας (security service) χρησιμοποιεί έναν ή και περισσότερους μηχανισμούς ασφάλειας

ΕΝΕΡΓΗΤΙΚΕΣ ΚΑΙ ΠΑΘΗΤΙΚΕΣ ΕΠΙΘΕΣΕΙΣ

- **Παθητικές επιθέσεις (Passive):** Προσπαθούν να μάθουν ή να χρησιμοποιήσουν πληροφορίες χωρίς να επηρεάσουν τους πόρους του συστήματος
- **Ενεργητικές επιθέσεις (Active):** Προσπαθούν να μεταβάλλουν τους πόρους του συστήματος ή να επηρεάσουν τη λειτουργία του



ΣΤΟΧΟΙ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (ΥΠΗΡΕΣΙΕΣ)

- **Εμπιστευτικότητα** (***Confidentiality***): εξασφαλίζει ότι η πληροφορία που ανταλλάσσεται δεν θα αποκαλυφθεί σε μη-εξουσιοδοτημένες πλευρές
- **Ακεραιότητα** (***Integrity***): στην οποία εξασφαλίζεται ότι τα δεδομένα δε θα αλλοιωθούν κατά την μεταφορά τους
- **Πιστοποίηση Ταυτότητας** (***Authentication***): εξασφαλίζει την ταυτότητα των επικοινωνούντων πλευρών
- **Μη Απάρνηση** (***Non-reputation***): ο αποστολέας δεν μπορεί να αρνηθεί ότι έστειλε το μήνυμα ή ο παραλήπτης δεν μπορεί να αρνηθεί ότι έλαβε το μήνυμα

ΤΥΠΙΚΟΣ ΧΡΟΝΟΣ ΠΑΡΑΒΙΑΣΗΣ ΣΥΝΘΗΜΑΤΙΚΟΥ

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

ΜΕΣΑ ΠΑΡΑΒΙΑΣΗΣ

- Graphics Processing Units (GPUs)
- Nvidia's GeForce RTX 4090 (~1500 ευρώ)
- Νοικιάζοντας πόρους από το cloud
- Νέες τεχνολογίες
  - AI (έρευνα από το Home Security Heroes το 2023 κατέδειξε ότι αναλύθηκαν 15,600,000 και επαληθεύθηκαν με χρήση AI, το 81% σε ένα μήνα, το 71% σε λιγότερο από μια μέρα, το 65% σε λιγότερο από μια ώρα και το 51% σε λιγότερο από ένα λεπτό

ECSALab

Απορίες???