ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

# ΜΕΤΩΝ

## Ενότητα 13b: e-επιχειρηματικότητα και ασφάλεια

Διδάσκων: Γιάννης Σταματίου

Σχολή Οικονομικών Επιστημών και Διοίκησης Επιχειρήσεων

Τμήμα Διοίκησης Επιχειρήσεων

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού,
Εκπαίδευση και Διά Βίου Μάθηση
Ειδική Υπηρεσία Διαχείρισης
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

# Σκοποί ενότητας

- Να παρουσιάσει τις έννοιες της ασφάλειας πληροφοριακών συστημάτων και προστασίας της ιδιωτικότητας του ατόμου
- Να αναφέρει τις κυριότερες απειλές και μερικές βασικές στρατηγικές αντιμετώπισής τους
- Να αναδείξει κάποιες τεχνικές και τεχνολογικές προσεγγίσεις άμυνας
- Να εξηγήσει τους μελλοντικούς κινδύνους ως συνάρτηση των τεχνολογικών εξελίξεων

# Περιεχόμενα ενότητας

1. Τεχνολογικές εξελίξεις και Ψηφιακός Μετασχηματισμός
2. Οι κίνδυνοι για την ασφάλεια πληροφοριακών συστημάτων και την ιδιωτικότητα του ατόμου – γενικές πολιτικές άμυνας
3. Μερικές προσεγγίσεις κατά των απειλών της ασφάλειας πληροφοριακών συστημάτων και της προστασίας της ιδιωτικότητας
4. Οι (όχι και τόσο) μελλοντικοί κίνδυνοι

# Τεχνολογικές εξελίξεις και Ψηφιακός Μετασχηματισμός

# Ψηφιακός Μετασχηματισμός : οι νέες τεχνολογίες στην υπηρεσία του ανθρώπου και των δραστηριοτήτων του

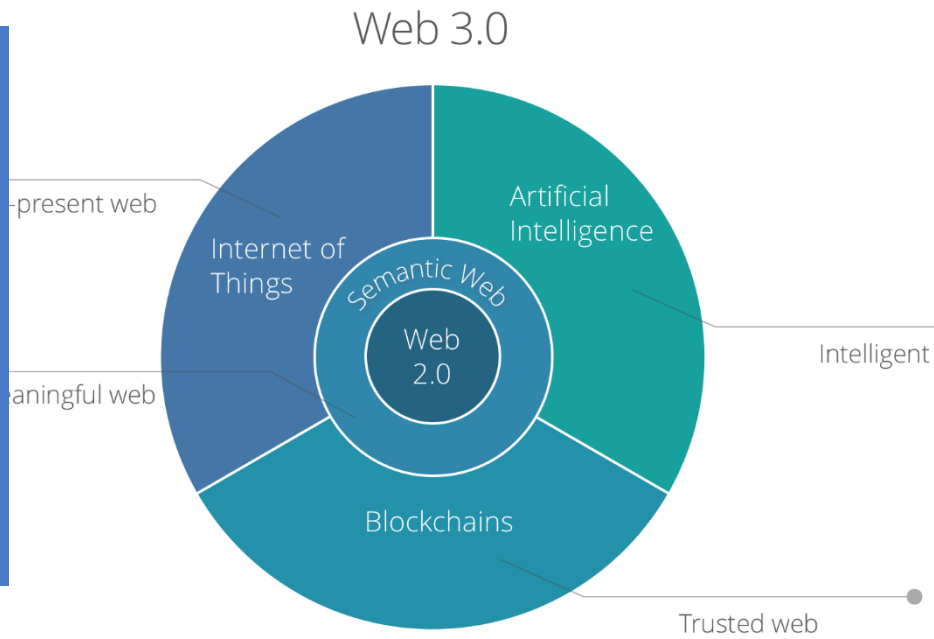
Διανύουμε μία περίοδο δραματικού μετασχηματισμού του Διαδικτύου στο Διαδίκτυο των Πραγμάτων: Άνθρωποι και Μηχανές κάθε είδους και δυνατοτήτων – πλήθος νέων υπηρεσιών

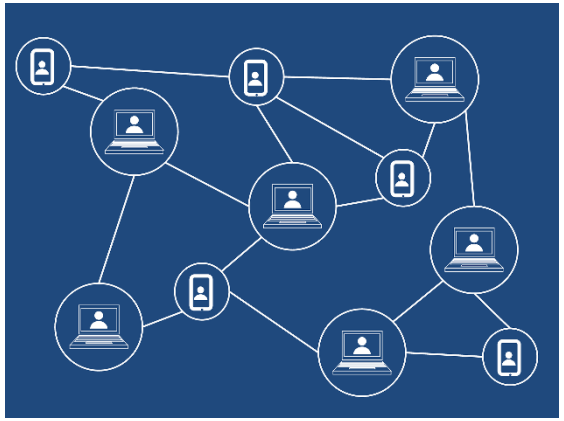
- eParticipation
- eDemocracy
- eCommerce
- eTaxation
- eBusiness
- eLearning/eEducation
- eVoting
- eHealth and Telemedicine
- eJustice
- eAuction
- eProcurement
- “Life events” management
- «ΔΙΑΥΓΕΙΑ»
- «ΠΟΘΕΝ ΕΣΧΕΣ»

- Information Society
- Interoperability
- BackOffice/Front Office
- e-shops
- e-services
- e-Identification
- e-Authentication
- Security
- Personalisation
- Broadband Communication
- G2C, G2B, G2G, G2E, B2B, B2C, B2E

**Το όχημα; οι ΤΠΕ (ουσιαστικά, οι υπολογιστικές/τηλεπικοινωνιακές συσκευές και το Διαδίκτυο/Παγκόσμιος Ιστός)**

# Το επερχόμενο <<κύμα> καινοτομίας που ο Ψηφιακός Μετασχηματισμός δεν πρέπει να χάσει!



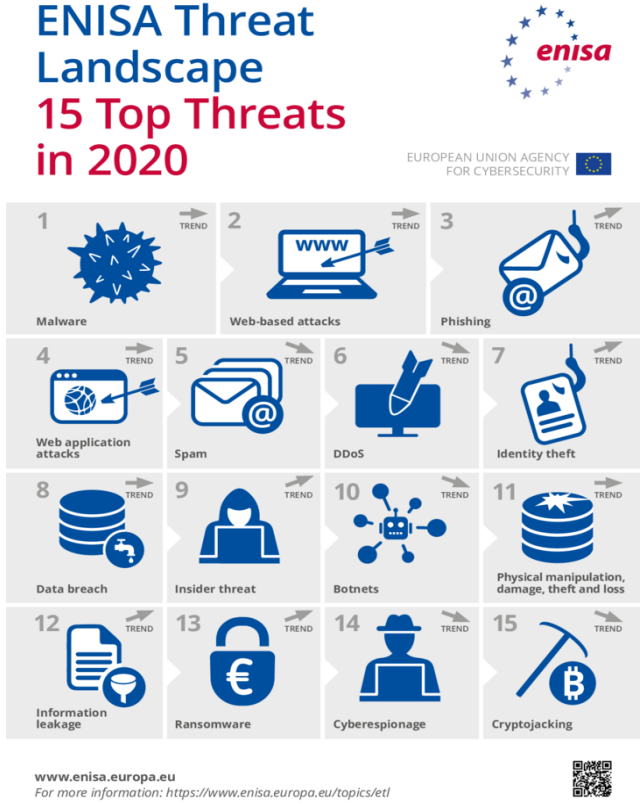
# Οι κίνδυνοι για την ασφάλεια πληροφοριακών συστημάτων και την ιδιωτικότητα του ατόμου – γενικές πολιτικές άμυνας

# ENISA (Ευρωπαϊκός Οργανισμός για την Ασφάλεια των Δικτύων και των Πληροφοριών) Top 15 Indicators

**European Network and Information Security Agency**

| Top Threats 2017 | Assessed Trends 2017 | Top Threats 2018 | Assessed Trends 2018 | Change in ranking |
|---|---|---|---|---|
| 1. Malware | ➲ | 1. Malware | ➲ | → |
| 2. Web Based Attacks | ↑ | 2. Web Based Attacks | ↑ | → |
| 3. Web Application Attacks | ↑ | 3. Web Application Attacks | ➲ | → |
| 4. Phishing | ↑ | 4. Phishing | ↑ | → |
| 5. Spam | ↑ | 5. Denial of Service | ↑ | ↑ |
| 6. Denial of Service | ↑ | 6. Spam | ➲ | ↓ |
| 7. Ransomware | ↑ | 7. Botnets | ↑ | ↑ |
| 8. Botnets | ↑ | 8. Data Breaches | ↑ | ↑ |
| 9. Insider threat | ➲ | 9. Insider Threat | ↓ | → |
| 10. Physical manipulation/ damage/ theft/loss | ➲ | 10. Physical manipulation/ damage/ theft/loss | ➲ | → |
| 11. Data Breaches | ↑ | 11. Information Leakage | ↑ | ↑ |
| 12. Identity Theft | ↑ | 12. Identity Theft | ↑ | → |
| 13. Information Leakage | ↑ | 13. Cryptojacking | ↑ | NEW |
| 14. Exploit Kits | ↓ | 14. Ransomware | ↓ | ↓ |
| 15. Cyber Espionage | ↑ | 15. Cyber Espionage | ↓ | → |

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down




*Πηγή: ENISA, CC BY 4.0*

# Τι αλλάζει στο τοπίο της Κυβερνοασφάλειας για τον σύγχρονο Ψηφιακό Μετασχηματισμό;

- Edge computing: διεύρυνση της *επιφάνειας επιθέσεων* (attack surface)
- IoT: εμφάνιση, στο τοπίο, συσκευών κάθε είδους και δυνατοτήτων με, συνήθως, μικρή έως ανύπαρκτη αντοχή απέναντι σε κυβερνοεπιθέσεις
- Web 3.0: ανυπολόγιστος αριθμών πληροφοριών και «ανώνυμων» ιχνών δομημένα για επεξεργασία από υπερυπολογιστές με στόχο την εξαγωγή συμπερασμάτων
- AI (Artificial Intelligence): ο ψηφιακός υπόκοσμος χρησιμοποιεί, όλο και περισσότερο, μεθόδους της Τεχνητής Νοημοσύνης για να ανιχνεύσει στόχους και να εξαπολύσει «έξυπνες» επιθέσεις
- APTs (Advanced Persistent Threats): οργανωμένη, επίμονη εφαρμογή μιας μεγάλης γκάμας κακόβουλου λογισμικού και τεχνολογιών εισβολής σε επιλεγμένους στόχους, συνήθως επιχειρηματικούς ή κυβερνητικούς
- Μεγάλη πολυπλοκότητα στην ανάλυση και θωράκιση των υποδομών: πολλές διαφορετικές συσκευές, πολλοί δίαυλοι επικοινωνίας και τηλεπικοινωνιακά πρωτόκολλα, μεγάλο πλήθος προσωπικών δεδομένων κάθε τύπου σε διασκορπισμένα πληροφοριακά συστήματα

# Πλαίσιο πολιτικών και δράσεων για την προστασία πληροφοριακών συστημάτων και της ιδιωτικότητας

- Ανάλυση και αποτίμηση κινδύνων με χρήση τυπικών, ημι-τυπικών και άτυπων μεθόδων
- Καθορισμός πολιτικών, διαδικασιών, και τεχνικών ασφάλειας
- Διαχείριση/έλεγχος εγκατάστασης και ρύθμισης συσκευών και λογισμικού (ειδικότερα σε συσκευές IoT)
- Καθορισμός στρατηγικής αντιμετώπισης επιθέσεων και περιστατικών παραβίασης ασφάλειας
- Ενημέρωση και εκπαίδευση γύρω από την ασφάλεια πληροφοριακών συστημάτων
- Ασφάλεια φυσικών υποδομών
- Ασφάλεια προσωπικού
- Συνεχής επιτήρηση

- Μηχανισμοί ελέγχου πρόσβασης
- Μηχανισμοί ταυτοποίησης (biometrics, tokens, passwords)
- Μηχανισμοί καταγραφής και ελέγχου (logging και auditing)
- Τεχνικές κρυπτογράφησης και ανωνυμοποίησης δεδομένων
- Ασφάλεια περιμέτρου (cloud και edge)
- Συστήματα ανίχνευσης/αντιμετώπισης εισβολών (και σε συσκευές IoT)
- Πρωτόκολλα καθορισμού και ελέγχου παραμέτρων ασφάλειας
- Διαρκώς ενημερωμένα λογισμικά προστασίας (Anti-viral, anti-spyware, anti-spam software)
- Χρήση secure tokens, σε περίπτωση που οι απαιτήσεις ασφάλειας είναι υψηλές

**Οι αντίπαλοι επιτίθενται στον πιο αδύναμο κρίκο ... Ποιος είναι ο δικός μας;**

# Μερικές προσεγγίσεις κατά των απειλών της ασφάλειας πληροφοριακών συστημάτων και της προστασίας της ιδιωτικότητας

# Θεμελιώδεις απαιτήσεις ασφάλειας

## Στόχος:

Η προστασία ψηφιακών πόρων και αγαθών όπως μιας κυβερνητικής ιστοσελίδας, των δεδομένα υγείας των πολιτών μιας χώρας ή μιας βάσης δεδομένων πελατών μιας επιχείρησης.

## Βασικές απαιτήσεις ασφάλειας πληροφοριακών συστημάτων:

- Αυθεντικοποίηση ή Ταυτοποίηση: Αποσκοπεί στην εξακρίβωση της ταυτότητας ενός χρήστη.
- Εμπιστευτικότητα: Αφορά την ιδιωτικότητα και τη μυστικότητα των πληροφοριών που ανταλάσσονται μεταξύ δύο επικοινωνούντων μερών – επιτυγχάνεται με χρήση ειδικών μεθόδων κρυπτογράφησης όπως θα εξηγήσουμε πιο κάτω).
- Εξουσιοδότηση: Ο έλεγχος πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες.
- Ακεραιότητα: Η προστασία των δεδομένων από τυχαία ή σκόπιμη τροποποίησή τους.
- Μη αποποίηση ευθύνης (μη άρνηση υπογραφής): Ένας χρήστης δεν μπορεί να αρνηθεί την υπογραφή του σε ένα ηλεκτρονικό αρχείο δηλαδή δεν μπορεί να αποποιηθεί την ευθύνη του για κάτι που έχει υπογράψει ηλεκτρονικά με χρήση ηλεκτρονικών υπογραφών (π.χ. με μία μη συμμετρική μέθοδο κρυπτογράφησης – δείτε πιο κάτω σχετικά με αυτό).
- Διαθεσιμότητα: Η άμεση πρόσβαση στις υπηρεσίες του συστήματος για τους νόμιμους χρήστες του.

# Συμμετρική κρυπτογραφία

- Ένα κρυπτογραφικό σύστημα ονομάζεται συμμετρικό όταν το κλειδί αποκρυπτογράφησής του μπορεί εύκολα να υπολογιστεί από το αντίστοιχο κλειδί κρυπτογράφησης. Στην πληθώρα των περιπτώσεων των συμβατικών κρυπτογραφικών συστημάτων, τα δύο κλειδιά είναι ίδια.

- Η διαμοίραση του κλειδιού πρέπει να γίνει με ***ασφαλή*** τρόπο, δηλαδή μέσω ενός ***ασφαλούς*** καναλιού επικοινωνίας π.χ. με συνάντηση μεταξύ των δύο μερών.

# Μη συμμετρική κρυπτογραφία

- Στα κρυπτογραφικά συστήματα δημοσίου κλειδιού, οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι με τέτοιο τρόπο σχεδιασμένοι ώστε τα αντίστοιχα κλειδιά, κρυπτογράφησης και αποκρυπτογράφησης, να είναι διαφορετικά μεταξύ τους.
- Η επιτυχία, και συνεπώς η ασφάλεια, αυτού του είδους των κρυπτογραφικών συστημάτων βασίζεται στο ότι παρά το γεγονός ότι το δημόσιο κλειδί κρυπτογράφησης είναι γνωστό σε όλους, ο υπολογισμός του κλειδιού αποκρυπτογράφησης είναι δύσκολος έως αδύνατος.
- Στα συστήματα αυτά, δημόσιο κλειδί καλείται το κλειδί κρυπτογράφηση, που είναι σε όλους γνωστό και ιδιωτικό κλειδί καλείται το άλλο κλειδί, το κλειδί αποκρυπτογράφησης.

# Πλεονεκτήματα και μειονεκτήματα των μεθόδων κρυπτογράφησης

| Συμμετρική κρυπτογράφηση | Ασύμμετρη κρυπτογράφηση |
|---|---|
| (-) Η διαμοίραση του κλειδιού πρέπει να γίνει με ασφαλή τρόπο (π.χ. με συνάντηση από κοντά των δύο επικοινωνούντων μερώ). | (+) Παρέχουν τη δυνατότητα υποστήριξης ψηφιακών υπογραφών τέτοιες ώστε να μην μπορεί να γίνει *αποποίηση ευθύνης (δηλαδή άρνηση υπογραφής)* από τον υπογράφοντα. |
| (+) Η κρυπτογράφηση πραγματοποιείται με ταχύτατους ρυθμούς. | (-) Η κρυπτογράφηση πραγματοποιείται με μικρή ταχύτητα. |
| (+) Δεν υπάρχει ανάγκη για πιστοποίηση των κλειδιών καθώς έχουν διαμοιραστεί με συμφωνία μεταξύ των επικοινωνούντων μερών άρα γνωρίζει ο καθένας την ταυτότητα του άλλου (π.χ. έχουν συναντηθεί και επιβεβαιώσει ο ένας ποιος είναι ο άλλος). | (-) Σημαντικό! Υπάρχει ανάγκη για *πιστοποίηση και επαλήθευση* των δημόσιων κλειδιών από οργανισμούς (έμπιστες οντότητες π.χ. Υπουργείο Εσωτερικών) καθώς ο καθένς μπορεί να κατασκευάσει ένα δημόσιο κλειδί και ένα μυστικό και να ισχυρίζεται ότι είναι κάποιος που δεν είναι στην πραγματικότητα. |

# Ψηφιακές ή ηλεκτρονικές υπογραφές

*Ορισμός:* Μία μέθοδος διασφάλισης του περιεχομένου ενός ηλεκτρονικού εγγράφου ή μηνύματος, ως προς:

Τη γνησιότητα,

Την ακρίβεια,

Την ταυτότητα του υπογράφοντα του εγγράφου αυτού,

Τη μη αλλοίωση του κειμένου αυτού.

*Κατηγορίες ψηφιακών υπογραφών:*

Υπογραφές με χρήση μεθόδων Κρυπτογραφίας Μυστικού Κλειδιού.

Υπογραφές με χρήση μεθόδων Κρυπτογραφίας Δημοσίου Κλειδιού (οι ψηφιακές υπογραφές υλοποιούνται κυρίως με κρυπτογραφία δημόσιου κλειδιού – *υποθέστε, στα πλαίσια του μαθήματος, ότι οι ψηφιακές υπογραφές υλοποιούνται μόνο με τέτοιες μεθόδους*).

# Τρόπος λειτουργίας των ψηφιακών υπογραφών

Ο υπογράφοντας ***υπογράφει*** το αρχείο Μ κρυπτογραφώντας το μήνυμα Μ (π.χ. ένα αρχείο) με το μυστικό του κλειδί (private key). Το κρυπτογραφημένο μήνυμα που προκύπτει από τη διαδικασία αυτή αποτελεί την υπογραφή S του μηνύματος Μ.

Ο παραλήπτης ***ελέγχει*** την υπογραφή S στο μήνυμα Μ, *αποκρυπτογραφώντας* το S με το δημόσιο κλειδί αυτού που ισχυρίζεται ότι έχει υπογράψει. Αν η αποκρυπτογράφηση του S δώσει το Μ, τότε ο παραλήπτης βεβαιώνεται για την ταυτότητα του υπογράφοντα καθώς, όπως έχουμε πει, η δράση του ενός κλειδιού πρέπει να ***αναιρεί*** τη δράση του άλλου.

# Η «περίληψη» ενός μηνύματος

Η ***περίληψη*** (message digest ή fingerprint) ενός μηνήματος ή ενός αρχείου είναι αυτό που προκύπτει με την επεξεργασία του μηνύματος με μία ***συνάρτηση κατακερματισμού*** (hash function). Η συνάρτηση κατακερματισμού είναι τέτοια που:

1) Αν ***δοθεί*** μία περίληψη, είναι υπολογιστικά **δύσκολο** να βρεθεί ένα μήνυμα που έχει την ***δοθείσα*** περίληψη μετά την επεξεργασία του από τη συνάρτηση κατακερματισμού. Με άλλα λόγια, η συνάρτηση κατακερματισμύ είναι υπολογιστικά δύσκολο (δηλαδή πολύ χρονοβόρο) να **αντιστραφεί**.
2) Αν αλλάξει ***έστω και ένα bit*** του μηνύματος, τότε η τιμή που δίνει η συνάρτηση κατακερματισμού αλλάζει δραστικά (αλλάζουν δηλαδή πολλά bits στην έξοδο). Με άλλα λόγια, η συνάρτηση κατακερματισμού είναι ***εξαιρετικά ευαίσθητη*** σε αλλαγές της εισόδου της (π.χ. προσπάθειες ***παραποίησης*** του μηνύματος ή του αρχείου) τις οποίες και αντανακλά στην έξοδο.

# Έλεγχος ακεραιότητας ενός μηνύματος

Ας υποθέσουμε ότι έχουμε υπολογίσει τη συνάρτηση κατακερματισμού σε κάποιο αρχείο και έχει προκύψει κάποια συγκεκριμένη τιμή, η οποία ονομάζεται *προηγούμενη ή αρχική περίληψη* (previous digest).

Έστω ότι υπολογίζουμε την τιμή αυτή ξανά σε κάποια επόμενη χρονική στιγμή, την οποία τιμή ονομάζουμε *τρέχουσα περίληψη* (current digest).

Από τις ιδιότητες που αναφέραμε στην προηγούμενη διαφάνεια, προκύπτει ότι αν έχει υποστεί αλλαγές το αρχείο μας από την στιγμή που είχε υπολογιστεί το previous digest τότε *η τιμή του current digest θα είναι διαφορετική από το previous digest*. Συνεπώς, συμπεραίνουμε ότι το έγγραφό μας έχει υποστεί ***τροποποίηση*** πιθανότατα κακόβουλη.

# Υπογράφοντας την «περίληψη» ενός μηνύματος

Επιπλέον, οι συναρτήσεις κατακερματισμού έχουν εφαρμογή και στις ηλεκτρονικές υπογραφές εκτός από τον έλεγχο ακεραιότητας ενός μηνύματος, ως εξής: *αντί να υπογράφουμε το ίδιο το αρχείο ή μήνυμα Μ, υπογράφουμε την περίληψή του*. Καθώς η περίληψη ενός αρχείου είναι πολύ μικρότερη από το ίδιο το μήνυμα, η διαδικασία υπογραφής και ελέγχου υπογραφής εκτελείται ***ταχύτατα***.

# Μη αποποίηση ευθύνης/μη άρνηση υπογραφής

Φυσικά, για να λειτουργήσουν σωστά οι ψηφιακές υπογραφές θα πρέπει να υπάρχει μία ***Έμπιστη Τρίτη Οντότητα*** (Trusted Third Party ή Trusted Center) που να έχει ***εξακριβώσει*** την ταυτότητα ενός χρήστη και να έχει ***εκδώσει*** τα κλειδιά του (δημόσιο και μυστικό) σε μία αρχική διαδικασία που μοιάζει με την διαδικασία έκδοσης της κανονικής μας ταυτότητας (το ρόλο του Trusted Center στη διαδικασία της έκδοσης της συμβατικής ταυτότητας έχει κάποιο αστυνομικό τμήμα).

Από εκεί και μετά κάθε χρήστης που ***υπογράφει*** ένα αρχείο, όπως η Αλίκη στο πιο κάτω σχήμα που θέλει να στείλει ένα υπογεγραμμένο αρχείο Μ στον Bob, στέλνει το υπογεγραμμένο αρχείο πρώτα στο trusted center. Το trusted center πιστοποιεί αν η υπογραφή προέρχεται, πράγματι, από τον χρήστη Alice και στη συνέχεια ***προωθεί*** το υπογεγραμμένο αρχείο μαζί με ***την δική του υπογραφή*** (του trusted center δηλαδή) στον Bob ο οποίος και πείθεται για την ταυτότητα του υπογράφοντα, της Αλίκης, γιατί το πιστοποιεί με την υπογραφή του το trusted center.

# SSL/TLS

Το πρωτόκολλο SSL (*Secure Socket Layer*), παρέχει *ασφαλή και πιστοποιημένη επικοινωνία μεταξύ δύο εφαρμογών ή υπολογιστικών συστημάτων* και αποτελεί σήμερα το πιο διαδεδομένο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο καθώς και κάθε είδους διαδικτυακή επικοινωνία που χρειάζεται προστασία από κακόβουλες επιθέσεις.

# Δεδομένα προσωπικού χαρακτήρα και Ιδιωτικότητα στην εποχή του διαδικτύου

- Προσωπικά δεδομένα είναι πληροφορίες που χαρακτηρίζουν και ταυτοποιούν ένα φυσικό πρόσωπο.
- Απλά προσωπικά δεδομένα: (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, εκπαίδευση, ενδιαφέροντα, οικογενειακή-οικονομική κατάσταση, δραστηριότητες, συνήθειες).

Τα ευαίσθητα προσωπικά δεδομένα συμπεριλαμβάνουν τα εξής:

- Φυλετική καταγωγή
- Πολιτικά φρονήματα
- Θρησκευτικές ή Φιλοσοφικές πεποιθήσεις
- Συμμετοχή σε συνδικαλιστικές οργανώσεις
- Υγεία
- Κοινωνική πρόνοια
- Σεξουαλικός προσανατολισμός
- Καταδίκες
- Γενετικά δεδομένα

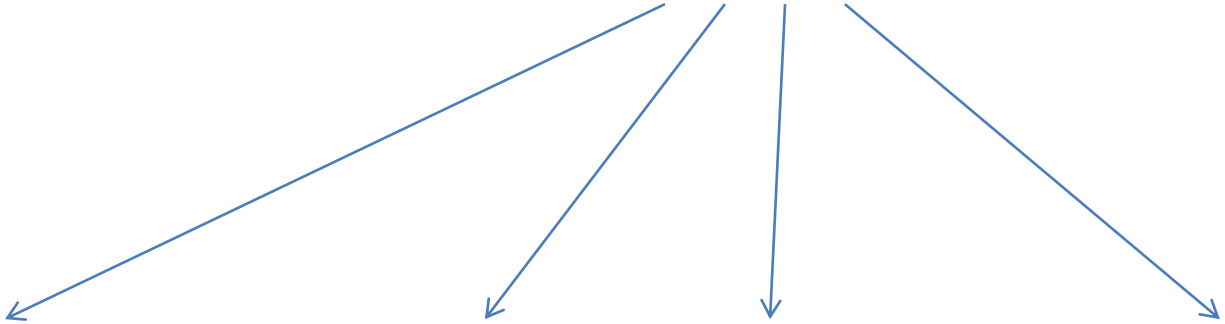
# Δεδομένα προσωπικού χαρακτήρα και Ιδιωτικότητα στην εποχή του διαδικτύου

“The right of an individual to be left alone”

«Το δικαίωμα στον σεβασμό της ιδιωτικής ζωής των πολιτών»
(Άρθρο 8, Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου)

*Η **ιδιωτικότητα** των πληροφοριών αποτελεί την αξίωση των ατόμων στο να θέτουν όρια σχετικά με τη διαθεσιμότητα των πληροφοριών που αφορούν τους ίδιους αλλά είναι δυνατόν να γνωστοποιούνται και σε άλλους.*

<u>Η Ιδιωτικότητα γενικά διακρίνεταισε:</u>



Ιδιωτικότητα των πληροφοριών

Ιδιωτικότητα Επικοινωνίας

Εδαφική Ιδιωτικότητα

Φυσική-Βιολογική Ιδιωτικότητα

# Δεδομένα προσωπικού χαρακτήρα και Ιδιωτικότητα στην εποχή του διαδικτύου

Ενδεικτικές διεργασίες επεξεργασίας των προσωπικών δεδομένων :

- Διατήρηση
- Αποθήκευση
- Καταχώρηση
- Τροποποίηση
- Χρήση
- Διαβίβαση
- Διάδοση
- Συσχέτιση
- Διασύνδεση
- Δέσμευση
- Διαγραφή
- Καταστροφή

Οι Αρχές που διέπουν την προστασία των προσωπικών δεδομένων ώστε να διασφαλίζεται η προστασία της Ιδιωτικότητας είναι:

- Νόμιμος τρόπος της συλλογής
- Αναλογικότητα
- Προσδιορισμός νόμιμου σκοπού
- Ποιότητα/ακρίβεια των δεδομένων
- Χρονικός περιορισμός της χρήσης
- Κατοχύρωση της ασφάλειας
- Συμμετοχή του υποκειμένου
- Μη συνδεσιμότητα
- Ανωνυμία/ψευδωνυμία
- Κρυπτογράφηση
- Διαφάνεια
- Ευθύνη

# Δεδομένα προσωπικού χαρακτήρα και Ιδιωτικότητα στην εποχή του διαδικτύου - νομικό πλαίσιο

Ευρωπαϊκή Νομοθεσία για την προστασία των προσωπικών δεδομένων

- Οδηγία 95/46/ΕΚ Προστασία ατόμου από επεξεργασία Δ.Π.Χ.
- Κανονισμός 45/2001/ΕΚ Προστασία από οργανισμούς της Ε.Ε.
- Οδηγία 2002/58/ΕΚ Προστασία στις ηλεκτρ. επικοινωνίες
- Οδηγία 2009/136/ΕΚ Επικαιροποίηση της 2002/58/ΕΚ
- Οδηγία 2013/40/ΕΕ Αποτροπή κινδύνων για τα Π.Σ.
- Γενικός Κανονισμός Προστασίας των Δεδομένων 679/2016 (General Data Protection Regulation – GDPR)

Ελληνική Νομοθεσία για την προστασία των προσωπικών δεδομένων

- Νόμος 2472/1997 Προστασία ατόμου από επεξεργασία Δ.Π.Χ.
- Νόμος 3471/2006 Προστασία Δ.Π.Χ. & Ιδιωτικότητας στις Τηλεπικοινωνίες
- Σύνταγμα Άρ.9Α Ψήφισμα 27/5/08 Η' Αναθεωρ. Βουλής των Ελλήνων
- Νόμος 3783/2009 Ταυτοποίηση στις υπηρεσίες Κινητής Τηλεφωνίας
- Νόμος 3917/2011 Διατήρηση δεδομένων
- Νόμος 4411/2016 Προστασία Π.Σ.

Ίδρυση ανεξάρτητης Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

# Ασφάλεια περιμέτρου

*Ορισμός:*

Όλα τα σημεία πρόσβασης του δικτύου του παρόχου σε εξωτερικά δίκτυα.

*Σκοπός:*

Η προστασία των διάφορων πόρων του παρόχου από εισβολείς, και η αποτροπή από μη εξουσιοδοτημένη πρόσβαση σε στοιχεία του δικτύου του.

*Μέσα Προστασίας:*

Σύστημα firewall:Ένας μηχανισμός «περιμετρικής άμυνας» ελέγχει την πρόσβαση από και προς το ιδιόκτητο δίκτυο.

# Firewalls

## *Δυνατότητες των Firewalls:*

- Το firewall απλοποιεί τη διαχείριση ασφάλειας, αφού ο έλεγχος προσπέλασης στο δίκτυο επικεντρώνεται κυρίως σε αυτό το σημείο.
- Το firewall εφαρμόζει έλεγχο προσπέλασης από και προς το δίκτυο, υλοποιώντας την πολιτική ασφάλειας του οργανισμού.
- Το firewall προσφέρει αποτελεσματική καταγραφή της δραστηριότητας στο δίκτυο.
- Το firewall προστατεύει τα διαφορετικά δίκτυα εντός του ίδιου οργανισμού.
- Το firewall έχει τη δυνατότητα απόκρυψης των πραγματικών διευθύνσεων της επιχείρησης.

# Firewalls

*Αδυναμίες των Firewalls:*

- Το firewall δεν μπορεί να προστατεύσει από προγράμματα-ιούς.
- Το firewall δεν μπορεί να προστατεύσει απέναντι στις επιθέσεις κακόβουλων χρηστών από το εσωτερικό του οργανισμού.
- Το firewall δε μπορεί να προστατέψει τον οργανισμό απέναντι σε επιθέσεις σχετιζόμενες με δεδομένα.
- Το firewall δεν μπορεί να προστατέψει τον οργανισμό από απειλές άγνωστου τύπου.
- Το firewall δεν μπορεί να προστατέψει από συνδέσεις οι οποίες δε διέρχονται από αυτό.
- Η αυστηρή ρύθμιση της ασφάλειας διαμέσου του firewall.

# Ασφάλεια Web εξυπηρετητών

*Ορισμός*:

Ο web εξυπηρετητής διαχειρίζεται και διανέμει πληροφορίες στο διαδίκτυο και προστατεύει τα ευαίσθητα δεδομένα που στέλνονται από το πρόγραμμα πλοήγησης (web browser) του χρήστη στον εξυπηρετητή αυτού που επικοινωνεί. Είναι η πρώτη οντότητα μιας επιχείρησης που πρέπει να προστατευτεί από ένα firewall μαζί με άλλα λογισμικά προστασίας.

Οι εξυπηρετητές διακρίνονται από τα εξής χαρακτηριστικά:

Απόδοση.

Πλατφόρμες (π.χ. Windows, Linux κ.λπ.).

Ασφάλεια.

Υποστήριξη ειδικών λειτουργιών Ηλεκτρονικού Εμπορίου.

# Ασφάλεια Web εξυπηρετητών

*Λειτουργίες των Web Εξυπηρετητών (Web Servers):*

- Εξυπηρετούν αιτήσεις για σύνδεση με την ιστοσελίδα ενός οργανισμού (συνδέσεις HTTP).
- Παρέχουν έλεγχο προσπέλασης.
- Εκτελούν scripts ή προγράμματα, είτε για να προσθέσουν λειτουργικότητα στις ιστοσελίδες που παρέχουν είτε για να παράσχουν πρόσβαση πραγματικού χρόνου με μεγάλες ταχύτητες μεταφοράς δεδομένων.
- Καταγράφουν στοιχεία των συναλλαγών ηλεκτρονικού εμπορίου που πραγματοποιούν οι χρήστες.

# Certificates – Authentication των εξυπηρετητών (servers)

1. Σε έναν browser, πληκτρολογείστε το όνομα του site που σας ενδιαφέρει με https στην αρχή (κρυπτογράφηση), για παράδειγμα, https://www.upatras.gr

2. Επάνω στον browser, στη γραμμή διεύθυνσης θα σας εμφανίσει το https και το λουκέτο – χαρακτηριστικό του SSL, με πράσινο χρώμα.

3. Κάντε κλικ επάνω στο λουκέτο και επιλέξτε Connection Secure και μετά More Information. Στο νέο παράθυρο διαλόγου που θα εμφανιστεί, επιλέξτε Security και μετά View Certificate

4. Στο νέο παράθυρο διαλόγου, εμφανίζονται οι ημερομηνίες έναρξης και λήξης του πιστοποιητικού που έχετε εγκαταστήσει.

ΣΗΜΕΙΩΣΗ: Τις παραπάνω πληροφορίες μπορείτε να τις δείτε για όλα τα site που επισκέπτεστε, καθώς είναι πληροφορία που εμφανίζει ο browser.

# Οι (όχι και τόσο) μελλοντικοί κίνδυνοι

# Το μέλλον: Semantic Web (Σημασιολογικός Ιστός) ή το «μυαλό του Θεού» κατάλληλα δομημένο για επεξεργασία από τις *ίδιες τις μηχανές*!

Παράδειγμα απλού *μηχανιστικού* συλλογισμού modus ponens:

- ***Εάν*** σήμερα είναι Τρίτη, ***τότε*** θα πάω στη δουλειά

  Σήμερα ***είναι*** Τρίτη

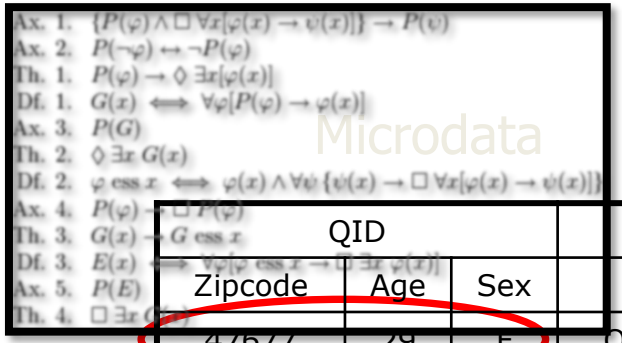
  Συνεπώς, θα ***πάω*** στη δουλειά

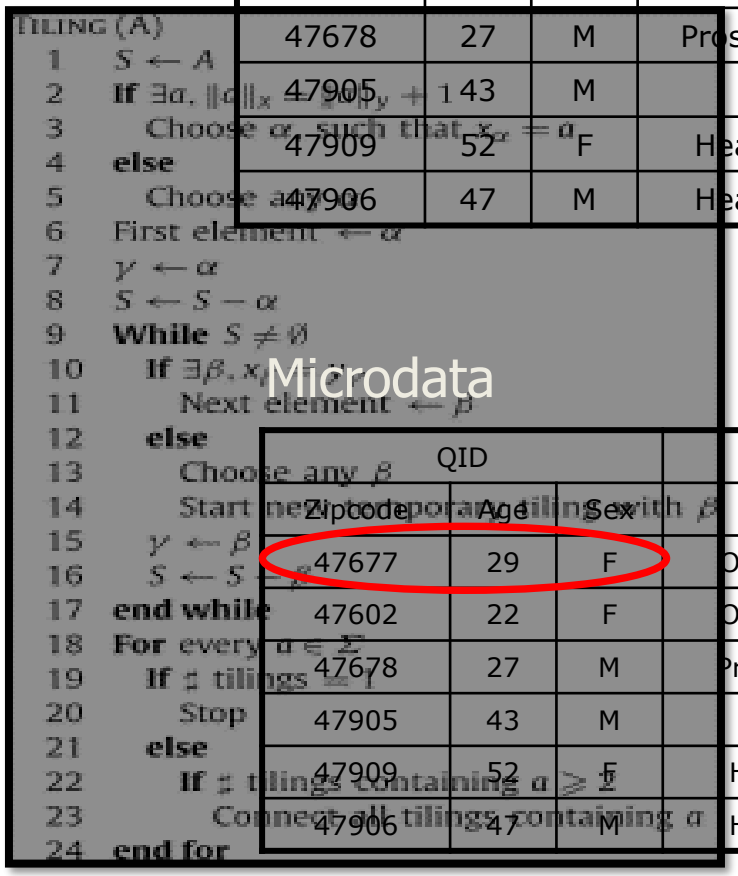
- Γενικά, εάν αληθεύει το p και, επίσης, αληθεύει το p ⇒ q, τότε αληθεύει και το q

$$\forall X(man(X) \Rightarrow mortal(X))$$

$$man(socrates)$$

$$man(socrates) \Rightarrow mortal(socrates)$$





Microdata

| QID | | | SA |
|---|---|---|---|
| Zipcode | Age | Sex | Disease |
| 47677 | 29 | F | Ovarian Cancer |
| 47602 | 22 | F | Ovarian Cancer |
| 47678 | 27 | M | Prostate Cancer |
| 47905 | 43 | M | Flu |
| 47909 | 52 | F | Heart Disease |
| 47906 | 47 | M | Heart Disease |

Voter registration data

| Name | Zipcode | Age | Sex |
|---|---|---|---|
| Alice | 47677 | 29 | F |
| Bob | 47983 | 65 | M |
| Carol | 47677 | 22 | F |
| Dan | 47532 | 23 | M |
| Ellen | 46789 | 43 | F |

Microdata

| QID | | | SA |
|---|---|---|---|
| Zipcode | Age | Sex | Disease |
| 47677 | 29 | F | Ovarian Cancer |
| 47602 | 22 | F | Ovarian Cancer |
| 47678 | 27 | M | Prostate Cancer |
| 47905 | 43 | M | Flu |
| 47909 | 52 | F | Heart Disease |
| 47906 | 47 | M | Heart Disease |

Generalized table

| QID | | | SA |
|---|---|---|---|
| Zipcode | Age | Sex | Disease |
| 476** | 2* | * | Ovarian Cancer |
| 476** | 2* | * | Ovarian Cancer |
| 476** | 2* | * | Prostate Cancer |
| 4790* | [43,52] | * | Flu |
| 4790* | [43,52] | * | Heart Disease |
| 4790* | [43,52] | * | Heart Disease |

!!

## SUPERCOMPUTER FUGAKU - SUPERCOMPUTER FUGAKU, A64FX 48C 2.2GHZ, TOFU INTERCONNECT D

| | |
|---|---|
| Site: | RIKEN Center for Computational Science |
| System URL: | https://www.r-ccs.riken.jp/en/fugaku/project |
| Manufacturer: | Fujitsu |
| Cores: | 7,630,848 |
| Memory: | 5,087,232 GB |
| Processor: | A64FX 48C 2.2GHz |
| Interconnect: | Tofu interconnect D |

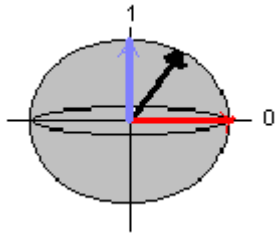
## A64FX leading-edge Si-technology

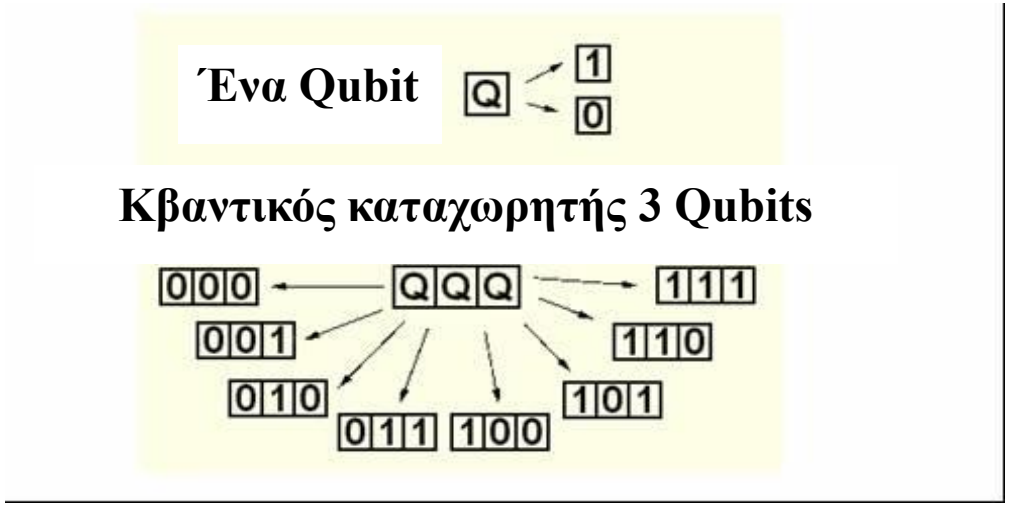
TILING (A)

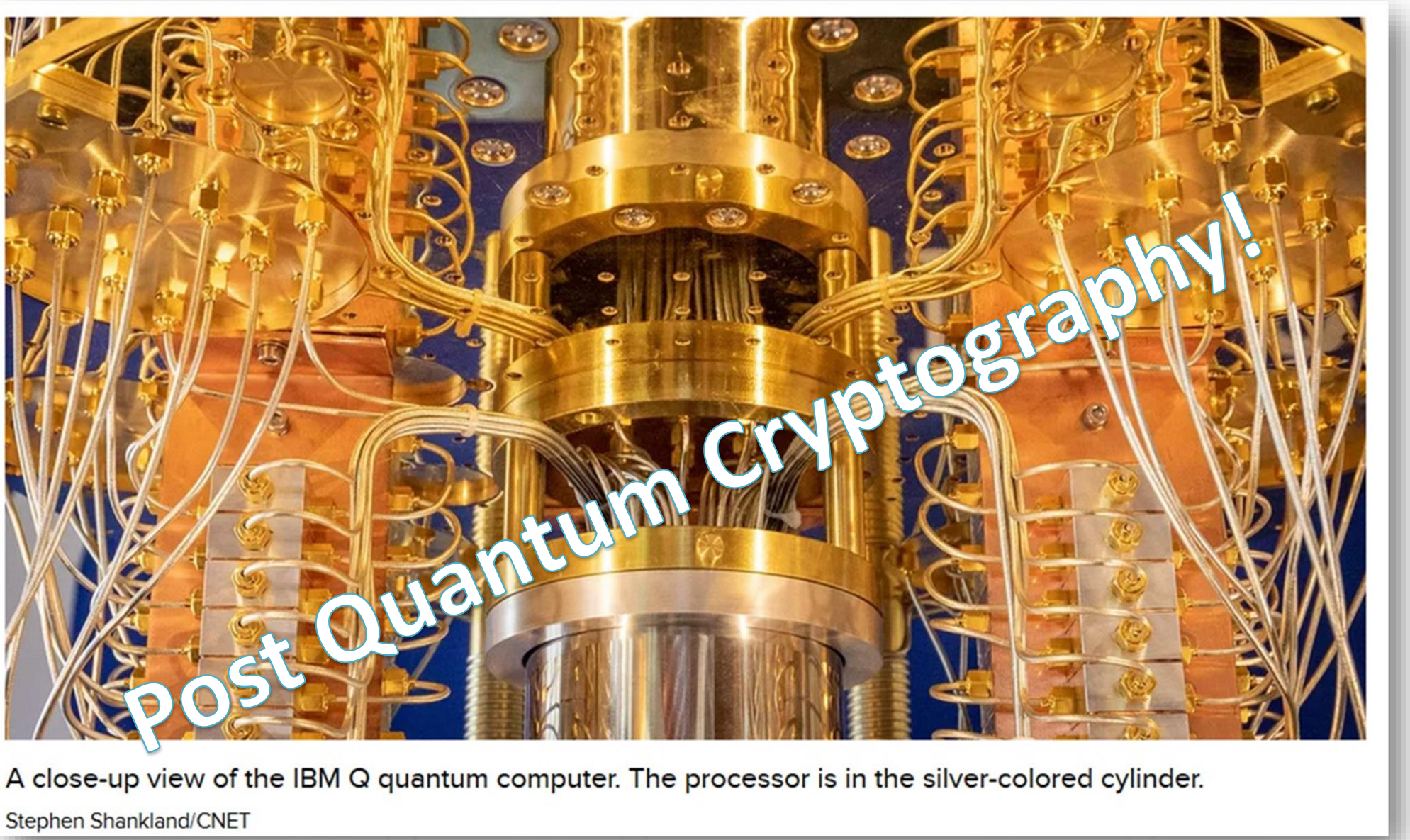
```
1   S ← A
2   If ∃α, ‖α‖_x = [illegible]
3     Choose α [illegible]
4   else
5     Choose any α
6   First element [illegible]
7   γ ← α
8   S ← S − α
9   While S ≠ ∅
10    If ∃β, x_β = [illegible]
11      Next element ← β
12    else
13      Choose any β
14      Start new temporary tiling with β
15    γ ← β
16    S ← S − β
17  end while
18  For every α ∈ Σ
19    If ♯ tilings = 1
20      Stop
21    else
22      If ♯ tilings containing α ⩾ 2
23        Connect all tilings containing α
24  end for
```

| Rank | System | Cores | (TFlop/s) | (TFlop/s) | (kW) |
|---|---|---|---|---|---|
| | Japan | 7,630,848 | 442,010.0 | 537,212.0 | 29,899 |
| | | | | 194.9 | 10,096 |
| 8 | NVIDIA Tesla V100, Mellan… Eni S.p.A. Italy | 669,760 | 35,450.0 | | |
| 9 | Frontera - Dell C6420, Xeon Platinum … Mellanox InfiniBand HDR, Dell EMC Texas Advanced Computing Center/Univ. … United States | | | | |
| 10 | Dammam-7 - Cray CS-Storm, Xeon Gold 6248 … 2.5GHz, NVIDIA Tesla V100 SXM2, InfiniBand HDR … HPE Saudi Aramco Saudi Arabia | 672,520 | 22,400.0 | 55,423.6 | |

- **<u>Θεωρία πολυπλοκότητας:</u>** *Το πρόβλημα εύρεσης πρώτων παραγόντων ενός ακεραίου θεωρείται δύσκολο υπολογιστικά πρόβλημα*
- **<u>Peter Shor, 1994:</u>** *Υπάρχει γρήγορος <<αλγόριθμος>> που επιλύει το παραπάνω πρόβλημα γρήγορα!*
- **<u>Η λύση του παράδοξου:</u>** *Ο <<αλγόριθμος>> είναι σχεδιασμένος για κβαντικούς υπολογιστές* [όραμα του μεγάλου φυσικού του αιώνα μας, Richard Feynmann, το 1982]






A close-up view of the IBM Q quantum computer. The processor is in the silver-colored cylinder.

Stephen Shankland/CNET

*IBM quantum computer by IBM Research, CC BY-ND 2.0, Πηγή: https://flic.kr/p/259cSVy*

# Μα δεν υπάρχει ένας μηχανισμός (π.χ. εργαλείο ή εφαρμογή) για την προστασία μας;

Είναι ***αδύνατον*** (προσοχή, όχι απλά *δύσκολο*!) να κατασκευαστεί μία μηχανή/εφαρμογή απόλυτης προστασίας από κακόβουλο λογισμικό και επιθέσεις (Cohen, 1984)

# Αναφορές


- Stallings, W. (2012). *Κρυπτογραφία και Ασφάλεια Δικτύων*. Εκδόσεις ΙΩΝ.
- Γκρίτζαλης Σ., Κάτσικας Σ., Χρυσικόπουλος Β., & Burmester M (επιμελητές συλλογικού τόμου). (2011). Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές. Εκδόσεις Παπασωτηρίου.


# Τέλος Ενότητας

# Χρηματοδότηση


- Το παρόν εκπαιδευτικό υλικό (κείμενο, εικόνες, διαγράμματα, κλπ.) έχει αναπτυχθεί στο πλαίσιο της Πράξης «Υποστήριξη Δράσεων Στήριξης της Επιχειρηματικότητας, Καινοτομίας και Ωρίμανσης για την Αξιοποίηση της Ερευνητικής Δραστηριότητας και των Νέων Προϊόντων και Υπηρεσιών που αναπτύσσονται στο Πανεπιστήμιο Πατρών» - «ΜΕΤΩΝ, MIS 5132546».
- Η πράξη «ΜΕΤΩΝ» υλοποιείται στο πλαίσιο του Ε.Π. «ΑΝΑΠΤΥΞΗ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ, ΕΚΠΑΙΔΕΥΣΗ & ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από Εθνικούς πόρους.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Ειδική Υπηρεσία Διαχείρισης
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

# Σημειώματα

# Σημείωμα Ιστορικού Εκδόσεων Έργου

Το παρόν έργο αποτελεί την έκδοση 1.0

# Σημείωμα Αναφοράς

# Σημείωμα Αδειοδότησης

# Διατήρηση Σημειωμάτων

Οποιαδήποτε αναπαραγωγή ή διασκευή του υλικού θα πρέπει να συμπεριλαμβάνει:

- το Σημείωμα Αναφοράς
- το Σημείωμα Αδειοδότησης
- τη δήλωση Διατήρησης Σημειωμάτων
- το Σημείωμα Χρήσης Έργων Τρίτων (εφόσον υπάρχει)

μαζί με τους συνοδευόμενους υπερσυνδέσμους.

# Σημείωμα Χρήσης Έργων Τρίτων (1/1)

Το Έργο αυτό κάνει χρήση των ακόλουθων έργων:

**Εικόνες/Σχήματα/Διαγράμματα/Φωτογραφίες**
Από https://pixabay.com/ με ελεύθερη άδεια χρήσης, οι εξής εικόνες:


anatomy-g95de440be_1280


artificial-intelligence-ga72c06c74_1920


blockchain-g6cef84a0c_1920

chatgpt-g60de8d77b_1280


long-shadow-gd07c3186d_1280


network-gf45636fe1_1280