Ασφάλεια Δικτύων: Στοιχεία από την Έρευνα της Δρ Anca Jurcut

Ενίσχυση Επικοινωνιών Δικτύων μέσω Προηγμένων Πρωτοκόλλων Ασφαλείας

Περίληψη

Η έρευνα της Δρ Anca Jurcut επικεντρώνεται στην ενίσχυση της ασφάλειας των επικοινωνιών στο Διαδίκτυο μέσω του σχεδιασμού και της ανάπτυξης προηγμένων πρωτοκόλλων ασφαλείας. Το έργο της αποσκοπεί στην επίλυση κρίσιμων ζητήματος, όπως η ανίχνευση και η πρόληψη επιθέσεων δικτύου, η δημιουργία τεχνολογιών ανθεκτικών στην κβαντική απειλή και η ανάπτυξη ανθεκτικών συστημάτων επικοινωνίας. Αυτές οι βελτιώσεις αποσκοπούν στη δημιουργία ασφαλέστερων υποδομών δικτύων με μακροπρόθεσμες επιπτώσεις για την παγκόσμια κυβερνοασφάλεια.

Βασικοί Όροι

- **Ασφάλεια Δικτύου**: **Μέτρα που λαμβάνονται για την προστασία δεδομένων κατά τη μετάδοσή τους και την αποτροπή μη εξουσιοδοτημένης πρόσβασης, κακής χρήσης ή τροποποίησης του δικτύου.**
- **Πρωτόκολλα Ασφαλείας: Κανόνες και αλγόριθμοι που σχεδιάζονται για να διασφαλίζουν τη μετάδοση δεδομένων μέσω δικτύων.**
- **Τεχνολογία Ανθεκτική στην Κβαντική Απειλή: Κρυπτογραφικές μέθοδοι που παραμένουν ασφαλείς ακόμη και απέναντι σε επιθέσεις από κβαντικούς υπολογιστές.**
- **Επιθέσεις Δικτύου: Μη εξουσιοδοτημένες ενέργειες που θέτουν σε κίνδυνο την ασφάλεια των δεδομένων που μεταδίδονται σε δίκτυα.**

Co-funded by the Erasmus+ Programme of the European Union

Εισαγωγή

Με την αυξανόμενη εξάρτηση από τις επικοινωνίες μέσω Διαδικτύου για επιχειρήσεις, οικονομικά, κυβερνήσεις και προσωπική χρήση, η ανάγκη για ασφαλείς και αξιόπιστες υποδομές δικτύου δεν ήταν ποτέ μεγαλύτερη. Οι κυβερνοεπιθέσεις αποτελούν συνεχή απειλή για την ιδιωτικότητα και την ακεραιότητα των δεδομένων, απαιτώντας την ανάπτυξη ισχυρότερων, πιο ανθεκτικών πρωτοκόλλων ασφαλείας.

Η έρευνα της Δρ Anca Jurcut **στην ασφάλεια δικτύων επικεντρώνεται στον σχεδιασμό πρωτοκόλλων που αποτρέπουν επιθέσεις και ενισχύουν την ασφάλεια της μετάδοσης δεδομένων. Οι συνεισφορές της είναι ιδιαίτερα σχετικές καθώς ο κόσμος προετοιμάζεται για την άφιξη της κβαντικής υπολογιστικής, η οποία θα θέσει σε κίνδυνο τα τρέχοντα κρυπτογραφικά πρότυπα.**

Μέθοδοι

1. **Σχεδιασμός Πρωτοκόλλων Ασφαλείας**: Δημιουργία **πρωτοκόλλων που διασφαλίζουν τη μετάδοση δεδομένων και προστατεύουν από διάφορους τύπους επιθέσεων, όπως επιθέσεις** "man-in-the-middle", **επιθέσεις άρνησης υπηρεσιών** (DoS) **και** phishing.
2. **Κρυπτογραφία Ανθεκτική στην Κβαντική Απειλή**: **Αντιμετώπιση πιθανών απειλών από την κβαντική υπολογιστική μέσω ανθεκτικών κρυπτογραφικών μεθόδων που θα διασφαλίζουν την ασφάλεια των δικτύων στο μέλλον.**
3. **Ανίχνευση και Πρόληψη Επιθέσεων**: **Ανάπτυξη συστημάτων που ανιχνεύουν και αντιμετωπίζουν παραβιάσεις ασφάλειας σε πραγματικό χρόνο, αποτρέποντας την κλοπή δεδομένων και τη διακοπή του δικτύου..**

Πληροφορίες για τη Συγγραφέα

Η Δρ. Anca Jurcut είναι καταξιωμένη ειδικός στην ασφάλεια δικτύων. Κατέχει διδακτορικό δίπλωμα στην Ασφάλεια Πληροφοριών και Δικτύων και έχει εργαστεί εκτενώς στην ανάπτυξη πρωτοκόλλων ασφαλείας ανθεκτικών στην κβαντική απειλή.

Κατά τη διάρκεια της καριέρας της, έχει αντιμετωπίσει σημαντικές προσωπικές και επαγγελματικές προκλήσεις, όπως το σύνδρομο του απατεώνα και την πλοήγηση σε ένα ανδροκρατούμενο πεδίο. Παρά τα εμπόδια, έχει συνεισφέρει ουσιαστικά στη διασφάλιση των διαδικτυακών επικοινωνιών.

Επιπλέον, η Δρ. Jurcut **είναι αφοσιωμένη μέντορας, με δέσμευση να ενθαρρύνει και να καθοδηγεί τη νέα γενιά γυναικών στους τομείς** STEAM (**Επιστήμη, Τεχνολογία, Μηχανική, Τέχνες, Μαθηματικά**)

Co-funded by the Erasmus+ Programme of the European Union

Αποτελέσματα

Η έρευνα της Δρ Jurcut **έχει οδηγήσει σε** πρωτοποριακά **αποτελέσματα**, **όπως**:

- **Προηγμένα Πρωτόκολλα Ασφαλείας**: **Σχεδιασμός ασφαλών** πρωτοκόλλων **που προστατεύουν από νέες και διαρκώς** μεταβαλλόμενες **απειλές δικτύου**.
- **Κρυπτογραφία Ανθεκτική στην Κβαντική Απειλή**: Δημιουργία **τεχνικών κρυπτογράφησης ικανών να προστατεύουν δεδομένα στην εποχή της κβαντικής υπολογιστικής**.
- **Ανίχνευση Επιθέσεων σε Πραγματικό Χρόνο**: **Συστήματα που εντοπίζουν** πιθανές παραβιάσεις **και εξουδετερώνουν απειλές** πριν **θέσουν σε κίνδυνο την ακεραιότητα του δικτύου**.

Τα αποτελέσματα αυτά δείχνουν πώς **το έργο της** Dr. Jurcut **ανταποκρίνεται τόσο στις σημερινές όσο και στις** μελλοντικές **προκλήσεις ασφαλείας στην ψηφιακή εποχή**.

Συζήτηση

Η έρευνα της Δρ Jurcut **παρέχει σημαντικές πληροφορίες για το** μέλλον **της ασφάλειας δικτύων**:

- **Διασφάλιση του Μέλλοντος**: **Καθώς η κβαντική υπολογιστική γίνεται** πιο προσβάσιμη, **η ανάγκη για τεχνολογίες ανθεκτικές στην κβαντική απειλή θα αυξάνεται, καθιστώντας επιτακτική την ανάπτυξη ανθεκτικών κρυπτογραφικών μεθόδων**.
- **Ανταπόκριση σε Απειλές σε Πραγματικό Χρόνο**: **Τα συστήματα ασφάλειας δικτύων πρέπει να εξελιχθούν από στατικές άμυνες σε δυναμικά συστήματα ικανά να ανταποκρίνονται σε απειλές σε πραγματικό χρόνο**.
- **Η Σημασία της Διαφορετικότητας στις STEAM Επιστήμες**: **Η εμπειρία της** Δρ Jurcut **αναδεικνύει την ανάγκη για μεγαλύτερη εκπροσώπηση φύλων στην ασφάλεια δικτύων και στους** STEAM **κλάδους. Η υποστήριξη προς την ένταξη περισσότερων γυναικών σε αυτούς τους κλάδους υπογραμμίζει πόσο ουσιαστικός είναι ο ρόλος του μέντορα, αλλά και η ύπαρξη δικτύων ενδυνάμωσης και αλληλοϋποστήριξης**.

Συμπεράσματα

Το έργο της Δρ Anca Jurcut **στην ασφάλεια δικτύων είναι ένα θεμέλιο για το μέλλον ασφαλών επικοινωνιών στο Διαδίκτυο. Οι συνεισφορές της στον σχεδιασμό πρωτοκόλλων ασφαλείας, την ανθεκτική στην κβαντική απειλή κρυπτογραφία και τα συστήματα ανίχνευσης απειλών σε πραγματικό χρόνο θα διαδραματίσουν κρίσιμο ρόλο στην προστασία δεδομένων σε έναν ολοένα και πιο συνδεδεμένο κόσμο. Καθώς ο τομέας της ασφάλειας δικτύων συνεχίζει να εξελίσσεται, το έργο της λειτουργεί σημείο αναφοράς για τη μελλοντική έρευνα και ανάπτυξη στον χώρο αυτό**.

Co-funded by the Erasmus+ Programme of the European Union

ΠΗΓΕΣ :

- Original article: R. Shafique, F. Rustam, G. S. Choi and A. D. Jurcut, "Enhancing In-Vehicle Network Security Against AI-Generated Cyberattacks Using Machine Learning," *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, Dubai, United Arab Emirates, 2024, pp. 1-6, doi: 10.1109/WCNC57260.2024.10571300.
- National Institute of Standards and Technology (NIST): Guidelines on Quantum-Resistant Cryptography.
- European Cybersecurity Organization (ECSO): Reports on Real-Time Threat Detection.

Ερωτήσεις Αντανάκλασης

---

1. **Τι ενέπνευσε τη Δρ. Anca Jurcut να ακολουθήσει καριέρα στην ασφάλεια δικτύων;**
   α) Ένα έντονο ενδιαφέρον για τα πρωτόκολλα δικτύων από νεαρή ηλικία
   β) Συμμετοχή σε διαγωνισμούς μαθηματικών και πληροφορικής
   γ) Ενθάρρυνση από τον καθηγητή της στο πανεπιστήμιο να υποβάλει αίτηση για μεταπτυχιακή υποτροφία
   δ) Ένα πρώιμο ενδιαφέρον για το ηθικό hacking

Απάντηση: **γ) Ενθάρρυνση από τον καθηγητή της στο πανεπιστήμιο να υποβάλει αίτηση για μεταπτυχιακή υποτροφία**

---

2. **Ποια είναι η κύρια δυσκολία που δημιουργεί η ανάπτυξη της κβαντικής υπολογιστικής στην ασφάλεια δικτύων;**

Co-funded by the Erasmus+ Programme of the European Union

α) **Κάνει τις συνδέσεις στο Διαδίκτυο γρηγορότερες αλλά λιγότερο ασφαλείς**
β) **Οι κβαντικοί υπολογιστές μπορούν εύκολα να σπάσουν τις τρέχουσες κρυπτογραφικές μεθόδους**
γ) **Αυξάνει την κατανάλωση ενέργειας των συστημάτων δικτύου**
δ) **Μειώνει την ανάγκη για κρυπτογράφηση στις επικοινωνίες**

Απάντηση: β) **Οι κβαντικοί υπολογιστές μπορούν εύκολα να σπάσουν τις τρέχουσες κρυπτογραφικές μεθόδους**

---

3. **Πώς η κρυπτογραφία ανθεκτική στην κβαντική απειλή αντιμετωπίζει την πρόκληση της κβαντικής υπολογιστικής στην ασφάλεια δικτύων;**
α) **Με τη χρήση προηγμένου** hardware**για την αποτροπή επιθέσεων**
β) **Με τη δημιουργία αλγορίθμων κρυπτογράφησης που δεν μπορούν να αποκρυπτογραφηθούν από κβαντικούς υπολογιστές**
γ) **Με την ανίχνευση πιθανών απειλών πριν συμβούν**
δ) **Με την επιτάχυνση των ρυθμών μετάδοσης δεδομένων μέσω του δικτύου**

Απάντηση: β) **Με τη δημιουργία αλγορίθμων κρυπτογράφησης που δεν μπορούν να αποκρυπτογραφηθούν από κβαντικούς υπολογιστές**

---

4. **Ποιο από τα παρακάτω είναι ένα παράδειγμα επίθεσης δικτύου που στοχεύουν να αποτρέψουν τα πρωτόκολλα ασφαλείας της Δρ. Jurcut;**
α) **Φυσική παραβίαση της υποδομής δικτύου**
β) **Επιθέσεις** "man-in-the-middle", **όπου οι επιτιθέμενοι παρεμβάλλονται στις επικοινωνίες**
γ) **Περιβαλλοντικές διαταραχές, όπως σεισμοί**
δ) **Βελτιστοποιήσεις ταχύτητας δικτύου**

Απάντηση: β) **Επιθέσεις** "man-in-the-middle", **όπου οι επιτιθέμενοι παρεμβάλλονται στις επικοινωνίες**

---

5. **Πώς τα συστήματα ανίχνευσης επιθέσεων σε πραγματικό χρόνο βελτιώνουν την ασφάλεια δικτύων;**

Co-funded by the Erasmus+ Programme of the European Union

α) Επιτρέπουν στα δίκτυα να λειτουργούν πιο γρήγορα
β) Αποκλείουν αυτόματα όλα τα δεδομένα από μη αξιόπιστες πηγές
γ) Εντοπίζουν και αποκρίνονται σε πιθανές παραβιάσεις ασφαλείας καθώς συμβαίνουν, αποτρέποντας ζημιές
δ) Μειώνουν την πολυπλοκότητα των αλγορίθμων κρυπτογράφησης

Απάντηση: **γ) Εντοπίζουν και αποκρίνονται σε πιθανές παραβιάσεις ασφαλείας καθώς συμβαίνουν, αποτρέποντας ζημιές**

Απαντήσεις:

1. **Τι ενέπνευσε τη Δρ. Anca Jurcut να ακολουθήσει καριέρα στην ασφάλεια δικτύων;**
   Απάντηση: **γ) Ενθάρρυνση από τον καθηγητή της στο πανεπιστήμιο να υποβάλει αίτηση για μεταπτυχιακή υποτροφία**
2. **Ποια είναι η κύρια πρόκληση που θέτει η κβαντική υπολογιστική στην ασφάλεια δικτύων;**
   Απάντηση: **β) Οι κβαντικοί υπολογιστές μπορούν εύκολα να αποκρυπτογραφηθούν τις τρέχουσες κρυπτογραφικές μεθόδους**
3. **Πώς η κρυπτογραφία ανθεκτική στην κβαντική απειλή αντιμετωπίζει την πρόκληση της κβαντικής υπολογιστικής στην ασφάλεια δικτύων;**
   Απάντηση: **β) Με τη δημιουργία αλγορίθμων κρυπτογράφησης που δεν μπορούν να σπάσουν από κβαντικούς υπολογιστές**
4. **Ποιο από τα παρακάτω είναι ένα παράδειγμα επίθεσης δικτύου που στοχεύουν να αποτρέψουν τα πρωτόκολλα ασφαλείας της Δρ. Jurcut;**
   Απάντηση: **β) Επιθέσεις** "man-in-the-middle", **όπου οι επιτιθέμενοι παρεμβάλλονται στις επικοινωνίες**
5. **Πώς τα συστήματα ανίχνευσης επιθέσεων σε πραγματικό χρόνο βελτιώνουν την ασφάλεια δικτύων;**
   Απάντηση: **γ) Εντοπίζουν και αποκρίνονται σε πιθανές παραβιάσεις ασφαλείας καθώς συμβαίνουν, αποτρέποντας ζημιές**

Co-funded by the
Erasmus+ Programme
of the European Union

Μάθημα: Ασφαλίζοντας το Μέλλον – Κατανόηση της Ασφάλειας Δικτύων και της Κρυπτογραφίας

Στόχος:
Οι μαθητές θα μάθουν τα βασικά της ασφάλειας δικτύων, συμπεριλαμβανομένων των κοινών απειλών, της σημασίας της κρυπτογράφησης και των μεθόδων προστασίας των δεδομένων κατά τη μετάδοση. Το μάθημα θα εισαγάγει βασικές έννοιες όπως η κρυπτογραφία, η ασφάλεια ανθεκτική στην κβαντική απειλή και η ανίχνευση επιθέσεων σε πραγματικό χρόνο.

Υλικά:

- **Προβολέας για διαφάνειες σχετικά με την ασφάλεια δικτύων**
- **Φυλλάδια για κοινές επιθέσεις δικτύων** (π.χ., man-in-the-middle, denial of service, phishing)
- **Υπολογιστές ή λάπτοπ για προσομοίωση της ασφάλειας δικτύων**
- **Εργαλεία λογισμικού για ασφάλεια δικτύων** (π.χ., Wireshark, **βασικά εργαλεία κρυπτογράφησης**)
- **Πρόσβαση στο Διαδίκτυο για έρευνα σε τρωτά σημεία δικτύων και μεθόδους άμυνας**

Βασικές Πληροφορίες:

Η ασφάλεια δικτύων αφορά πρακτικές και τεχνολογίες που έχουν σχεδιαστεί για να προστατεύουν την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των δεδομένων κατά τη μετάδοσή τους μέσω δικτύων. Καθώς οι κυβερνοεπιθέσεις γίνονται όλο και πιο εξελιγμένες, είναι απαραίτητη η εφαρμογή ισχυρών μέτρων ασφαλείας, όπως η κρυπτογράφηση, τα firewalls **και η ανίχνευση επιθέσεων σε πραγματικό χρόνο. Αναδυόμενες απειλές, όπως η κβαντική υπολογιστική, δημιουργούν νέες προκλήσεις στις παραδοσιακές κρυπτογραφικές μεθόδους**.

Co-funded by the
Erasmus+ Programme
of the European Union

Δραστηριότητες Μαθήματος

1. **Εισαγωγή στην Ασφάλεια Δικτύων (15 λεπτά):**
    - **Ξεκινήστε με μια επισκόπηση της σημασίας της ασφάλειας δικτύων στη σημερινή ψηφιακή εποχή**.
    - **Εξηγήστε πώς τα δίκτυα είναι ευάλωτα σε διάφορες μορφές επιθέσεων**, **όπως επιθέσεις** man-in-the-middle (MITM), denial of service (DoS), **και** phishing.
    - **Εισάγετε βασικούς όρους**, **όπως κρυπτογράφηση**, firewalls, **και πρωτόκολλα δικτύων**.
    - **Συζητήστε την ανερχόμενη πρόκληση της κβαντικής υπολογιστικής και πώς απειλεί τα παραδοσιακά συστήματα κρυπτογράφησης**.
2. **Κοινές Επιθέσεις Δικτύων και Άμυνα (20 λεπτά):**
    - **Χωρίστε την τάξη σε μικρές ομάδες και αναθέστε σε κάθε ομάδα μια κοινή επίθεση δικτύου** (π.**χ**., MITM, DoS, phishing **ή** SQL injection).
    - **Ζητήστε από κάθε ομάδα να ερευνήσει και να παρουσιάσει**:
        - **Πώς λειτουργεί η επίθεση**
        - **Τι ζημιά μπορεί να προκαλέσει**
        - **Μεθόδους πρόληψης ή μετριασμού της επίθεσης** (π.**χ**., **χρήση κρυπτογράφησης**, firewalls **ή πολυπαραγοντική ταυτοποίηση**).
    - **Μετά από κάθε παρουσίαση**, **συζητήστε τη σημασία των πρωτοκόλλων ασφαλείας που μπορούν να ανιχνεύσουν και να αποτρέψουν τέτοιες επιθέσεις**.
3. **Δραστηριότητα: Προσομοίωση Κυκλοφορίας Δικτύου και Ανίχνευση Επιθέσεων (30 λεπτά):**
    - **Στήστε ένα προσομοιωμένο δίκτυο χρησιμοποιώντας ένα εργαλείο ασφάλειας δικτύων**, **όπως το** Wireshark.
    - **Επιτρέψτε στους μαθητές να παρατηρήσουν φυσιολογική και κακόβουλη κυκλοφορία στο δίκτυο**, **κατανοώντας πώς εντοπίζονται επιθέσεις όπως** MITM **και** DoS.
    - **Οδηγήστε τους μαθητές να εντοπίσουν πιθανές αδυναμίες στο προσομοιωμένο δίκτυο και να προτείνουν πιθανές άμυνες**, **όπως ισχυρότερη κρυπτογράφηση ή τμηματοποίηση δικτύου**.

Co-funded by the Erasmus+ Programme of the European Union

- Δείξτε πώς τα δεδομένα προστατεύονται κατά τη μετάδοση μέσω κρυπτογράφησης.

4. **Εξερεύνηση Κβαντικά Ανθεκτικής Κρυπτογραφίας (15 λεπτά):**
   - **Εισάγετε την έννοια της κβαντικής υπολογιστικής και γιατί αποτελεί απειλή για τις τρέχουσες μεθόδους κρυπτογράφησης**.
   - **Συζητήστε την κρυπτογραφία ανθεκτική στην κβαντική απειλή και πώς χρησιμοποιεί αλγορίθμους που σχεδιάζονται για να αντέχουν σε επιθέσεις κβαντικού επιπέδου**.
   - **Εξηγήστε πώς ερευνητές, όπως η** Δρ. Anca Jurcut, **αναπτύσσουν αυτούς τους αλγόριθμους για να διασφαλίσουν την ασφάλεια των μελλοντικών επικοινωνιών**.

Οπτικοποίηση και Συζήτηση:

- Δημιουργήστε έναν οπτικό χάρτη διαφορετικών επιπέδων ασφάλειας δικτύου (firewalls, **κρυπτογράφηση, συστήματα ανίχνευσης εισβολών**, κ.λπ.) **σε έναν πίνακα**.
- **Συζητήστε πώς αυτά τα επίπεδα συνεργάζονται για να δημιουργήσουν ένα ασφαλές δίκτυο**.
- **Ζητήστε από τους μαθητές να εξετάσουν πώς μπορεί να εξελιχθούν τα πρωτόκολλα ασφαλείας καθώς η τεχνολογία κβαντικής υπολογιστικής γίνεται πιο διαδεδομένη**.

Επιπλέον συζήτηση:

• Εφαρμογές της ασφάλειας δικτύων: **Συζητήστε τη σημασία της ασφάλειας δικτύων σε τομείς όπως οι τράπεζες, η υγεία, το κράτος, αλλά και σε προσωπικό επίπεδο** (π.χ. **ασφάλεια στις διαδικτυακές συναλλαγές, τα** email **και τα μέσα κοινωνικής δικτύωσης**).
• Το μέλλον της κρυπτογραφίας: **Ενθαρρύνετε τους μαθητές να συζητήσουν για το πώς μπορεί να εξελιχθεί η κρυπτογραφία στο μέλλον και πώς οι ανθεκτικοί στην κβαντική τεχνολογία αλγόριθμοι θα προστατεύουν τα δεδομένα**.
• Ηθικό hacking: **Εισαγάγετε την έννοια του ηθικού** hacking, **όπου ειδικοί στην**

Co-funded by the Erasmus+ Programme of the European Union

ασφάλεια ελέγχουν σκόπιμα τα δίκτυα για τρωτά σημεία και ευπάθειες, με σκοπό την ενίσχυση της προστασίας τους.

Αξιολόγηση:

Ζητήστε από τους μαθητές να γράψουν μια ανασκόπηση σχετικά με:

- **Ποια επίθεση δικτύου βρήκαν πιο επικίνδυνη και γιατί.**
- **Πώς η κρυπτογράφηση προστατεύει τα δεδομένα κατά τη μετάδοση.**
- **Γιατί η κβαντική υπολογιστική αποτελεί πρόκληση για τις τρέχουσες μεθόδους κρυπτογράφησης και πώς η κρυπτογραφία ανθεκτική στην κβαντική απειλή βοηθά στην αντιμετώπιση αυτής της πρόκλησης.**

Αξιολογήστε τις ομαδικές παρουσιάσεις και τη συμμετοχή στη δραστηριότητα προσομοίωσης.

Ερωτήσεις Αντανάκλασης:

1. **Ποιοι είναι οι κύριοι στόχοι της ασφάλειας δικτύων;**
   α) Να αυξήσει την ταχύτητα μετάδοσης δεδομένων
   β) Να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων
   γ) Να κάνει τα δεδομένα προσβάσιμα σε όλους τους χρήστες του δικτύου
   δ) Να περιορίσει τον αριθμό των συσκευών που συνδέονται στο δίκτυο
   Απάντηση: β) Να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων

---

2. **Πώς βοηθά η κρυπτογράφηση στην ασφάλεια των δεδομένων που μεταδίδονται μέσω δικτύου;**
   α) Κρύβει τα δεδομένα μέσα σε άλλα αρχεία

Co-funded by the Erasmus+ Programme of the European Union

β) Μετατρέπει τα δεδομένα σε έναν κώδικα που μόνο εξουσιοδοτημένοι χρήστες μπορούν να αποκρυπτογραφήσουν
γ) Μειώνει το μέγεθος των δεδομένων για ταχύτερη μετάδοση
δ) Εμποδίζει την πρόσβαση στα δεδομένα από κινητές συσκευές
Απάντηση: β) Μετατρέπει τα δεδομένα σε έναν κώδικα που μόνο εξουσιοδοτημένοι χρήστες μπορούν να αποκρυπτογραφήσουν

---

3. **Ποια είναι η σημασία της κρυπτογραφίας ανθεκτικής στην κβαντική απειλή για το μέλλον της ασφάλειας δικτύων;**
   α) Επιταχύνει την επεξεργασία δεδομένων στα συστήματα δικτύων
   β) Εμποδίζει τους χάκερ να χρησιμοποιούν κβαντικούς υπολογιστές για να σπάσουν την κρυπτογράφηση
   γ) Επιτρέπει στα δίκτυα να λειτουργούν χωρίς firewalls
   δ) Απλοποιεί τη διαχείριση των πρωτοκόλλων δικτύων
   Απάντηση: β) Εμποδίζει τους χάκερ να χρησιμοποιούν κβαντικούς υπολογιστές για να σπάσουν την κρυπτογράφηση

Co-funded by the
Erasmus+ Programme
of the European Union