Πανεπιστήμιο Θεσσαλίας
Σχολή Θετικών Επιστημών
Τμήμα Μαθηματικών

Περίληψη:

Η κρυπτογραφία είναι η επιστήμη που επιτρέπει σε δύο συμμετέχοντες να επικοινωνούν με ασφάλεια εν παρουσία αντιπάλων. Από τη δεκαετία του '70 έχουν αναπτυχθεί πολλά διαφορετικά κρυπτοσυστήματα που επιτρέπουν τη διασφάλιση της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας των επικοινωνιών και των συναλλαγών. Σε αυτήν την ομιλία θα ξεκινήσουμε βλέποντας μερικές βασικές αρχές της σύγχρονης κρυπτογραφίας πριν εστιάσουμε στους αλγόριθμους συμμετρικού κλειδιού. Η συμμετρική κρυπτογραφία είναι ένας κλάδος της κρυπτογραφίας, όπου οι δύο συμμετέχοντες μοιράζονται το ίδιο μυστικό κλειδί για να επικοινωνούν. Οι αλγόριθμοι συμμετρικού κλειδιού έχουν την ιδιαιτερότητα να είναι εξαιρετικά γρήγοροι και συνεπώς έχουν αναπτυχθεί σε διάφορα είδη πρωτοκόλλων και σε όλους τους τύπους συσκευών. Θα παρουσιάσουμε μερικές από τις πιο σημαντικές τεχνικές σχεδιασμού για αυτόν τον τύπο αλγορίθμων, θα δείξουμε μερικές από τις μαθηματικές τους ιδιότητες και θα συζητήσουμε εν συντομία την ασφάλειά τους.

Ομιλήτρια:

Δρ Χριστίνα Μπούρα,
Αναπληρώτρια Καθηγήτρια,
Université de Versailles Saint-Quentin-en-Yvelines.

Διάλεξη με θέμα:

Μέθοδοι της σύγχρονης συμμετρικής κρυπτογραφίας

Παρασκευή **21 Μαΐου 2021**
στις **12:00**

Εικονική αίθουσα του **MsTeams**: **802yfg5**