UNIVERSITATEA TEHNICĂ "GHEORGHE ASACHI" DIN IAŞI
Facultatea de Automatică şi Calculatoare
Departamentul de Calculatoare

Concurs pentru ocuparea postului de şef de lucrări, poz. 33

Disciplinele postului: Criptografie şi Securitatea Datelor, Tehnici de procesare digitală a semnalelor, Calcul cuantic şi aplicaţii în securitate

Tematica de concurs

privind

Prelegerea din aria tematică a postului

pentru ocuparea postului de şef de lucrări poziţia 33
din Statul de funcţii al Departamentului de Calculatoare
pe anul universitar 2022-2023

Criptografie şi Securitatea Datelor

1. Noţiuni de bază

- Definiţii
- Obiective de securitate
- Descrierea arhitecturii
- Stabilirea cerinţelor funcţionale
- Definirea parametrilor relevanţi privind ciclul de viaţă, calitatea şi performanţa sistemelor de protecţie criptografică

2. Sisteme criptografice simetrice

- Scheme clasice de criptare
- Cunoaşterea şi înţelegerea principiilor de funcţionare pentru principalele categorii şi familii de sisteme criptografice
- Analiza factorilor care influenţează securitatea unui sistem criptografic
- Rezistenţa la atacuri
- Stabilirea de măsuri de protecţie adecvate pentru cheile şi algoritmul implementat
- Confidenţialitatea folosind sistemele simetrice
- Cifruri bloc:
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)
- Generatoare aleatoare şi cifruri stream

3. Sisteme criptografice cu chei publice

- Dobândirea cunoştinţelor matematice care stau la baza proiectarii sistemelor criptografice
- Criptarea datelor cu chei publice
- Schema DH (Diffie-Hellman)
- Schema RSA (Rivest–Shamir–Adleman)

4. Problema autentificării şi funcţii hash

- Autentificare mesaje
- Funcţii hash, MAC (Message Authentication Code), HMAC (Hash-based Message Authentication Code)
- Semnături digitale
- Scheme de semnare: RSA şi DSA (Digital Signature Algorithm)

5. Criptografia pe curbe eliptice

- Operaţii matematice bazate pe curbe eliptice
- Generarea şi parametrizarea cheilor pe curbe eliptice
- Scheme criptografice pe curbe eliptice, ECDH (Elliptic-curve Diffie–Hellman) şi ECDSA (Elliptic Curve Digital Signature Algorithm)

6. Infrastructuri PKI (public key infrastructure)

- Managementul cheilor
- Transportul cheilor folosind sistemele cu cheie publică
- Certificate digitale şi infrastructuri PKI

Bibliografie:

1) Victor Shoup, "Computational Introduction to Number Theory and Algebra", 2004
2) Schneier Bruce, "Applied Cryptography", Second Edition, John Wiley & Sons, 1996
3) Stinson Doug, "Cryptography Theory and Practice", Third Edition, CRC Press, 2005
4) Menezes, van Oorschot, Vanstone, "Handbook of Applied Cryptography", CRC Press, 2001
5) Ferguson Niels, Schneier Bruce, "Practical Cryptography", Wiley, 2003
6) Katz Jonathan, Yehuda Lindell "Introduction to Modern Cryptography", CRC Press, 2007
7) Wenbo Mao, "Modern Cryptography: Theory and Practice", Prentice Hall, 2003
8) William Stallings, "Cryptography & Network Security" (4th Edition), Prentice Hall, 2010.

Decan,
Prof. Vasile-Ion Manta

Director de departament,
Conf. Andrei Stan