

UNIVERSITATEA TEHNICĂ "GHEORGHE ASACHI" DIN IAȘI
Facultatea de Automatică și Calculatoare
Departamentul de Calculatoare

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

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

Tematica de concurs
privind
Prelegerea din aria tematică a postului
pentru ocuparea postului de șef de lucrări poziția 33
din Statul de funcții al Departamentului de Calculatoare
pe anul universitar 2022-2023

Criptografie și Securitatea Datelor

1. Noțiuni de bază

- Definiții
- Obiective de securitate
- Descrierea arhitecturii
- Stabilirea cerințelor funcționale
- Definirea parametrilor relevanți privind ciclul de viață, calitatea și performanța sistemelor de protecție criptografică

2. Sisteme criptografice simetrice

- Scheme clasice de criptare
- Cunoașterea și înțelegerea principiilor de funcționare pentru principalele categorii și familii de sisteme criptografice
- Analiza factorilor care influențează securitatea unui sistem criptografic
- Rezistența la atacuri
- Stabilirea de măsuri de protecție adecvate pentru cheile și algoritmul implementat
- Confidențialitatea folosind sistemele simetrice
- Cifruri bloc:
 - o DES (Data Encryption Standard)
 - o AES (Advanced Encryption Standard)
- Generatoare aleatoare și cifruri stream

3. Sisteme criptografice cu chei publice

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

4. Problema autentificării și funcții hash

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

5. Criptografia pe curbe eliptice

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

6. Infrastructuri PKI (public key infrastructure)

- Managementul cheilor
- Transportul cheilor folosind sistemele cu cheie publică
- Certificate digitale și 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