Securitatea Sistemelor Informatice (2023-2024)
Seriile 34, 35

Lista de subiecte de pregatit pentru examen

1. Definiții (toate definițiile de la laborator).
2. Triada CIA: Confidentialitate, Integritate, Disponibilitate (Availability). Autentificare. Non-repudiere.
3. Sisteme de criptare istorice
   - Sisteme monoalfabetice și polialfabetice (generale), sistemul Cezar, sistemul afin
   - Atacul prin forta bruta
   - Analiza de frecventa.
4. Securitate perfecta. Sistemul de criptare One Time Pad (OTP). Reutilizarea cheii în OTP.
5. Securitate computationala.
   - Adversar PPT.
   - Functii neglijabile si ne-neglijabile. Determinarea dacă o funcție data este/nu este neglijabilă.
6. PseudoRandom Generator (PRG).
   - Identificarea unui PRG nesigur (slab) dpdv criptografic
   - Utilizarea PRG in cadrul sistemelor de criptare fluide
7. Linear Feedback Shift Register (LFSR).
   - Crearea figurii LFSR-ului pornind de la relația de recurenta a acestuia
   - Determinarea primilor (ex.10) biti de output
   - Determinarea periodicitatii maxime a unui LFSR
8. Criptografia simetrica si criptografía asimetrica. Sisteme de criptare simetrice si asimetrice. Proprietati, avantaje si dezavantaje.
9. Sisteme de criptare simetrice
   - Sistemele bloc DES si AES (fara constructie)
   - Atacul Meet-in-the-Middle
   - Moduri de operare bloc ECB, CTR, CBC. Necesitatea modurilor de operare. Proprietati.
10. Message Authentication Code (MAC). Identificarea unui MAC nesigur (slab) dpdv criptografic.
11. Notiuni preliminare
    - Orice noțiuni de bază necesare pentru celelalte subiecte: numere prime, grupuri, ordin al unui grup, etc.
    - Calculul inversului modular
    - Algoritmul lui Euclid pentru determinarea CMMDC (GCD)
    - Simbol Legendre. Simbol Jacobi. Calculul unui simbol Legendre/Jacobi
12. Sistemul de criptare RSA.
    - Identificarea unei chei de criptare valide
    - Calcului cheii secrete cunoscand cheia publica
    - Criptarea/Decriptarea unui mesaj
    - Probleme de securitate pentru Textbook RSA (sistem determinist)
13. Sistemul de criptare ElGamal

Securitatea Sistemelor Informatice (2023-2024)
Seriile 34, 35

- Criptarea/Decriptarea unui mesaj
- Problema Discrete Logarithm Problem (DLP)
- Reutilizarea valorii aleatoare k

Nota: ElGamal pe curbe eliptice nu este materie de examen

14. Protocolul de schimb de chei Diffie Hellman.
    - Problemele Decisional Diffie-Hellman (DDH) si Computational Diffie-Hellman (CDH)
    - Atacul Man-in-the-Middle
15. Functii hash.
    - Proprietati. Rezistență la prima preimagine, rezistență la a doua preimagine, rezistenta la coliziuni. Notiunea de one-way function
    - MD5, familia SHA (fara constructie)
    - Utilizarea funcțiilor hash pentru stocarea parolelor
16. Semnaturi digitale.
    - Identificarea unei scheme de semnatura digitala nesigură (slaba) dpdv criptografic
    - Utilizarea RSA într-o schema de semnatura digitala
    - Crearea unei semnături RSA false (mesaje relationate)