CMSE-512 Problem session 30.05.2025

[Digital signatures, Certificates, Kerberos, SET, Electronic money, Web security](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE512/Spring%202022/Digital%20Signatures%2024052022.docx), 2) [Authentication procedures](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE512/Spring2023/Authentication%20Procedure.docx), 3) [Database security control measures](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE512/Spring%202022/Database%20Security%20Control%20Measures.docx), 4) [Database protection](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE512/Spring%202025/Protecting_Data_through_Perturbation_Techniques_Th.pdf) (p. 15-17)

1. Digital signatures
   1. Digital signature, hash function, verification
   2. Certificate, three validation checks
   3. SSL, Session key exchange
   4. Kerberos, Ticket, Authenticator, Nonces
   5. Single Sign-On Kerberos
   6. Microsoft Passport
   7. E-Wallet, Pay Pal
   8. Secure Electronic Transactions (SET) protocol
   9. SET protocol dual signature
   10. Goods atomicity and certified delivery; escrow service
   11. Simple electronic cash; redundancy predicate; denomination keys; spending money
   12. Blind signature of the serial number; anonymity
   13. Money atomicity
   14. XML encryption
2. Authentication procedures
   1. Simple unprotected and protected authentication procedures
   2. One-, two-, and three-way complex authentication procedures
   3. Three-way authentication procedure flaw and Man-in-the-Middle attack on it
   4. Lamport’s one-time password authentication, number of authentications, small number attack on it
3. Database control measures
   1. Granting and revoking privileges
   2. Grant option, vertical and horizontal restrictions on the privileges propagation
   3. Mandatory access control, no-read up rule, no-write down rule, classification attributes, expanded primary key, different views for different security level users, poly-instantiation
   4. Role-based access control
   5. SQL injection attack
   6. Statistical database security, Database protection by perturbation, General additive data perturbation method
   7. Flow control in discretionary and mandatory access control models
   8. Covert channels in networks, Steganography, LSB method
   9. Audit, audit types