CMSE-512 Problem session 29.05.2024

[DES](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE512/Spring%202022/DES.docx)​ (​​p. 7), [SHA512](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE512/Spring%202022/SHA512%2028032022.docx) ​, [Digital signatures, Certificates, Kerberos, SET, Electronic money, Web security](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE512/Spring%202022/Digital%20Signatures%2024052022.docx), [Authentication procedures](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE512/Spring2023/Authentication%20Procedure.docx), and [Database security control measures](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE512/Spring%202022/Database%20Security%20Control%20Measures.docx)​​ (p. 1-3, Mandatory access control and the rest are not included)

1. DES
   1. Left circular shifts for a round key generation; schedule of shifts
   2. Permuted choice 2
2. SHA-512
   1. General schema
   2. message padding, block size, hash size, initial value size and initialization
   3. use of roots of prime numbers, decimal-to-hexadecimal conversion of the fractional parts
   4. elementary function F
   5. addition mod 2^64
   6. 80 rounds of F, constants Kt, words Wt, round structure, functions used: Maj, Ch, Sum0, Sum1, constants Kt calculation, words Wt recursive calculation, ROTR, SHIFT.
3. 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
4. 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
5. Database control measures
   1. Granting and revoking privileges
   2. Grant option, vertical and horizontal restrictions on the privileges propagation