CMSE-512 Problem session 06.06.2023

1. Digital signatures
   1. SET protocol dual signature
   2. Goods atomicity and certified delivery; escrow service
   3. Simple electronic cash; redundancy predicate; denomination keys; spending money
   4. Blind signature of the serial number; anonymity
   5. Money atomicity
   6. 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, no write-down rules
   4. Multilevel security in databases, attribute and tuple classification attributes
   5. Database filtering according to the viewer’s classification level
   6. Poly-instantiation of the multilevel security databases
   7. Role-based access control
   8. SQL injection attack
   9. Statistical databases, population, allowed queries
   10. Attacks on statistical databases and counter-measures; k-anonymity, data and response perturbation
   11. Flow control for multilevel databases
   12. Timing covert channels in networks