CMSE-512 Problem session 07.06.2022

1. 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
2. Digital signatures
	1. Digital signature creation; hash and public key cryptography
	2. Kerberos protocol; Key distribution server; Ticket; Authenticator; Countering replay attack
	3. Single sign-on in Kerberos
	4. Certificate
	5. SSL protocol
	6. Single sign-on in MS Passport
	7. SET protocol dual signature
	8. Goods atomicity and certified delivery; escrow service
	9. Simple electronic cash; redundancy predicate; denomination keys; spending money
	10. Blind signature of the serial number; anonymity
	11. Money atomicity
	12. XML encryption
3. SHA512
	1. General structure of a hash function
	2. Message padding
	3. Hash buffer initialization
	4. Structure of elementary SHA-512 hash function
	5. SHA-512 round function
	6. Creation of words Wi, i=0..79