**Problem Session CMSE-353 “Security of Software Systems” 06.11.2023**

**Security requirements, Access control models, DES p. 2-8, not including BLOCK CIPHER DESIGN PRINCIPLES and the rest, AES (p. 5-7, 10,11)**

1. What CIA requirements are?
2. What Authenticity, Assurance, Anonymity requirements are?
3. What a cryptosystem is? What is it comprised of?
4. Caesar cipher. Substitution table obtained by circular shifts. Encryption/decryption using substitution table. Key space cardinality. Encryption/decryption using modular arithmetic.
5. Caesar cipher. Substitution table by any permutation. Encryption/decryption using substitution table. Key space cardinality. Use of key sentences to get a substitution table,
6. Asymmetric cryptography principles. Use of the public and private keys. Confidential data exchange using public-key cryptography. Digital signature algorithm. Digital signature verification algorithm.
7. Hash functions, check-sums, message authentication code (MAC)
8. Certificates, certification authority, subject, subject public key,
9. User authentication, passwords, biometrics, two-factor authentication
10. Authorization. What is Access Control Matrix? List? Capability list?
11. Role-based access control.
12. What is Mandatory Access Control (MAC) model? MAC security levels. What two rules does MAC use?
13. Passwords, dictionary attack, security of passwords, secure and insecure passwords
14. Social engineering, pretexting, baiting, quid pro quo
15. What are the classes of intruders? Insider, external intruder. Back doors, logic bombs. Defense from insider attacks.
16. How intrusion can be detected?
17. What are the types of malware? Viruses, virus life cycle, virus signature, virus detection, quarantine, encrypted viruses, polymorphic and metamorphic viruses. Worms, rootkits. botnets, adware, spyware
18. DES: How DES encryption is organized? Why DES decryption is possible without nonlinear round function F(Ri-1, Ki) inverting?
19. DES: How DES is related to Feistel structure cipher? What part of an input is encrypted in each round? Why swaps are used?
20. DES: What Initial permutation is? How Inverse initial permutation is constructed?
21. DES: What is a round key? What is the bit-size of a round key? What is the source for round keys generation?
22. DES: How a right half is expanded by Expansion-Permutation transformation?
23. DES: How S-boxes work? What is a middle bit? What is an end bit?
24. DES: How outputs of S-boxes are transformed? How does permutation P work?
25. DES: How to decide what S-boxes in a current round are affected by a given S-box in the previous round?
26. DES: How round keys are generated? What is the aim of Permuted choice 1? What is Permuted choice 2? What is the schedule of circular left shifts (CLS)? How the number of CLS is defined for the given round? How CLS are done? How the results of CLS are used?
27. AES: How many rounds are used in AES? What are the key sizes of AES? How plaintext and key are arranged for AES with 10 rounds, 128 bit block size, and 128 bit key size? What is state array? How is it related to the plaintext? What is column-major order of storing multi-dimensional arrays? Row-major? How ciphertext is obtained? How many round keys are constructed and how are they arranged?
28. AES: What transformations are used in a round of AES? What transformation mixes state with secret information? What is shift row transformation? What is mix column transformation? What is a substitution transformation?
29. AES: How S-box is used for substitution transformation? How inverse S-box is used? Find S(AB). Find S-1(AB).