**Problem Session CMSE-353 “Security of Software Systems” 14.11.2022**

**Security requirements, Access control models, DES, AES**

1. What CIA concepts are?
2. What Authenticity, Assurance, Anonymity are?
3. What are the classes of intruders? What insider is? External intruder?
4. How intrusion can be detected?
5. What are the types of malware?
6. What are the methods of password cracking?
7. What are the requirements to strong passwords?
8. What social engineering (SE) is? What are the methods of SE?
9. What is Access Control Matrix? List? Capability list?
10. What is Mandatory Access Model? What rules are used in it?
11. DES: How DES encryption is organized? Why DES decryption is possible without nonlinear round function F(Ri-1, Ki) inverting?
12. DES: How DES is related to Feistel cipher? What part of an input is encrypted in each round? Why swaps are used?
13. DES: What Initial permutation is? How Inverse initial permutation is constructed?
14. DES: What is a round key? What is the bit-size of a round key? What is the source for round keys generation?
15. DES: How a right half is expanded by Expansion-Permutation transformation?
16. DES: How S-boxes work?
17. DES: What is a middle bit?
18. DES: What is an end bit?
19. DES: How outputs of S-boxes are transformed?
20. DES: How to decide what S-boxes are affected by a given S-box?
21. DES: How round keys are generated? What is the aim of Permuted choice 1?
22. AES: How many rounds are used in AES? What GF is used AES? What irreducible polynomial is 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?
23. 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?
24. AES: How S-box is used for substitution transformation? How inverse S-box is used? Find S(AB). Find S-1(AB).
25. AES: How S-box is constructed? What are the steps of its construction?
26. AES: Calculate Shift row transformation for

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12 | 34 | 56 | 78 |  |  |  |  |  |
| 9a | bc | de | Ef | => |  |  |  |  |
| 4A | 4b | 4c | 4d |  |  |  |  |  |
| 8C | De | bd | 3f |  |  |  |  |  |

1. AES: For the mix column transformation,

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 87 | F2 | 4D | 97 |  | 47 | 40 | A3 | 4C |
| 6E | 4C | 90 | EC | => | 37 | D4 | 70 | 9F |
| 46 | E7 | 4A | C3 |  | 94 | E4 | 3A | 42 |
| A6 | 8C | D8 | 95 |  | ED | A5 | A6 | BC |

show that actually 40 is obtained in the State(0,1). Mix column transformation is as follows

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 02 | 03 | 01 | 01 |  | S00 | S01 | S02 | S03 |  | S00’ | S01’ | S02’ | S03’ |  |
| 01 | 02 | 03 | 01 | \* | S10 | S11 | S12 | S13 | = | S10’ | S11’ | S12’ | S13’ | (5.3) |
| 01 | 01 | 02 | 03 |  | S20 | S21 | S22 | S23 |  | S20’ | S21’ | S22’ | S23’ |  |
| 03 | 01 | 01 | 02 |  | S30 | S31 | S32 | S33 |  | S30’ | S31’ | S32’ | S33’ |  |