**Problem Session CMSE-353 “Security of Software Systems” 7.01.2022**

**DES, Modes of block cipher operation, AES, Simple authentication procedures, One-, two-, and tree-way authentication procedures, One-time password, Network security**

1. DES: How DES encryption is organized? Why DES decryption is possible without nonlinear round function F(Ri-1, Ki) inverting?
2. DES: How DES is related to Feistel cipher? What part of an input is encrypted in each round? Why swaps are used?
3. DES: What Initial permutation is? How Inverse initial permutation is constructed?
4. DES: What is a round key? What is the bit-size of a round key? What is the source for round keys generation?
5. DES: How a right half is expanded by Expansion-Permutation transformation?
6. DES: How S-boxes work?
7. DES: What is a middle bit?
8. DES: What is an end bit?
9. DES: How outputs of S-boxes are transformed?
10. DES: How to decide what S-boxes are affected by a given S-box?
11. DES: How round keys are generated? What is the aim of Permuted choice 1? How shifts are used for key generation? What is the aim of Permuted choice 2?
12. DES: What is the difference between Cipher Block Chaining (CBC) and Electronic Code Book (ECB) modes?
13. DES: What is the difference between Cipher Feedback Mode and Output Feedback Mode? Why Counter mode is useful?
14. AES: What is identity element? What is identity element for addition? For multiplication? What is additive inverse? What is multiplicative inverse? What is associativity for addition? For multiplication? What is commutativity for addition? For multiplication? What is distributive law?
15. AES: What is Zn? Is a (Z10, +,\*) a field? Is (Z7,+,\*) a field?
16. AES: Polynomials arithmetic. Monic polynomial. Find (x2+3x+1)(x4-2x3+2)mod(x5+2x+1) over Z6.
17. AES: What is reducible polynomial? What is irreducible polynomial? Check reducibility of x2+2x+1 over Z3. Of x2+2x+2?
18. AES: What is GF(p)? GF(pn)? Show that 2\*5=1 in GF(23) with irreducible polynomial x3+x+1. Use EEA to find multiplicative inverse of 5 in GF(23) with irreducible polynomial x3+x+1.
19. 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?
20. 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?
21. AES: How S-box is used for substitution transformation? How inverse S-box is used? Find S(AB). Find S-1(AB).
22. AES: How S-box is constructed? What are the steps of its construction?
23. AES: Find multiplicative inverse of {25} in GF(28), irreducible polynomial is 
24. 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(1,2). 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’ |  |

1. AES: How AddRoundKey transformation works? If first byte of the State and Key are AB and CD, what is the result of the AddRoundKey transformation for the first byte

Consider

KeyExpansion(byte key[16], word w[44]){

 Word temp;

 For(i=0;i<4;i++) w[i]=(key[4\*i], key[4\*i+1], key[4\*i+2], key[4\*i+3]);

 For(i=4;i<44;i++){

 Temp=w[i-1];

 If(I mod 4 = 0) temp = SubWord(RotWord(temp)) XOR Rcon[i/4];

 W[i]=w[i-4] XOR temp;

 }

}

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| J | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| RC[j] | 01 | 02 | 04 | 08 | 10 | 20 | 40 | 80 | 1b | 36 |

For example, suppose that the round key for round 8 is

EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F

Then the 1st four bytes (1st column) of the round key for round 9 are calculated as follows:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| I(decimal) | temp | After RotWord | After SubWord | Rcon(9) | After XORWith Rcon | W[i-4] | W[i]=temp XOR w[i-4] |
| 36 | 7f8d292f | 8d292f7f | 5da515d2 | 1b000000 | 46a515d2 | Ead27321 | Ac7766f3 |

1. What are the second four bytes of round 9?
2. Authentication procedures: What is simple unprotected authentication procedure?
3. Authentication procedures: How in simple unprotected authentication client is authenticated to the server?
4. Authentication procedures: How in simple protected authentication client is authenticated to the server?
5. Authentication procedures: Who is authenticated in X.509 one-way authentication works? In two-way authentication? In three-way authentication?
6. Authentication procedures: How client is authenticated to server in Lamport’s One-Time password? Why re-initialization is necessary after N authentications?
7. Authentication procedures: How small number attack is conducted on OTP?
8. Network security: five layer Internet structure, IP addresses, IPv4, IPv6, hosts, routers, hops, packets, headers, footers, payload
9. Network security: Ethernet, common bus, star topology, hubs, switches, MAC addresses, MAC address structure, local MAC addresses administering
10. Network security: Ethernet frame structure, CRC32, ARP Protocol, ARP request, ARP reply, ARP cache, ARP Spoofing, ARP cache poisoning