**Problem Session CMSE-353 “Security of Software Systems” 23.12.2019**

**Modes of block cipher operation, Groups, Fields, AES, RSA, Digital signature, Certificate, SSL, Passport, MD5, Simple authentication procedures, One-, two-, and tree-way authentication procedures, One-time password**

1. What is the difference between Cipher Block Chaining (CBC) and Electronic Code Book (ECB) modes?
2. What is the difference between Cipher Feedback Mode and Output Feedback Mode? Why Counter mode is useful?
3. Groups: Find an inverse, p-1, of a permutation p=(3,2,4,1). Find p(a,b,c,d)
4. Groups: 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?
5. Groups: What is a group? What is a field?
6. Groups: What is Zn? Is a (Z10, +,\*) a field? Is (Z7,+,\*) a field?
7. Groups: Find 5-1mod7, 5-1mod8, 6-1mod8
8. Groups: Calculate 2137mod25 manually
9. Groups: What is a prime number? How to check primality? Pseudocode?
10. Groups: What is GCD(a,b)? How to calculate it? Euclidean algorithm for GCD?
11. Groups: What is relative primality? How to decide that two numbers are relatively prime? Find GCD(123, 34)
12. Finite fields: Extended Euclidean algorithm (EEA). Find 34-1mod123 using EEA.
13. Finite fields: Polynomials arithmetic. Monic polynomial. Find (x2+3x+1)(x4-2x3+2)mod(x5+2x+1) over Z6.
14. Finite fields: What is reducible polynomial? What is irreducible polynomial? Check reducibility of x2+2x+1 over Z3. Of x2+2x+2?
15. Finite fields: 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.
16. 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?
17. 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?
18. AES: How S-box is used for substitution transformation? How inverse S-box is used? Find S(AB). Find S-1(AB).
19. AES: How S-box is constructed? What are the steps of its construction?
20. AES: Find multiplicative inverse of {25} in GF(28), irreducible polynomial is 
21. AES: Calculate

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| B0’ |  | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |  | B0 |  | 1 |  |
| B1’ |  | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |  | B1 |  | 1 |  |
| B2’ |  | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |  | B2 |  | 0 |  |
| B3’ | = | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | x | B3 | + | 0 | (5.2) |
| B4’ |  | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |  | B4 |  | 0 |  |
| B5’ |  | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |  | B5 |  | 1 |  |
| B6’ |  | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 |  | B6 |  | 1 |  |
| B7’ |  | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |  | B7 |  | 0 |  |

For B=(32)

1. AES: Calclulate 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. RSA: For p and q from [15,20], define RSA pair of keys, encrypt and decrypt M=11.
3. RSA: What is public key? What is private key? What for private key is used? What for public key is used?
4. Digital signature: Using result of Task 23, and hash(x)= x mod 5, digitally sign M=28.
5. Digital signature: How in SSL protocol a client authenticates a server? How a server authenticates a client?
6. Digital signature: How a server authenticates a client in Microsoft Passport protocol?
7. Certificates: What for certificates are used? Who issues them? How certificates are protected from forge? How certificate is validated? What three checks are necessary to validate a certificate?
8. Diffie-Hellman key exchange
9. Authentication procedures: What is simple unprotected authentication procedure?
10. Authentication procedures: How in simple unprotected authentication client is authenticated to the server?
11. Authentication procedures: Who is authenticated in X.509 one-way authentication works? In two-way authentication? In three-way authentication?
12. Authentication procedures: How client is authenticated to server in Lamport’s One-Time password? Why re-initialization is necessary after N authentications?
13. Authentication procedures: How small number attack is conducted on OTP?
14. MD5: Messages of what sizes can be used as input to MD5? How original message length is saved in MD5 padding process? What is the length of a message after appending? How appending is conducted? Why in the result 0’s and 1’s padding, the message length shall be congruent to 448 mod 512 bits? What happens if the original message length is divisible by 512?
15. How message is processed in MD5? What two inputs are used by each block in the processing chain? What is the resulting hash? What is the number of bits used in each input of MD5 block? How 128-bit input is represented? How 512-bit is represented? How IV is initialized?
16. How many rounds has MD5 block? What are the inputs/outputs of the rounds? What is the difference between the rounds? What is the similarity of the rounds? How MD5 output is obtained? What arrays, permutations, and logical functions are used in the rounds? How arrays X and T are initialized? What is the use of the permutations? How many steps each round has? What transformations are made in one step of a round?
17. Network security: five layer Internet structure, IP addresses, IPv4, IPv6, hosts, routers, hops, packets, headers, footers, payload
18. Network security: Ethernet, common bus, star topology, hubs, switches, MAC addresses, MAC address structure, local MAC addresses administering
19. Network security: Ethernet frame structure, CRC32, ARP Protocol, ARP request, ARP reply, ARP cache, ARP Spoofing, ARP cache poisoning, ARP Spoofing counter-measures.