**Problem Session CMPE-553 “Cryptography and Network Security” 3.01.2023**

1) [AES CIPHER.Part2](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE553/AES%20CIPHER.Part2.doc) (p. 3,4, 6,7); 2)  [Ch. 9 RSA](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE553/Chapter%209.doc); 3) [Ch. 10 Key Distribution](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE553/KeyDistribution250505.doc); and 4)   [**SHA-512**](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE553/CMPE553%20Fall2022/SHA512%2028032022.docx) (p. 1-9, not including W generation).

1. AES: Mix column and Inverse Mix transforamtion
2. AES. 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 XOR  With Rcon | W[i-4] | W[i]=temp XOR w[i-4] |
| 36 | 7f8d292f | 8d292f7f | 5da515d2 | 1b000000 | 46a515d2 | Ead27321 | Ac7766f3 |

What are the second four bytes of round 9?

1. RSA: For p and q from [15,20], define RSA pair of keys, encrypt and decrypt M=11.
2. RSA: What is public key? What is private key? What for private key is used? What for public key is used?
3. Key distribution: Public key distribution, Private key distribution, Diffie-Hellman key exchange
4. Message authentication: Use of encryption and hashing
5. SHA-512: Messages of what sizes can be used as input to SHA-512? How original message length is saved in SHA-512 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 896 mod 1024 bits? What happens if the original message length is divisible by 1024?
6. How message is processed in SHA-512? 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 SHA-512 block? How 512-bit input is represented? How IV is initialized?
7. How many rounds has SHA-512 block? What are the inputs/outputs of the rounds? How SHA-512 output is obtained? What words, constants, and logical functions are used in the rounds? How constants K are defined? What transformations are made in each round?