FERHAT ABBAS UNIVERSITY

COMPUTER SCIENCE DEPARTMENT

MASTER 1 CYBER SECURITY (2024-2025)

Advanced Cryptography

-Mini AES-

Objectives:

- ✓ To implement a mini version of advanced encryption standard (AES)[1].
- ✓ To apply modes of operation.

Recommendations:

- All codes should be written in Java.

- All encrypted and decrypted messages are saved in text files.

Required work:

1. Mini-AES operates on 16-bits plaintext blocks with a secret key of 16-bits. It is mathematically based on the finite field GF(2^4) with the irreducible polynomial (x^4+x+1). It consists of two rounds that require four steps: *NibbleSub*, *ShiftRow*, *MixColumn* and *KeyAddition*, as shown in Figure 1.

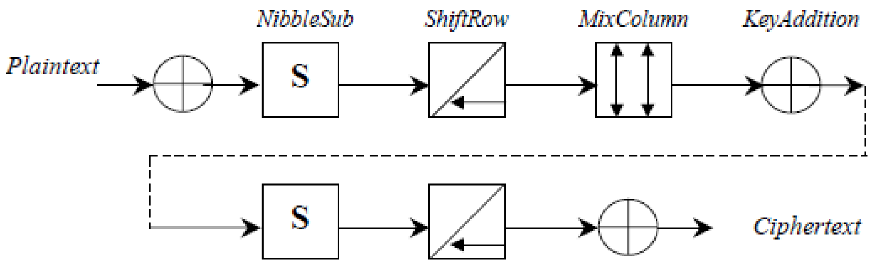
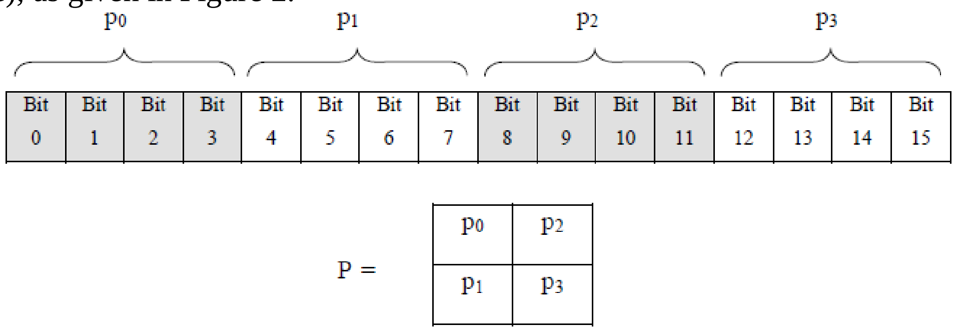


Figure 1. Mini-AES encryption.

The input plaintext block of 16 bits, P = (p0, p1, p2, p3) is represented as a matrix of 2 rows and 2 columns of 4 bits (a nibble), as given in Figure 2.



p0				p1				p2				p3			
Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8	Bit 9	Bit 10	Bit 11	Bit 12	Bit 13	Bit 14	Bit 15

$$P = \begin{array}{|c|c|} \hline p_0 & p_2 \\ \hline p_1 & p_3 \\ \hline \end{array}$$

Figure 2. Matrix representation of 16-bits block

[1] Mini-AES is an educational cipher and is not considered secure for actual applications.

The round keys are obtained from the secret key, as in Table 1. Note that in each round, round constants rcon(i) are used, where rcon(1) = 0001 and rcon(2) = 0010.

Round	**Round Key Value**

0	w0 = k0
	w1 = k1
	w2 = k2
	w3 = k3

1	w4 = w0 ⊕ SubBytes(w3) ⊕ rcon(1)
	w5 = w1 ⊕ w4
	w6 = w2 ⊕ w5
	w7 = w3 ⊕ w6

2	w8 = w4 ⊕ SubBytes(w7) ⊕ rcon(2)
	w9 = w5 ⊕ w8
	w10 = w6 ⊕ w9
	w11 = w7 ⊕ w10

Table 1. Key expansion

NibbleSub is a simple operation that substitutes each input nibble with an output nibble according to a substitution table (S-box), as given in Table 2.

Input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Output	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Table 2. S-box of Mini-AES

ShiftRow rotates each row of the input block to the left by different nibble amounts. The first row is unchanged while the second row is rotated left by one nibble.

MixColumn takes each column of the input block and multiplies it with a constant matrix, as shown in Figure 2.

$$\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$$

Figure 2. Constant matrix of Mini-AES

Give the steps of decryption.

2. Write a code for each function: NibbleSub, ShiftRow, MixColumn[2], and KeyAddition.
3. Generate randomly a secret key of 16-bits (4 numbers between 0 and 15).
4. Compute the two round keys.
5. Write a code that encrypts **one block** of plaintext.
6. Write a code that inputs the S-box and returns the InvNibbleSub.
7. Noting that the inverse of MixColumn is the same, write a code that decrypts the obtained ciphertext.
8. Consider the plaintext “9C639C62”, encrypt it with the secret key “C3F0”.
9. Generate randomly an initialization vector (IV) of 16-bits.
10. Apply CBC mode to encrypt the same plaintext and compare the two ciphertexts.

[2] It requires polynomial multiplication over GF(2^4).