Introduction to Data and Cyber-Security (DCS3101) - Assignment 2

Kiran Raja (kiran.raja@usn.no)

October 1, 2020

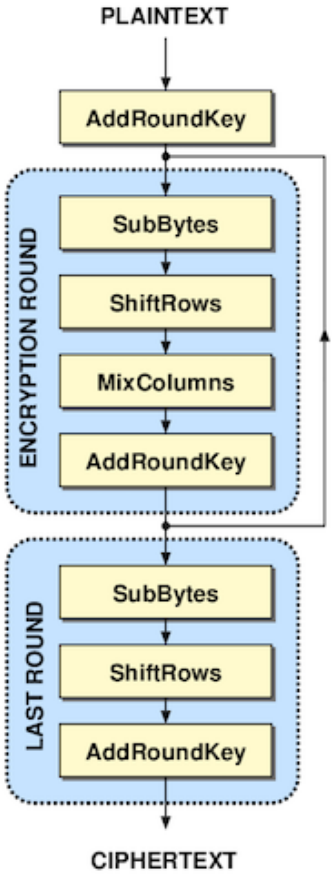
Universitetet i Sørøst-Norge

1 Organization and Information

1. This is the second assignment of the total 4 assignments for this course.
2. The assignment is mandatory and must be passed to attend the final exam.
3. Group work is tolerated but submissions are individual.
4. Each submission will be graded independently.
5. *Deadline for submission of assignment is 15 Oct, 2020.*
6. The extra credit point (Q6) can be used carried to assignments 4 in case you obtain lower points.
7. Assignments are to be submitted via Canvas.

2 Assignment

Q1 Below is a simplified figure of Advanced Encryption Standard with 9 encryption rounds for a given **plaintext**. Please provide a decryption algorithm using the similar approach for a given **ciphertext**. [1 Point]



Q2 AES Key scheduling - Given the rounding operation as described below:

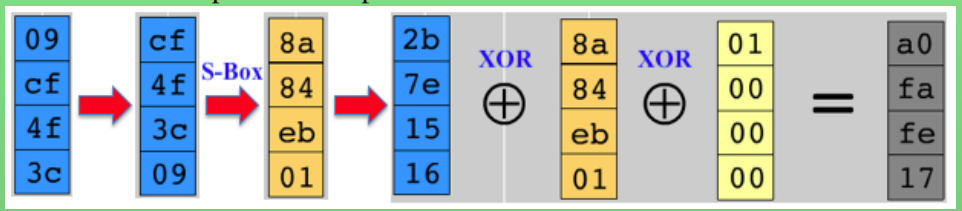
AES Key scheduling

(a) Take w_{i-1} column and rotate 1 byte up

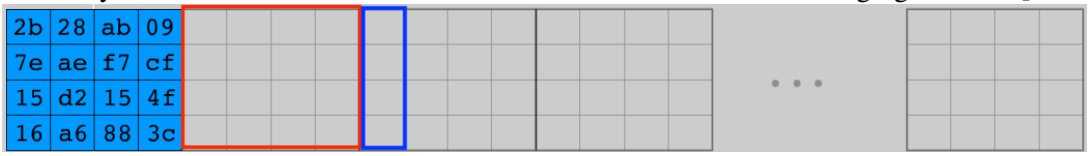
(b) Apply S-box to each of the 4 bytes

(c) XOR w_{i-4} to the result and XOR $RCON(i/4)$ to the result, where $RCON$ stands for Round Constant.

Below is an example of such operation:



Provide your answers for the block marked in red and blue in the following figure. [1 Points]



*Note - The calculations of one of the three columns within red-box (except the first column) and the calculations of values for blue box must be shown.

Q3 Consider a message string "DCS-3101", the initialization vector "NO" and the key "EU". For this exercise, consider one block consists of 16 bits and encryption is simply XOR operation. Please refer to lecture notes on Block ciphers and Stream ciphers to solve this problem.

Q3.1 Illustrate the encryption using ECB on the whole message string. [2 Points]

Q3.2 Illustrate the encryption using CBC on the whole message string. [2 Points]

Q3.3 Illustrate the encryption using OFB on the whole message string. [2 Points]

Q3.4 From the output in first block from OFB, flip the last bit. Using the new output, illustrate the impact on the output (i.e., decryption). [2 Points]

Q4 Extra Credit - Discuss and identify the challenges in Symmetric versus Asymmetric cryptography. Provide the examples of both class of algorithms. Please use figures and tables if necessary. [2 Points]

Appendix

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 1: S-Box