Advanced Encryption Standard (AES) Modes of Operation

Arya Rohan
Under the guidance of Dr. Edward Schneider
University of Maryland, College Park

MISSION:
TO SIMULATE BLOCK CIPHER MODES OF OPERATION FOR AES IN MATLAB

- Simulation of the AES (Rijndael Algorithm) in MATLAB for 128 bit key-length.
- Simulation of the five block cipher modes of operation for AES as per FIPS publication.
- Comparison of the five modes based on Avalanche Effect.
- Future Work

OUTLINE

- A brief history of AES
- Galois Field Theory
- De-Ciphering the Algorithm-ENCRYPTION
- De-Ciphering the Algorithm-DECRYPTION
- Block Cipher Modes of Operation
- Avalanche Effect
- Simulation in MATLAB
- Conclusion & Future Work
- References

A Brief History of AES

- In January 1997, researchers world-over were invited by NIST to submit proposals for a new standard to be called Advanced Encryption Standard (AES).

- From 15 serious proposals, the Rijndael algorithm proposed by Vincent Rijmen and Joan Daemen, two Belgian cryptographers won the contest.
- The Rijndael algorithm supported plaintext sizes of 128, 192 and 256 bits, as well as, key-lengths of 128, 192 and 256 bits.
- The Rijndael algorithm is based on the Galois field theory and hence it gives the algorithm provable security properties.

Galois Field

Galois Field - Group

- **Group/Albelian Group:** A group G or {G, ·} is a set of elements with a binary operation denoted by · , that associates to each ordered pair (a, b) of elements in G an element (a · b) such that the following properties are obeyed:
  - **Closure:** If a & b belong to G, then a · b also belongs to G.
  - **Associative:** For elements a, b & c in G, a · (b · c) = (a · b) · c.
  - **Identity element:** There is an element e in G such that a · e = e · a = a, for all a in G.
  - **Inverse element:** For each element a in G there is an element a' in G such that a · a' = a' · a= e.
  - **Commutative:** for all elements a & b in G, a · b = b · a.

Galois Field - Ring

- **Ring/Commutative Ring:** A ring R or {R, +, x} is a set of elements with two binary operations , addition and multiplication, such that for all a, b & c in R the following properties are obeyed.
  - All properties inside the definition of a 'Group' are obeyed.
  - **Closure under multiplication:** If a & b belong to R, then a x b also belongs to R.
  - **Associativity of multiplication:** a x (b x c) = (a x b) x c for all a, b & c in R.
  - **Distributive laws:** a x (b + c) = a x b + a x c; (a + b) x c = a x c + b x c for all a, b & c in R.
  - **Commutativity of multiplication:** a x b = b x a, for a & b in R.
  - **Multiplicative identity:** There is an element 1 in R such that a x 1 = 1 x a = a, for all a in R.
  - **No zero divisors:** If a, b in R and a x b = 0, then either a = 0 or b = 0.

Galois Field - Field

- **Field:** A field F or {F, +, x} is a set of elements with two binary operations, addition and multiplication, such that for all a, b & c in F the following properties are obeyed.
  - All properties inside the definition of 'Group' and 'Ring' are obeyed.
  - **Multiplicative inverse:** For each element a in F, except 0, there is an element a-1 in F such that $aa^{-1} = (a^{-1})a = 1$.
- **Note:** Finite field of the order p^n, is written as GF (p^n). We will study this field when n = 1 and when p = 2.
- **Finite field of form GF (p):** For a given prime p, finite field of order p, GF (p), is defined as the set Z_p of integers {0, 1, 2…..p-1} together with the arithmetic operations modulo p.
  - **Addition:** a + b ⇔ (a + b) mod p
  - **Multiplication:** a * b ⇔ (a * b) mod p

Galois Field of form GF(p)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Multiplication modulo 7

GALOIS FIELD OF FORM GF(2^N)

- Arithmetic operations follow the ordinary rules of polynomial arithmetic using the basic rules of algebra, with the following two rules:
- **Rule 1:** Arithmetic on coefficients is performed modulo p. (In simple words addition, subtraction are done modulo 2 or equivalently XORed)
- **Rule 2:** If multiplication results in a polynomial of degree n-1 or greater, then the polynomial is reduced modulo some irreducible polynomial m(x) of degree n. Hence, f(x)*g(x) → f(x)*g(x) mod m(x)

GF(2^3) [m(x) = x^3+x^2+1 or x^3+x+1]

		000	001	010	011	100	101	110	111
	+	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Addition

		000	001	010	011	100	101	110	111
	+	0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

Addition

GF(2^3) [M(X) = X^3+X^2+1 OR X^3+X+1]

	×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Multiplication

	×	000 0	001 1	010 2	011 3	100 4	101 5	110 6	111 7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

Multiplication

AES – GF(2^8)

- For AES, the finite field defined is GF(2^8).
- Addition and subtraction operations are equivalent to XOR operation.
- Multiplication is done using $m(x) = x^8 + x^4 + x^3 + x + 1$.
- $F(x) = x^6+x^4+x^2+x+1 \rightarrow 87$
- $G(x) = x^7+x+1 \rightarrow 131$
- $F(x) + G(x) = x^7+x^6+x^4+x^2 = 212$
- $F(x)*G(x) = F(x)*G(x) \bmod m(x)$
  - $F(x)*G(x) = x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$
  - $F(x)*G(x) \bmod m(x) = x^7+x^6+1 = 193$

De-Ciphering the Algorithm-Encryption

- The Rijndael algorithm starts with the key-expansion step. In this step, the 128, 192 or 258 bit key is expanded into 11, 13 and 15 sub-keys respectively, representing the number of rounds.

- Each sub-key has the same number of bits as the primary symmetric key.

- The four major steps of the Rijndael algorithm during encryption are
    - SubBytes Step
    - ShiftRows Step
    - MixColumns Step
    - Add Round Key step

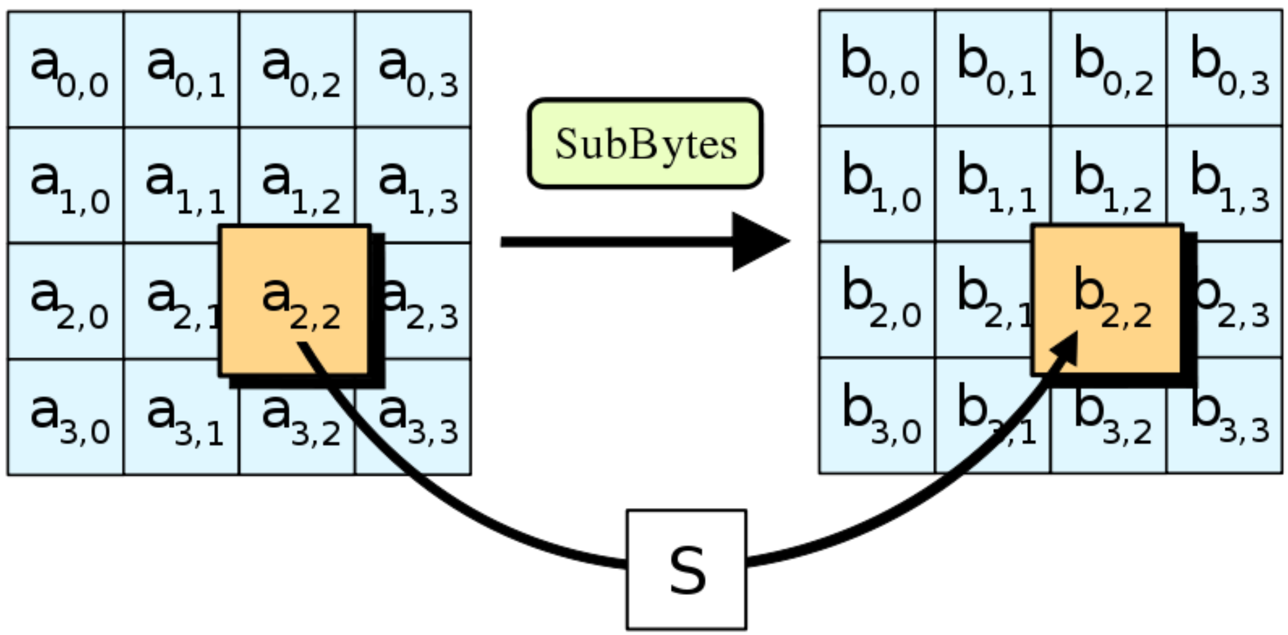
SubBytes Step-I

- Here each byte in the plain-text array is substituted using an 8-bit substitution box.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

SUBBYTES STEP-II

- It provides non-linearity to the cipher.



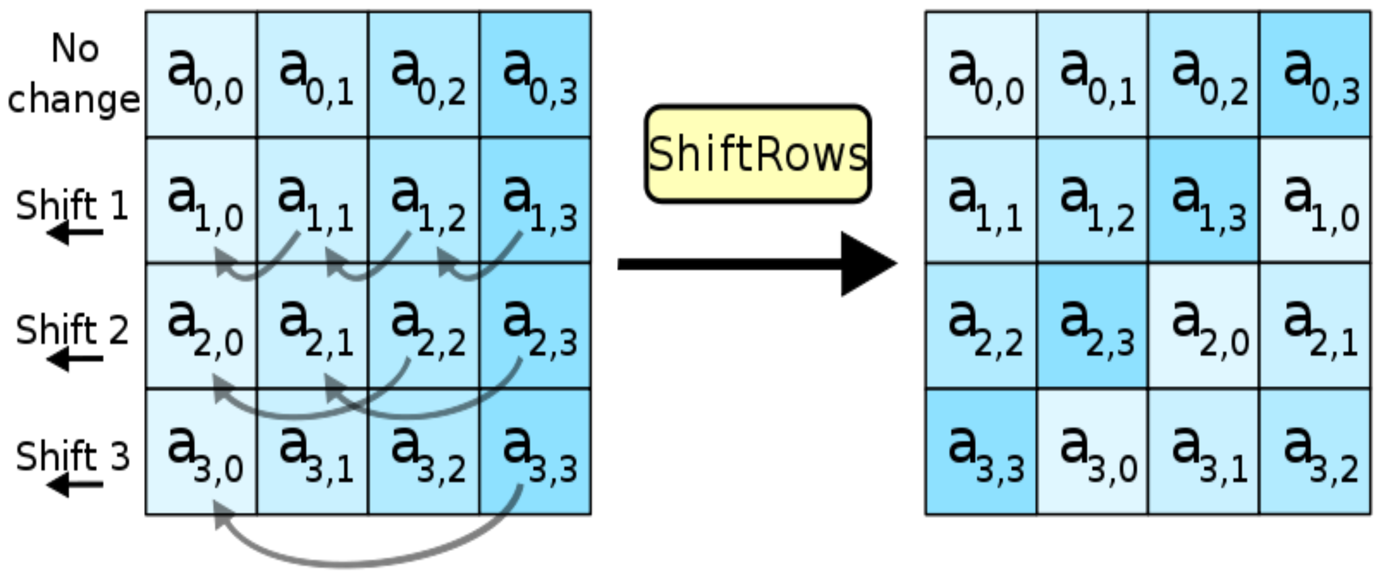
SubBytes Step – III

- For any F(x), find its multiplicative inverse.
- Or, find G(x) such that F(x)*G(x) mod m(x) = 1
- Perform the affine transform on G(x) to get the substitution value

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

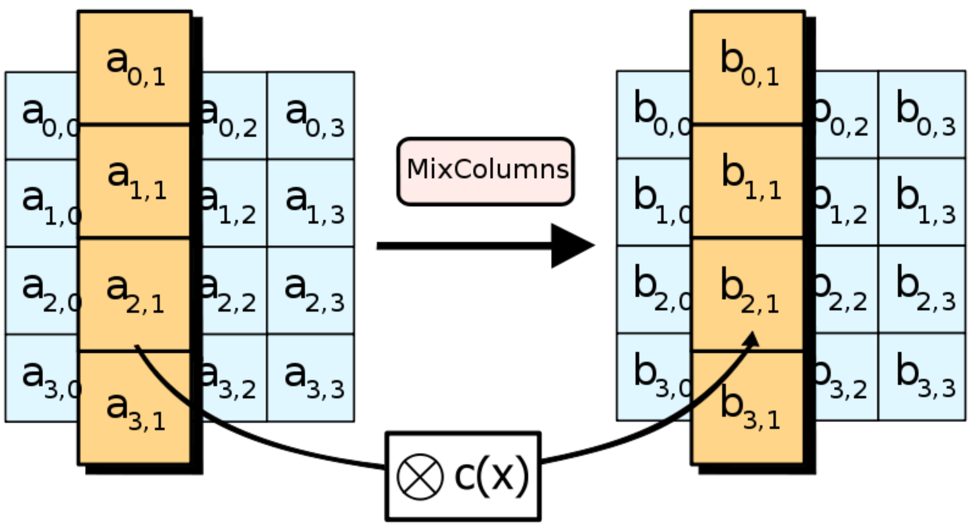
ShiftRows Step

- This step operates on the rows of the state, cyclically shifting it by a fixed offset.
- The Shiftrows and the next step (Mixcolumns step) provides diffusion to the cipher.



MixColumns Step – I

- Here the four bytes of each column of the state are combined using an invertible linear transformation.
- The transformation function takes each of the four bytes as input and gives four output bytes with each input byte affecting all four output bytes.



MixColumns Step – II

- The MixColumns step is performed by carrying out the following transformation on each column.

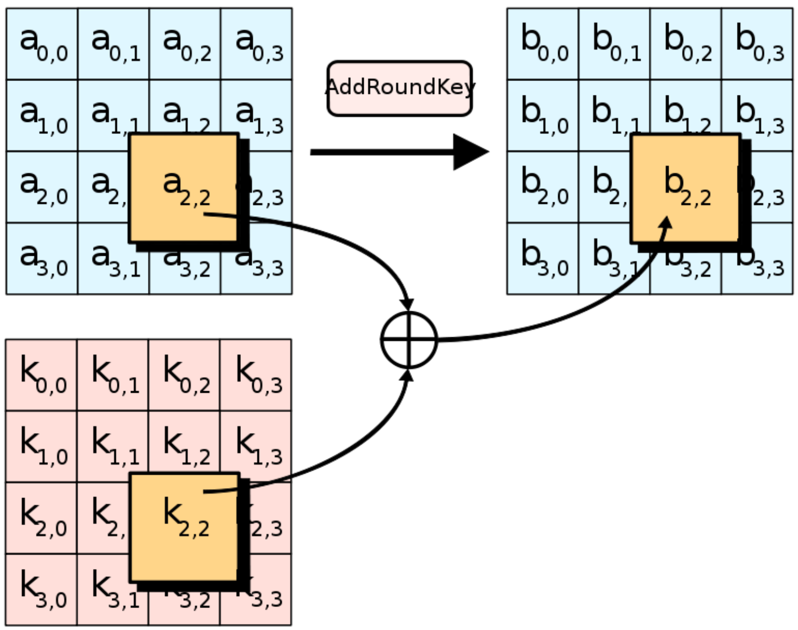
$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

$$r_0 = 2a_0+3a_1+a_2+a_3$$
$$r_1 = a_0+2a_1+3a_2+a_3$$
$$r_2 = a_0+a_1+2a_2+3a_3$$
$$r_3 = 3a_0+a_1+a_2+2a_3$$

- The multiplication and additions are performed as discussed before.

AddRoundKey Step

- In this step the sub-key is combined with the state.
- Each byte of the state is XOR-ed with the respective bytes of the sub-key



- All the four steps are repeated for each round.

De-Ciphering the Algorithm- Decryption

- The decryption applies the inverse operation of the encryption routine
- However, the first step is to expand the key through the key-expansion step.
- The inverse of addroundkey is exactly the same
- The inverse of subbytes step uses an inverse 8-bit substitution box
- The inverse of shiftrows step is shifting the rows over a suitable distance

- The inverse substitution box

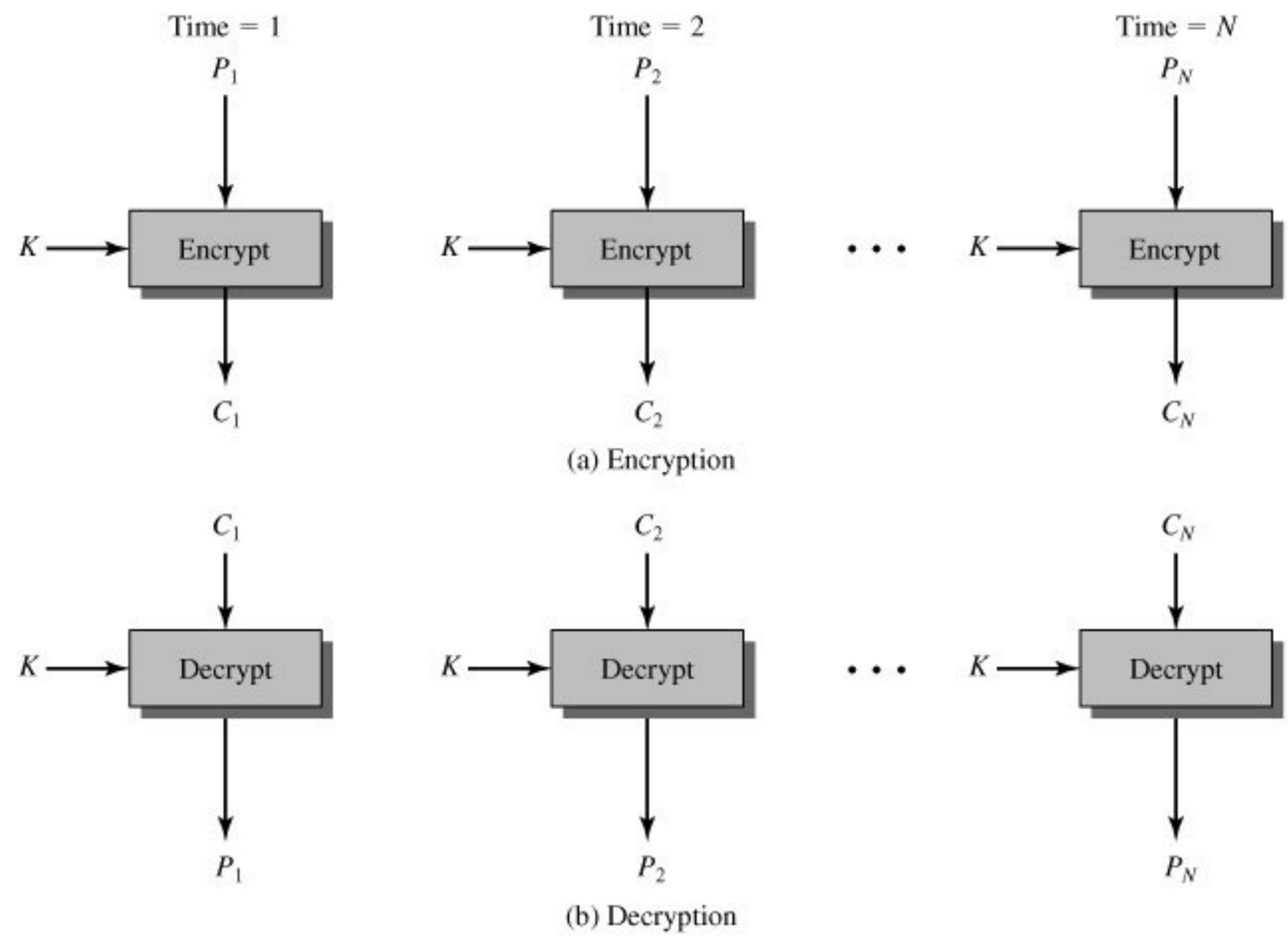
	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1x	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2x	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3x	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4x	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5x	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6x	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7x	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8x	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9x	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
ax	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
bx	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
cx	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
dx	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
ex	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
fx	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Block Cipher Modes of Operation

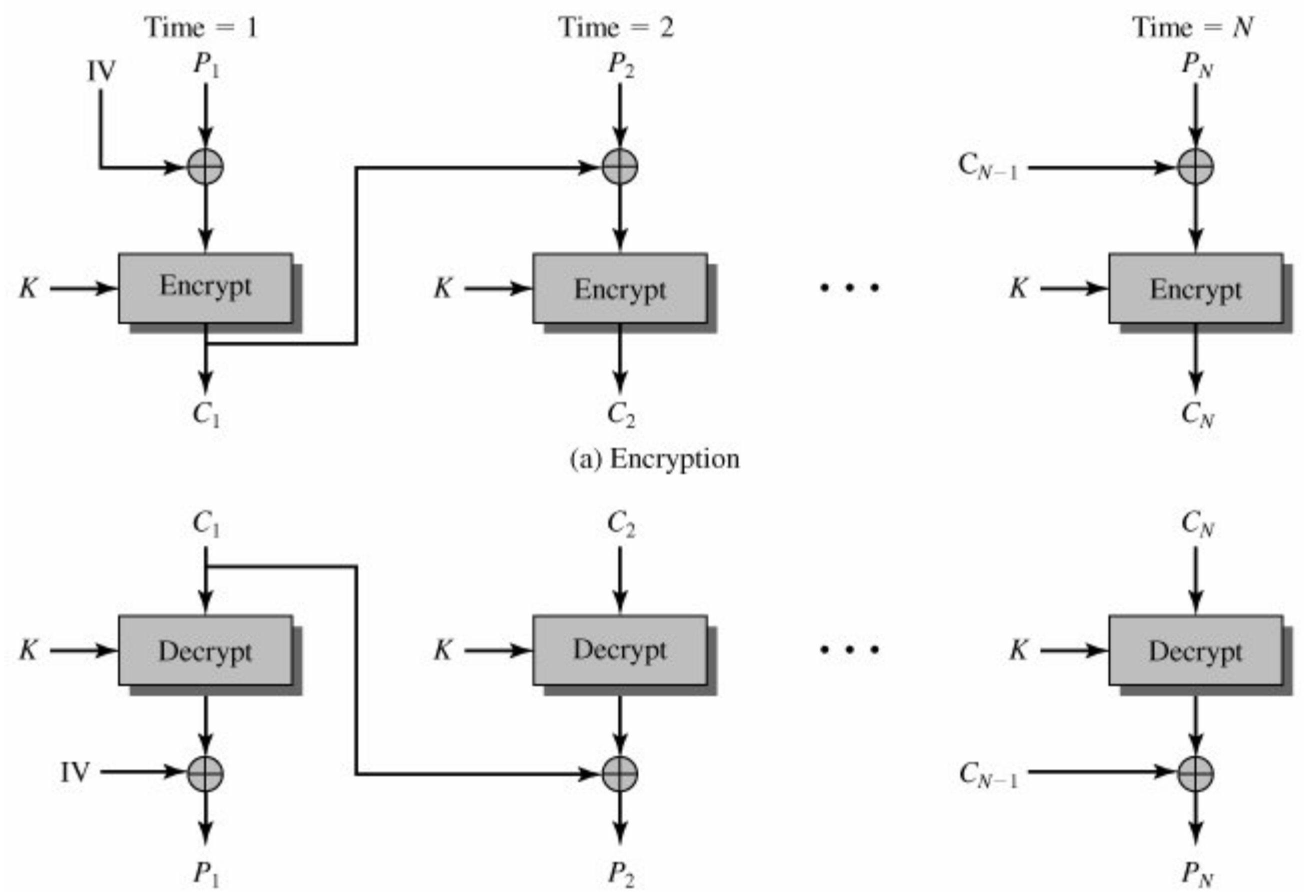
Block Cipher Modes of Operation

- A mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application such as applying a block cipher to a sequence of data blocks or a data stream.
- Can be used with any symmetric block cipher algorithm such as DES, 3DES or AES.
- NIST originally defined four modes of operation, as part of FIPS 81, through which block ciphers can be applied to a variety of applications. However, with newer applications the NIST extended the list of federal recommended modes to five in Special Publication 800-38A.

Electronic Codebook (ECB)



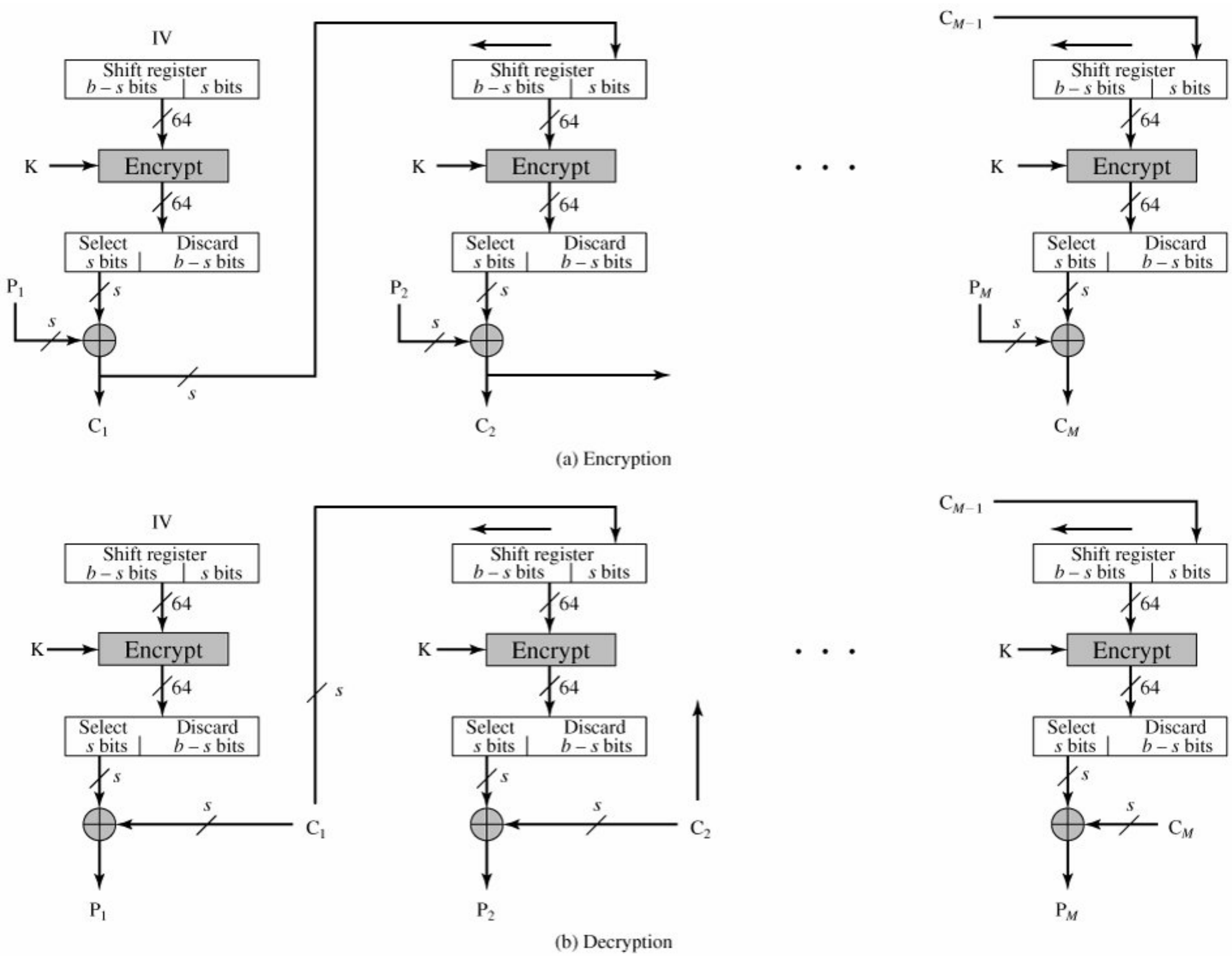
Cipher Block Chaining (CBC)



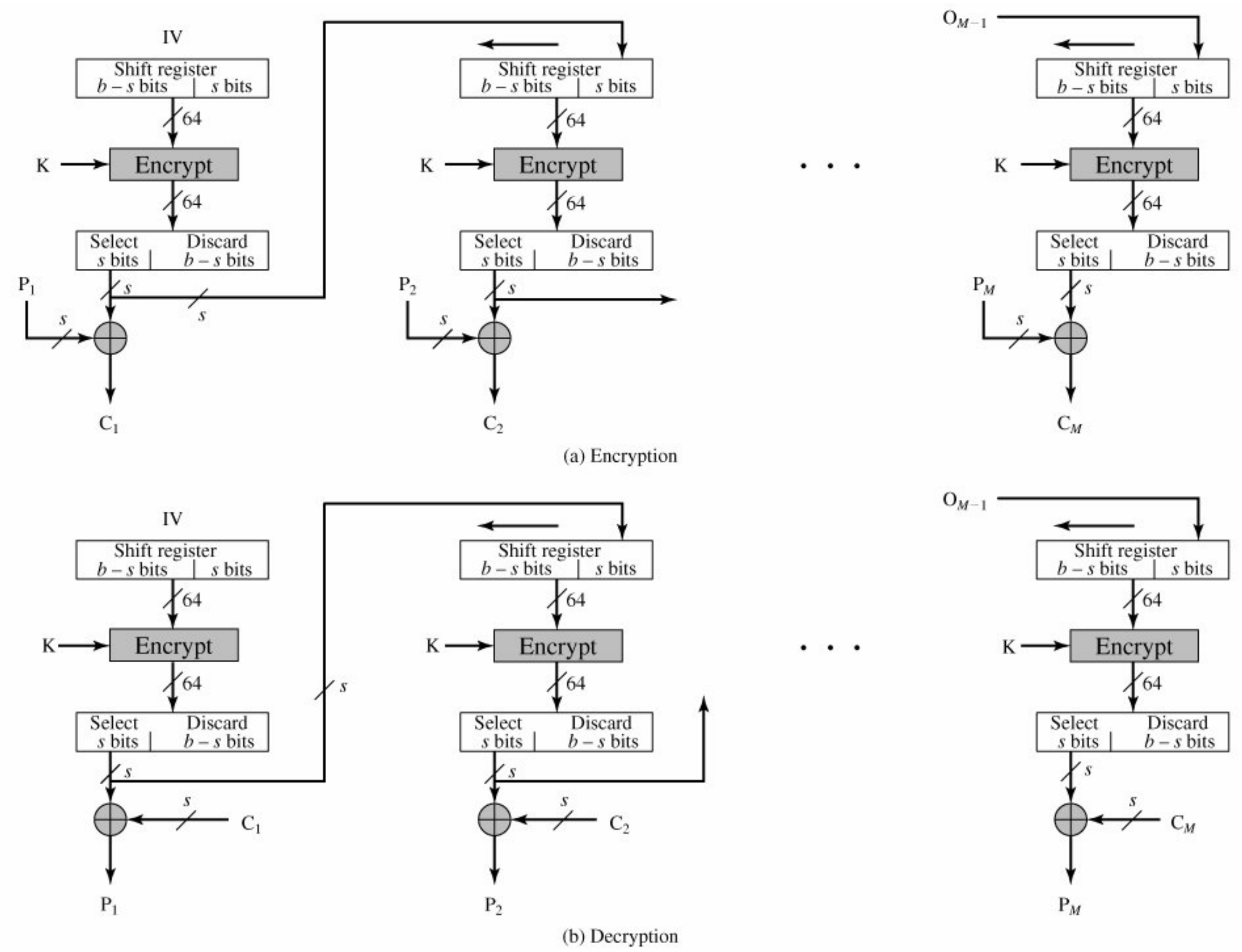
(a) Encryption

(b) Decryption

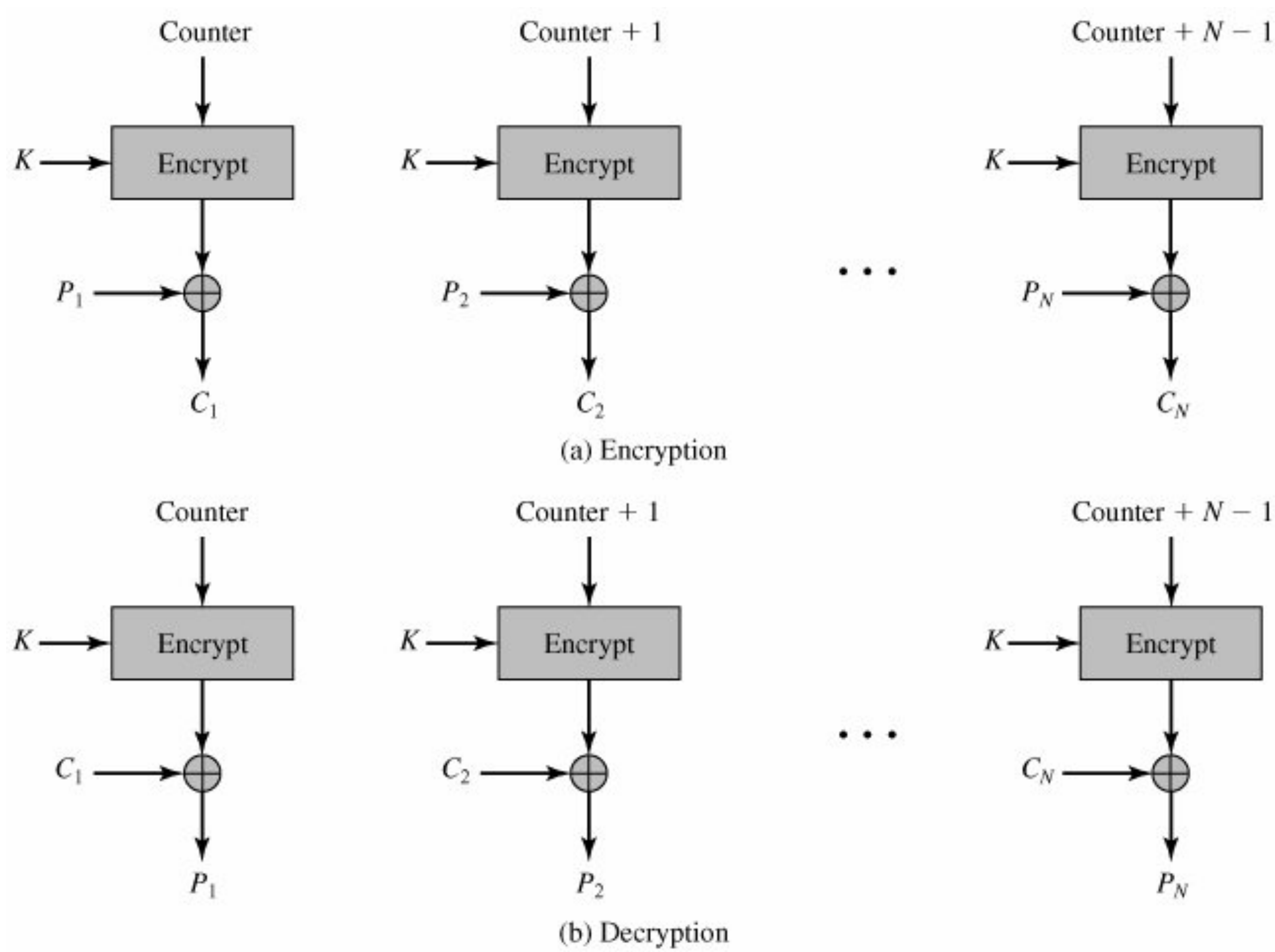
Cipher Feedback Mode (CFB)



Output Feedback Mode (OFB)



Counter Mode (CTR)



Avalanche Effect

Avalanche Effect

- When the input (plaintext or key) to any cryptographic algorithm is changed slightly, then there must be significant change in the output.
- It is the most desirable property of any cryptographic algorithm is the avalanche effect. It was a term coined by Horst Feistel.
- It accounts for the randomization in the algorithm or can be thought of as a metric for diffusion & confusion.
- Normally, a change of about 50% is desirable as it makes the algorithm truly random.

Simulation in MATLAB

Simulation Parameters

- A plaintext-key combination is given as input.
- First, a random bit in the plaintext is changed and percentage change in the cipher for all five modes is outputted.
- Then, a random bit in the key is changed and percentage change in the cipher for all five modes is outputted.
- This process is repeated for several plaintext-key combinations (20).
- The results are averaged over all different plaintext-key combinations.

Simulation Results

	ECB	CBC	CFB	OFB	CTR
Key	52%	53%	48%	48%	47%
Plaintext	93%	74%	87%	*98%	*98%

CONCLUSION & FUTURE WORK

- We learnt the mathematics behind the design of the Rijndael Algorithm (AES)
- We briefly analyzed the five block cipher modes of operation for AES based on the Avalanche effect.
- For the future, I would like to simulate the DES and 3-DES algorithms and compare them with AES.
- And of course, my constant efforts to break the Rijndael algorithm. ☺

References

- The Design of Rijndael, AES-The Advanced Encryption Standard, Joan Daemen & Vincent Rijmen, 2002 by Springer.
- Advanced Encryption Standard (AES), FIPS Publication 97, Nov 26, 2001.
- Cryptography and Network Security, William Stallings, Fourth Edition, 2006 by Pearson Education-Prentice Hall.
- http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- http://en.wikipedia.org/wiki/Rijndael_S-box
- http://en.wikipedia.org/wiki/Rijndael_key_schedule
- http://en.wikipedia.org/wiki/Rijndael_mix_columns

Questions?

☺

Thank You