Advance Encryption Standard

Yebeltal Asseged

Topic

- Background
- Algorithm
- Architecture and Implementation
- Question

Background

- Intended to replace DES
  - Developed by IBM
  - Triple DES – too slow
- NIST call for a new cipher in 1997
  - Only 15 candidates submitted algorithms 1998
  - Only 5 were shortlisted

Background – cont’d

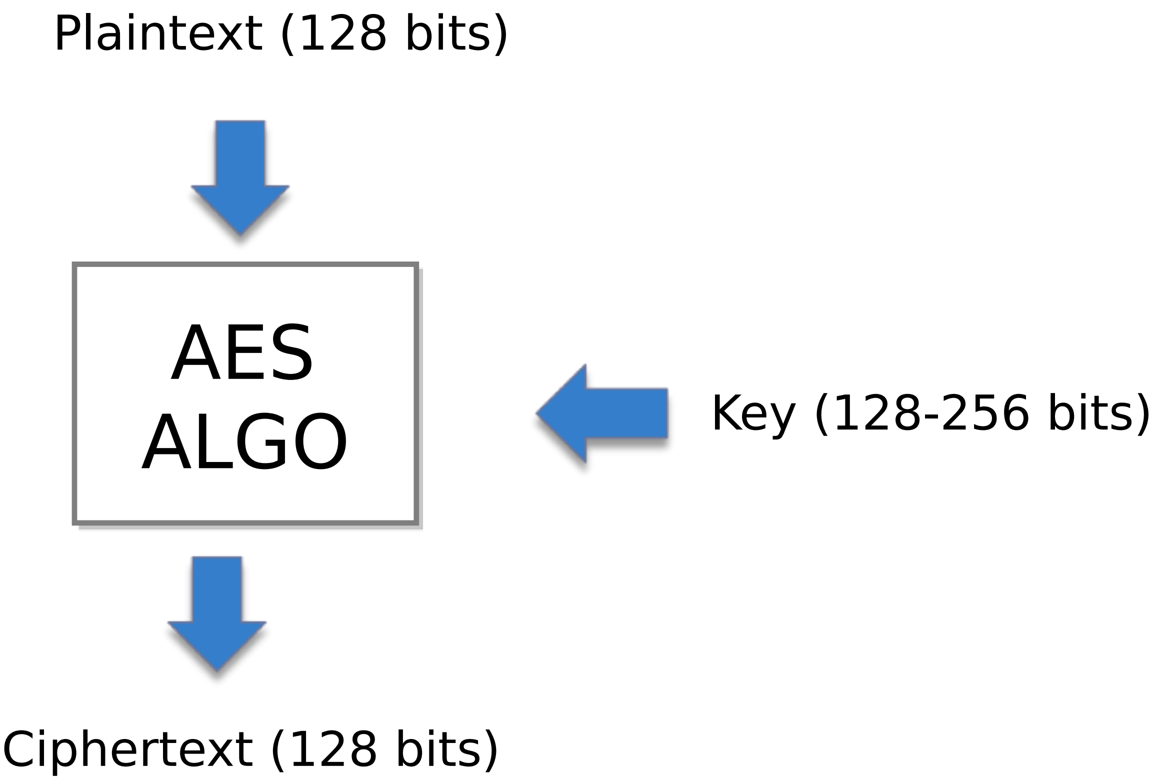
- The 5 short lists
  - Serpent - high security margin but slow
  - Twofish - high security margin but complex
  - RC6 - simple but low security margin
  - IBM’s MARS – fast but complex
  - Rijndael - good security margin, fast, not complex

Background - cont’d

- Rijndael was selected in 2000
  - V. Rijmen and J.Daemen from Belgium
  - Has capability 128, 192 and 256 bit key, 128 bits data
  - Tested
  - NSA endorsed

Algorithm

- overview`



Plaintext (128 bits)

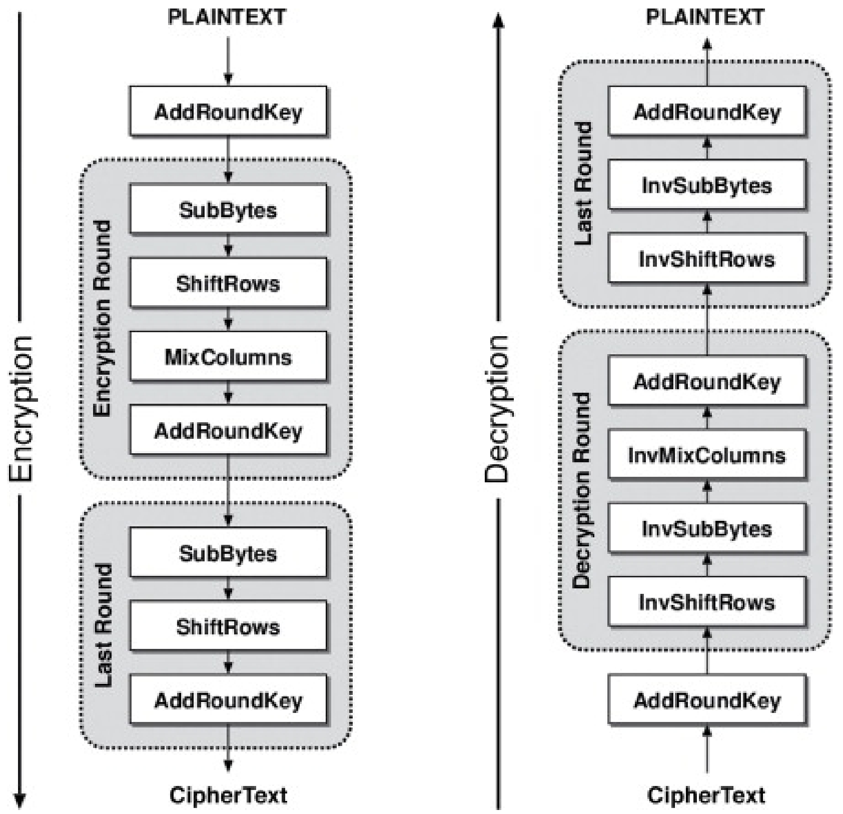
AES ALGO

Key (128-256 bits)

Ciphertext (128 bits)

Algorithm cont'd

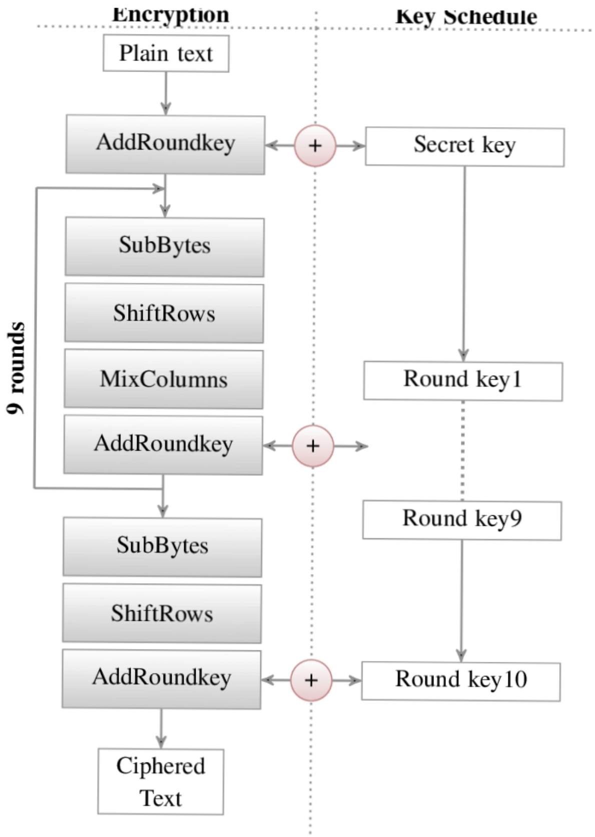
- AES Algo
  - 128 – 10 rounds
  - 192 – 12 rounds
  - 256 – 14 rounds



Source:
www.sciencedirect.com

Algorithm cont’d

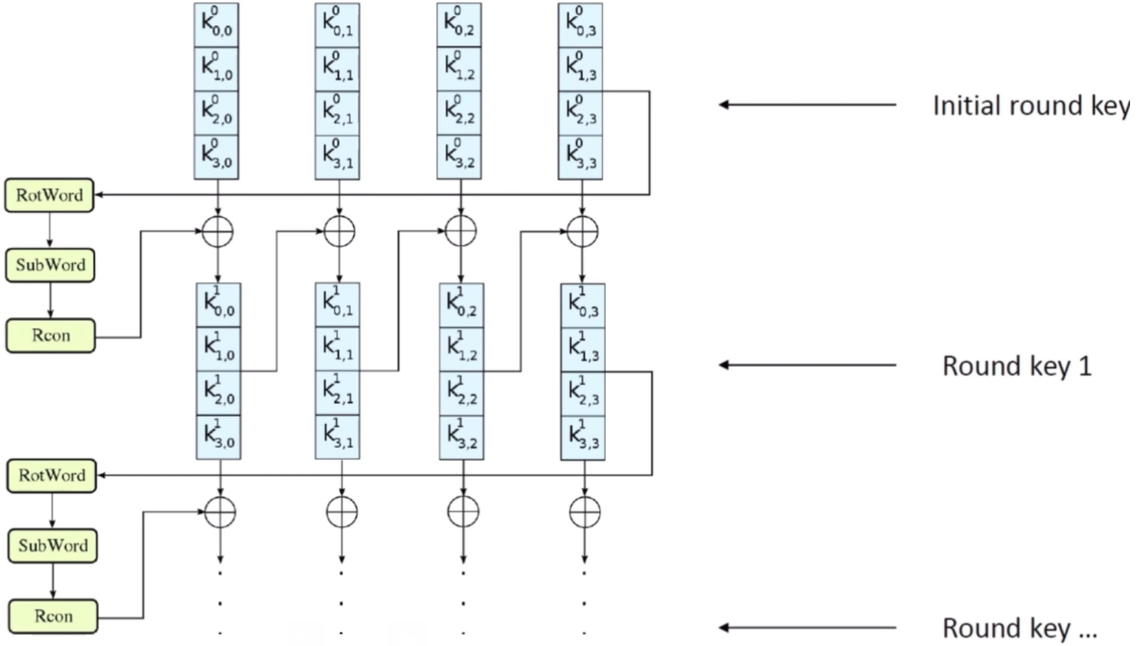
- AES algo
  - 128 bit key



Source: www.sciencedirect.com

Architecture and Impl.

- Key Expansion
  - AES 128 -- 11
  - AES 192 -- 13
  - AES 256 – 15
  - Involves Rotate, Substitute, Round


$K^0_{0,0}$ $K^0_{0,1}$ $K^0_{0,2}$ $K^0_{0,3}$
$K^0_{1,0}$ $K^0_{1,1}$ $K^0_{1,2}$ $K^0_{1,3}$
$K^0_{2,0}$ $K^0_{2,1}$ $K^0_{2,2}$ $K^0_{2,3}$
$K^0_{3,0}$ $K^0_{3,1}$ $K^0_{3,2}$ $K^0_{3,3}$
Initial round key
RotWord
SubWord
Rcon
$K^1_{0,0}$ $K^1_{0,1}$ $K^1_{0,2}$ $K^1_{0,3}$
$K^1_{1,0}$ $K^1_{1,1}$ $K^1_{1,2}$ $K^1_{1,3}$
$K^1_{2,0}$ $K^1_{2,1}$ $K^1_{2,2}$ $K^1_{2,3}$
$K^1_{3,0}$ $K^1_{3,1}$ $K^1_{3,2}$ $K^1_{3,3}$
Round key 1
RotWord
SubWord
Rcon
Round key ...

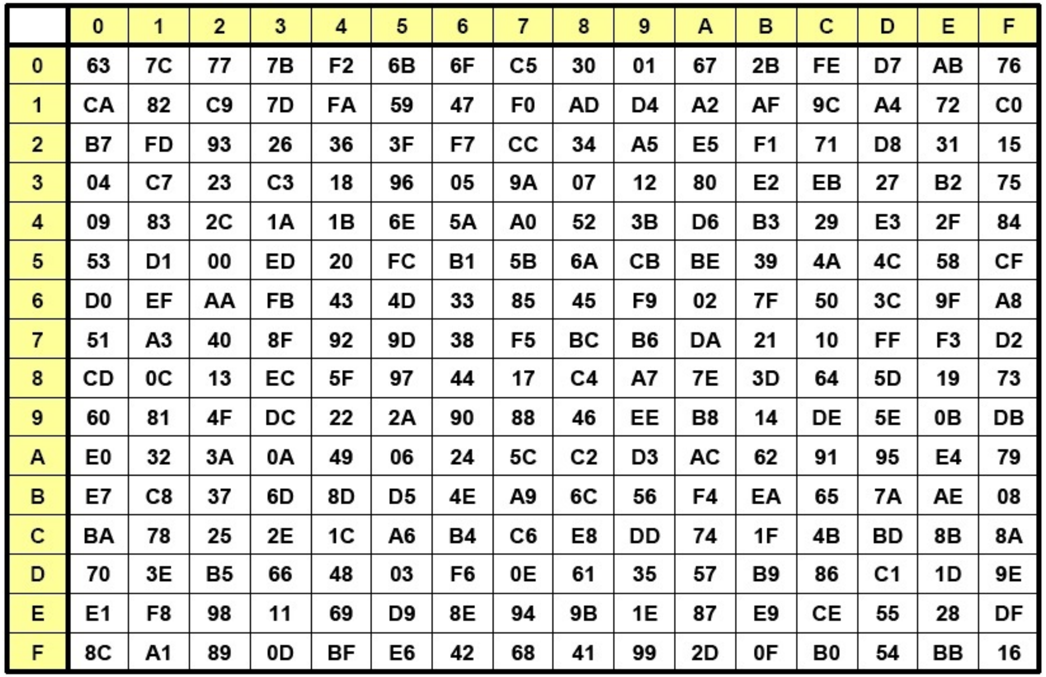
Source:
www.sciencedirect.com

Architecture and Impl.

- AddRoundKey
  - XOR expanded key to the plain text

Architecture and Impl.

- SubBytes
  - Substituting each byte
  - Calculated in Galois/finite Field

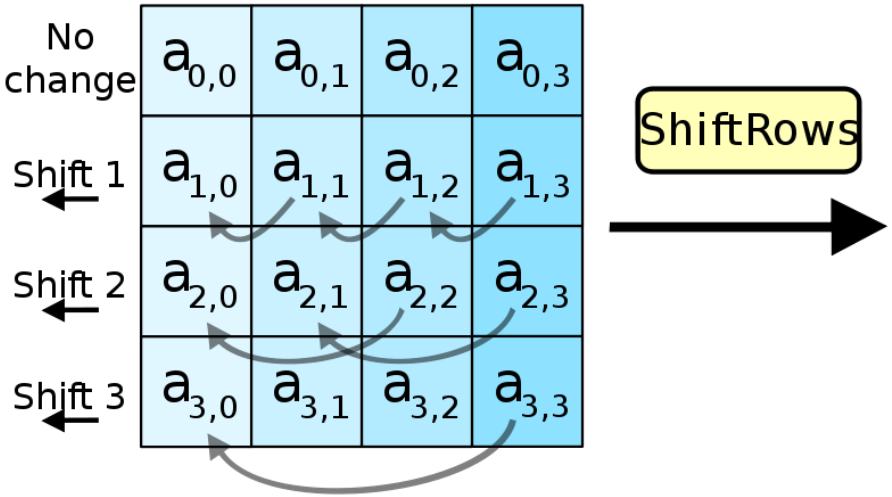


	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	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

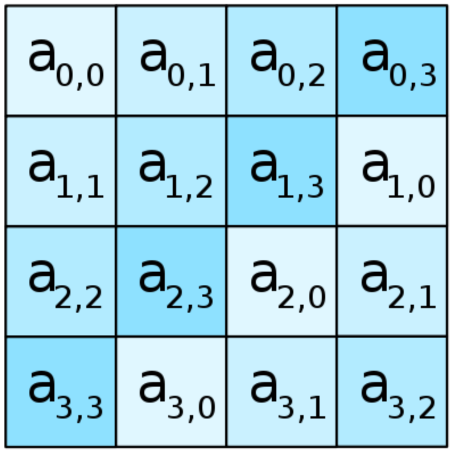
Source: wiki

Architecture and Impl.

- ShiftRow



No change	$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
Shift 1	$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
Shift 2	$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
Shift 3	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

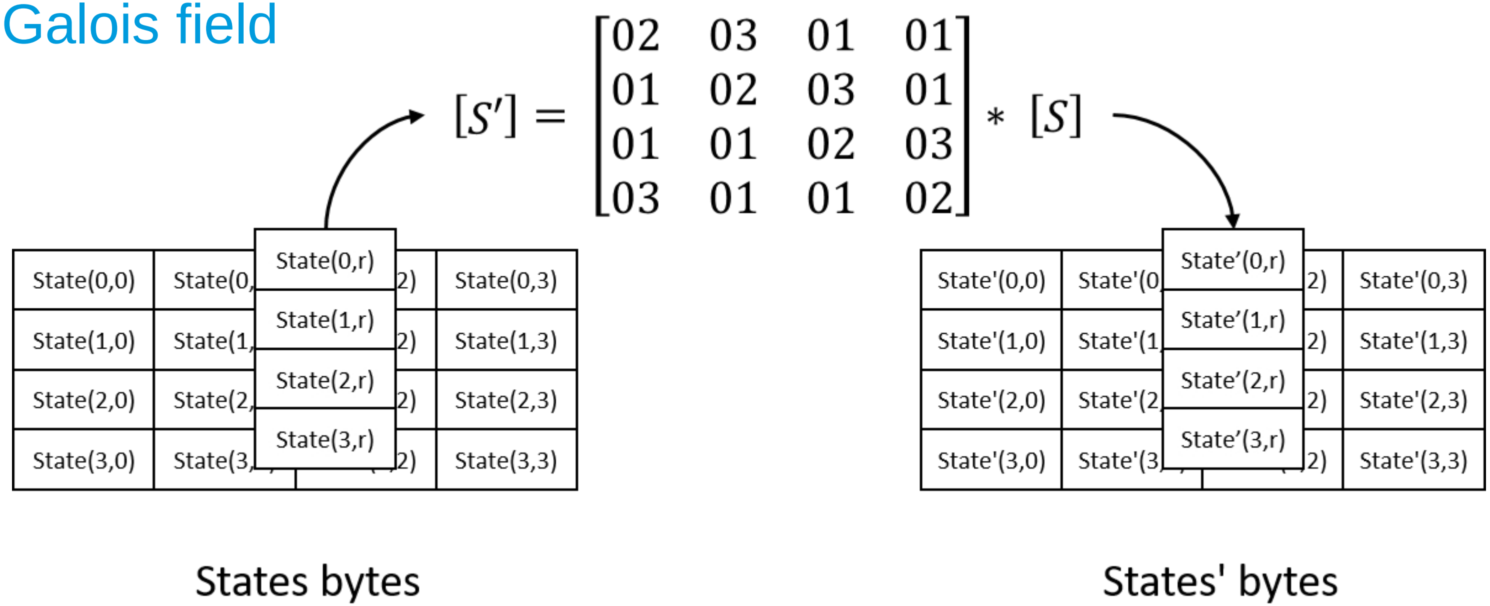


$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,0}$
$a_{2,2}$	$a_{2,3}$	$a_{2,0}$	$a_{2,1}$
$a_{3,3}$	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$

Source: wiki

Architecture and Impl.

- Mixcolumns
  - Two way of implementation
  - Performed in Galois field



$$[S'] = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * [S]$$

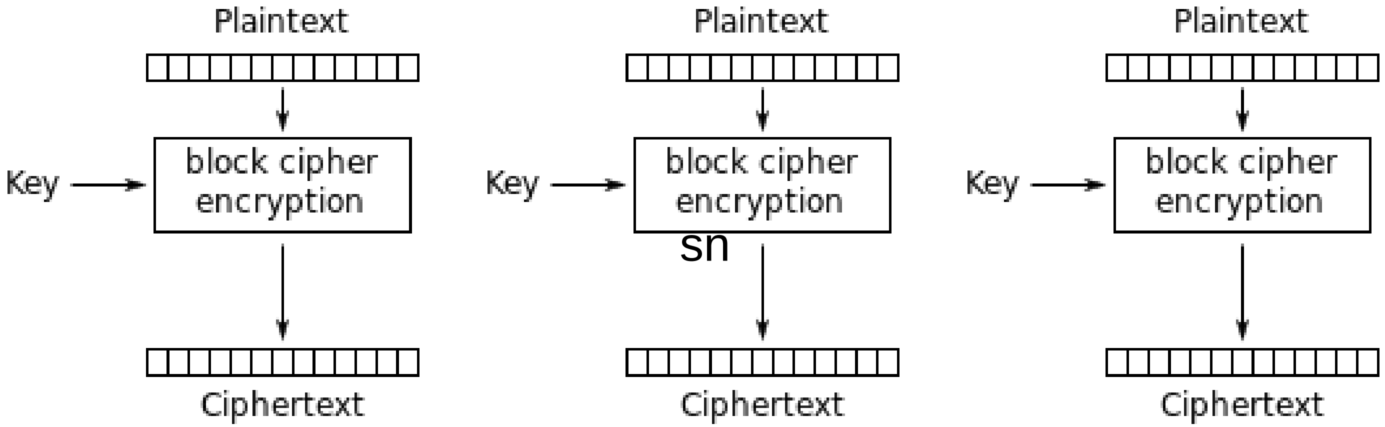
Source: wiki

States bytes

States' bytes

Architecture and Impl.

- Types of Block Cipher Modes
  - ECB

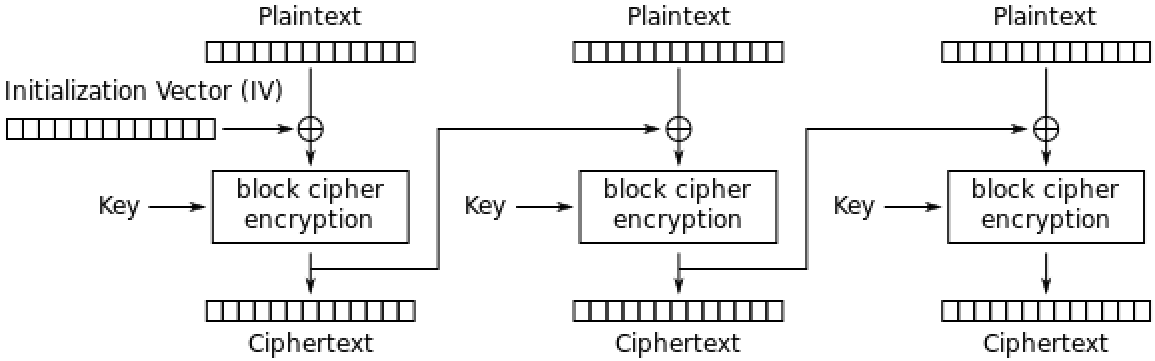


Electronic Codebook (ECB) mode encryption

Source: wiki

Architecture and Impl.

- Types of Block Cipher Modes
  - CBC

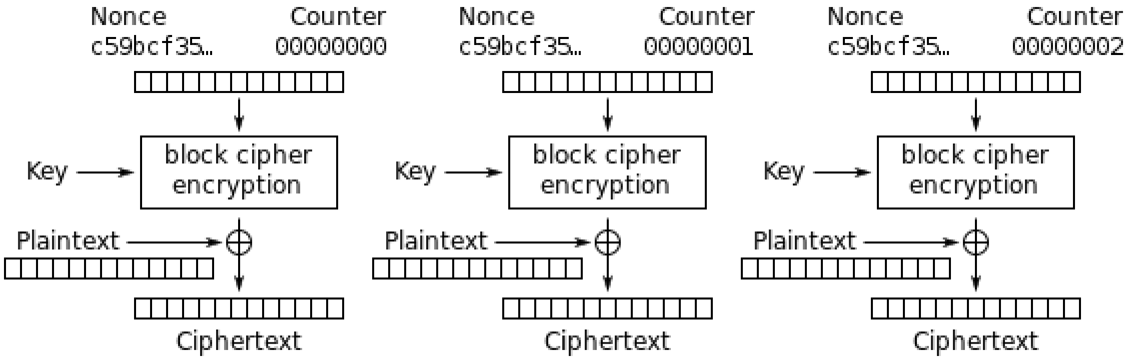


Cipher Block Chaining (CBC) mode encryption

Source: wiki

Architecture and Impl.

- Types of Block Cipher Modes
  - Counter Mode



Counter (CTR) mode encryption

Source: wiki

Questions

- https://github.com/yebeman