Cryptography and Network Security Chapter 5

> Fourth Edition by William Stallings

Lecture slides by Lawrie Brown

Origins

clear a replacement for DES was needed

- have theoretical attacks that can break it
- have demonstrated exhaustive key search attacks
- > can use Triple-DES but slow, has small blocks
- US NIST(National Institute of Standards and Technology) issued call for ciphers in 1997
- > 15 candidates accepted in Jun 98
- Rijndael was selected as the AES in Oct-2000
- issued as FIPS PUB 197 standard in Nov-2001

AES Requirements

private key symmetric block cipher
128-bit data, 128/192/256-bit keys
stronger & faster than Triple-DES
provide full specification & design details
both C & Java implementations

AES Evaluation Criteria

initial criteria:

- security effort for practical cryptanalysis
- cost in terms of computational efficiency
- algorithm & implementation characteristics

> final criteria

- general security
- ease of software & hardware implementation
- implementation attacks
- flexibility (in en/decrypt, keying, other factors)

AES Shortlist

after testing and evaluation, shortlist in Aug-99:
MARS (IBM) - complex, fast, high security margin
RC6 (USA) - v. simple, v. fast, low security margin
Rijndael (Belgium) - clean, fast, good security margin
Serpent (Euro) - slow, clean, v. high security margin

• Twofish (USA) - complex, v. fast, high security margin

The AES Cipher - Rijndael

> designed by Rijmen-Daemen in Belgium
> has 128/192/256 bit keys, 128 bit data
> an iterative rather than feistel cipher

- processes data as block of 4 columns of 4 bytes
- operates on entire data block in every round
- > designed to be:
 - resistant against known attacks
 - design simplicity

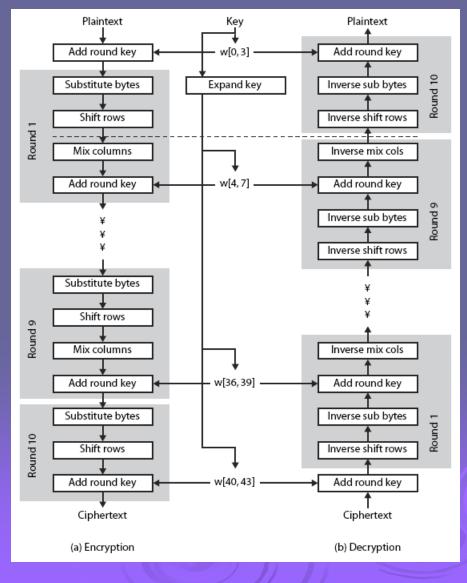
AES Parameters

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

Rijndael

- > data block of 4 columns of 4 bytes is state
- key is expanded to array of words
- > has 10/12/14 rounds in which state undergoes:
 - byte substitution (1 S-box used on every byte)
 - shift rows (permute bytes between groups/columns)
 - mix columns (subs using matrix multipy of groups)
 - add round key (XOR state with key material)
 - view as alternating XOR key & scramble data bytes

Rijndael

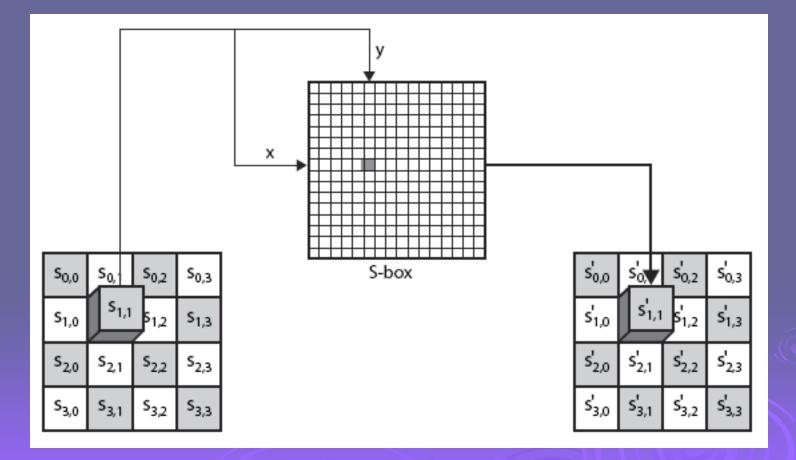


Byte Substitution

a simple substitution of each byte
uses one table of 16x16 bytes containing a permutation of all 256 8-bit values
each byte of state is replaced by byte indexed by row (left 4-bits) & column (right 4-bits)
eg. byte {95} is replaced by byte in row 9 column 5
which has value {2A}

> designed to be resistant to all known attacks

Byte Substitution



S-box

										y							
		0	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	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	C 0
	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	A 0	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
x	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
	Α	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	В	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	С	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F 6	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	0 D	BF	E6	42	68	41	99	2D	0F	B 0	54	BB	16

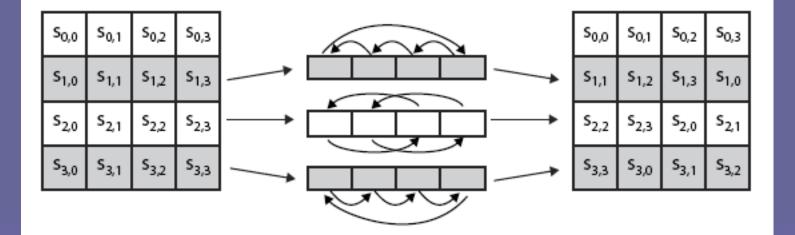
(a) S-box

Shift Rows

> a circular byte shift in each each

- 1st row is unchanged
- 2nd row does 1 byte circular shift to left
- 3rd row does 2 byte circular shift to left
- 4th row does 3 byte circular shift to left
- decrypt inverts using shifts to right
- since state is processed by columns, this step permutes bytes between the columns

Shift Rows

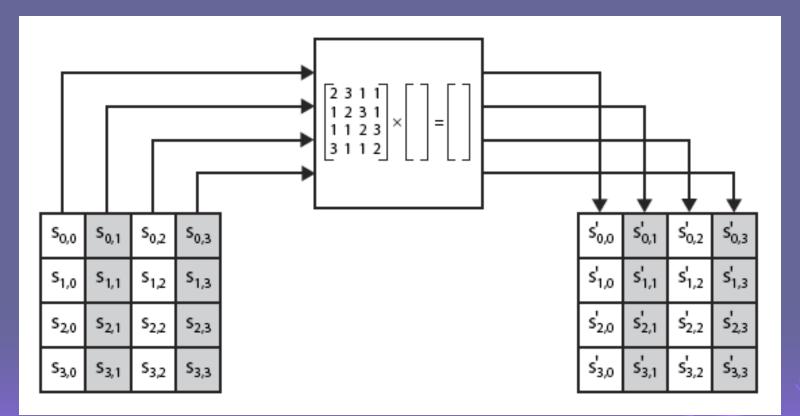


Mix Columns

 each column is processed separately
 each byte is replaced by a value dependent on all 4 bytes in the column

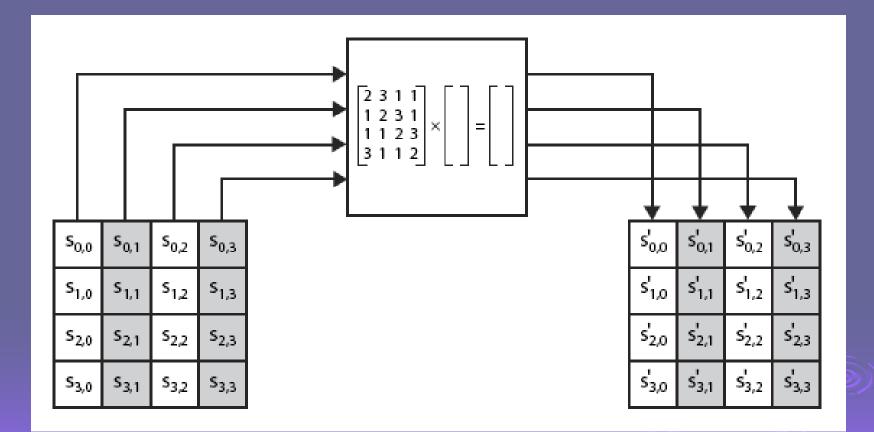
[02	03	01	$01][s_{0,0}]$	S _{0,1}	s _{0,2}	S0,3	[s0.0	$s_{0,1}$	S _{0,2}	s0,3
01	02	03	01 s _{1,0}	<i>s</i> _{1,1}	s _{1,2}	s _{1,3}	s _{1,0}	s _{1,1}	s _{1,2}	s _{1,3}
01	01	02	03 S _{2,0}	<i>s</i> _{2,1}	s _{2,2}	s _{2,3}	= s _{2,0}	\$2,1	S2,2	\$2,3
03	01	01	$ \begin{array}{c} 01 \\ 01 \\ s_{1,0} \\ 03 \\ 02 \end{array} \begin{bmatrix} s_{0,0} \\ s_{1,0} \\ s_{2,0} \\ s_{3,0} \end{bmatrix} $	s _{3,1}	s _{3,2}	s33	s _{3,0}	$s_{3,1}$	\$3,2	s3,3

Mix Columns



 (\bigcirc)

Mix Columns



Press enter

Add Round Key

> XOR state with 128-bits of the round key again processed by column (though effectively a series of byte operations) inverse for decryption identical since XOR own inverse, with reversed keys > designed to be as simple as possible a form of Vernam cipher on expanded key requires other stages for complexity / security

Add Round Key

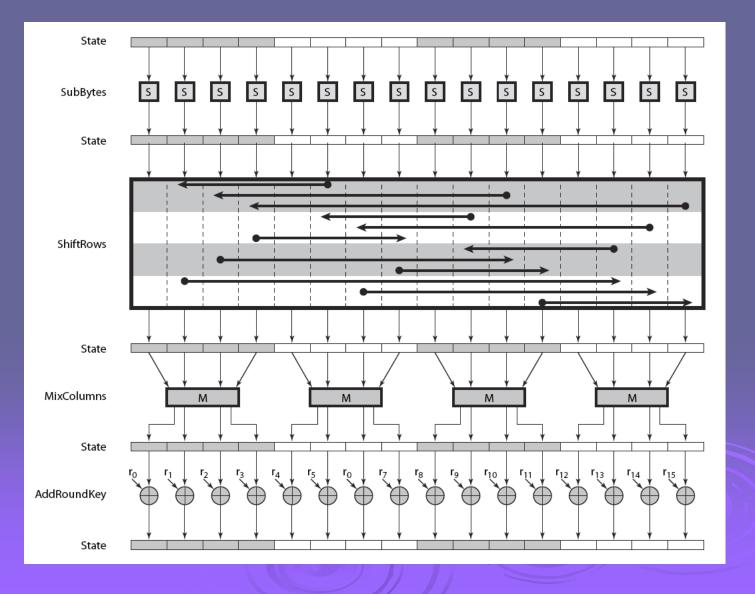
s _{0,0}	s _{0,1}	\$ _{0,2}	\$ _{0,3}
s _{1,0}	s _{1,1}	\$ _{1,2}	s _{1,3}
s _{2,0}	s _{2,1}	\$ _{2,2}	\$ _{2,3}
S _{3,0}	s _{3,1}	s _{3,2}	S _{3,3}

 \oplus

	Wi	W _{i+1}	W _{i+2}	W _{i+3}	=
--	----	------------------	------------------	------------------	---

s' _{0,0}	s' _{0,1}	s' _{0,2}	s' _{0,3}
s' _{1,0}	s' _{1,1}	s' _{1,2}	s' _{1,3}
s' _{2,0}	s' _{2,1}	s' _{2,2}	s' _{2,3}
s' _{3,0}	s' _{3,1}	s' _{3,2}	s' _{3,3}

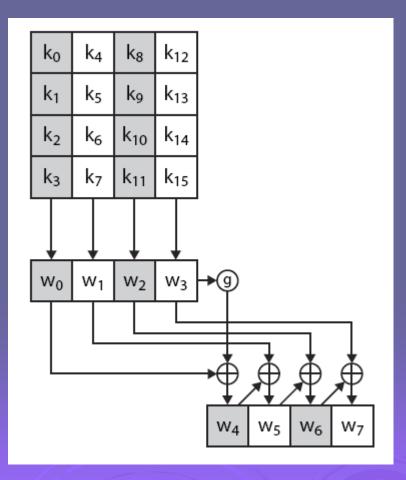
AES Round



AES Key Expansion

> takes 128-bit (16-byte) key and expands into array of 44/52/60 32-bit words start by copying key into first 4 words > then loop creating words that depend on values in previous & 4 places back • in 3 of 4 cases just XOR these together 1st word in 4 has rotate + S-box + XOR round constant on previous, before XOR 4th back

AES Key Expansion



Function g

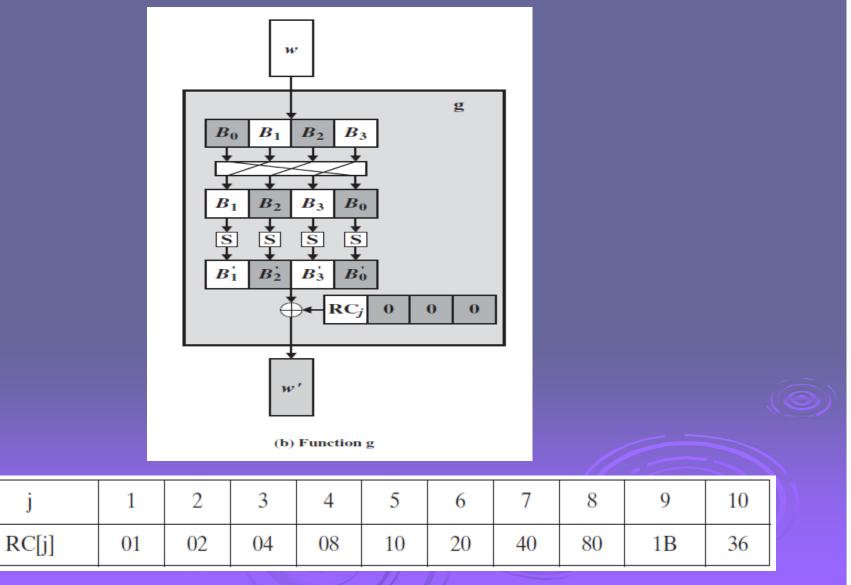


Table 5.5 Key Expansion for AES Example					
Key Words	Auxiliary Function				
w0 = 0f 15 71 c9	RotWord (w3) = 7f 67 98 af = $x1$				
w1 = 47 d9 e8 59	SubWord $(x1) = d2$ 85 46 79 = y1				
w2 = 0c b7 ad	$Rcon(1) = 01 \ 00 \ 00 \ 00$				
w3 = af 7f 67 98	$y1 \oplus Rcon(1) = d3 85 46 79 = z1$				
$w4 = w0 \oplus z1 = dc 90 37 b0$	RotWord (w7) = 81 15 a7 $38 = x2$				
w5 = w4 \oplus w1 = 9b 49 df e9	SubWord $(x4) = 0c 59 5c 07 = y2$				
w6 = w5 ⊕ w2 = 97 fe 72 3f	$Rcon(2) = 02 \ 00 \ 00 \ 00$				
w7 = w6 ⊕ w3 = 38 81 15 a7	$y2 \oplus Rcon(2) = 0e 59 5c 07 = z2$				
$w8 = w4 \oplus z2 = d2 c9 6b b7$	RotWord(w11) = ff d3 c6 e6 = $x3$				
w9 = w8 \oplus w5 = 49 80 b4 5e	SubWord $(x2) = 16 66 b4 83 = y3$				
w10 = w9 \oplus w6 = de 7e c6 61	$Rcon(3) = 04 \ 00 \ 00 \ 00$				
wll = wl0 \oplus w7 = e6 ff d3 c6	$y_3 \oplus Rcon(3) = 12$ 66 b4 8e = z3				
$w12 = w8 \oplus z3 = c0$ af df 39	RotWord (w15) = ae 7e c0 b1 = $x4$				
w13 = w12 \oplus w9 = 89 2f 6b 67	SubWord(x3) = e4 f3 ba $c8 = y4$				
$w14 = w13 \oplus w10 = 57$ 51 ad 06	$Rcon(4) = 08 \ 00 \ 00 \ 00$				
w15 = w14 \oplus w11 = b1 ae 7e c0	$y4 \oplus Rcon(4) = ec f3 ba c8 = 4$				

Table 5.3 Key Expansion for AES Example

Table 5.3 Continued

Key Words	Auxiliary Function
$w16 = w12 \oplus z4 = 2c 5c 65 f1$	RotWord(w19) = 8c dd 50 43 = x5
w17 = w16 \oplus w13 = a5 73 0e 96	SubWord(x4) = 64 c1 53 1a = y5
w18 = w17 \oplus w14 = f2 22 a3 90	Rcon(5) = 10 00 00 00
w19 = w18 \oplus w15 = 43 8c dd 50	$y5 \oplus Rcon(5) = 74 c1 53 1a = z5$
$w20 = w16 \oplus z5 = 58 9d 36 eb$	RotWord (w23) = 40 46 bd $4c = x6$
$w21 = w20 \oplus w17 = fd ee 38 7d$	SubWord (x5) = 09 5a 7a 29 = y6
$w22 = w21 \oplus w18 = 0f cc 9b ed$	Rcon(6) = 20 00 00 00
$w23 = w22 \oplus w19 = 4c 40 46 bd$	$y6 \oplus Rcon(6) = 29$ 5a 7a 29 = z6
$\begin{array}{l} w24 \ = \ w20 \oplus z6 \ = \ 71 \ c7 \ 4c \ c2 \\ w25 \ = \ w24 \oplus w21 \ = \ 8c \ 29 \ 74 \ bf \\ w26 \ = \ w25 \oplus w22 \ = \ 83 \ e5 \ ef \ 52 \\ w27 \ = \ w26 \oplus w23 \ = \ cf \ a5 \ a9 \ ef \end{array}$	RotWord (w27) = a5 a9 ef cf = x7 SubWord (x6) = 06 d3 bf $8a = y7$ Rcon (7) = 40 00 00 00 $y7 \oplus Rcon(7) = 46 d3 df 8a = z7$
$w28 = w24 \oplus z7 = 37 \ 14 \ 93 \ 48$	RotWord $(w31) = 7d a1 4a f7 = x8$
$w29 = w28 \oplus w25 = bb \ 3d \ e7 \ f7$	SubWord $(x7) = ff 32 d6 68 = y8$
$w30 = w29 \oplus w26 = 38 \ d8 \ 08 \ a5$	Rcon $(8) = 80 00 00 00$
$w31 = w30 \oplus w27 = f7 \ 7d \ a1 \ 4a$	$y8 \oplus Rcon(8) = 7f 32 d6 68 = z8$
$w32 = w28 \oplus z8 = 48 \ 26 \ 45 \ 20$	RotWord (w35) = be 0b 38 $3c = x9$
$w33 = w32 \oplus w29 = f3 \ 1b \ a2 \ d7$	SubWord (x8) = ae 2b 07 $eb = y9$
$w34 = w33 \oplus w30 = cb \ c3 \ aa \ 72$	Rcon (9) = 1B 00 00 00
$w35 = w34 \oplus w32 = 3c \ be \ 0b \ 3$	$y9 \oplus Rcon (9) = b5 2b 07 eb = z9$
$w36 = w32 \oplus z9 = fd 0d 42 cb$	RotWord (w39) = 6b 41 56 f9 = x10
$w37 = w36 \oplus w33 = 0e 16 e0 1c$	SubWord (x9) = 7f 83 b1 99 = y10
$w38 = w37 \oplus w34 = c5 d5 4a 6e$	Rcon (10) = 36 00 00 00
$w39 = w38 \oplus w35 = f9 6b 41 56$	y10 ⊕ Rcon (10) = 49 83 b1 99 = z10
$w40 = w36 \oplus z10 = b4$ 8e f3 52 $w41 = w40 \oplus w37 = ba$ 98 13 4e $w42 = w41 \oplus w38 = 7f$ 4d 59 20 $w43 = w42 \oplus w39 = 86$ 26 18 76	

Start of Round After Subleyes After ShiftRows After MixColumns Round Key 01 89 fe 76 01 69 fe 76 07 47 00 after ShiftRows 23 ab dc 54 15 d9 b7 71 e8 after ShiftRows 0ft 47 00 after ShiftRows 24 cd ba 32 06 cd ba 93 55 b9 94 57 55 d6 98 36 72 65 05 40 7f 1 65 e4 e4 21 c5 d6 f5 30 45 73 65 90 73 74 72 15 ad 65 90 72 15 ad 65 91 74 72 93 37 df 72 15 ae 64 48 21 65 67 67 68 67 74 72 93 75 74 74 20 </th <th>Table 5.4 AES E</th> <th>xample</th> <th></th> <th colspan="8">Table 5.4 AES Example</th>	Table 5.4 AES E	xample		Table 5.4 AES Example							
23 ab cc 54 15 d9 D7 71 e8 ad 67 67 ef 98 10 25 b9 94 57 75 dc 9b 97 38 36 72 6b 20 05 40 7f 1 05 e4 e1 65 90 94 57 55 dc 9b 97 38 36 72 6b 20 05 40 7f 10 71 16 16 15 10 49 fe 81 37 df 72 15 38 37 df 72 15 36 67 74 70 93 37 df 72 15 37 df de e6 17 16 b0 37 df de e6 17 16 b0 7 ff b0 ff ff <t< th=""><th>Start of Round</th><th>After SubBytes</th><th>After ShiftRows</th><th>After MixColumns</th><th>Round Key</th></t<>	Start of Round	After SubBytes	After ShiftRows	After MixColumns	Round Key						
45 cd ba 32 71 e8 ad 67 67 ef 98 10 71 e8 ad 67 c9 59 d6 98 0e ce f2 d9 ab 8b 89 35 ab 8b 89 35 b9 94 57 75 dc 9b 97 38 36 72 6b 2b 05 40 7f 10 10 10 14 77 10 93 37 df 72 15 ae b6 4e 8e e4 42 fc c4 e4 e2 db 10	01 89 fe 76				0f 47 0c af						
67 eff 98 10 c c 95 d.6 98 0e ce f2 d.9 ab b.8 b d.8 35 b 99 45 77 5 d.c 9b 97 38 36 72 6b 2b 05 40 7f f1 40 7f f1 05 e4 8e 16 51 90 49 fe 81 34 25 17 55 18 3f f0 fc 16 be 44 42 fc 44 42 fc 6 bf 70 g.d fd 60 ff 60 ff fd fd fd ff fd 60 <td>23 ab dc 54</td> <td></td> <td></td> <td></td> <td>15 d9 b7 7f</td>	23 ab dc 54				15 d9 b7 7f						
De ce field field	45 cd ba 32				71 e8 ad 67						
36 72 6b 2b 05 40 7f f1 05 e4 8e 16 51 90 49 fe 81 34 25 17 55 18 3f 10 fc 16 16 3f 47 20 9a 3f 37 df 72 15 ae b6 4e 88 e4 42 17 16 ba 89 22 db 12 df 47 20 9a 3f 37 df 72 15 ae b6 4e 88 e4 42 fc ba 65 50 70 92 b2 f2 dc 92 c5 80 76 ff f6 b1 ff 60 f7 f1 60 f7 f1 60 f6 f6 f6 f5 f6 f6 f6 f6 f6 f6 f6 f5 f6 f6 f6 f6 f6 f6 f6 f7 f6	67 ef 98 10				C9 59 d 6 98						
34 25 17 55 18 37 07 0 2 15 ae b6 4e 88 e4 42 17 16 5 16 15 31 07 07 12 15 ae b6 4e 88 e4 42 17 16 5 31 10 12 11 12 12 12 14 12 12 12 12 14 12 12 12 12 12 12 12 12 12 12 12 12 1	0e ce f2 d9	ab 8b 89 35	ab 8b 89 35	b9 94 57 75	dc 9b 97 38						
ae b6 4e 8e e4 4e 2f c5 d6 f5 b0 e9 3f a7 65 0f 00 4d 76 ba 3 8e 22 db 12 d2 49 de e6 74 c7 e8 00 92 c5 9b 05 51 16 df 80 ff db b4 c6 d3 75 3f ca 9d 75 74 de e9 d75 74 2d c5 le 52 b7 5e 61 c6 5c 6b 05 f4 4a 7f 6b bf b1 c1 ob cc 08 57 b1 7b 72 22 6d 18 f9 1f 6a c3 df 6b af f6 f6 f6 f6 f6 f6	36 72 6b 2b	05 40 7f fl	40 7f fl 05	e4 8e 1651	90 49 fe 81						
65 0f c0 4d 4d 76 ba e3 4d 76 ba e3 8e 22 db 12 d2 49 de e6 74 c7 e8 d0 92 c6 9b 70 c6 9b 70 92 b2 f2 dc 92 c9 80 7e ff 70 ff e8 2a 51 16 9b e5 9b e5 51 16 df 80 f7 c1 6b b4 c6 d3 75 3f ca 9c 9d 75 74 de de 9d 75 74 2d c5 1e 52 b7 5e 61 c6 5c 6b 05 f4 4a 7f 6b bf 4a 7f 6b bf b1 c1 0b cc c0 89 57 b1 7b 72 a2 6d 21 40 3a 3c 40 3a 3c 21 ba f3 8b 07 af 2f 51 ae b4 34 31 12 8d 18 c7 c9 c7 c9 8d 18 f9 1f 6a c3 df 6b ad 7e 9a 9b 7f 94 b6 14 d2 22 22 b8 14 d2 1d 19 24 5c 39 67 06 c0 71 48 5c 7d a3 52 4a ff a3 52 4a ff d4 11 fe 0f 2c a5 f2 43 15 dc da a9 59 86 57 d3 86 57 d3 96 57 33 91 b4 40 673 5c 73 22 8c c6 7a 27 bd f7 92 cb ab 62 37 65 0e a3 dd 24 7e 22 9c 36 f3 93 de de 36 f3 93 19 b7 07 cc f1 96 90 50 f8 b4 0c 4c 41 8d fe 29 41 8d fe	34 25 17 55	18 31 10 fc	f0 fc 18 3f	47 20 9a 3f	37 df 72 15						
74c7e80092c69b7092b2f2dc 92c9807eff70ffe82a51169be55116df80f7c16bb4c6d3753fca9c9d7574de9d75742dc5le 52b75e61c65c6b05f44a7f6bbf4a7f6bbfblc10bccc08957bl7b72222621403a3c21baf38b07af2f51ae9a9b7f94b814d22222b814d21d19245c396766c071485c7da3524affa3524affd411feff2casff431dadfe2aff	ae b6 4e 88	e4 4e 2f c4	c4 e4 4e 2f	c5 d6 f5 3b	b0 e9 3f a7						
70 ff e8 2a 51 16 9b e5 51 16 df 80 f7 c1 6b b4 c6 d3 75 3f ca 9c 9d 75 74 de 9d 75 74 2d c5 le 52 b7 5e 61 c6 5c 6b 05 f4 4a 7f 6b bf b1 c1 0b cc c0 89 57 b1 7b 72 a2 6d 18 c7 c9 c7 c9 8d 18 c7 c9 c7 c9 8d 19 16 ac c3 df 6b ad ce 9a 9b 7f<94	65 01 c0 40	4d 76 ba e3	4d 76 ba e3	8e 22 db 12	d2 49 de e6						
75 3f ca 9c 9d 75 74 de 9d 75 74 2d c5 1e 52 b7 5e 61 c6 5c 6b 05 f4 4a 7f 6b bf b1 c1 0b cc c0 89 57 b1 7b 72 a2 6d 21 40 3a 3c 21 ba f3 8b 07 af 2f 51 ae b4 34 31 12 8d 18 c7 c9 c7 c9 8d 19 1f 6a c3 df 6b ad 7e 9a 9b 7f 94 b8 14 d2 22 2b 8d 1f d2 1d 19 24 5c 39 6f 06 c0 c7 c3 9b f4 06 73 5c f3 22 bc ba 62 37 65 0e ad d2 d2	74 c7 e8 d0	92 c6 9b 70	C6 910 70 92	b2 f2 dc 92	C9 80 7e ff						
5c 6b 05 f4 4a 7f 6b bf bl cl 0 0 cc c0 89 57 bl 7b 72 a2 6d 21 40 3a 3c 21 ba f3 8b 07 af 2f 51 ae b4 34 31 12 8d 18 c7 c9 c7 c9 8d 18 f9 1f 6a c3 df 6b ad 7e 9a 9b 7f 94 b8 14 d2 22 2b b14 d2 1d 19 24 5c 39 67 06 c0 71 48 5c 7d a3 52 4a ff d4 11 fe 0f 2c ab 67 35 57 d2 ac d5 fd d3 d6 fd fd	70 ff e8 2a				6b b4 c6 d3						
7b 72 a2 6d 21 40 3a 3c 21 ba f3 8b 07 af 2f 51 ae b4 34 31 12 8d 18 c7 c9 8d 18 f9 1f 6a c3 df 6b ad 7e 9a 9b 7f 94 b8 14 d2 22 b8 14 d2 1d 19 24 5c 39 67 06 c0 71 48 5c 7d a3 52 4a ff d4 11 fe of co a5 ff 35 g4 ff d4 ff d4 ff ed cf cf cf cf a5 cf cf a5 cf cf a5 cf a5 cf cf a5 cf cf a6 cf a6 a6 cf a6 a6 a6 a6 a6 a6 a6 a6 a6	75 3f ca 9c	90 75 74 de	đe 9đ 75 74	2d c5 le 52	b7 5e 61 c6						
b4 34 31 12 8d 18 c7 c9 8d 18 f9 1f 6a c3 df 6b ad 7e 9a 9b 7f 94 b8 14 d2 22 b8 14 d2 1d 19 24 5c 39 67 06 c0 71 48 5c 7d a3 52 4a ff d4 11 fe 0f c2 as ff d2 cs ff d4 11 fe 0f c2 as ff d2 cc as fc fa ff g2 cs ff d4 11 fe of c7 g2 as ff g2 as ff g3 g2 fs ff g3 g2 ff g2 as ff g3 g1 ff g2 as ff f5 g3 g6 ff g3 g1 ga f5 g2 ga f5 g1 <	5c 6b 05 14	4a 7f 6b bf	4a 7f 6b bf	bl cl Ob cc	CO 89 57 bl						
9a 9b 7f 94 b8 14 d2 22 b8 14 d2 1d 19 24 5c 39 67 06 c0 71 48 5c 7d a3 52 4a ff a3 52 4a ff d4 11 fe of 2c a5 f2 43 15 dc daa 59 86 57 d3 86 57 d3 59 3b 44 06 73 5c 73 22 8c 26 74 c7 bd f7 92 c6 7a c6 7a f7 92 cb ab 62 37 65 0e a3 dd fd fd <td>7b 72 a2 6đ</td> <td>21 40 3a 3c</td> <td>40 3a 3c 21</td> <td>ba f3 8b 07</td> <td>af 2f 51 ae</td>	7b 72 a2 6đ	21 40 3a 3c	40 3a 3c 21	ba f3 8b 07	af 2f 51 ae						
71 48 5c 7d a3 52 4a ff a3 52 4a ff d4 11 fe 0f 2c a5 f2 43 15 dc da a9 59 86 57 d3 59 3b 44 06 73 5c 73 22 8c 26 74 c7 bd f7 92 c6 7a c6 7a f7 92 cb ab 62 37 65 0e a3 dd 24 7e 22 9c 36 f3 93 de de 36 f3 93 19 b7 07 ec f1 96 90 50 f8 b4 0c 4c 41 8d fe 29 2a 47 c4 48 58 fd 0f 4c a2 5c 1a 86 f6 9a 36 16 85 83 e8 18 ba 9d ec c4 0 4d ad a fd ad <td>b4 34 31 12</td> <td>8đ 18 c7 c9</td> <td>c7 c9 8d 18</td> <td>f9 1f 6a c3</td> <td>df 6b ad 7e</td>	b4 34 31 12	8đ 18 c7 c9	c7 c9 8d 18	f9 1f 6a c3	df 6b ad 7e						
15 dc da a9 59 86 57 d3 59 3b 44 06 73 5c 73 22 8c 26 74 c7 bd f7 92 c6 7a f7 92 cb ab 62 37 65 0e a3 dd 24 7e 22 9c 36 f3 93 de de 36 f3 93 19 b7 07 ec f1 96 90 50 f8 b4 0c 4c 41 8d fe 29 41 8d fe 29 2a 47 c4 48 58 fd 0f 4c 67 37 24 ff 85 9a 36 16 9a 36 16 83 e8 18 ba 9d ee cc 40 ae a5 c1 ae 64 78 87 78 87 e4 06 84 18 27 23 36<	9a 9b 7f 94	b8 14 d2 22	22 b8 14 d2	1d 19 24 5c	39 67 06 C0						
26 74 c7 bd f7 92 c6 7a f7 92 cb ab 62 37 65 0e a3 dd 24 7e 22 9c 36 f3 93 de de 36 f3 93 le 36 f3 93 le ae 36 f3 93 le ac 36 f3 93 le la f1 96 90 50 f8 b4 0c 41 ff 29 2a 47 c4 48 58 fd of 4c ac ff ff ga 36 18 ga ac ac ff ff ga ac ff ff ga ac ff ff ac ff ff <	71 48 5c 7d	a3 52 4a ff	a3 52 4a ff	d4 11 fe 0f	2c a5 f2 43						
24 7e 22 9c 36 f3 93 de de 36 f3 93 19 b7 07 ec f1 96 90 50 f8 b4 0c 4c 41 8d fe 29 41 8d fe 29 2a 47 c4 48 58 fd 0f 4c 67 37 24 ff 85 9a 36 16 9a 36 16 83 e8 18 ba 9d ee cc 40 ae a5 c1 ea 64 78 87 78 87 e4 66 84 18 27 23 36 38 9b 46 e8 21 97 bc 9b fd 88 65 65 9b fd 88 eb 10 0a f3 eb 7d ed bd 72 ba cb 04 fd 1f f2 40 f4 1f f2 7b	15 dc da a9	59 86 57 d 3	86 57 d3 59	3b 44 06 73	5c 73 22 8c						
f8 b4 0c 4c 41 8d fe 29 41 8d fe 29 2a 47 c4 48 58 fd 0f 4c 67 37 24 ff 85 9a 36 16 9a 36 16 85 83 e8 18 ba 9d ee cc 40 ae a5 c1 ea e4 06 78 87 78 87 e4 06 84 18 27 23 36 38 9b 46 e8 21 97 bc 9b fd 88 65 65 9b fd 88 eb 10 0a f3 eb 7d ed bd 72 ba cb 04 40 f4 1f f2 40 f4 1f f2 7b 05 42 4a 71 8c 83 cf 1e 06 d4 fa 72 6f 48 2d 6f 48 2d 72 1e d0 20 40 c7 29 e5 a5 b2 20 bc 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef a9 00 6d e7 4e 63 3c 94 2f 2f 63 3c 94 94 c4 43 fb c2 bf 52 ef 0a 89 c1 85 67 a7 78 97 67 a7 78 97 ec 1a c0 80 37 bb 38 f7 d9 f9 c5 e5 35 99 a6 d9 99 a6 d9 35 0c 50 53 c7 14 3d d8 7d d8 f7 f7 fb 61 68 68 0f 68 0f 61 68 3b d7 00 ef 93 e7 08 a1 56 7b 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 4a db a1 f8 77	26 74 c7 bd	17 92 c6 7a	c6 7a f7 92	CD aD 62 37	65 0e a3 đđ						
67 37 24 ff 85 9a 36 16 83 e8 18 ba 9d ee cc 40 ae a5 c1 ea 06 78 87 78 87 e4 06 84 18 27 23 36 38 9b 46 e8 21 97 bc 9b fd 88 65 65 9b fd 88 eb 10 0a f3 eb 7d ed bd 72 ba cb 04 f4 1f f2 40 f4 1f f2 7b 05 42 4a 71 8c 83 cf 1e 06 d4 fa 72 6f 48 2d 72 1e d0 20 4c 74 ef a9 00 6d e7 4e 63 3c 94 c4 43 fb c2 bf 52 ef 0a 89 c185 <td>24 7e 22 9c</td> <td>36 f3 93 de</td> <td>de 36 f3 93</td> <td>19 b7 07 ec</td> <td>fl 96 90 50</td>	24 7e 22 9c	36 f3 93 de	de 36 f3 93	19 b7 07 ec	fl 96 90 50						
ae a5 c1 e4 06 78 87 e4 06 84 18 27 23 36 38 9b 46 e8 21 97 bc 9b fd 88 65 65 9b fd 88 eb 10 0a f3 eb 7d ed bd 72 ba cb 04 f4 1f f2 40 f4 1f f2 7b 05 42 4a 71 8c 83 cf 1e 06 d4 fa 72 6f 48 2d 72 1e d0 20 40 c7 29 e5 a5 b2 20 bc 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef a9 00 6d e7 4e 63 3c 94 2f 63 3c 94 c4 43 fb	18 b4 0c 4c	41 80 fe 29	41 80 fe 29	2a 47 c4 48	58 fd 0f 4c						
e8 21 97 bc 9b fd 88 65 9b fd 88 eb 10 0a f3 eb 7d ed bd 72 ba cb 04 f4 1f f2 40 f4 1f f2 7b 05 42 4a 71 8c 83 cf 1e 06 d4 fa 72 6f 48 2d 6f 48 2d 72 1e d0 20 40 c7 29 e5 a5 b2 20 bc 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef a9 00 6d e7 4e 63 3c 94 2f 63 3c 94 c4 43 fb c2 bf 52 ef 0a 89 c185 67 a7 78 97 ec 1a c0 80 37	67 37 24 ff	85 9a 36 16	9a 36 16 85	83 e8 18 ba	9đ ee cc 40						
72 ba cb 04 40 f4 1f f2 40 f4 1f f2 7b 05 42 4a 71 8c 83 cf 1e 06 d4 fa 72 6f 48 2d 6f 48 2d 72 1e d0 20 40 c7 29 e5 a5 b2 20 bc 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef a9 00 6d e7 4e 63 3c 94 2f 63 3c 94 94 c4 43 fb c2 bf 52 ef 0a 89 c1 85 67 a7 78 97 ec 1a c0 80 37 b3 & f7 d9 f9 c5 s5 35 99 a6 d9	ae a5 clea	e4 06 78 87	78 87 e4 06	84 18 27 23	36 38 9b 46						
1e 06 d4 fa 72 6f 48 2d 6f 48 2d 72 1e d0 20 d0 c7 29 e5 a5 b2 20 bc 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef a9 00 6d e7 4e 63 3c 94 2f 63 3c 94 94 c4 43 fb c2 bf 52 ef 0a 89 c1 85 67 a7 78 97 ec 1a c0 80 37 bb 38 f7 d9 f9 c5 e5 35 99 a6 d9 35 0c 50 53 c7 14 3d 87 70 83 16 65 70 14 3d 87 67 83 17 15 11 48 f7 a5 a1 16	e8 21 97 bc	9b fd 88 65	65 9b fd 88	eb 10 0a f3	eb 7d ed bd						
b2 20 bc 65 37 b7 65 4d 37 b7 94 83 18 52 4c 74 ef a9 00 6d e7 4e 63 3c 94 2f 63 3c 94 94 c4 43 fb c2 bf 52 ef 0a 89 c1.85 67 a7 78 97 67 a7 78 97 ec 1a c0 80 37 bb 38 f7 d9 f9 c5 e5 35 99 a6 d9 35 0c 50 53 c7 14 3d d8 7d d8 f7 f7 fb 61 68 68 of 61 68 3b d7 00 ef 93 e7 08 a1 56 7b 11 14 b1 21 82 fa b1 21 82 b7 22 72 e0 48 f7 <td>72 ba cb 04</td> <td>40 f4 1f f2</td> <td>40 f4 lf f2</td> <td>7b 05 42 4a</td> <td>71 8c 83 cf</td>	72 ba cb 04	40 f4 1f f2	40 f4 lf f2	7b 05 42 4a	71 8c 83 cf						
00 6d e7 4e 63 3c 94 2f 63 3c 94 c4 43 fb c2 bf 52 ef 0a 89 c1 85 67 a7 78 97 67 a7 78 97 ec 1a c0 80 37 bb 38 f7 d9 f9 c5 e5 35 99 a6 d9 35 0c 50 53 c7 14 3d d8 7d d8 f7 f7 fb f1 68 68 of f6 68 a5 a5 a7 08 a1 56 7b 11 44 b1 21 82 fa b1 21 82 b7 22 72 e0 48 f7 a5 4a db a1 f8 f7 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3c 3d f4 3d											
0a 89 cl 85 67 a7 78 97 67 a7 78 97 ec la c0 80 37 bb 38 f7 d9 f9 c5 e5 35 99 a6 d9 99 a6 d9 35 0c 50 53 c7 14 3d d8 7d d8 f7 f7 fb 61 68 68 0f 68 0f 61 68 3b d7 00 ef 93 e7 08 al 56 7b 11 14 bl 21 82 fa fa bl 21 82 b7 22 72 e0 48 f7 a5 4a db al f8 77 b9 32 41 f5 b9 32 41 f5 bl 1a 44 17 48 f3 cb 3c 18 6d 8b ba ad 3c 3d f4 3c 3d f4 ad 3d 2f ec b6 26 lb c3 be a8 30 08 4e c2 04 30 2f 30 2f c2 04 0a 6b 2f 42 45 a2 aa 0b											
d9 f9 c5 35 99 a6 d9 35 0c 50 53 c7 14 3d d8 7d d8 f7 f7 fb 61 68 0f 61 68 0f 61 68 3b d7 00 ef 93 e7 08 a1 56 7b 11 14 b1 21 82 fa b1 21 82 b7 22 72 e0 48 f7 a5 4a db a1 f8 f7 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3c 3d f4 ad 3d 2f ec b6 26 1b c3 be ae 30 2f ec b6 2f 1b c3 db af 3d 2f 45 ac ae 0b 18 6d 8b ba c2 04 30 2f c2 04	00 60Le74e	63 3C 94 2f	21 63 3C 94	94 C4 43 fb	c2 bf 52 ef						
d8 f7 f7 fb 61 68 0f 68 0f 61 68 3b d7 00 ef 93 e7 08 a1 56 7b 11 14 b1 21 82 fa b1 21 82 b7 22 72 e0 48 f7 a5 4a db a1 f8 77 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3c 3c 3d f4 ad 3d 2f ec b6 26 1b c3 be a8 30 08 4e c2 04 30 2f c2 04 0a 6b 2f 45 a2 aa 0b											
56 7b 11 14 b1 21 82 fa b1 21 82 fa b1 21 82 fa b1 21 82 b7 22 72 e0 48 f7 a5 4a db a1 f8 77 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3c 18 6d 8b ba ad 3c 3d f4 ad 3d 2f ec b6 26 1b c3 be a8 30 08 4e c2 04 30 2f c2 04 0a 6b 2f 42 45 a2 aa 0b											
db al f8 77 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3c 18 6d 8b ba ad 3c 3d f4 ad 3d 2f ec b6 26 1b c3 be a8 30 08 4e c2 04 30 2f c2 04 0a 6b 2f 45 a2 aa 0b											
18 6d 8b ba ad 3c 3d f4 ad 3d 2f ec b6 26 lb c3 be a8 30 08 4e c2 04 30 2f c2 04 0a 6b 2f 45 a2 aa 0b	56 7b 11 14	bl 21 82 fa	fa bl 21 82	b7 22 72 e0	48 17 a5 4a						
a8 30 08 4e c2 04 30 2f 30 2f c2 04 0a 6b 2f 42 45 a2 aa 0b	db al f8 77		b9 32 41 f5		48 f3 cb 3c						
ff d5 d7 aa 16 03 0e ac ac 16 03 0e 9f 68 f3 bl 20 d7 72 38											
	ff d5 d7 aa	16 03 0e ac	ac 16 03 0e	9f 68 f3 b1	20 07 72 38						

Summary

have considered:

- the AES selection process
- the details of Rijndael the AES cipher
- looked at the steps in each round
- the key expansion
- implementation aspects