

Advanced Encryption Standard (AES)

Raj Jain

Washington University in Saint Louis
Saint Louis, MO 63130

Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

<http://www.cse.wustl.edu/~jain/cse571-17/>



1. AES Structure
2. AES Round Function
3. AES Key Expansion
4. AES Decryption

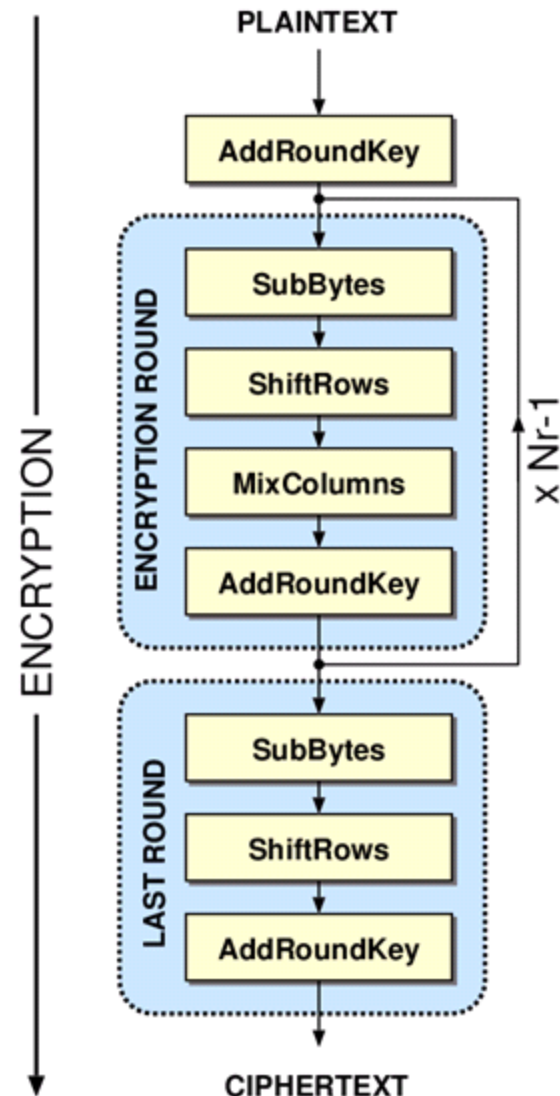
These slides are based on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 7th Ed, 2017.

Advanced Encryption Standard (AES)

- ❑ Published by NIST in Nov 2001: FIPS PUB 197
- ❑ Based on a competition won by Rijmen and Daemen (Rijndael) from Belgium
- ❑ 22 submissions, 7 did not satisfy all requirements
15 submissions 5 finalists: Mars, RC6, Rijndael, Serpent, Twofish. Winner: Rijndael.
- ❑ Rijndael allows many block sizes and key sizes
- ❑ AES restricts it to:
 - Block Size: 128 bits
 - Key sizes: 128, 192, 256 (AES-128, AES-192, AES-256)
- ❑ An iterative rather than Feistel cipher
 - operates on entire data block in every round
- ❑ Byte operations: Easy to implement in software

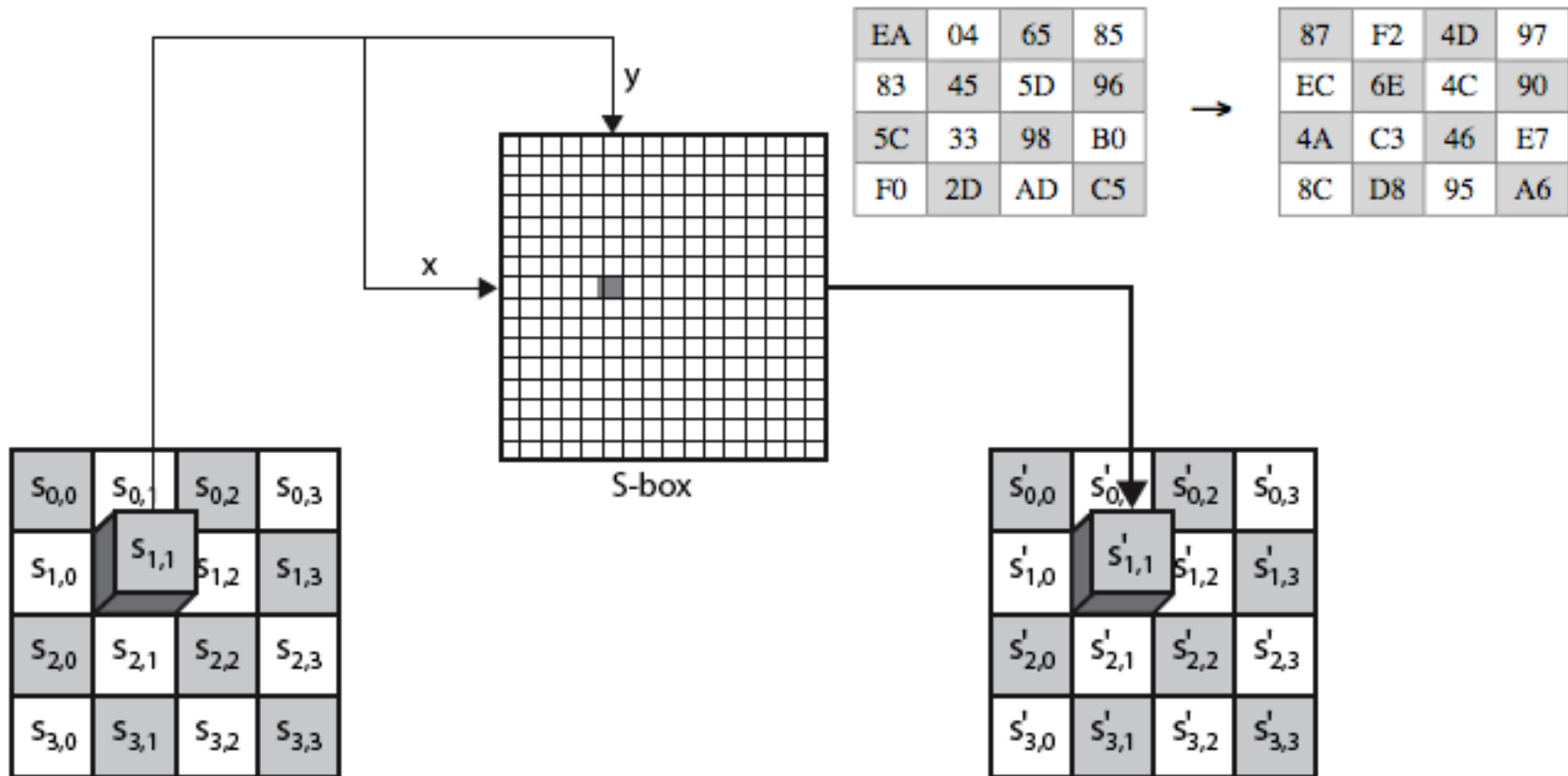
Basic Structure of AES

- ❑ # Rounds $N_r = 6 + \max\{N_b, N_k\}$
- ❑ $N_b = 32$ -bit words in the block
- ❑ $N_k = 32$ -bit words in key
- ❑ AES-128: 10
- ❑ AES-192: 12
- ❑ AES-256: 14



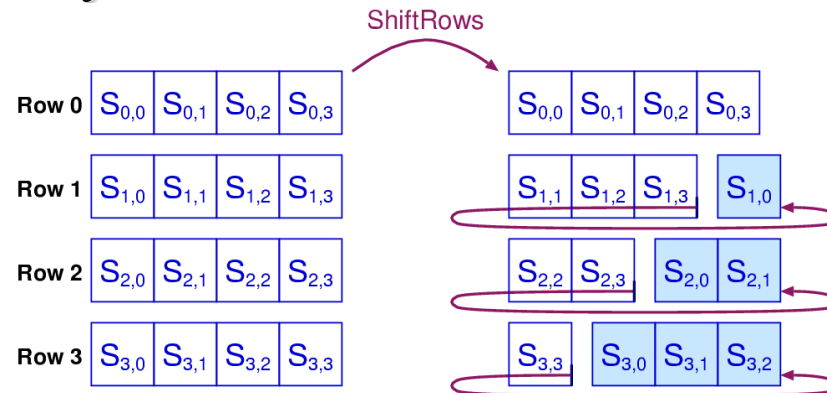
1. Substitute Bytes

- Each byte is replaced by byte indexed by row (left 4-bits) & column (right 4-bits) of a 16x16 table



2. Shift Rows

- ❑ 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



87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

3. Mix Columns

- Effectively a matrix multiplication in $GF(2^8)$ using prime polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}
 \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}
 =
 \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95



47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

$$(\{02\} \cdot \{87\}) \oplus (\{03\} \cdot \{6E\}) \oplus \{46\} \oplus \{A6\} = \{47\}$$

AES Arithmetic

- ❑ Uses arithmetic in the finite field $GF(2^8)$ with irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

which is (1 0001 1011) or {11B}

- ❑ Example:

- $\{02\} \cdot \{87\} \bmod \{11B\} = (0000\ 0010)(1000\ 0111)$

$$= x(x^7 + x^2 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$= (x^8 + x^3 + x^2 + x) \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$= x^4 + x^2 + 1 = (0001\ 0101)$$

- $\{03\} \cdot \{6E\} = \{11\} \{110\ 1110\} = (x+1)(x^6 + x^5 + x^3 + x^2 + x) \bmod (\dots)$

$$= (x^7 + x^6 + x^4 + x^3 + x^2 + x^6 + x^5 + x^3 + x^2 + x) \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$= x^7 + x^5 + x^4 + x = \{1011\ 0010\}$$

- $0001\ 0101 \oplus 1011\ 0010 \oplus 0100\ 0110 \oplus 1010\ 0110 = 0100\ 0111 = 47$

4. Add Round Key

- XOR state with 128-bits of the round key

Key=0f1571c947d9e8590cb7add6af7f6798

Text=0123456789abcdeffedcba9876543210

$$\begin{array}{ccc} \left(\begin{array}{cccc} 01 & 89 & fe & 76 \\ 23 & ab & dc & 54 \\ 45 & cd & ba & 32 \\ 67 & ef & 98 & 10 \end{array} \right) & \oplus & \left(\begin{array}{cccc} 0f & 47 & 0c & af \\ 15 & d9 & b7 & 7f \\ 71 & e8 & ad & 67 \\ c9 & 59 & d6 & 98 \end{array} \right) = \left(\begin{array}{cccc} 0e & ce & f2 & d9 \\ 36 & 72 & 6b & 2b \\ 34 & 25 & 17 & 55 \\ ae & b6 & 4e & 88 \end{array} \right) \\ \text{128-bit Text} & & \text{128-bit Key} & & \text{128-bit Sum} \\ & & \begin{array}{cccc} \uparrow & \uparrow & \uparrow & \uparrow \\ w_0 & w_1 & w_2 & w_3 \end{array} & & \end{array}$$

AES Key Expansion

- ❑ Use 4-byte subkeys w_i . Subkey = 4 words.

For AES-128:

- ❑ First subkey $(w_0, w_1, w_2, w_3) =$ cipher key
- ❑ Other words are calculated as follows:

$$w_i = w_{i-1} \oplus w_{i-4}$$

for all values of i that are not multiples of 4.

- ❑ For the words with indices that are a multiple of 4 (w_{4k}):
 1. *RotWord*: Bytes of w_{4k-1} are rotated left shift (nonlinearity)
 2. *SubWord*: *SubBytes* fn is applied to all four bytes. (Diffusion)
 3. The result r_{sk} is XOR'ed with w_{4k-4} and a round constant r_{conk} (breaks Symmetry):

$$w_{4k} = r_{sk} \oplus w_{4k-4} \oplus r_{conk}$$

- ❑ For AES-192 and AES-256, the key expansion is more complex.

AES Example Key Expansion

Key=0f1571c947d9e8590cb7add6af7f6798

	Key Words	Auxiliary Function
	$w_0 = 0f\ 15\ 71\ c9$ $w_1 = 47\ d9\ e8\ 59$ $w_2 = 0c\ b7\ ad\ d6$ $w_3 = af\ 7f\ 67\ 98$	$RotWord(w_3) = 7f\ 67\ 98\ af = x_1$ $SubWord(x_1) = d2\ 85\ 46\ 79 = y_1$ $Rcon(1) = 01\ 00\ 00\ 00$ $y_1 \oplus Rcon(1) = d3\ 85\ 46\ 79 = z_1$
1st	$w_4 = w_0 \oplus z_1 = dc\ 90\ 37\ b0$ $w_5 = w_4 \oplus w_1 = 9b\ 49\ df\ e9$ $w_6 = w_5 \oplus w_2 = 97\ fe\ 72\ 3f$ $w_7 = w_6 \oplus w_3 = 38\ 81\ 15\ a7$	$RotWord(w_7) = 81\ 15\ a7\ 38 = x_2$ $SubWord(x_2) = 0c\ 59\ 5c\ 07 = y_2$ $Rcon(2) = 02\ 00\ 00\ 00$ $y_2 \oplus Rcon(2) = 0e\ 59\ 5c\ 07 = z_2$
2nd	$w_8 = w_4 \oplus z_2 = d2\ c9\ 6b\ b7$ $w_9 = w_8 \oplus w_5 = 49\ 80\ b4\ 5e$ $w_{10} = w_9 \oplus w_6 = de\ 7e\ c6\ 61$ $w_{11} = w_{10} \oplus w_7 = e6\ ff\ d3\ c6$	$RotWord(w_{11}) = ff\ d3\ c6\ e6 = x_3$ $SubWord(x_3) = 16\ 66\ b4\ 8e = y_3$ $Rcon(3) = 04\ 00\ 00\ 00$ $y_3 \oplus Rcon(3) = 12\ 66\ b4\ 8e = z_3$
10th		

AES Example Encryption

Start of round	After SubBytes	After ShiftRows	After MixColumns	Round Key
01 89 fe 76 23 ab dc 54 45 cd ba 32 67 ef 98 10				0f 47 0c af 15 d9 b7 7f 71 e8 ad 67 c9 59 d6 98
0e ce f2 d9 36 72 6b 2b 34 25 17 55 ae b6 4e 88	ab 8b 89 35 05 40 7f f1 18 3f f0 fc e4 4e 2f c4	ab 8b 89 35 40 7f f1 05 f0 fc 18 3f c4 e4 4e 2f	b9 94 57 75 e4 8e 16 51 47 20 9a 3f c5 d6 f5 3b	dc 9b 97 38 90 49 fe 81 37 df 72 15 b0 e9 3f a7
65 0f c0 4d 74 c7 e8 d0 70 ff e8 2a 75 3f ca 9c	4d 76 ba e3 92 c6 9b 70 51 16 9b e5 9d 75 74 de	4d 76 ba e3 c6 9b 70 92 9b e5 51 16 de 9d 75 74	8e 22 db 12 b2 f2 dc 92 df 80 f7 c1 2d c5 1e 52	d2 49 de e6 c9 80 7e ff 6b b4 c6 d3 b7 5e 61 c6

$$01 + 0f = 0e$$

$$89 + 47 = ce$$

$$w_5 = w_4 + w_1$$

$$\begin{pmatrix} dc \\ 90 \\ 37 \\ b0 \end{pmatrix} \oplus \begin{pmatrix} 47 \\ d9 \\ e8 \\ 59 \end{pmatrix} = \begin{pmatrix} 9b \\ 49 \\ df \\ e9 \end{pmatrix}$$

$$dc = 1101\ 1100$$

$$47 = \underline{0100\ 0111}$$

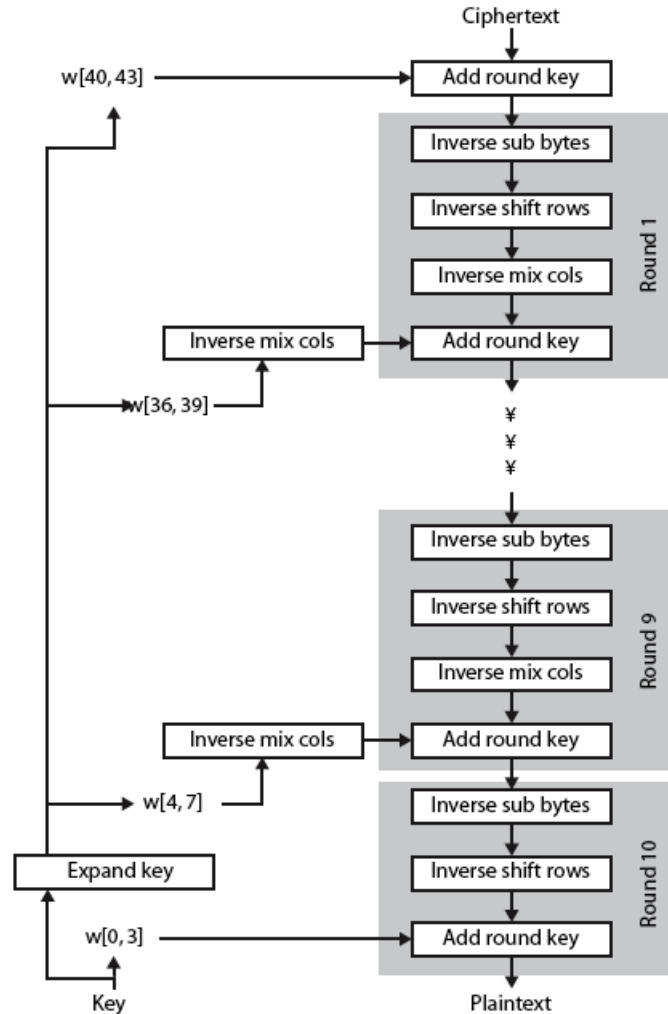
$$9b = 1001\ 1011$$

AES Example Avalanche

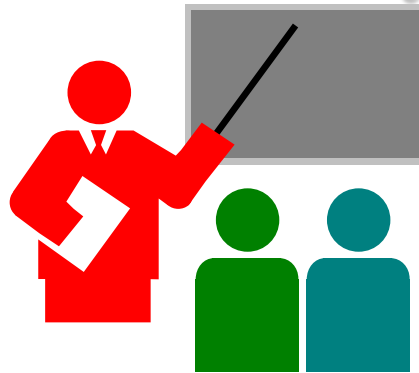
Round		Number of bits that differ
	0123456789abcdef fedcba9876543210 0023456789abcdef fedcba9876543210	1
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c4a9ad090fc7ff3fc0e8e8ca4dd02a9c	20
2	5c7bb49a6b72349b05a2317ff46d1294 fe2ae569f7ee8bb8c1f5a2bb37ef53d5	58
3	7115262448dc747e5cdac7227da9bd9c ec093dfb7c45343d689017507d485e62	59
4	f867aee8b437a5210c24c1974cffeabc 43efdb697244df808e8d9364ee0ae6f5	61
5	721eb200ba06206dcbd4bce704fa654e 7b28a5d5ed643287e006c099bb375302	68
6	0ad9d85689f9f77bc1c5f71185e5fb14 3bc2d8b6798d8ac4fe36ald891ac181a	64
7	db18a8ffa16d30d5f88b08d777ba4eaa 9fb8b5452023c70280e5c4bb9e555a4b	67
8	f91b4fbfe934c9bf8f2f85812b084989 20264e1126b219aef7feb3f9b2d6de40	65
9	cca104a13e678500ff59025f3bafaa34 b56a0341b2290ba7dfdfbddcd8578205	61
10	ff0b844a0853bf7c6934ab4364148fb9 612b89398d0600cde116227ce72433f0	58

AES Decryption

- ❑ AES decryption is not identical
- ❑ But each step has an inverse



Summary



1. AES encrypts 128 bit blocks with 128-bit, 192-bit or 256-bit keys using 10, 12, or 14 rounds, respectively.
2. Is not a Feistel cipher \Rightarrow All 128 bits are encrypted
3. Each round = 4 steps of SubBytes, ShiftRows, MixColumns, and AddRoundKey.
4. Last round has only 3 steps. No MixColumns.
5. Decryption is not the same as encryption (as in DES). Decryption consists of inverse steps.

Homework 5

Given the plaintext [0001 0203 0405 0607 0809 0A0B 0C0D 0E0F] and the key [0101 0101 0101 0101 0101 0101 0101 0101]

- a. Show the original contents of state, displayed as a 4x4 matrix.
Hint: First Row: 00 04 08 0C
- b. Show the value of state after initial AddRoundKey.
Hint: First Row: 01 05 09 0D
- c. Show the value of State after SubBytes.
Hint: First Row: 7C 6B 01 D7
- d. Show the value of State after ShiftRows.
Hint: First Row: 7C 6B 01 D7
- e. Compute the value of State after MixColumns.
Show detailed computations for all elements of the first row.
To practice, you may compute 2nd, 3rd, 4th rows for step e but there is no need to submit. *Submit only the first row for step e.*
For all other steps, show all 4 rows.
Hint: First Row: 75 87 0F B2

Acronyms

- ❑ AES Advance Encryption Standard
- ❑ DES Data Encryption Standard
- ❑ FIPS Federal Information Processing Standard
- ❑ GF Galois Field
- ❑ NIST National Institute of Science and Technology
- ❑ RC Ron's Code
- ❑ XOR Exclusive OR

Scan This to Download These Slides



Raj Jain

<http://rajjain.com>

Related Modules



CSE571S: Network Security (Spring 2017),
<http://www.cse.wustl.edu/~jain/cse571-17/index.html>

CSE473S: Introduction to Computer Networks (Fall 2016),
<http://www.cse.wustl.edu/~jain/cse473-16/index.html>



Wireless and Mobile Networking (Spring 2016),
<http://www.cse.wustl.edu/~jain/cse574-16/index.html>

CSE571S: Network Security (Fall 2014),
<http://www.cse.wustl.edu/~jain/cse571-14/index.html>



Audio/Video Recordings and Podcasts of
Professor Raj Jain's Lectures,
<https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw>