Key size differs

AES → Encryption Standard

MONDAY 5 AUG

Advanced Encryption Standard:

→ Symmetric, block ciper

↳ same key is used for both encryption and decryption

↳ Take a group of bits as input and produce a group of bits as the output

↳ Take 128 bits as the input - plaintext size, 128 bits as the output - ciphertext size

Rijndael [reign.dahl]
Joan Daemen
Vincent Rijmen

TUESDAY 6 AUG

Input State array

Final State array

Round 1 Transformations

↳ Substitute Bytes,
Shift Rows,
Mix Columns,
Add round Key

There is some relationship beth the Key size & the number of rounds to be performed in AES.

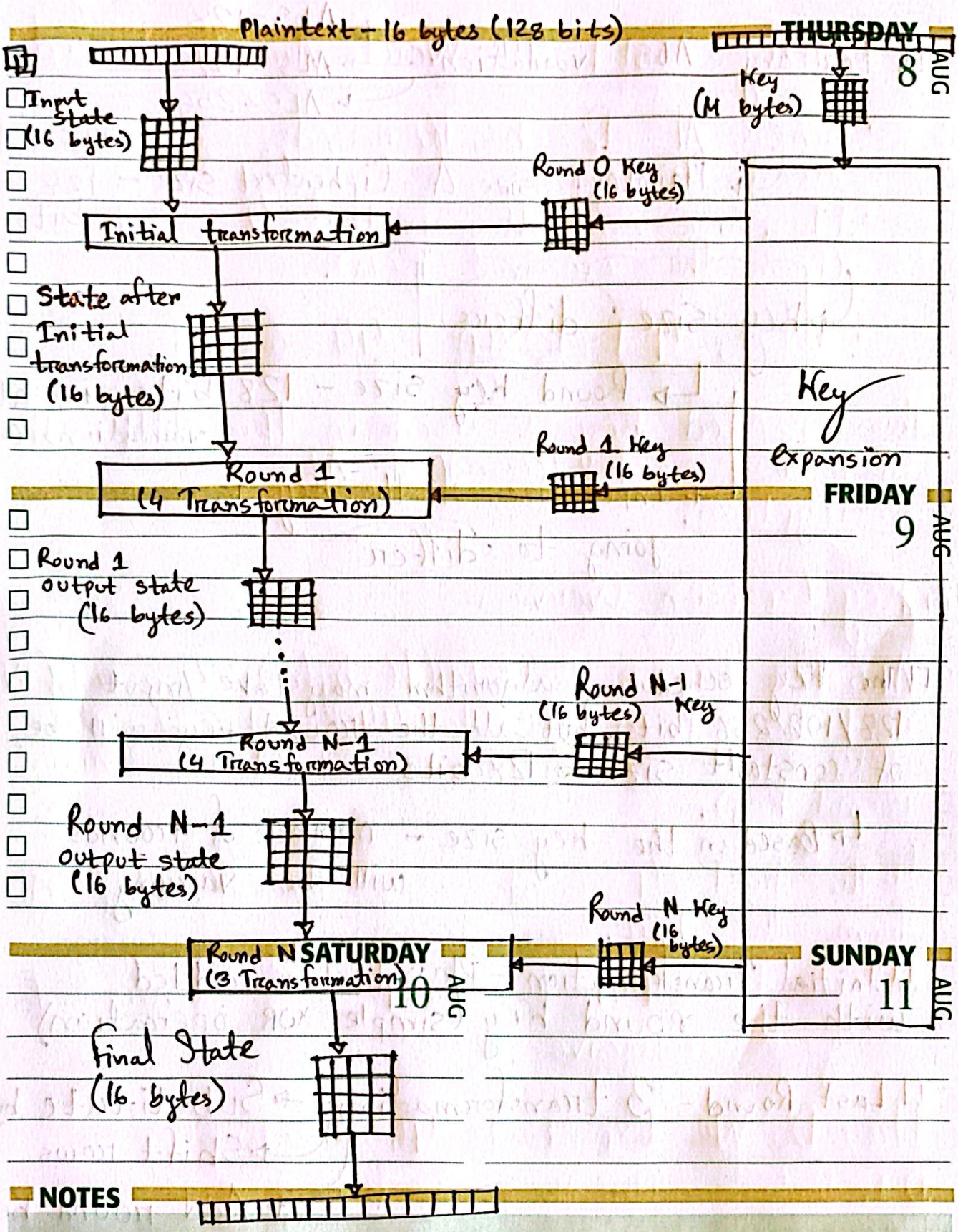
WEDNESDAY 7 AUG

This Key is used by the Key scheduling algorithm to generate the round keys that are required for every round.

No. of rounds	Key size (in bits)
10	128
12	192
14	256

AES Structure

Key - M bytes



THURSDAY 8 AUG

FRIDAY 9 AUG

SATURDAY 10 AUG

SUNDAY 11 AUG

NOTES

MONDAY 12 AUG

For any AES variation → AES-128, AES-192, AES-256

↳ Plaintext size & Ciphertext size - 128 bits

↳ Key size differs

↳ Round key size - 128 bits in all variations (same)

↳ Input size of the key is going to differ

TUESDAY 13 AUG

The key scheduling algorithm may take input of 128/192/256 bits, but all the round keys will be of constant size - 128 bits

↳ Based on the key size - number of rounds will be varying

WEDNESDAY 14 AUG

Initial Transformation - Plaintext is added with the round key (simple XOR operation)

Last Round - 3 transformations → Substitute bytes, Shift rows, Add round key

NO mix column transformation

1 word = 4 bytes

THURSDAY 15 AUG

Understanding Words in AES

- AES works with 4-byte (32-bit) words.
- AES-128 Key is 128 bits = $\frac{128}{8}$ = 16 bytes.
- Since 1 word = 4 bytes, the AES-128 Key consists of (4) words. → 4 words = 4 × 4 bytes = 16 bytes = 16 × 8 bits = 128 bits

Key Expansion Process:

- The goal is to generate 44 words for 11 round Keys (including the initial key). The Key schedule follows these steps:

FRIDAY 16 AUG

① Initialize with the Cipher Key

- The first four words (w[0] to w[3]) come directly from the original 128-bit key.

② Expand to 44 Words (w[4] to w[43])

- The expansion follows this formula:

$w[i] = w[i-4] \oplus g(w[i-1])$ (for words that are multiples of 4)

$w[i] = w[i-1] \oplus w[i-4]$ (otherwise)

SATURDAY 17 AUG

SUNDAY 18 AUG

- The g() function is applied every 4th word (w[i] where i is a multiple of 4). It includes:
  - Byte rotation (left circular shift by 1 byte)
  - Substitution (using the AES S-box)
  - XOR with Round Constant (Rcon)

NOTES

MONDAY 19 AUG

③ Continue until 44 Words Are Generated

- Since AES-128 has 10 rounds, each round needs 4 words.
- Plus, we need the initial 4 words (from the original key).
- Total: 4 + (10X4) = 44 words

This expanded key is used in the AddRoundKey step for each round of AES encryption.

TUESDAY 20 AUG

Key Expansion Overview

AES-128 key is 128 bits (16 bytes) = 4 words. We need to expand this to 44 words to use across 10 encryption rounds (+ the initial round key).

↳ The first 4 words are directly taken from the key. The remaining 40 words (w[4] to w[43]) are generated using a recursive process.

WEDNESDAY 21 AUG

How Do We Expand to 44 words:

① Initialize with the original key

w[0] = first 4 bytes of the key
w[1] = next 4 bytes
w[2] = next 4 bytes
w[3] = last 4 bytes

THURSDAY 22 AUG

② Generate words w[4] to w[43]
- For each new word w[i]:

→ If i is a multiple of 4, we apply a special transformation g(), which involves

Rotating bytes,
Substituting bytes using the S-box
XOR-ing with the round constant (Rcon)

→ Otherwise, we apply a simple XOR operation with w[i-4].

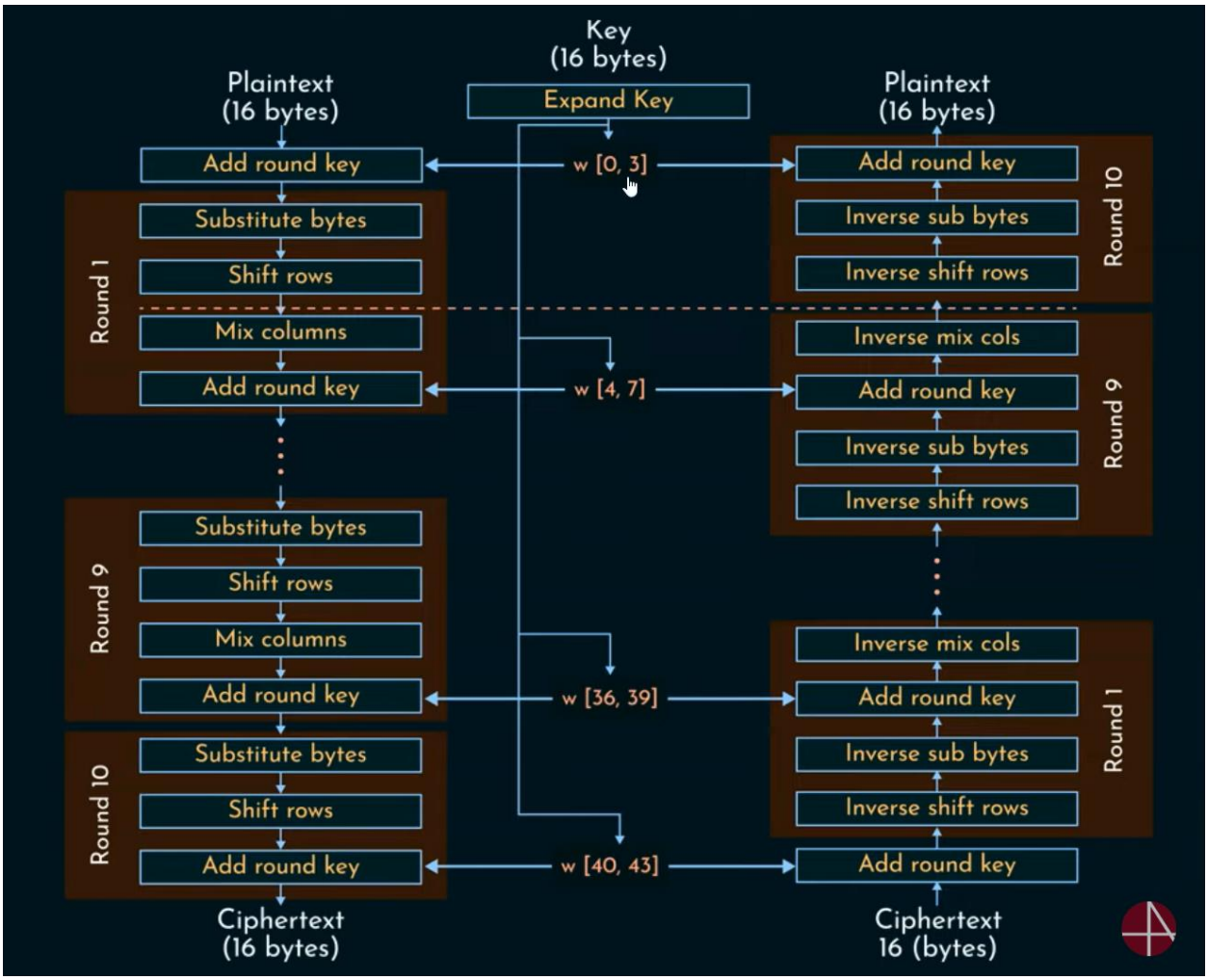
FRIDAY 23 AUG

③ Continue expanding until 44 words are generated

SATURDAY 24 AUG

SUNDAY 25 AUG

NOTES


Key
(16 bytes)
Plaintext
(16 bytes)
Expand Key
Plaintext
(16 bytes)
Add round key
w [0, 3]
Add round key
Round 10
Substitute bytes
Inverse sub bytes
Shift rows
Inverse shift rows
Round 1
Mix columns
Inverse mix cols
Add round key
w [4, 7]
Add round key
Round 9
Inverse sub bytes
Inverse shift rows
Substitute bytes
Shift rows
Mix columns
Inverse mix cols
Round 9
Add round key
w [36, 39]
Add round key
Substitute bytes
Inverse sub bytes
Round 10
Shift rows
Inverse shift rows
Round 1
Add round key
w [40, 43]
Add round key
Ciphertext
(16 bytes)
Ciphertext
16 (bytes)