AES Specification

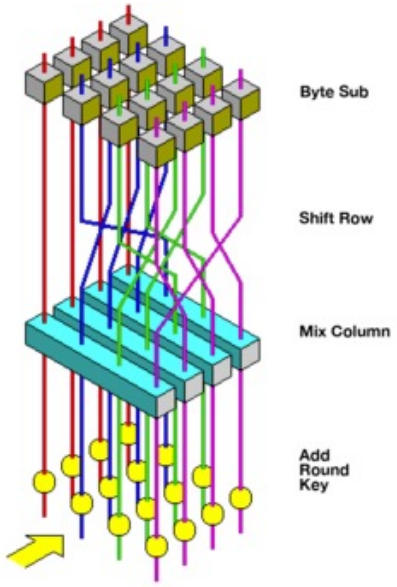
- symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- stronger & faster than Triple-DES
- provide full specification & design details
- both C & Java implementations
- NIST have released all submissions & unclassified analyses

https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/aes-development/Rijndael-ammended.pdf

The AES Cipher - Rijndael

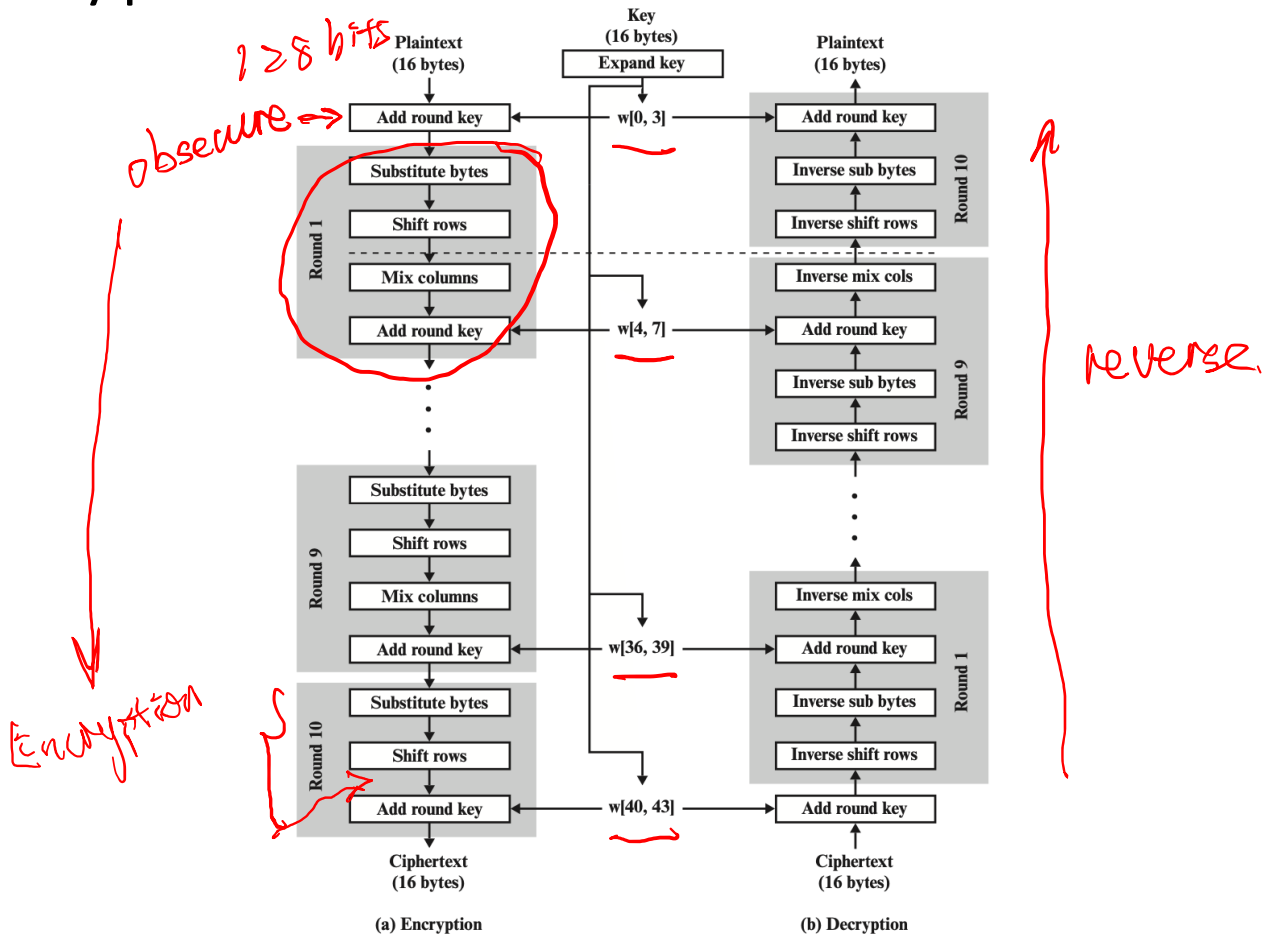
- an **iterative** rather than **feistel** cipher
  - treats data in 4 groups of 4 bytes
  - operates an entire block in every round
- designed to be:
  - resistant against known-plaintext attacks
  - speed and code compactness on many CPUs
  - design simplicity

Rijndael

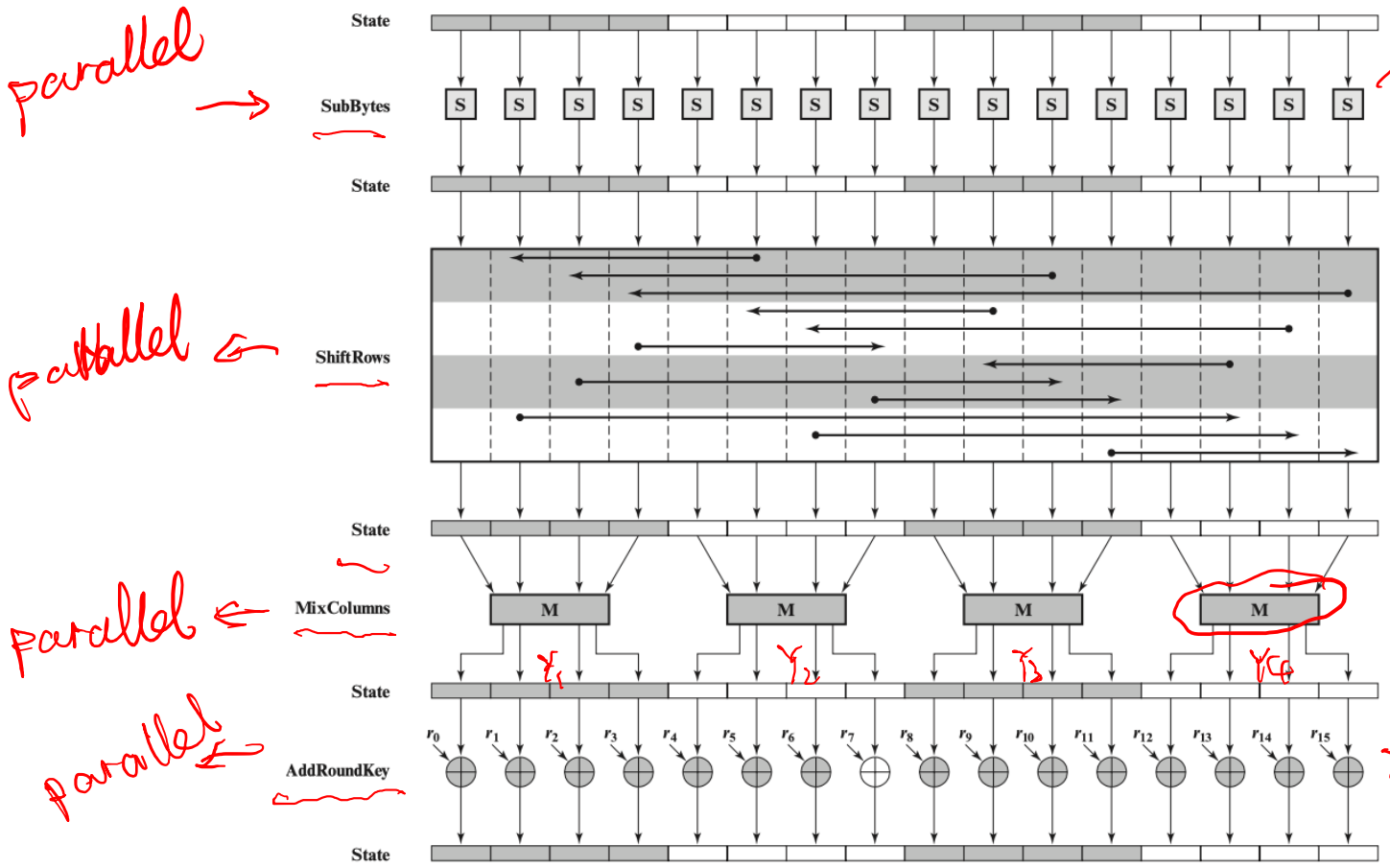


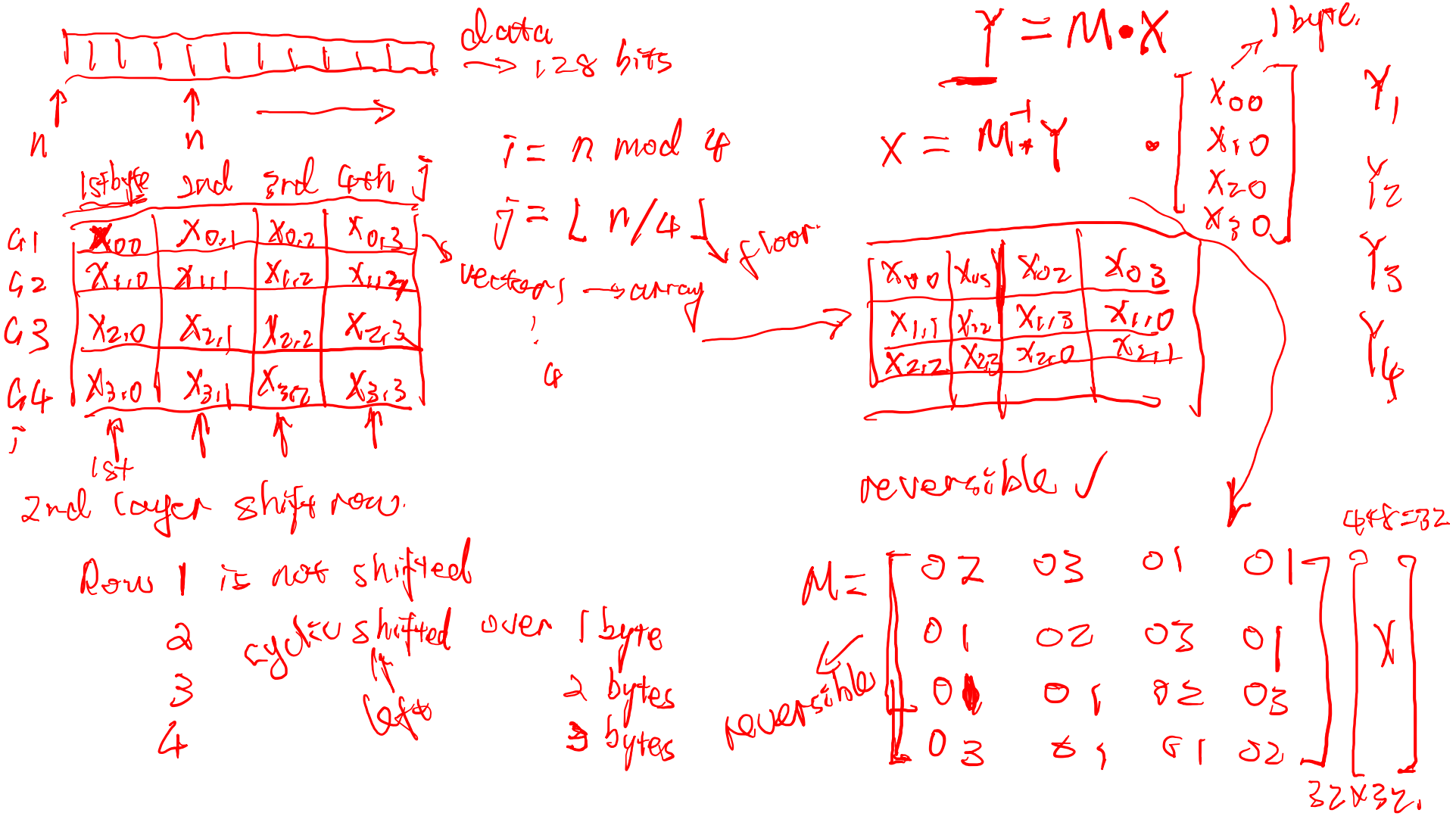
- processes data as 4 groups of 4 bytes (state) = 128 bits
- has 10/12/14 rounds in which state undergoes:
  - byte substitution (1 S-box used on every byte)
  - shift rows (permute bytes row by row)
  - mix columns (alter each byte in a column as a function of all of the bytes in the column)
  - add round key (XOR state with key material)
- 128-bit keys – 10 rounds, 192-bit keys – 12 rounds, 256-bit keys – 14 rounds

AES Encryption and Decryption



AES encryption round




data
→ 128 bits
n
n
i = n mod 4
j = ⌊ n/4 ⌋
floor
1st byte
2nd
3rd
4th
j
G1
G2
G3
G4
i
1st
vectors → array
4
Y = M • X
X = M⁻¹ • Y
1 byte.
reversible ✓
2nd layer shift row.
Row 1 is not shifted
2 cyclic shifted over 1 byte
3 2 bytes
4 3 bytes
left
reversible
M =
4*8=32
32x32.

AES pros

- Most operations can be combined into XOR and table lookups - hence very fast & efficient

Take-home Exercises

- Find an AES API to encrypt a text (A), then decrypt it and check whether the original text (A) equals the decrypted text (B). Whether A = B?
- Compare the decryption time with different key lengths, and with DES and 3DES.
  - Suggestions: find a large A file. Run decryption a couple of times and take the average.

Reading materials

- FIPS 197, Advanced Encryption Standard (AES) (nist.gov)

WPEC 2024: NIST Workshop on Privacy-Enhancing Cryptography

- Time: September 24–26, 2024
- Free to register
- Virtual conference via Zoom
- https://csrc.nist.gov/events/2024/wpec2024