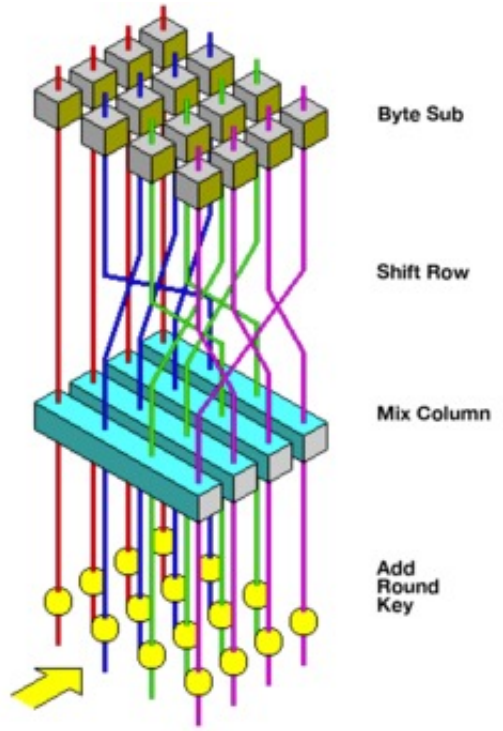
Lecture 7

Outline

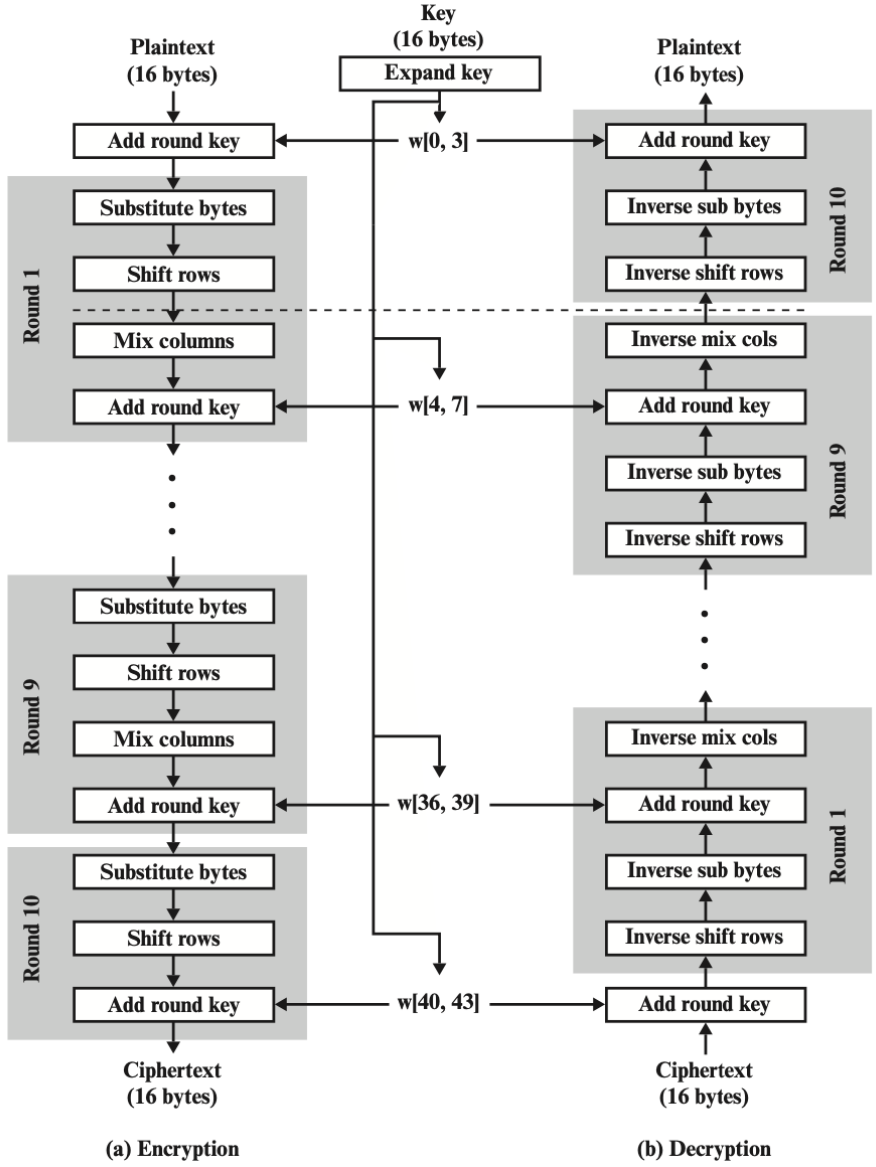
- AES
- Random number

Rijndael

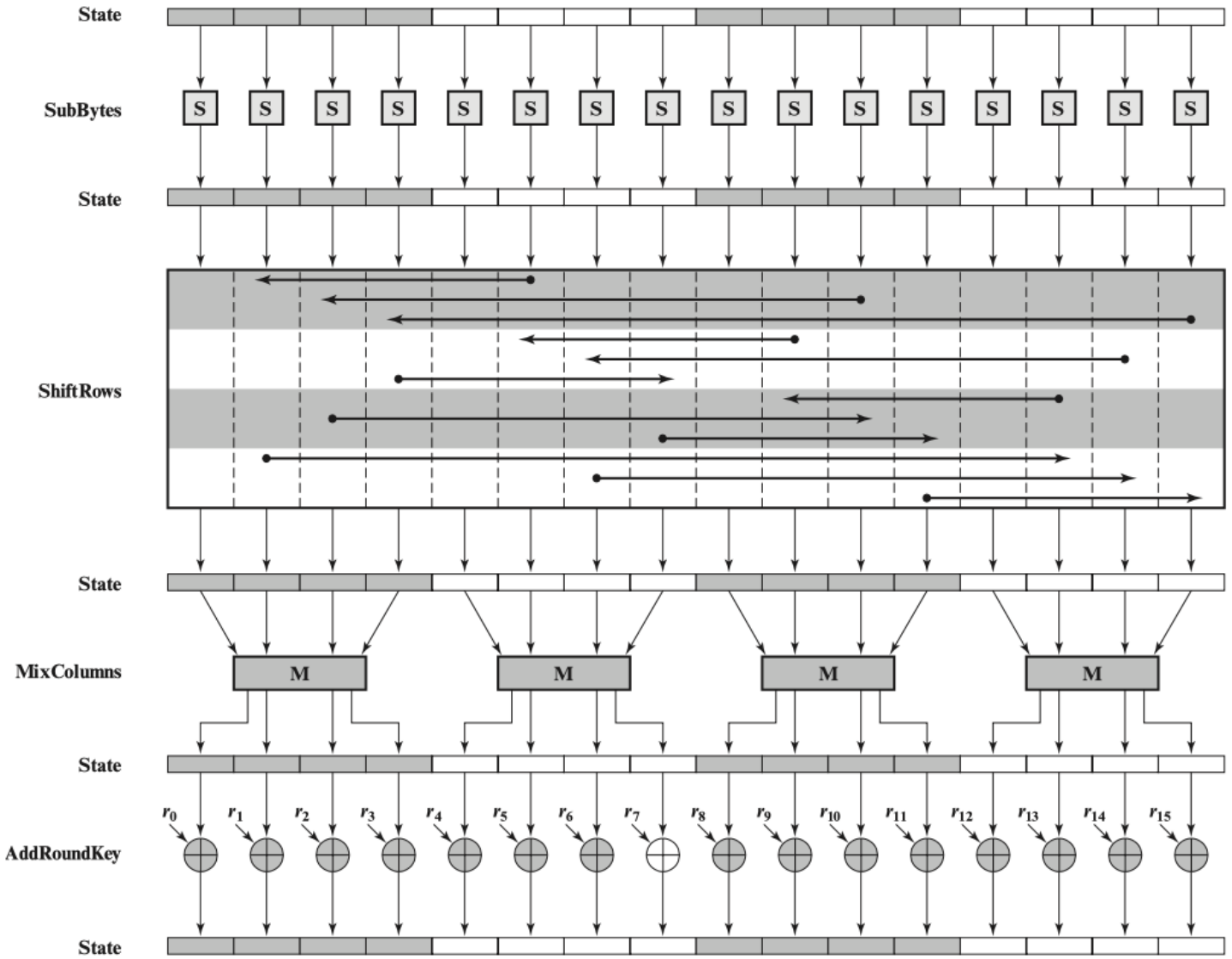


- processes data as 4 groups of 4 bytes (state) = 128 bits
- has 10/12/14 rounds in which state undergoes:
  - byte substitution (1 S-box used on every byte)
  - shift rows (permute bytes row by row)
  - mix columns (alter each byte in a column as a function of all of the bytes in the column)
  - add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



AES pros

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

Take-home Exercises

- Find an AES code 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)