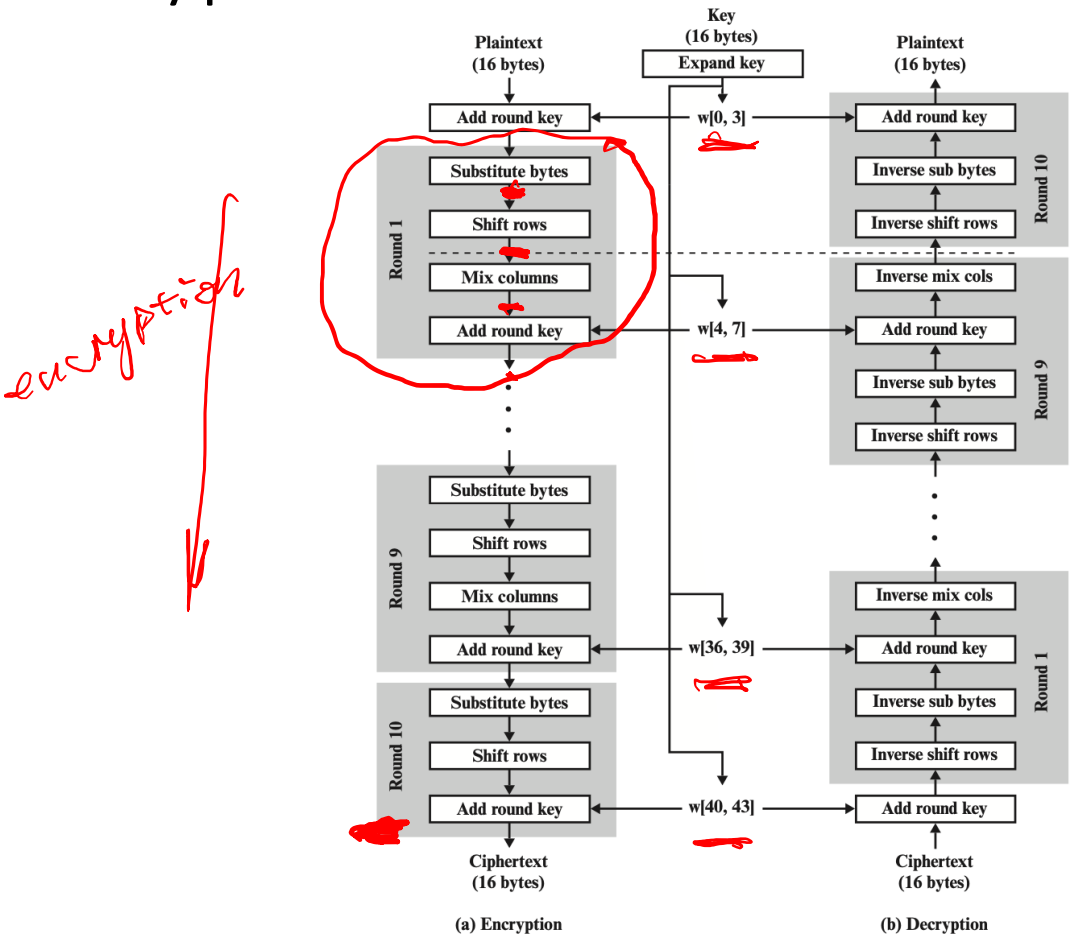
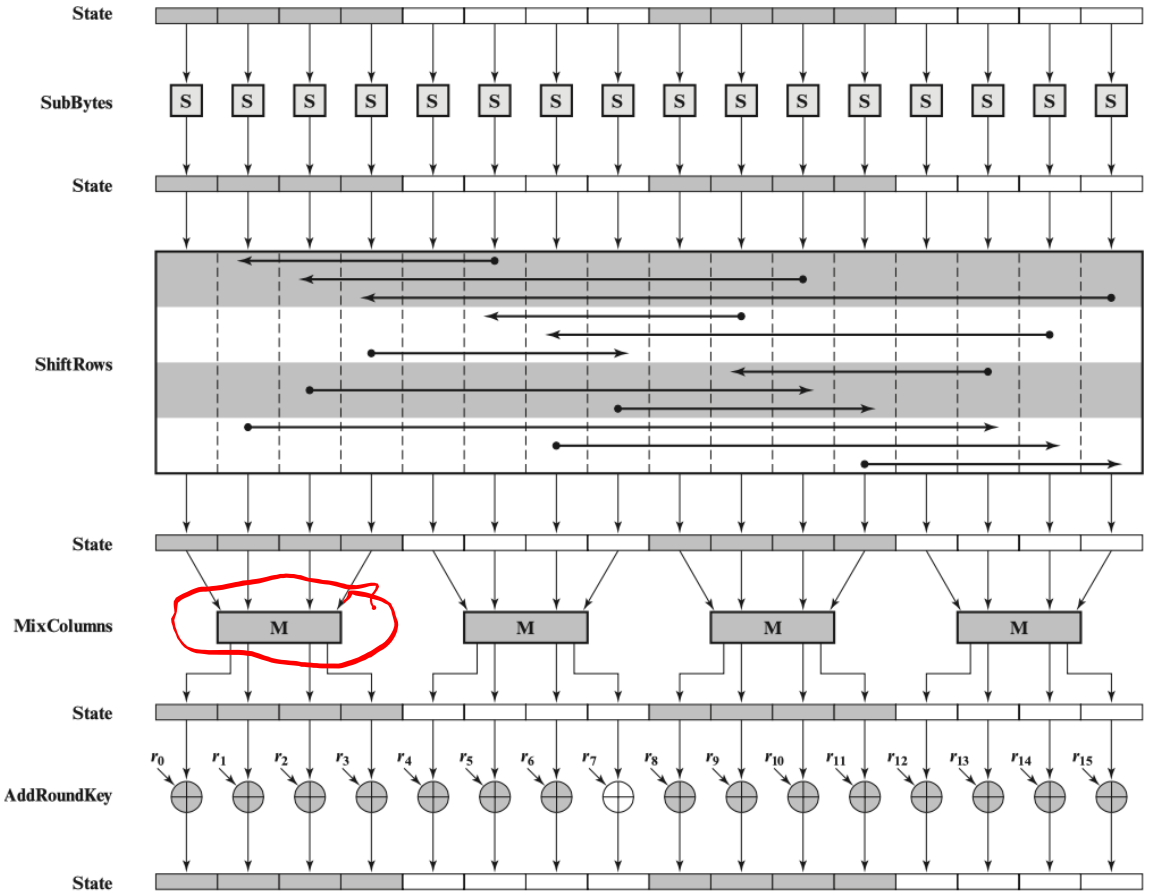
AES Encryption and Decryption



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 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)

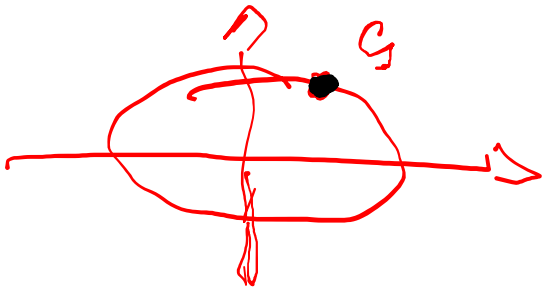
WPEC 2024: NIST Workshop on Privacy-Enhancing Cryptography

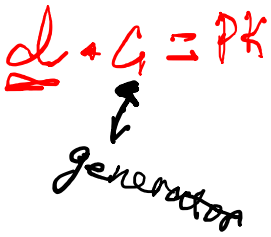
- Time: September 24–26, 2024
- Archive videos
- Virtual conference via Zoom
- https://csrc.nist.gov/events/2024/wpec2024

Random and Pseudorandom Numbers

When to use random numbers?

- Generation of a stream key for symmetric stream cipher
- Generation of keys for public-key algorithms
  - RSA public-key encryption algorithm (described in Chapter 3)
- Generation of a symmetric key for use as a temporary **session key**
  - used in a number of networking applications, such as Transport Layer Security (Chapter 5), Wi-Fi (Chapter 6), e-mail security (Chapter 7), and IP security (Chapter 8)
- In a number of key distribution scenarios
  - Kerberos (Chapter 4)





Two types of random numbers

- True random numbers:
  - generated in non-deterministic ways. They are not predictable and repeatable
- Pseudorandom numbers:
  - appear random, but are obtained in a deterministic, repeatable, and predictable manner

Properties of Random Numbers

- Randomness
  - Uniformity
    - distribution of bits in the sequence should be uniform
  - Independence
    - no one subsequence in the sequence can be inferred from the others
- Unpredictable
  - satisfies the "next-bit test“