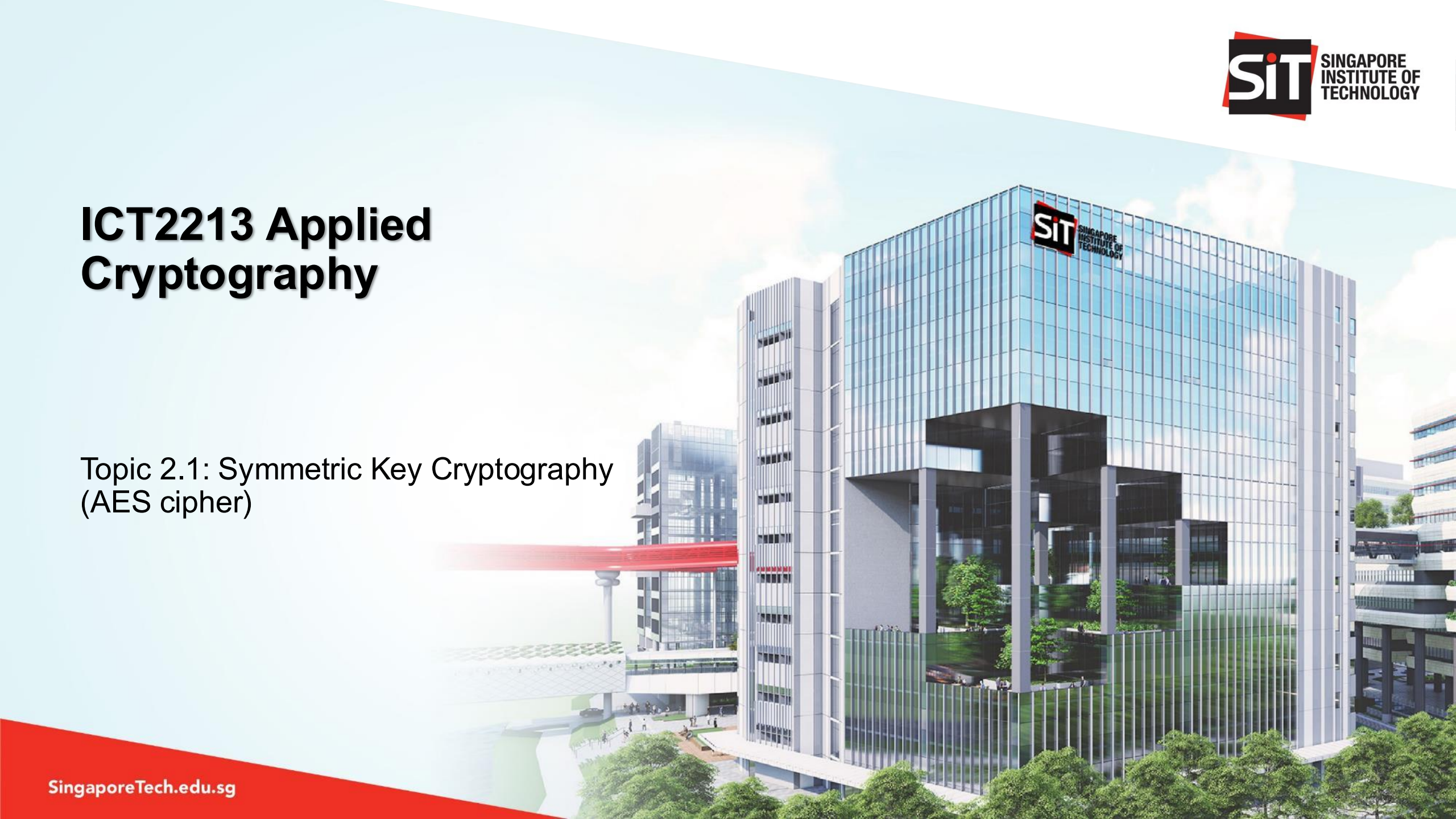
ICT2213 Applied Cryptography

Topic 2.1: Symmetric Key Cryptography (AES cipher)



Learning outcomes

- Understand the basic principles of modern block ciphers
- Explain the operation of the AES cipher

Block cipher principles

- Block ciphers look like an extremely large substitution cipher
  - Given a key, there is a one-to-one mapping between a plaintext block and a ciphertext block
- For a 128-bit block we would need a table of 2^{128} entries
- This is infeasible to store so, instead, we create the substitution from smaller building blocks
- Claude Shannon introduced the idea of substitution-permutation (S-P) networks in 1949
  - This forms the basis of modern block ciphers
- S-P nets are based on the two primitive cryptographic operations:
  - Substitution (S-box)
  - Permutation (P-box)

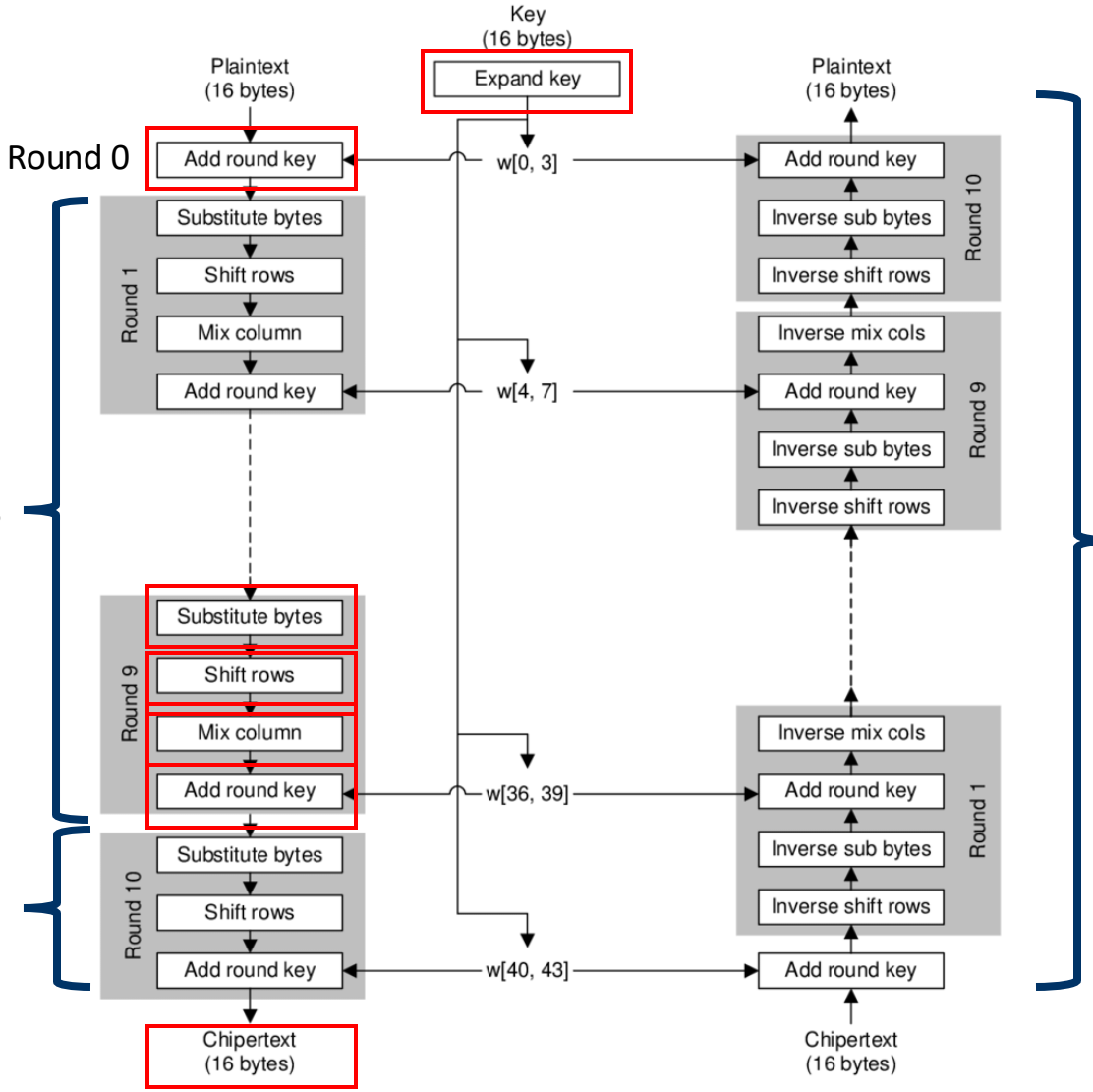
Block cipher principles

- Specifically, Shannon suggested combining S- and P-boxes to provide confusion and diffusion of message and key
- **Diffusion:** dissipates the statistical structure of plaintext over bulk of ciphertext
- **Confusion:** makes the relationship between ciphertext and key as complex as possible
- The avalanche effect is a key desirable property of encryption algorithms
  - A change of one plaintext or key bit results in changing approximately half output bits
  - This makes attempts to guess keys impossible

The AES cipher

- AES was selected to replace DES (Data Encryption Standard), which used to be the most widely used block cipher
  - DES was weak because it had a key of only 56 bits
- The U.S. National Institute of Standards and Technology (NIST) issued a call for ciphers in 1997
- The Rijndael cipher was selected in October 2000 as the Advanced Encryption Standard (AES)
  - It was issued as a FIPS PUB 197 standard in November 2001
- It was designed by two Belgian cryptographers, Rijmen and Daemen
- AES operates on 128-bit data and has 128/192/256-bit keys
- There are currently no known attacks on AES
  - Except for side-channel attacks on specific implementations

AES overview



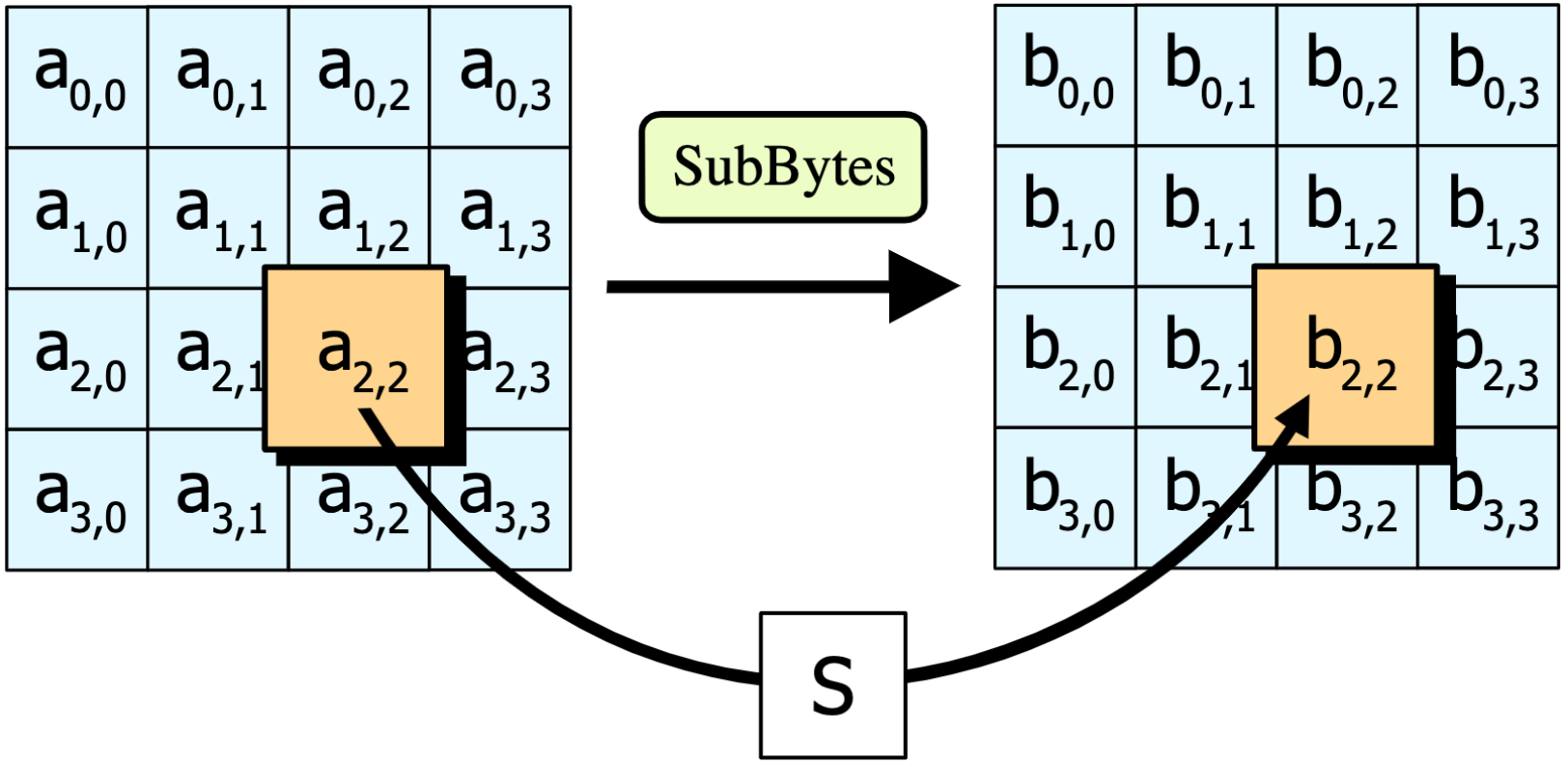
4 transformations

3 transformations

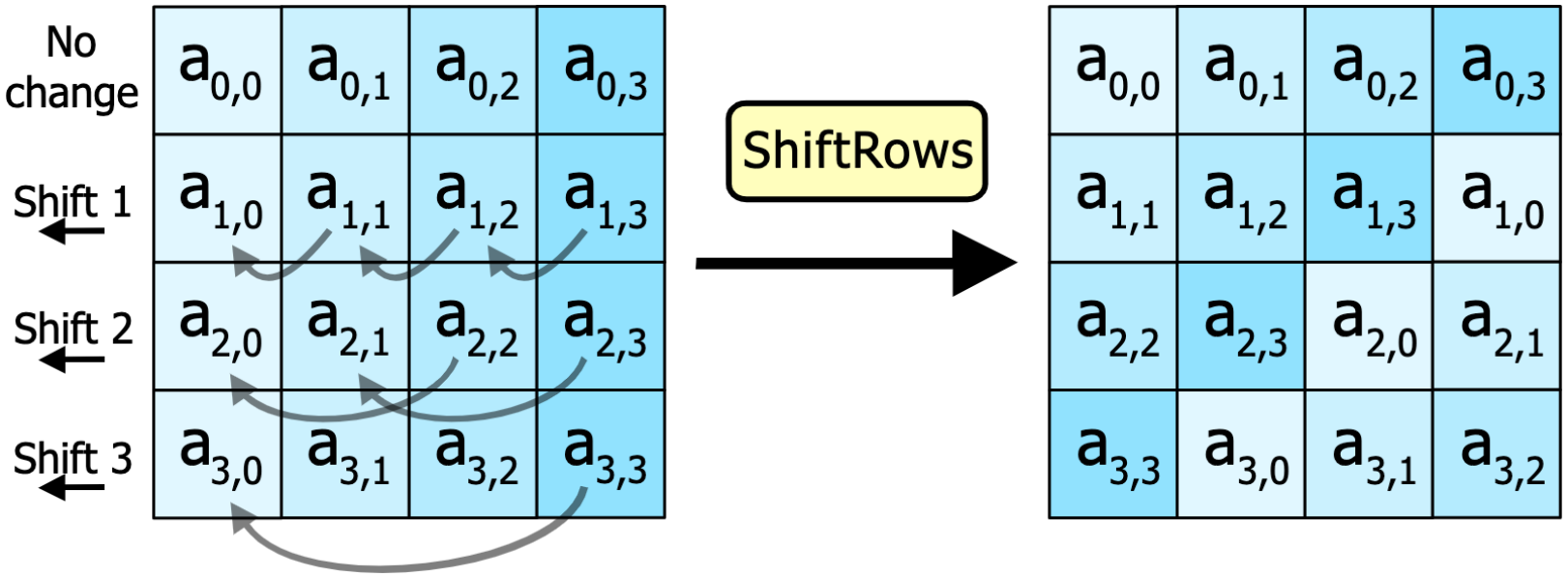
Inverse transformations for decryption

Key size (bytes)	16	24	32
Block size (bytes)	16	16	16
Number of rounds	10	12	14
Round key size (bytes)	16	16	16
Expanded key size (bytes)	176	208	240

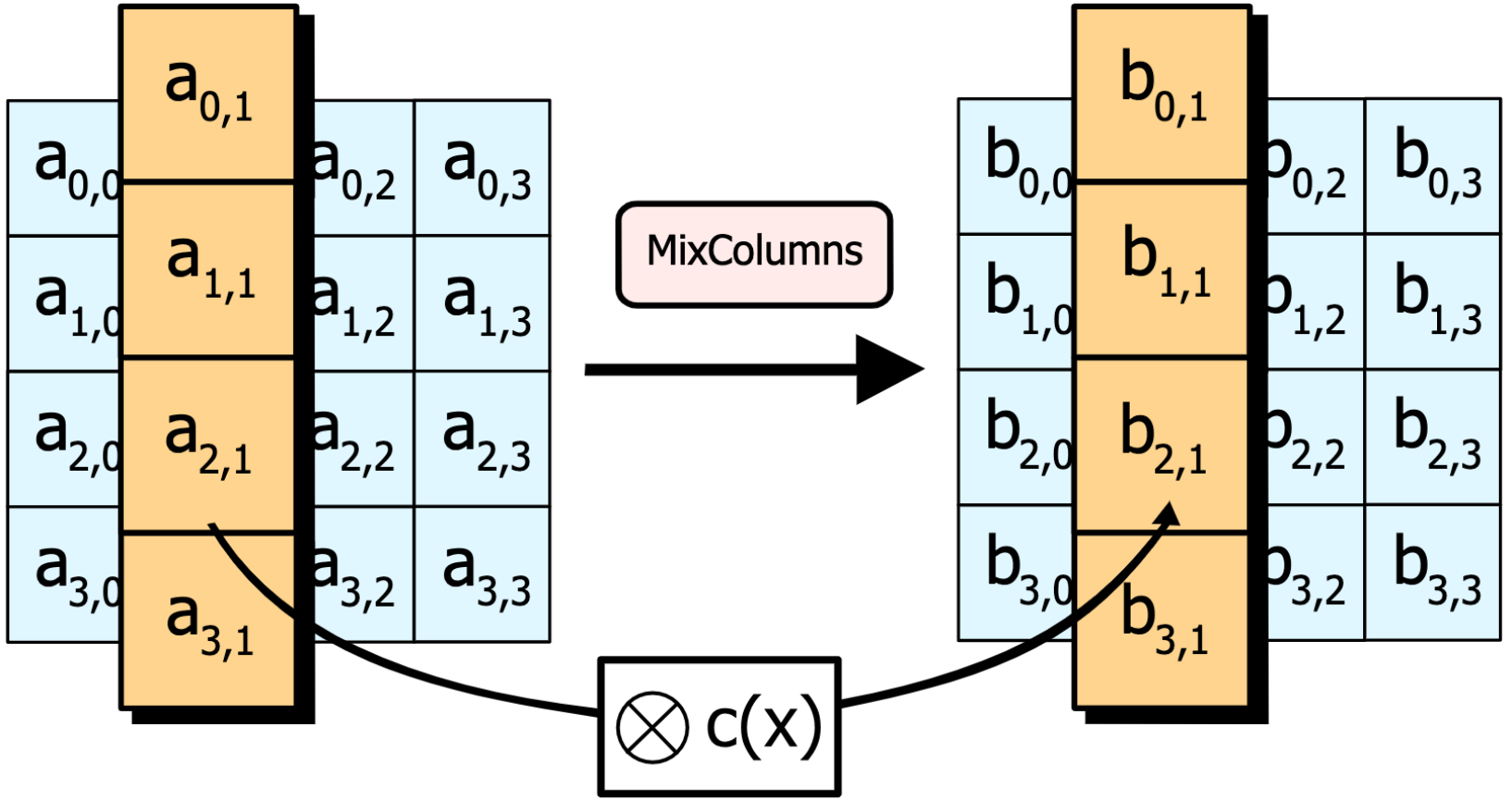
Substitute bytes function



Shift rows function



Mix columns function



Add round key function