Applied Cryptography
CPEG 472/672
Lecture 3A

Instructor: Nektarios Tsoutsos

Block Ciphers

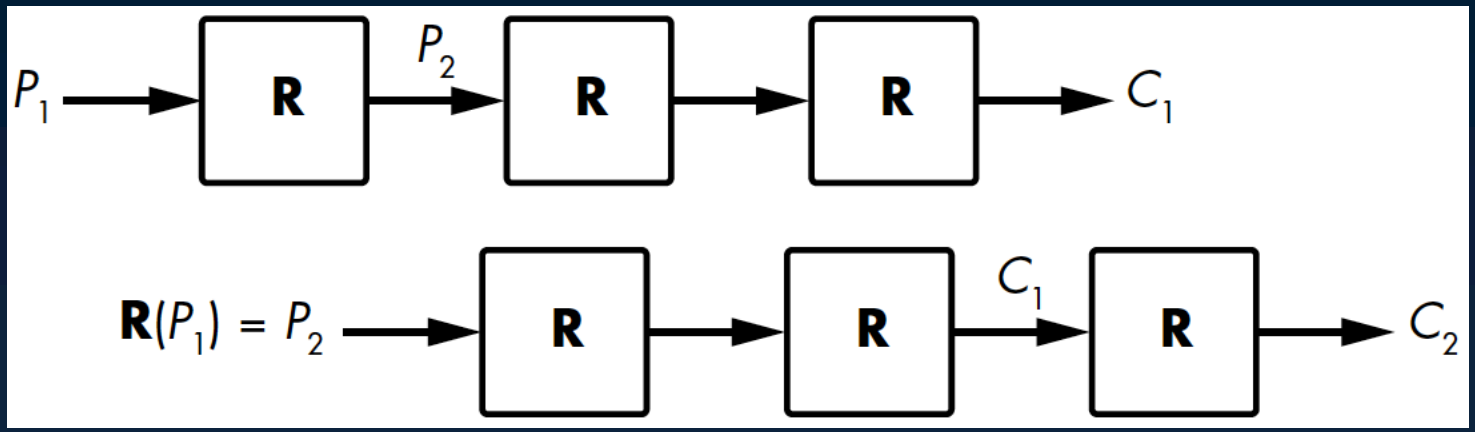
- Encryption: ctxt=**E**(*K, ptxt*)
- Decryption: ptxt=**D**(*K,ctxt*)
- Security objectives
  - Pseudorandom permutation (PRP)
  - Cannot produce any ctxt without K
  - Cannot discover any pattern in ptxt/ctxt
  - Indistinguishable from random permutation
  - Impossible to recover the secret key K
  - Cannot recover ptxt from ctxt

Block size

- DES: 64 bits
- AES: 128 bits
- Smaller blocks
  - Small ctxts
  - Reduced memory overhead
  - Codebook attacks (build table of ctxts/ptxts)
- Larger blocks
  - Increased memory overhead
  - Increased resilience to attacks

Construction of Block Ciphers

- Encrypt: Compute a sequence of rounds
  - Compute inverse rounds to Decrypt
- Each round performs a transformation
  - Should depend on a round key (sub-key)
- Each round key must be different
  - Slide attacks if rounds keys are the same

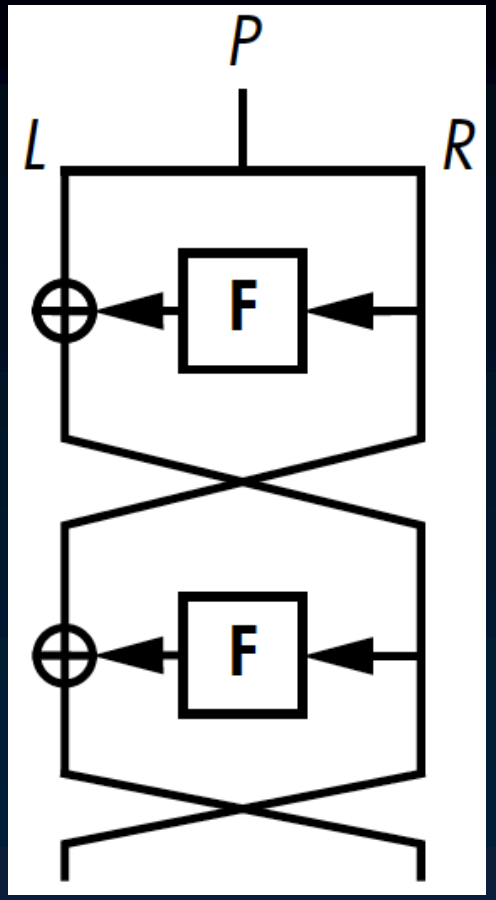


Construction of Block Ciphers

- Confusion and diffusion properties
  - A ctxt bit depends on many key bits
  - Flipping 1 ptxt bit affects half ctxt bits
- Substitution-Permutations (SP) Networks
  - Implement confusion and diffusion
  - Use of (non-linear) S-boxes
  - No statistical bias

Construction of Block Ciphers

- Feistel Networks
  - Split input block in L and R
  - Use an SP function F
  - L=L XOR F(R)
  - Swap L, R
  - Repeat
- F can be PRP or PRF
  - PRP: 1-to-1 and onto
  - PRF: not 1-to-1 [can be F(X) = F(Y)]

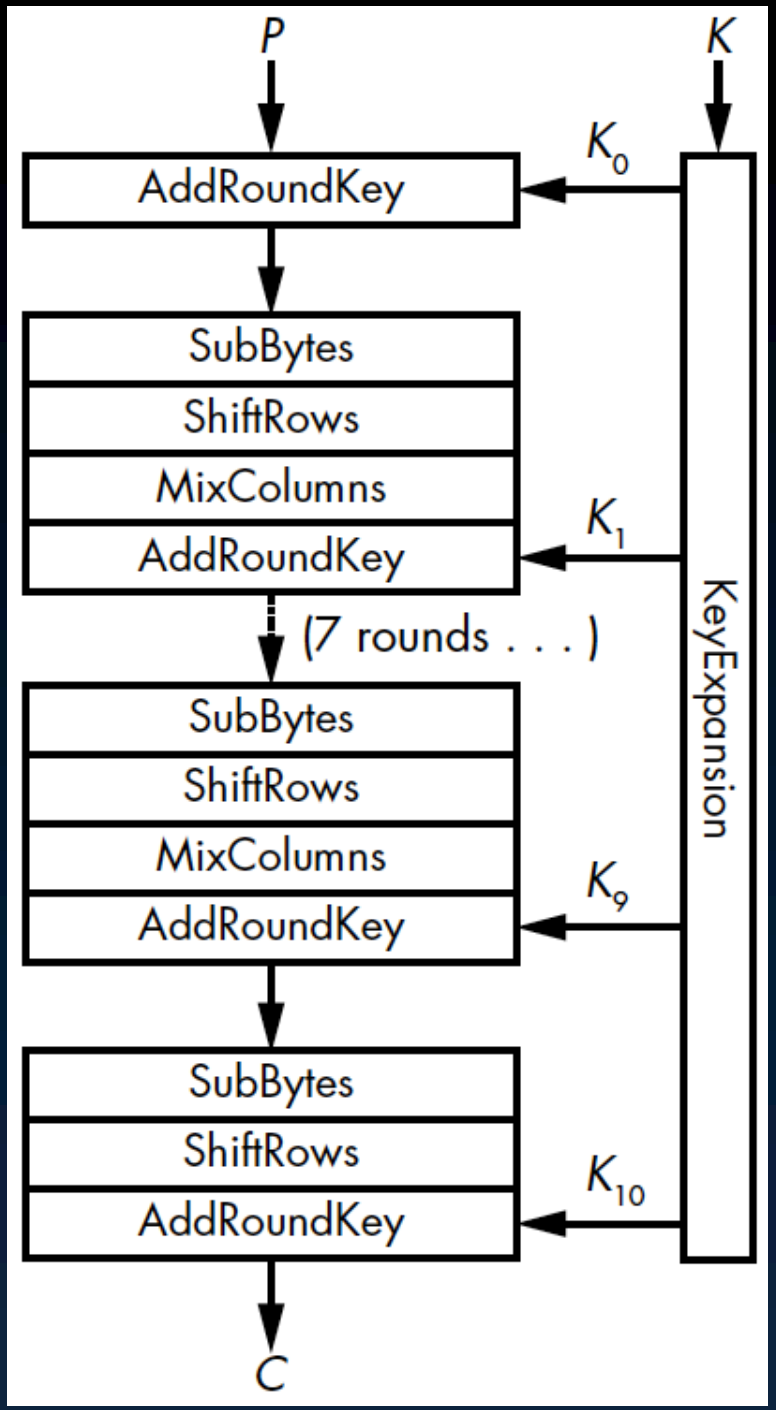


Advanced Encryption Standard

- AES facts:
  - Most widely used cipher
  - SP network design
  - Is a secure PRP
  - Improves over DES (56-bit security) and 3-DES (112-bit security for 168 bit keys)
  - 10-14 rounds
  - 128 bit blocks (state: 16 bytes, 4x4 array)
  - 128, 192, 256 bit keys
  - Developed in Belgium for NIST competition

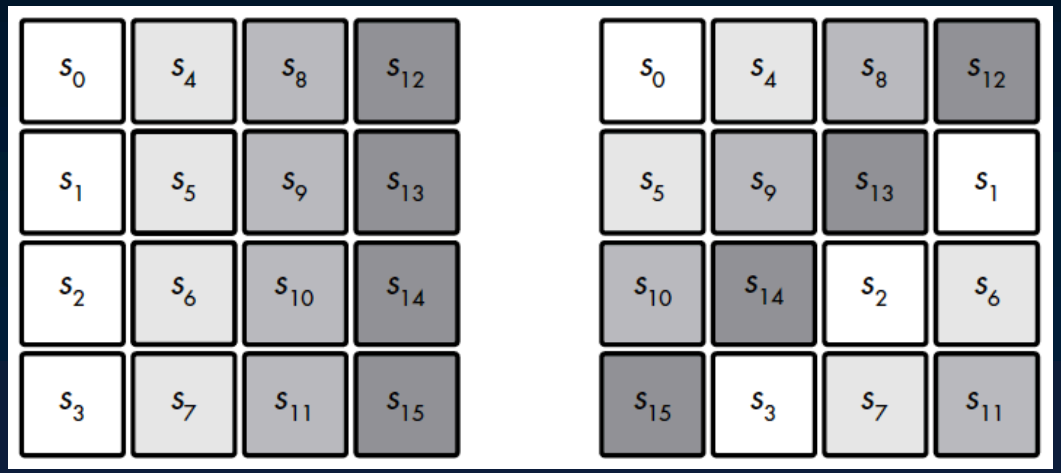
AES-128 Rounds

- 11 subkeys
- 10 rounds
- 4 operations
  - Add round key
  - Sub bytes
  - Shift Rows
  - Mix columns
- Last round different
  - Mix columns not required



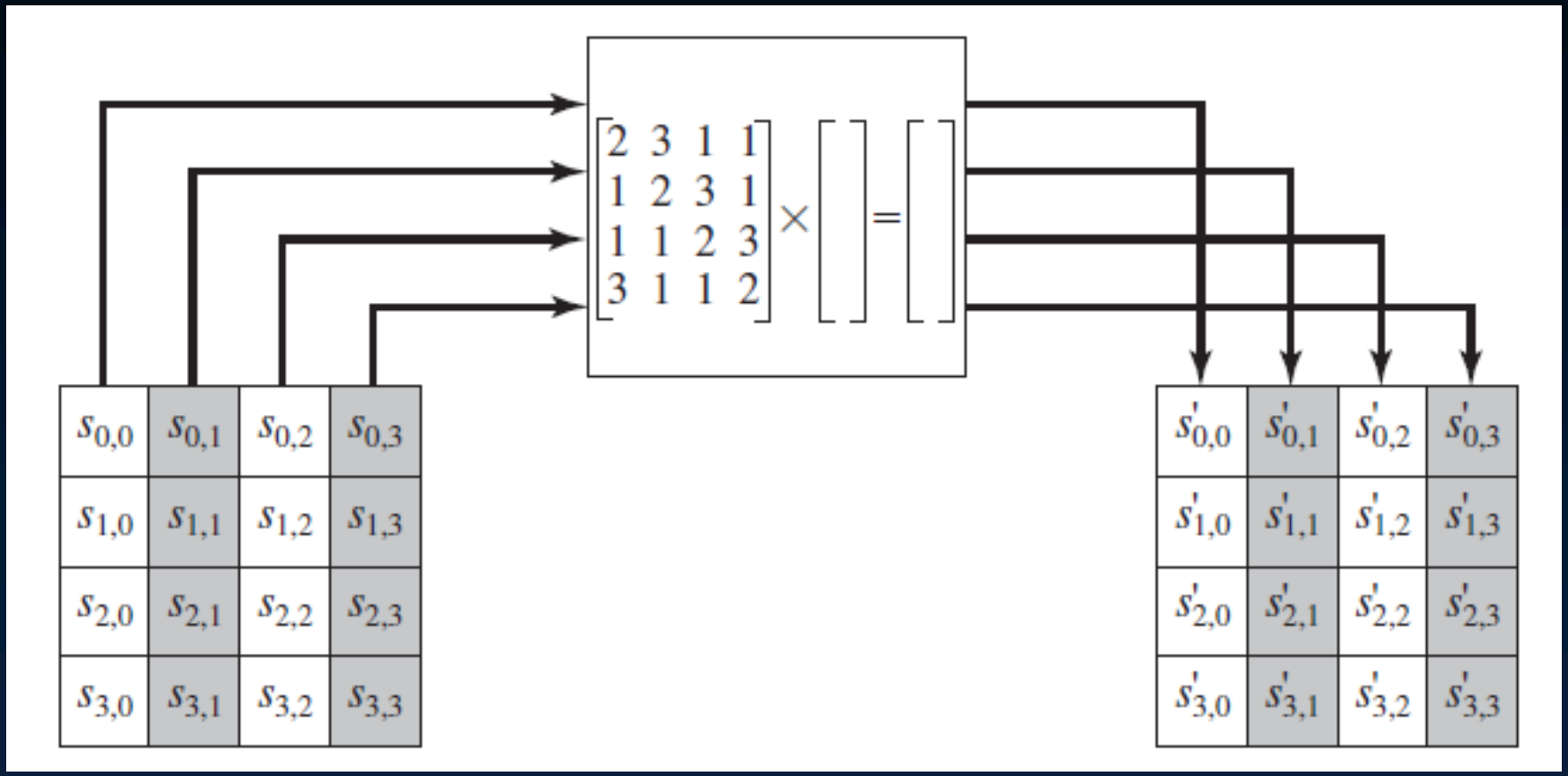
AES building blocks

- Add Round Key
  - An XOR operation with round key
- Sub Bytes
  - Uses the AES S-box to replace the 16 bytes
- Shift Rows
  - Rotate rows



- Mix Columns
  - Apply linear transformation to each column

MixColumns


2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2
×
=
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

AES today

- Implemented using lookup tables + XOR
  - Replace the sequence of subbytes, shiftrows, mixcolumns with tables
- 4 tables required for encryption
  - Each has 256 x 32-bit entries
  - Total cost = 1 kilobyte
- Another 4 tables from decryption
  - Possible to compress these tables
- Concern: Cache timing attacks

AES Native Instructions (AES-NI)

```
PXOR %xmm5, %xmm0
AESENC %xmm6, %xmm0
AESENC %xmm7, %xmm0
AESENC %xmm8, %xmm0
AESENC %xmm9, %xmm0
AESENC %xmm10, %xmm0
AESENC %xmm11, %xmm0
AESENC %xmm12, %xmm0
AESENC %xmm13, %xmm0
AESENC %xmm14, %xmm0
AESENCLAST %xmm15, %xmm0
```

4 cycles per AESENC

2.5 cycles/byte

Reading for next lecture

- Aumasson: Chapter 4