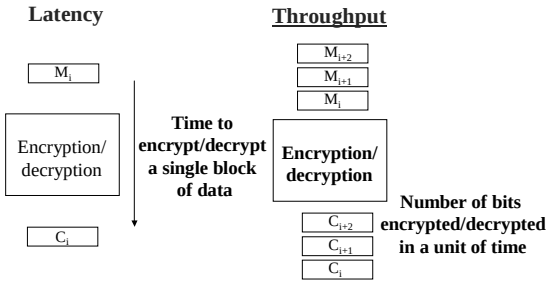
ECE 297:11 Lecture 8

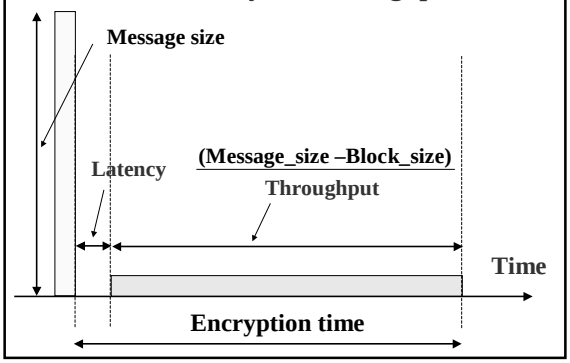
Architectures of secret-key ciphers

Primary parameters of hardware implementations for secret-key block ciphers



$$\text{Throughput} = \frac{\text{Block\_size} \cdot \text{Number\_of\_blocks\_processed\_simultaneously}}{\text{Latency}}$$

Dependence of the encryption time on latency and throughput



Primary factor in choosing the encryption/decryption unit architecture

Symmetric-key cipher mode of operation:

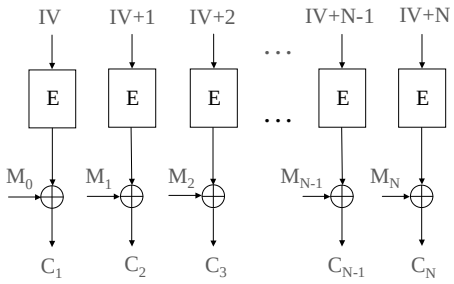
1. Non-feedback cipher modes

   ECB, counter mode

2. Feedback cipher modes

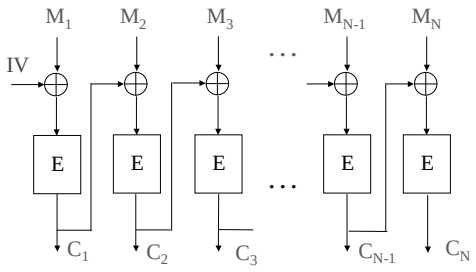
   CBC, CFB, OFB

Non-feedback Counter Mode - CTR



$C_i = M_i \oplus AES(IV+i)$ for i=0..N

Feedback cipher modes - CBC

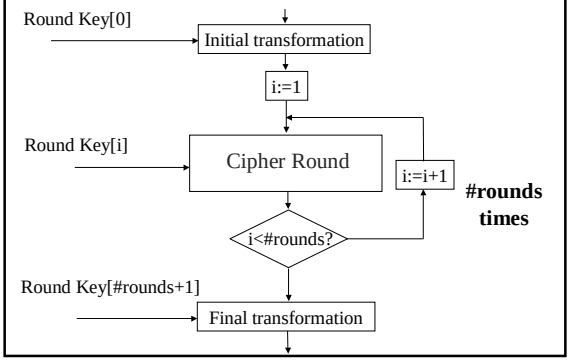


$C_1 = AES(M_i \oplus IV)$

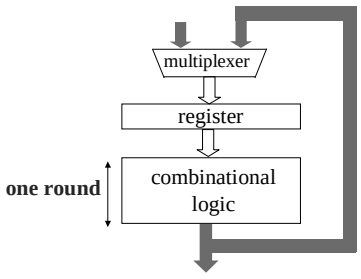
$C_i = AES(M_i \oplus C_{i-1})$ for i=2..N

Feedback cipher modes
CBC, CFB, OFB

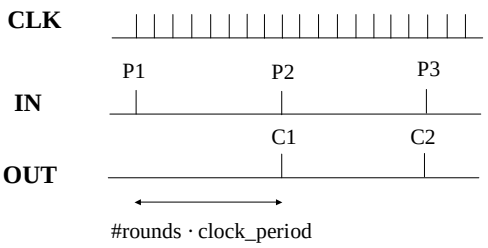
Typical Flow Diagram of a Secret-Key Block Cipher



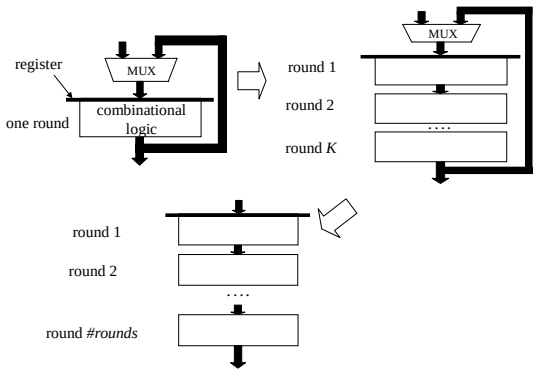
Basic iterative architecture



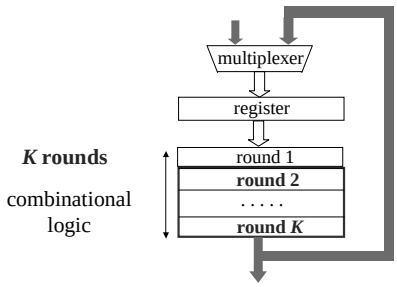
Basic architecture: Timing



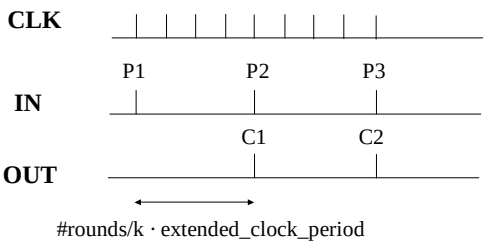
Architectures suitable for feedback modes



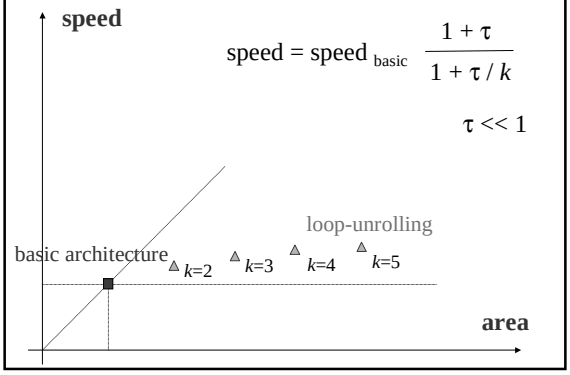
Partial Loop Unrolling



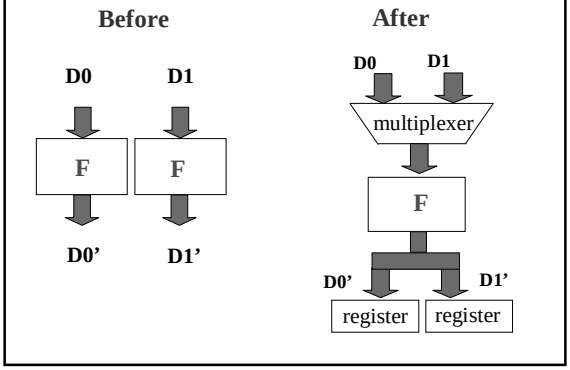
Loop Unrolling: Timing



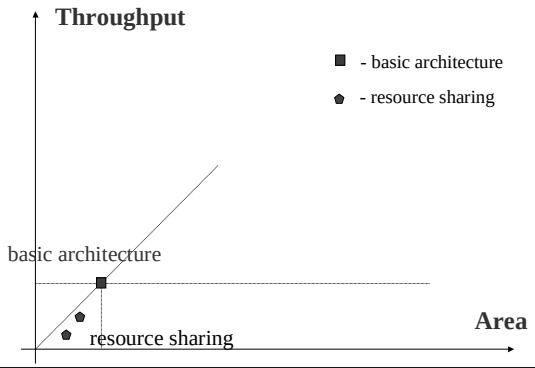
Loop Unrolling: Speed vs. Area



Decreasing area by resource sharing

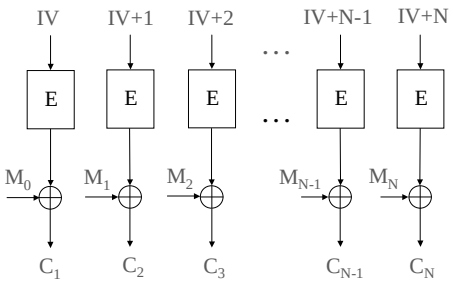


Resource sharing: Speed vs. Area



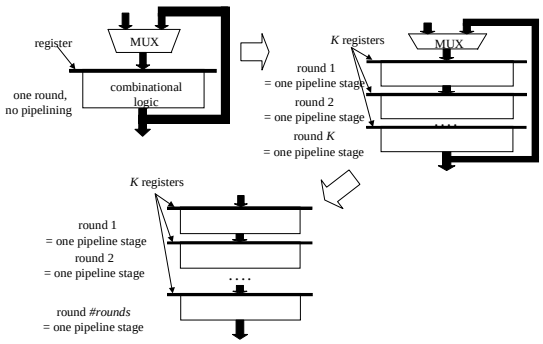
Non-Feedback Cipher Modes
ECB, counter

Comparison for non-feedback cipher modes, e.g. Counter Mode - CTR



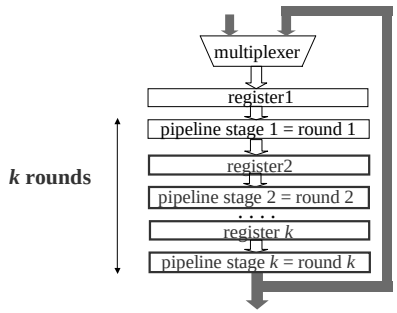
$C_i = M_i \oplus AES(IV+i)$ for i=0..N

Traditional methodology

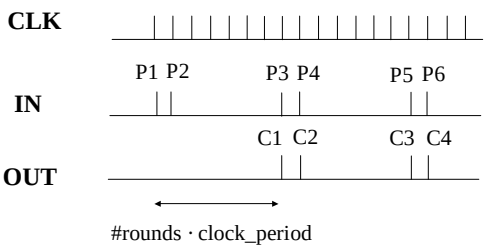


k-stage Outer-Round Pipelining

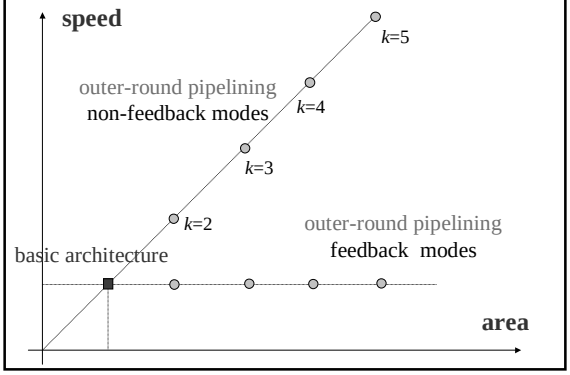
WPI: Partial Pipelining, PP-*k* **NSA:** Pipelined Architecture
UC Berkeley: Unrolled Pipeline



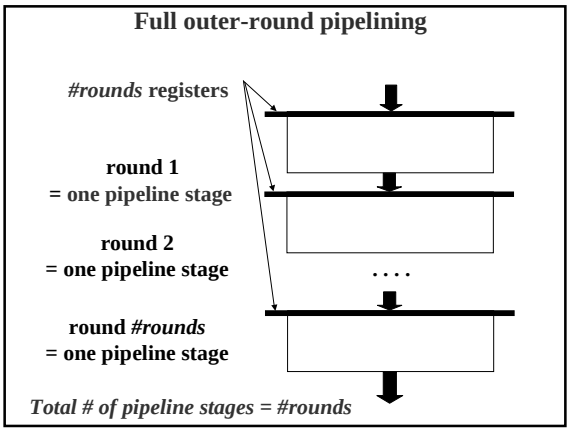
Outer-Round Pipelining: Timing



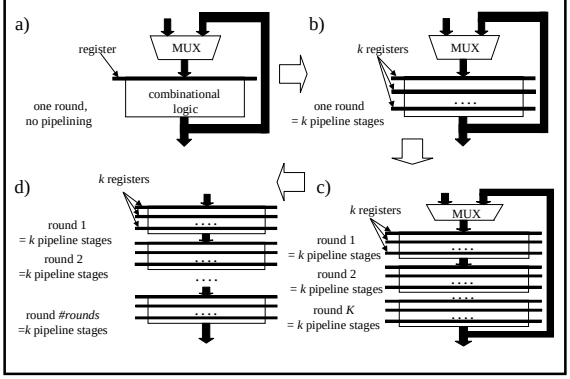
Outer-Round Pipelining: Speed vs. Area



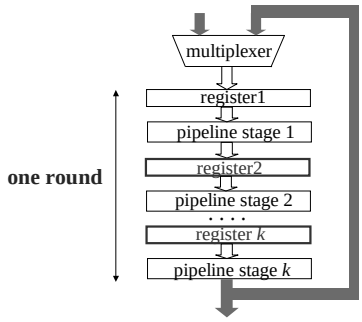
Full outer-round pipelining



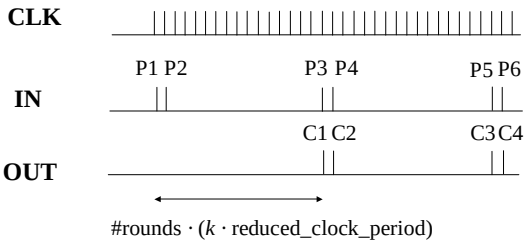
New methodology



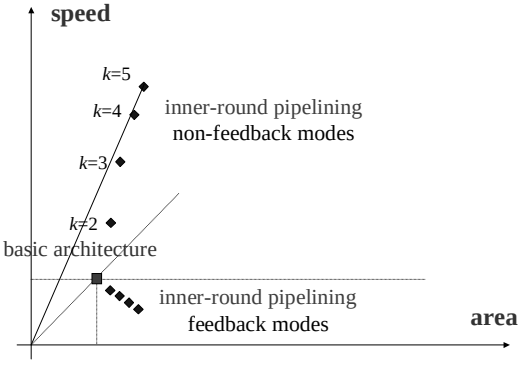
Inner-Round Pipelining



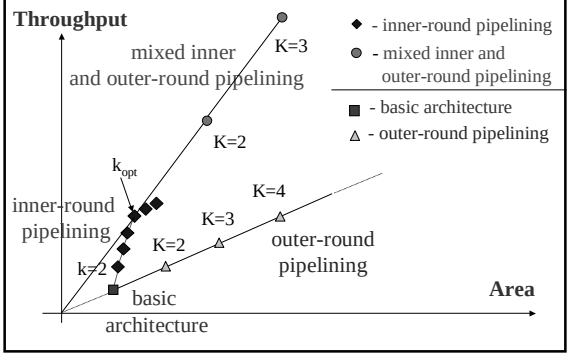
Inner-Round Pipelining: Timing



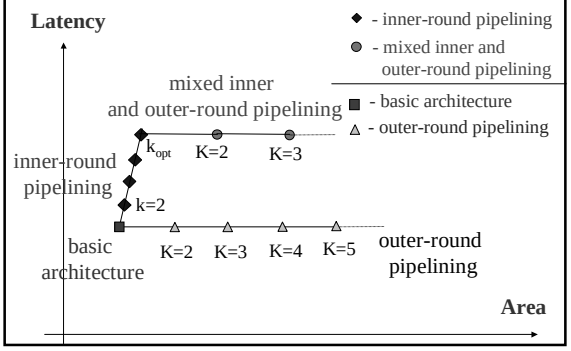
Inner-Round Pipelining: Speed vs. Area



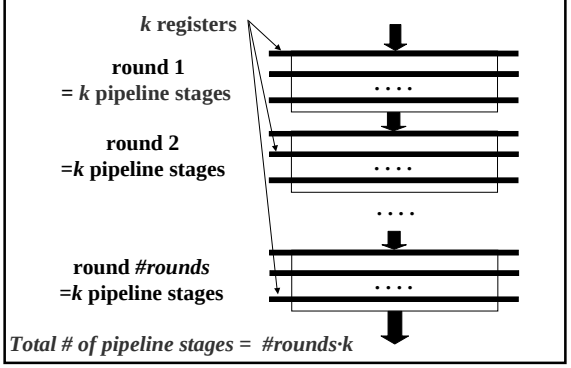
Comparison of the traditional and new design methodologies



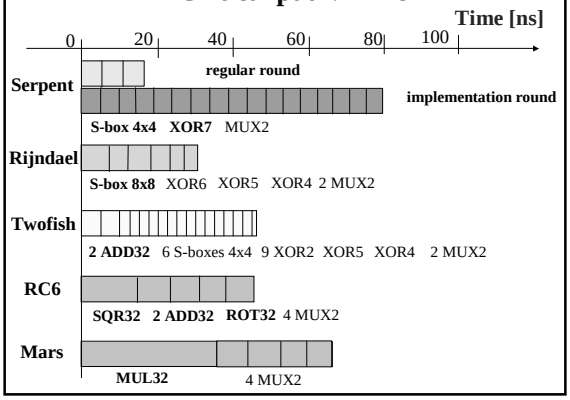
Latency vs. area dependence for the new design methodology



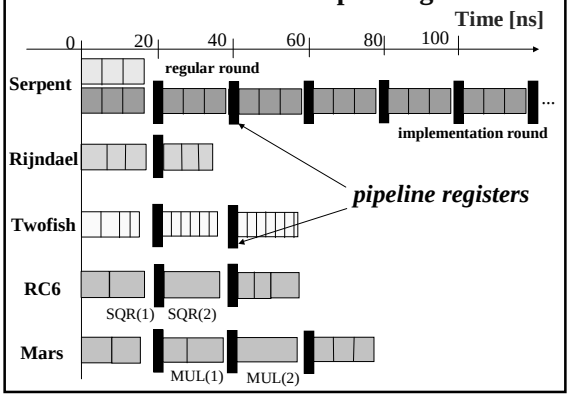
Full mixed inner- and outer-round pipelining



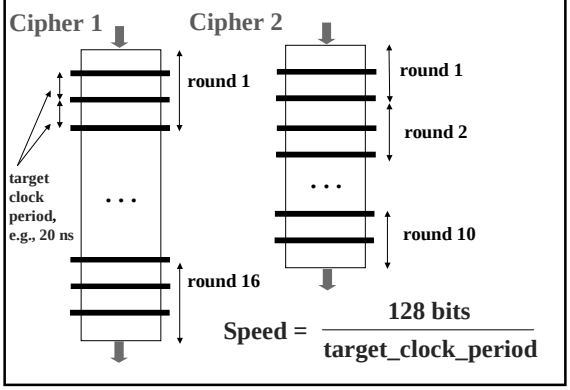
Critical path: Time



Inner-Round Pipelining



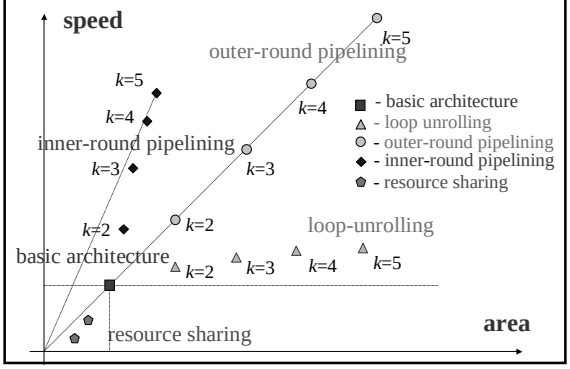
Full Mixed Inner and Outer-Round Pipelining



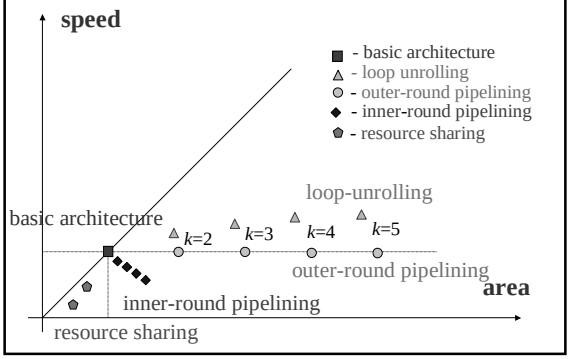
Conclusions for non-feedback cipher modes ECB, counter

- **All ciphers can achieve approximately the same speed. Area should be the primary criteria of comparison.**
- **Architecture with inner round pipelining combined with full outer round pipelining is the fastest**

Performance of alternative architectures: in non-feedback cipher modes (ECB, counter)



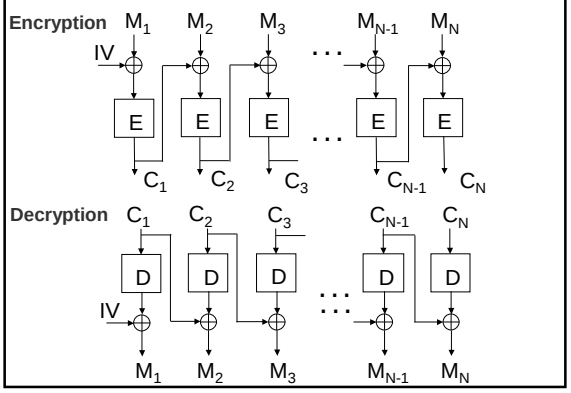
Performance of alternative architectures: in feedback cipher modes (CBC, CFB, OFB)



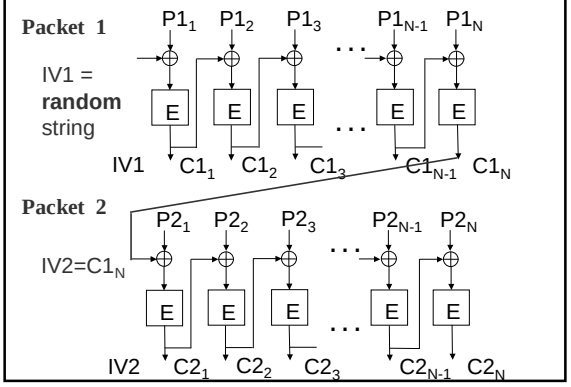
Encryption in Communication Protocols

Modes of operation: CBC

RFC 2405



CBC: Implementation Issues: Encryption



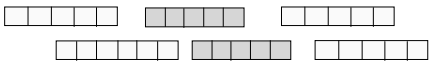
Parallel processing of data (1)

Sequential processing of data

Parallel processing of different security associations

Parallel processing of data (2)

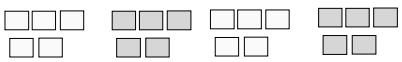
Parallel processing of packets belonging to the same security association



Encryption in CBC: multiple IVs required for the same SA
Decryption in CBC: no problems

Parallel processing of data (3)

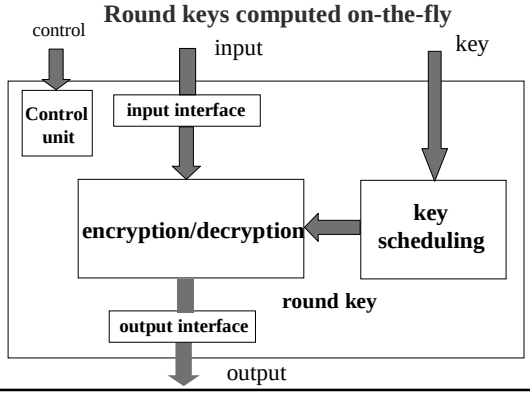
Parallel processing of blocks belonging to the same packet



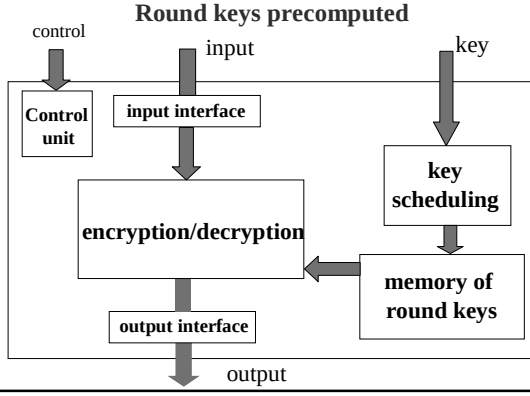
Encryption in CBC: not feasible
Decryption in CBC: no problems

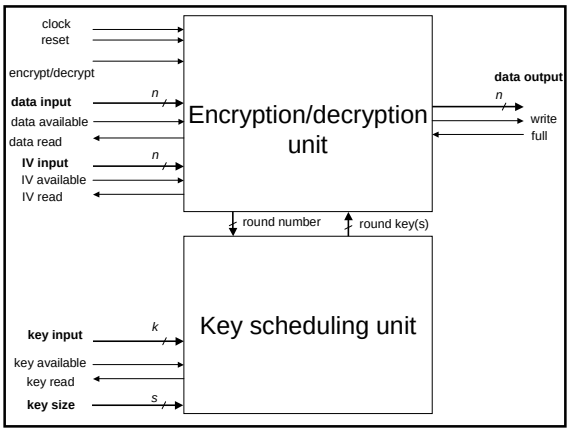
Secret-key ciphers
Interface

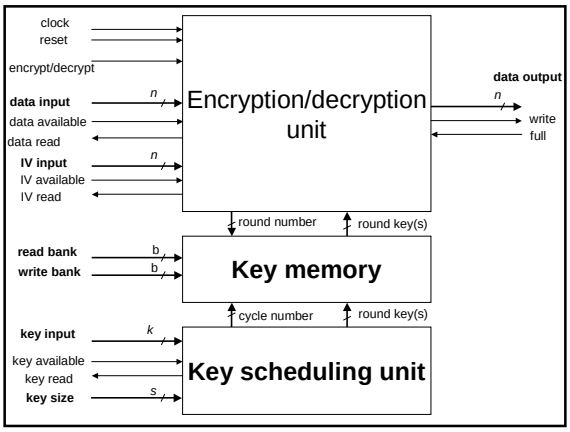
Implementation of a secret-key cipher
Round keys computed on-the-fly



Implementation of a secret-key cipher
Round keys precomputed




clock
reset
encrypt/decrypt
data input
data available
data read
IV input
IV available
IV read
n
Encryption/decryption unit
data output
n
write
full
round number
round key(s)
Key scheduling unit
key input
key available
key read
key size
k
s


clock
reset
encrypt/decrypt
data input
data available
data read
IV input
IV available
IV read
n
Encryption/decryption unit
data output
n
write
full
round number
round key(s)
read bank
write bank
b
Key memory
cycle number
round key(s)
key input
key available
key read
key size
k
Key scheduling unit
s