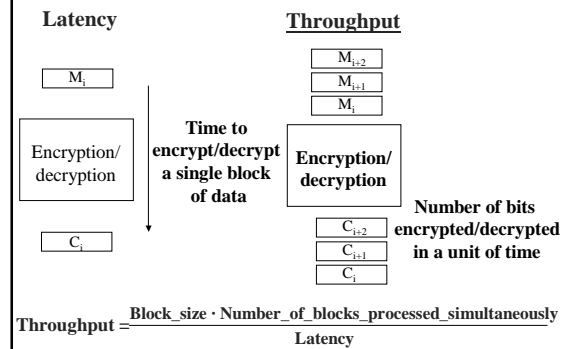


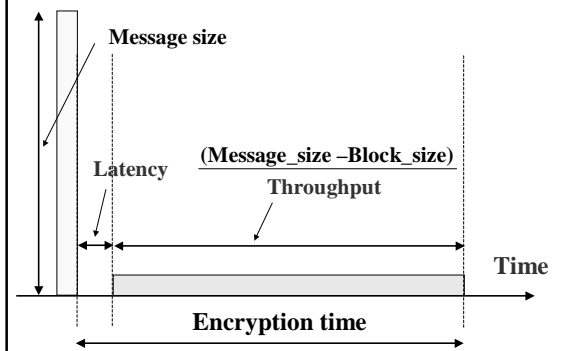
ECE 297:11 Lecture 8

Architectures of secret-key ciphers

Primary parameters of hardware implementations for secret-key block ciphers



Dependence of the encryption time on latency and throughput

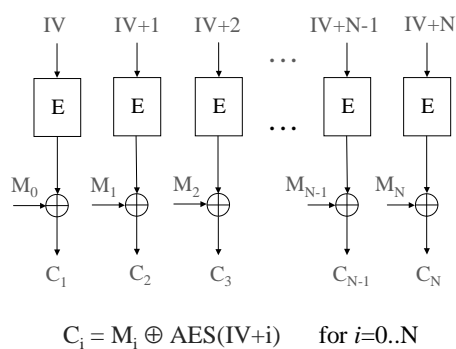


Primary factor in choosing the encryption/decryption unit architecture

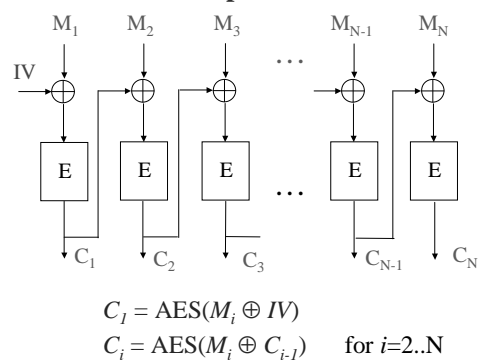
Symmetric-key cipher mode of operation:

1. Non-feedback cipher modes
ECB, counter mode
2. Feedback cipher modes
CBC, CFB, OFB

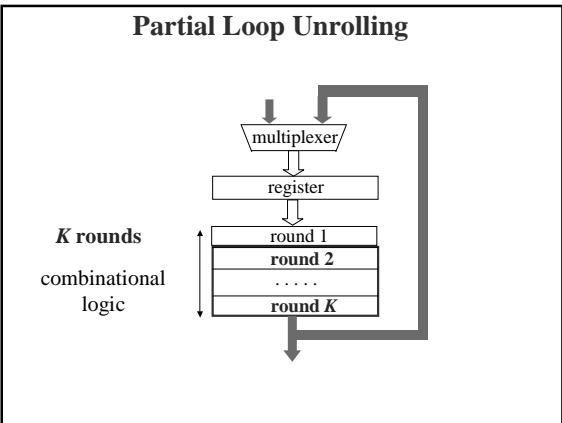
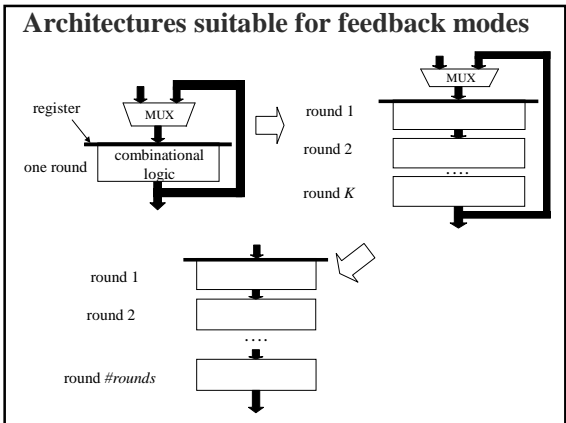
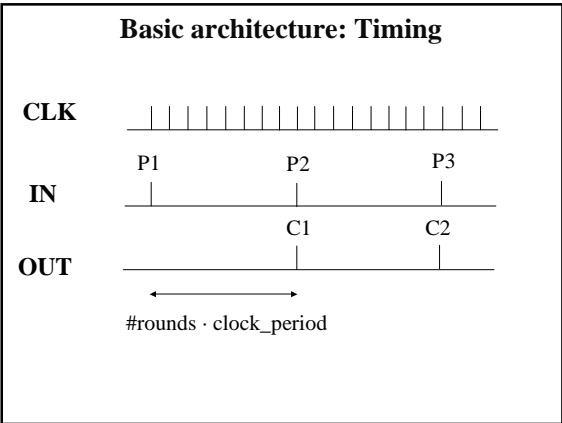
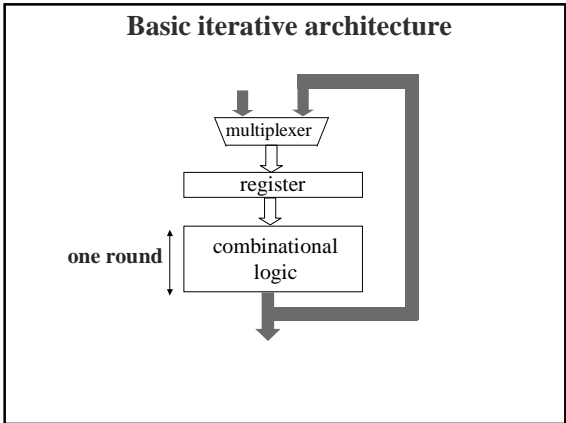
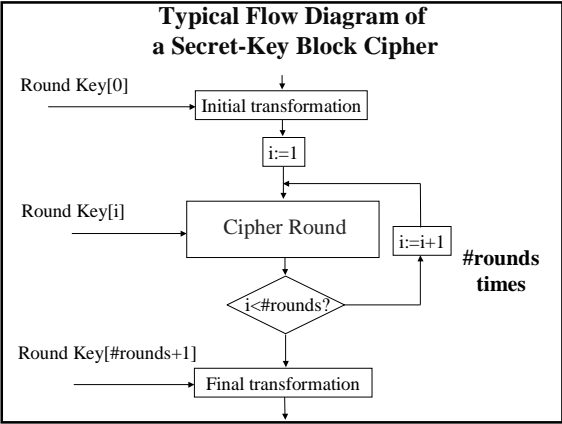
Non-feedback Counter Mode - CTR

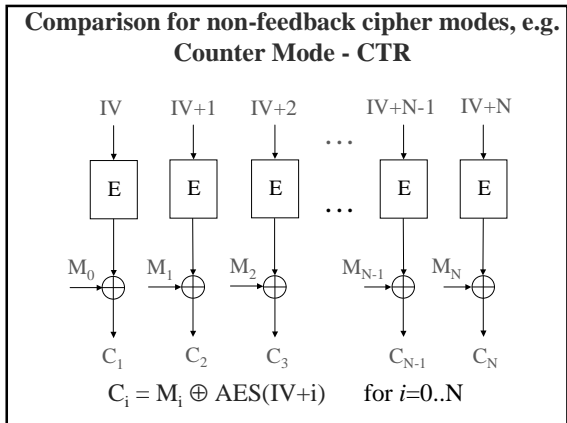
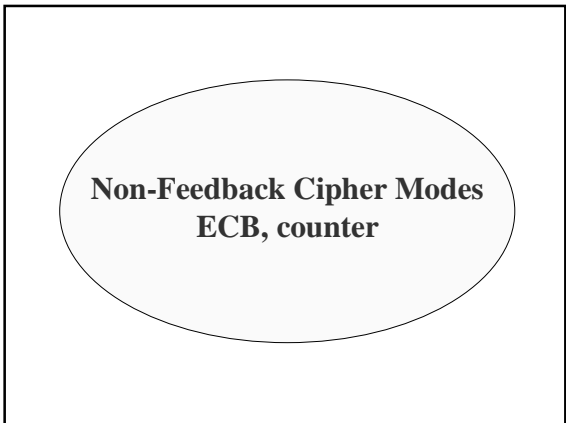
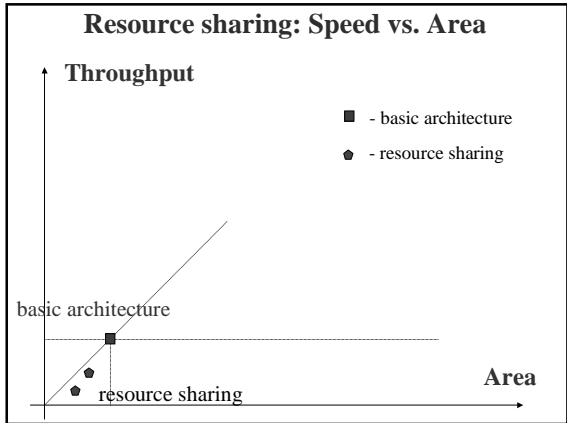
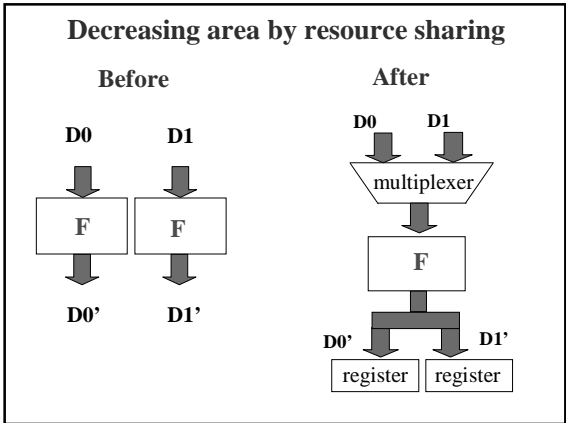
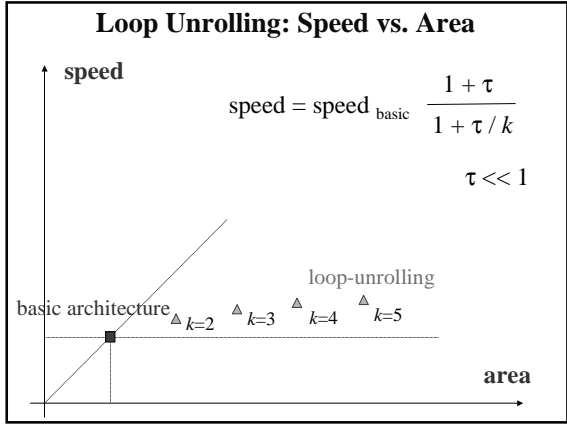
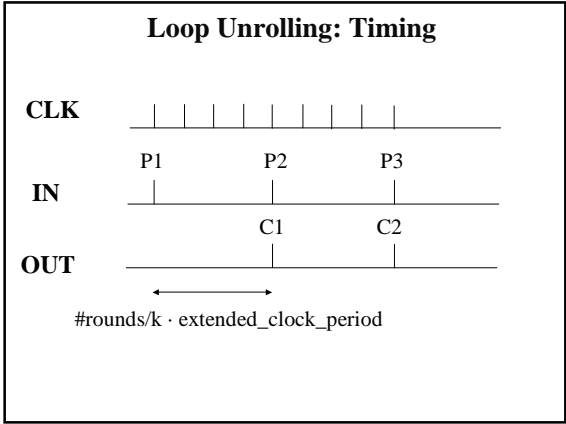


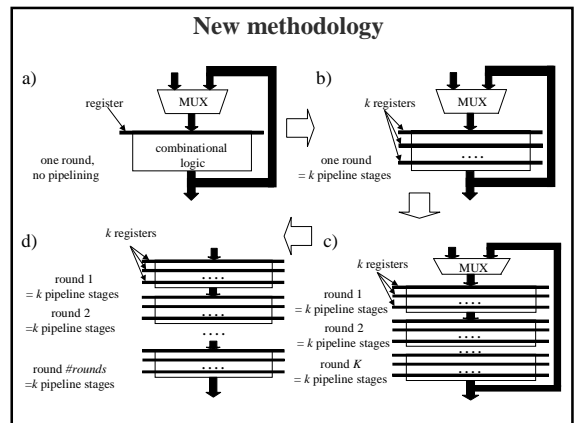
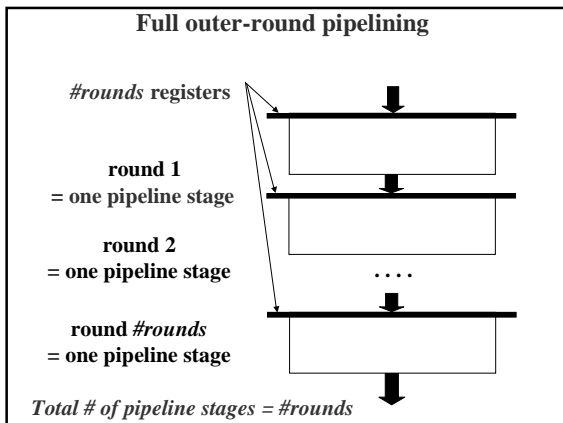
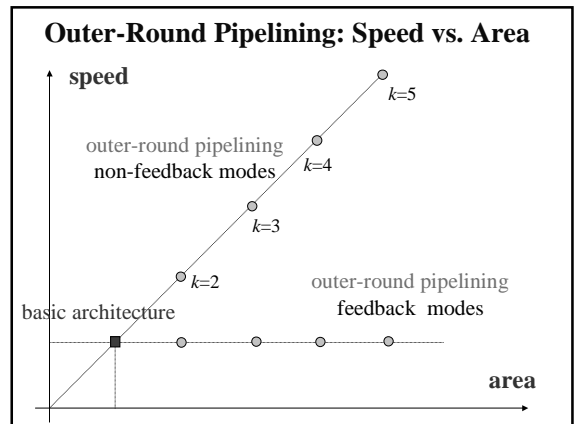
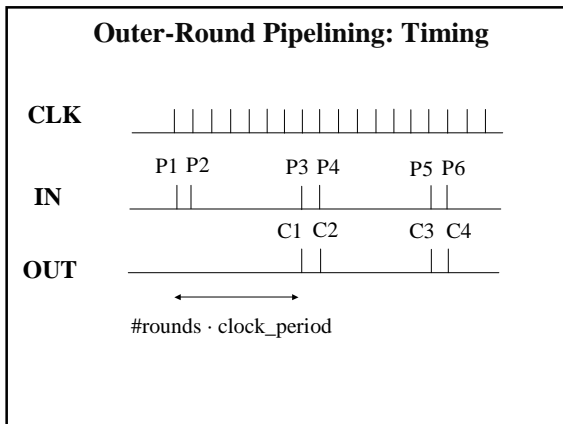
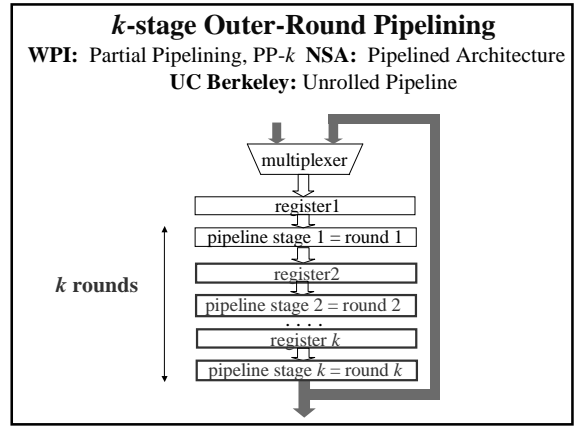
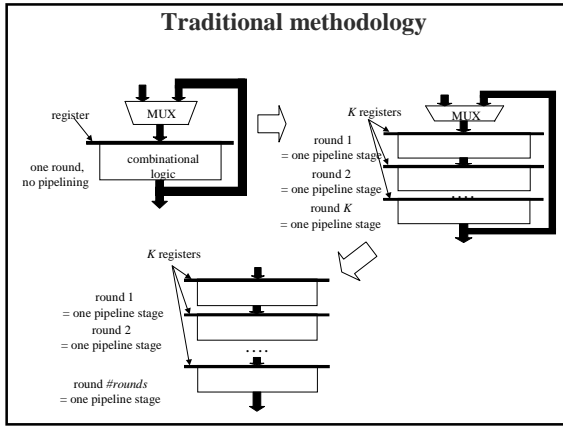
Feedback cipher modes - CBC

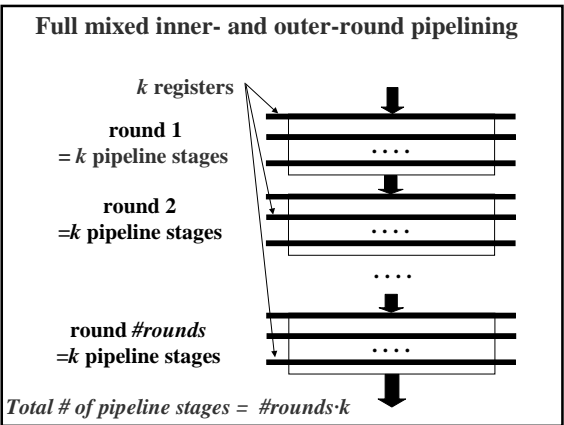
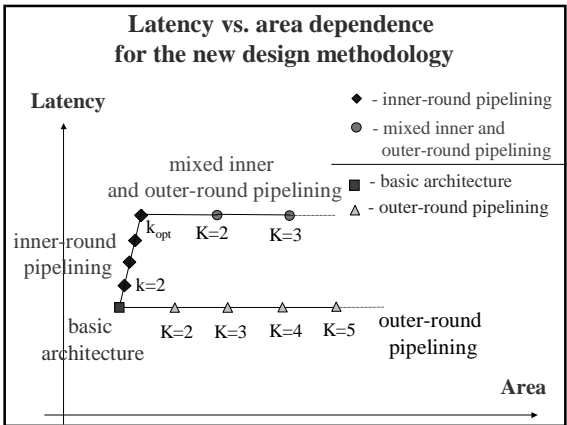
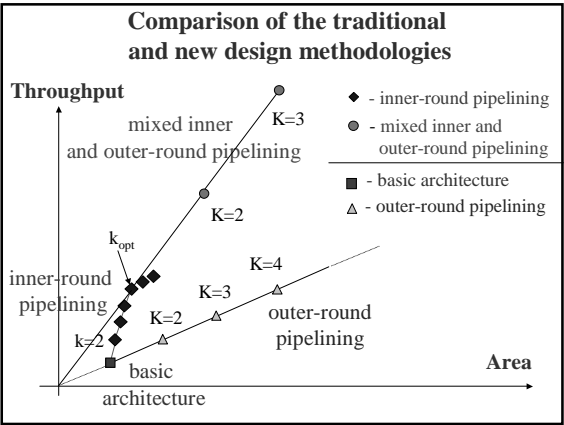
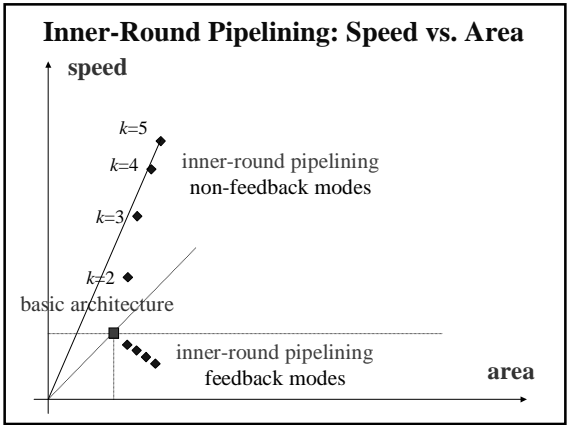
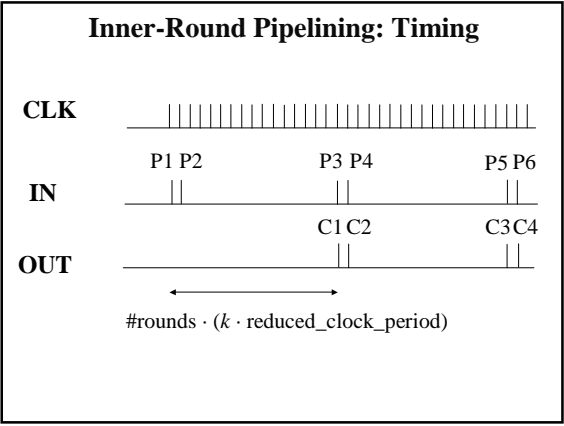
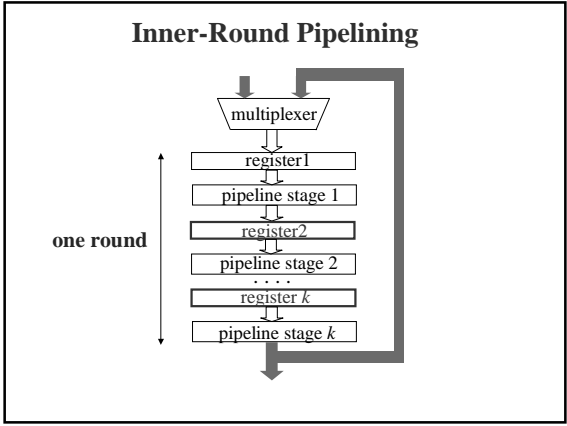


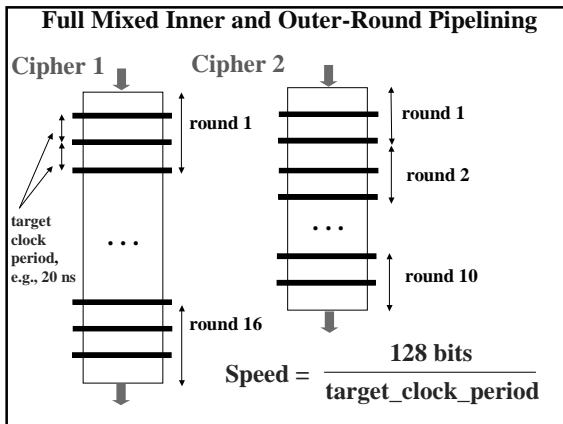
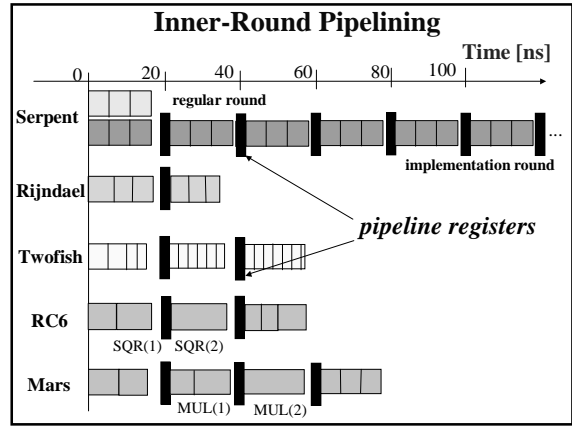
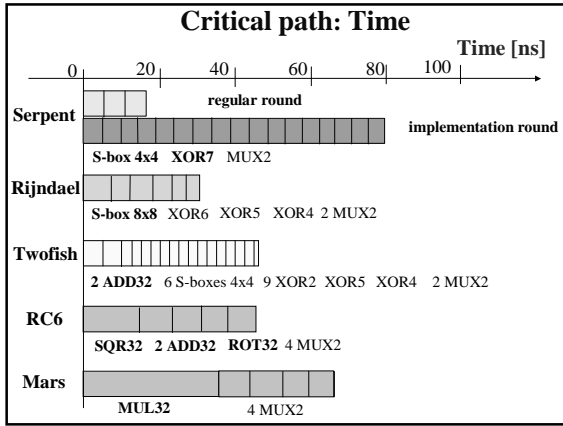
**Feedback cipher modes
CBC, CFB, OFB**





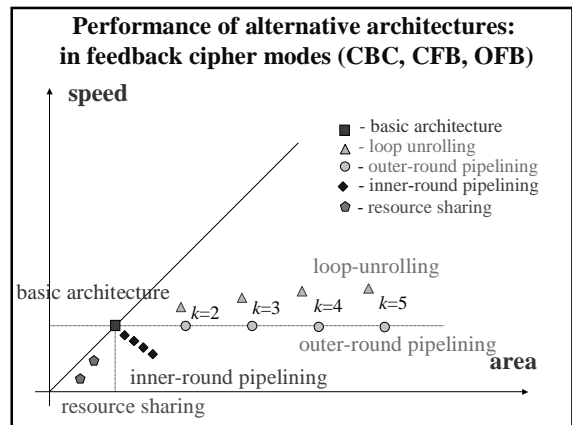
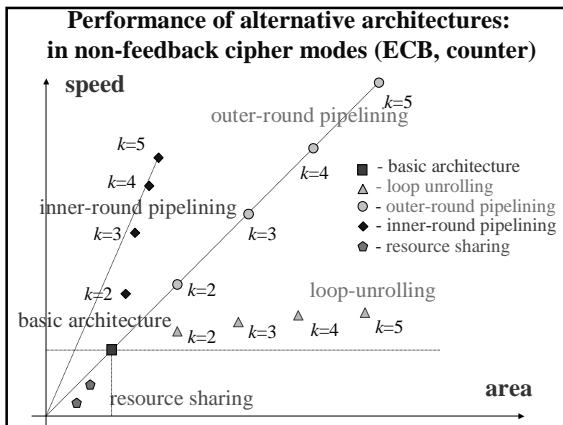




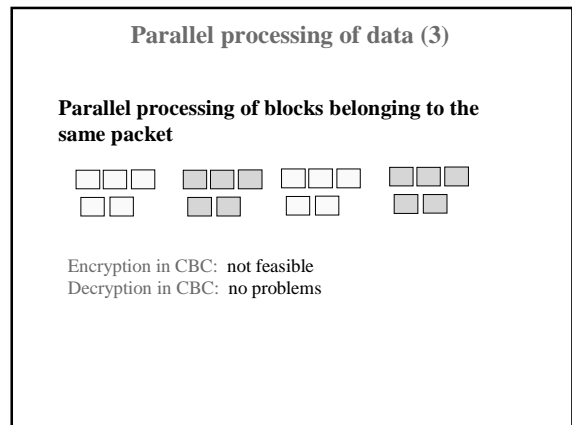
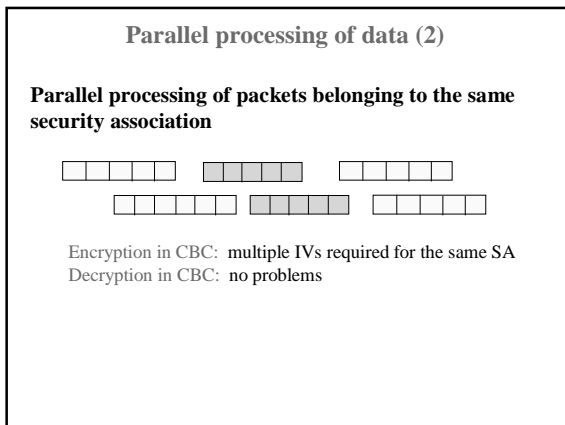
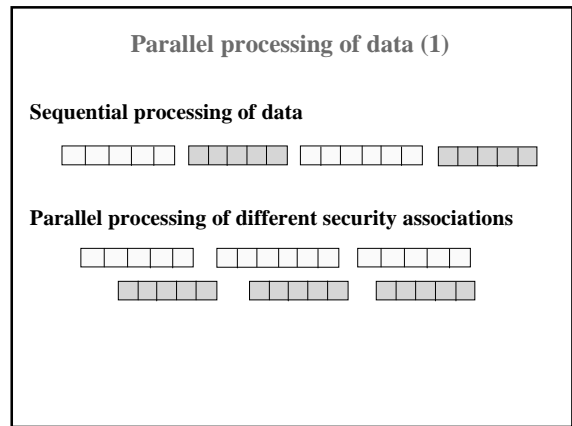
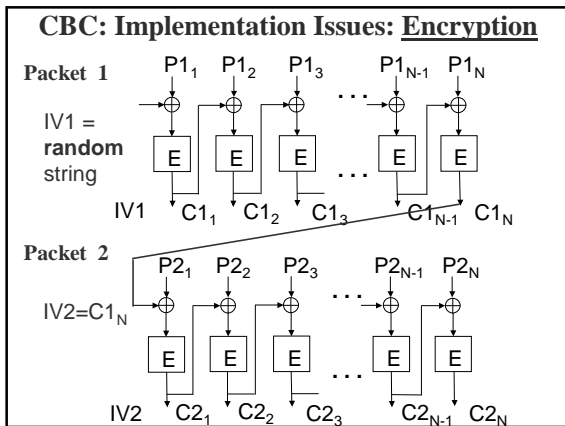
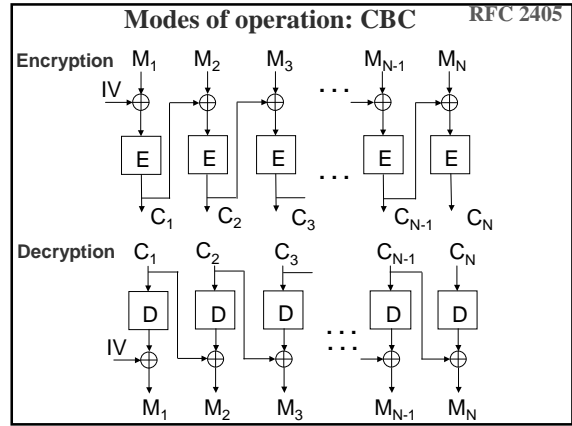


Conclusions for non-feedback cipher modes ECB, counter

- 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



Encryption in Communication Protocols



Secret-key ciphers Interface

