Cryptography Assignment

Modes of Block Cipher operation

Problem Statement:

Compare ECB, CBC, PCBC, CFB, OFB and CTR modes using different important features selected by you.

Comparison Table:

1. Synchronization

ECB	self-synchronizing
CBC	self-synchronizing

PCBC	self-synchronizing
CFB	self-synchronizing
OFB	self-synchronizing
CTR	self-synchronizing

2. Key length

ECB	64 bits
CBC	64 bits
PCBC	64 bits
CFB	64 bits
OFB	64/128 bits
CTR	128/192/256 bits.

3. Mode of encryption

ECB	Block Cipher
CBC	Block Cipher
PCBC	Block Cipher
CFB	Stream Cipher
OFB	Stream Cipher
CTR	Stream Cipher

4. Security

ECB	Low
CBC	High
PCBC	High
CFB	High
OFB	High
CTR	Medium

5. Encryption parallelizable

ECB	Yes
CBC	No
PCBC	No
CFB	No
OFB	No
CTR	Yes

6. Decryption parallelizable

ECB	Yes
CBC	Yes

PCBC	No
CFB	Yes
OFB	No
CTR	Yes

7. Random Read Access

ECB	Yes
CBC	Yes
PCBC	No
CFB	Yes
OFB	No
CTR	Yes