CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Encryption & Decryption – 4

Sujeet Shenoi
Tandy School of Computer Science
University of Tulsa, Tulsa, OK 74104
sujeet@utulsa.edu

NSF

ADVANCED TECHNOLOGICAL EDUCATION

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Using Encryption Wisely

Encryption provides a "false sense of security"

- Must be used correctly
- Practices
- Protocols

NSF

ADVANCED TECHNOLOGICAL EDUCATION

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Performance

01001010100101010101010011001010101010000101010101010101010100010100100

Delay Time

- Stream ≤ Stream-Block ≤ Block
- DES: 64-bit blocks
- RSA: 100-200-bit blocks (short blocks: limited security)

Speed

- Symmetric algorithms are much (10,000+ times) faster
- Hardware solutions are much faster
- RSA: 220K Bits/s vs 0.5K Bits/s/MIPS
- DES: 1,200,000K Bits/s vs 400K Bits/s/MIPS

NSF

ADVANCED TECHNOLOGICAL EDUCATION

Block Replay

Transaction Format

- Depositor Name SrcAct DestAct Amount
  ← 24 bytes → ← 8 → ← 8 → ← 8 →
  3 DES blocks 1 DES 1 DES 1 DES

Original Transactions

- ← Intruder → ←xxx→ ← I# → ← zz$ →
- ← John Doe → ←yyy→ ←JD#→ ←8K$→

Fabricated Transaction

- ← Intruder → ←yyy→ ← I# → ←8K$→

Block Chaining

- Prevents "Block Replay"
  - $x \oplus x = 0$ $(1011 \oplus 1011 = 0000)$
- Encryption
  - C_1: $\{P_1\}_K$
  - C_2: $\{P_2 \oplus C_1\}_K$
  - C_j: $\{P_j \oplus C_{j-1}\}_K$
- Decryption
  - P_1: $\{C_1\}_K$
  - P_2: $\{C_2\}_K \oplus C_1$
  - P_j: $\{C_j\}_K \oplus C_{j-1}$

Initial Chaining Value

- Block Chaining conceals identical blocks
- Only if each block is preceded by something unique
- Suppose messages always begin with: "US Army HQ"
- Encryption
  - C_1: $\{ IV \}_K$ (IV: Random Initial Vector)
  - C_2: $\{ P_1 \oplus C_1 \}_K$
  - C_j: $\{ P_{j-1} \oplus C_{j-1} \}_K$
- Decryption
  - P_0: $\{ C_1 \}_K$
  - P_j: $\{ C_{j+1} \}_K \oplus C_j$

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

One Way Encryption

Uses Special Functions

- $f(x) = x^3 \Rightarrow x = (f(x))^{1/3}$ (difficult to compute)
- $f(x) = x^2 \Rightarrow x = (f(x))^{1/2}$ (no unique inverse, e.g., for $f(x) = 4$)
- System stores f(*pwd*)
- User enters *string*
- System computes f(*string*) and compares with f(*pwd*)
- Internet Worm (Nov. 2, 1988)

NSF

ADVANCED TECHNOLOGICAL EDUCATION

Cryptographic Sealing

Integrity (as opposed to Secrecy)

- Store <file> and SHA(<file>)
- A cryptographic checksum could be the last block of a chained DES encryption

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Authentication and Time Stamps

Authentication

- Biometrics

Time Stamps

- Prevent replays
- Chronology
- Sender's and receiver's time stamps must match

NSF

ADVANCED TECHNOLOGICAL EDUCATION

Encryption Modes

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)

Electronic Code Book (ECB)

- Each block is encrypted individually
- Identical plaintext blocks produce identical ciphertext blocks

Electronic Code Book (ECB) (contd.)

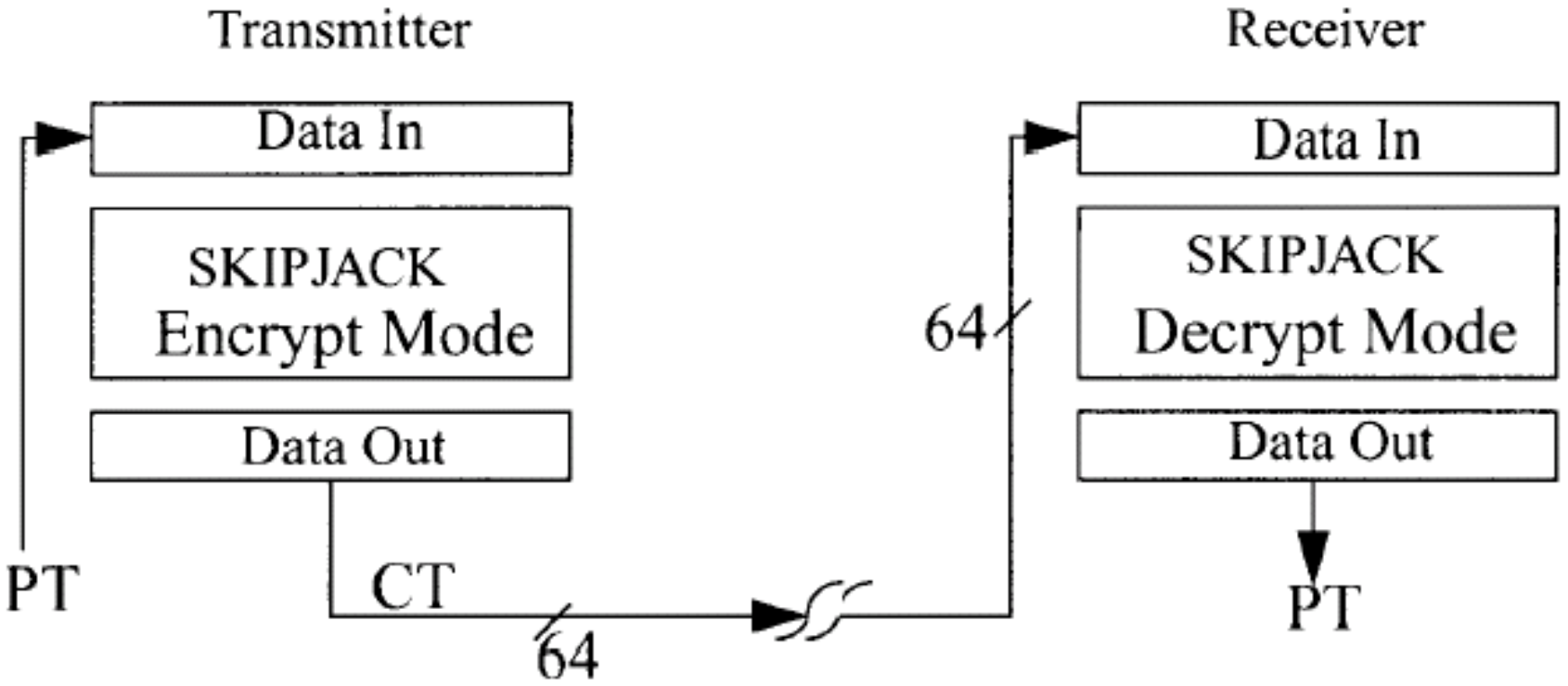
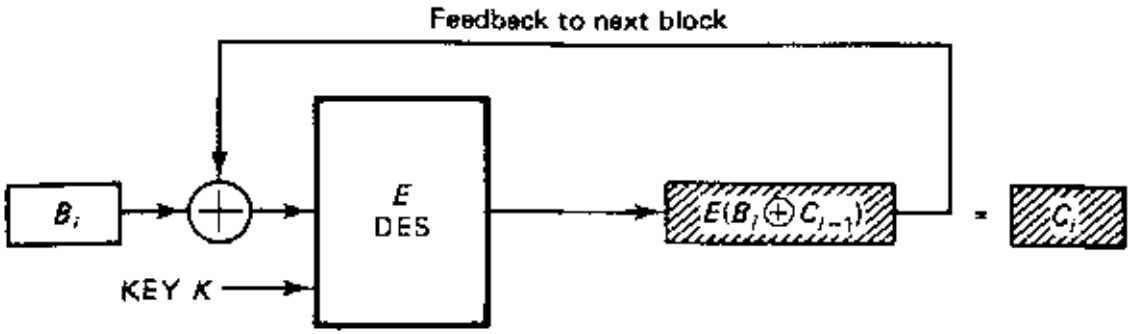


Figure 3. "Codebook Mode Diagram"

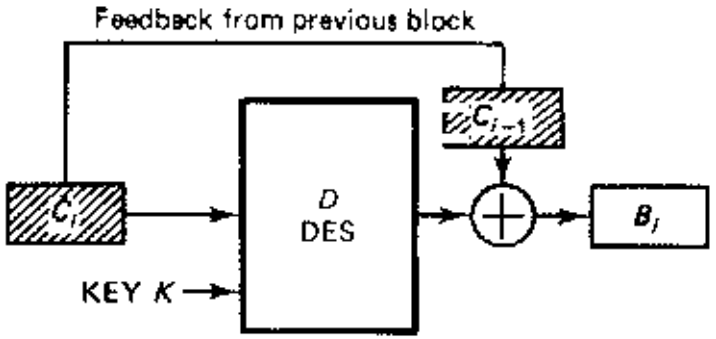
Cipher Block Chain (CBC)

- Prevents block replay
- Self-healing (Error in block C_j affects B_j and B_{j+1})
- Encryption
  - C_1: $\{ B_1 \}_K$ (Usually B_1 = Initial Vector)
  - C_2: $\{ B_2 \oplus C_1 \}_K$
  - C_j: $\{ B_j \oplus C_{j-1} \}_K$
- Decryption
  - B_j: $\{ C_j \}_K \oplus C_{j-1}$

Cipher Block Chain (CBC) (contd.)



(a) Encryption



(b) Decryption

Figure 4-24 Cipher Block Chaining

Cipher Block Chain (CBC) (contd.)

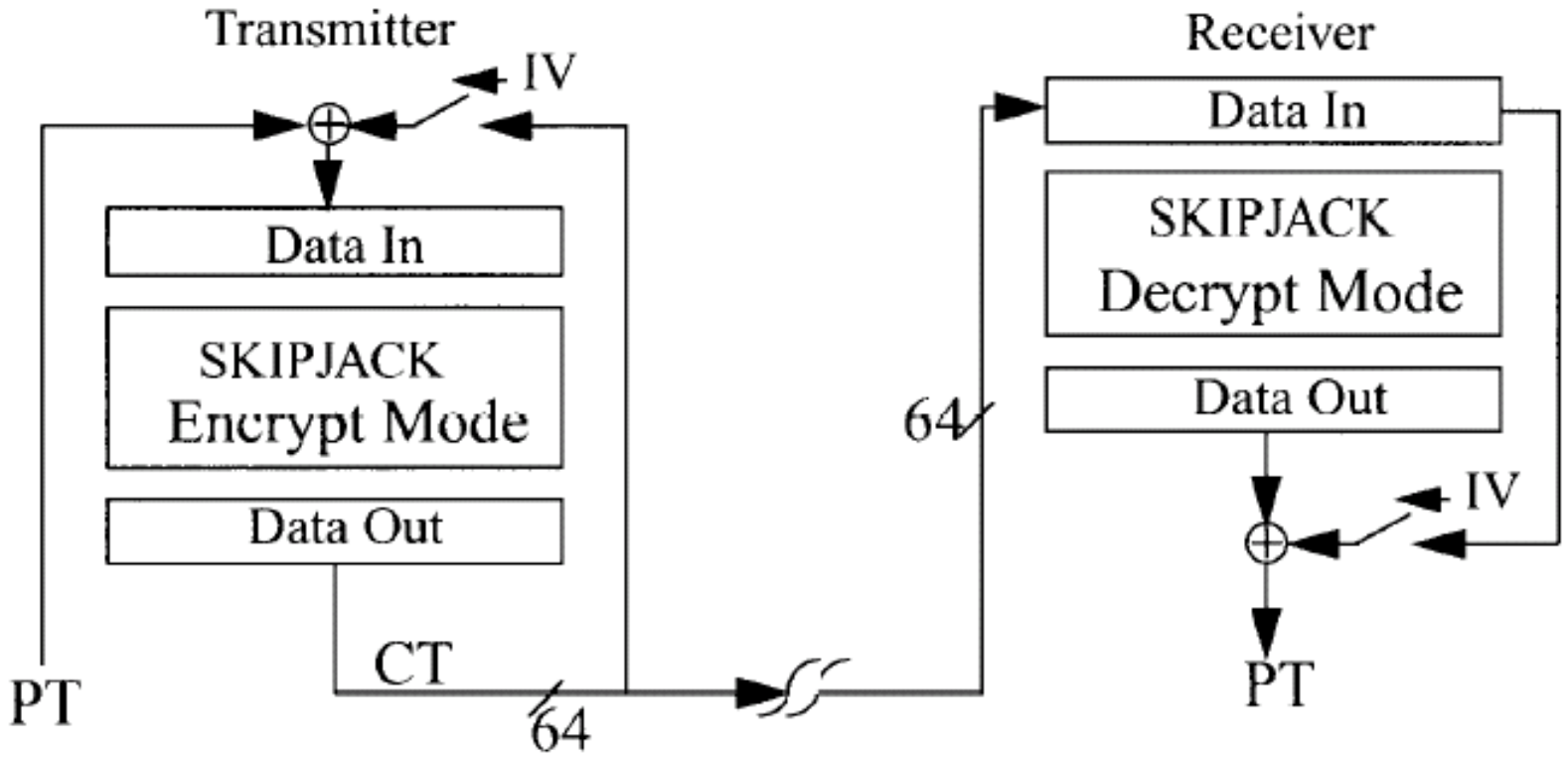


Figure 4. "Cipher-Block Chaining Mode Diagram"

Cipher Feedback (CFB)

- Block nature of DES is inconvenient
  - Partial final block must be padded (size of ciphertext > size of plaintext)
  - Encryption cannot begin until entire 64-bit block is input (secure networks: every character must be encrypted)
- CFB: Block → Stream
  - Encryption error only affects the next 8 characters

Cipher Feedback (CFB) (contd.)

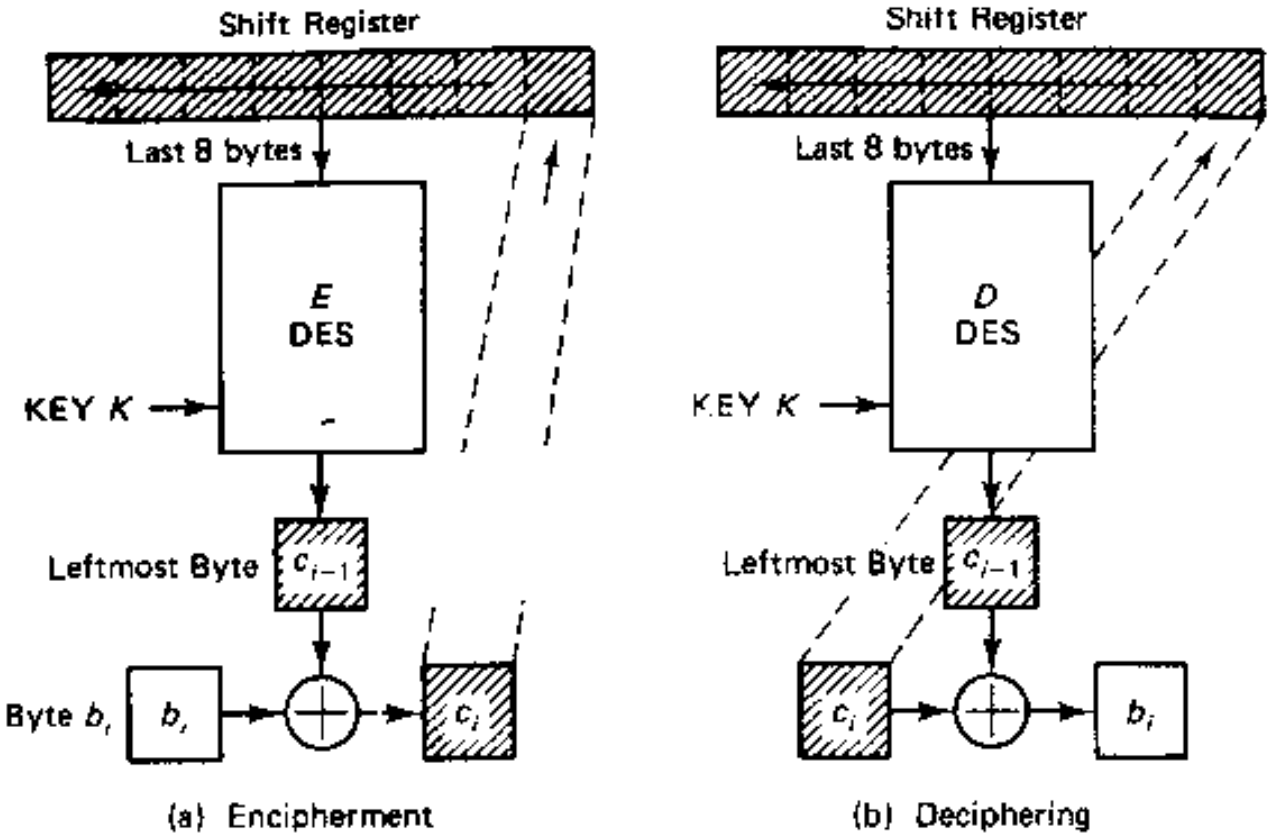


Figure 4-25 Cipher Feedback

Cipher Feedback (CFB) (contd.)

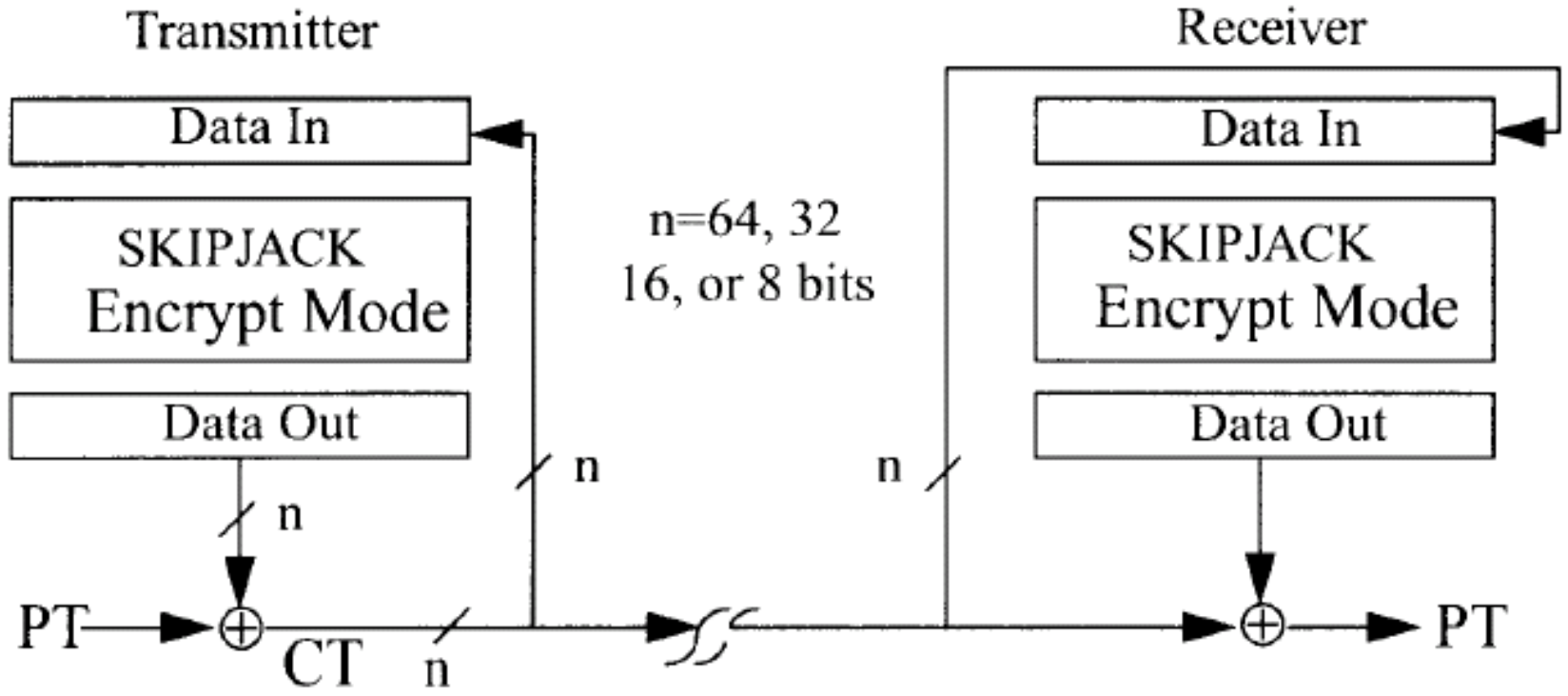


Figure 2. "Cipher Feed-Back Mode Diagram"

Output Feedback (OFB)

- Similar to CFB
- Main Difference
  - The term XOR'ed with plaintext (called "data block") is generated independently of plaintext and ciphertext
  - Initialization vector is used as a "seed" for data blocks
  - Bit errors in ciphertext are not propagated to affect the decryption of subsequent blocks

Output Feedback (OFB) (contd.)

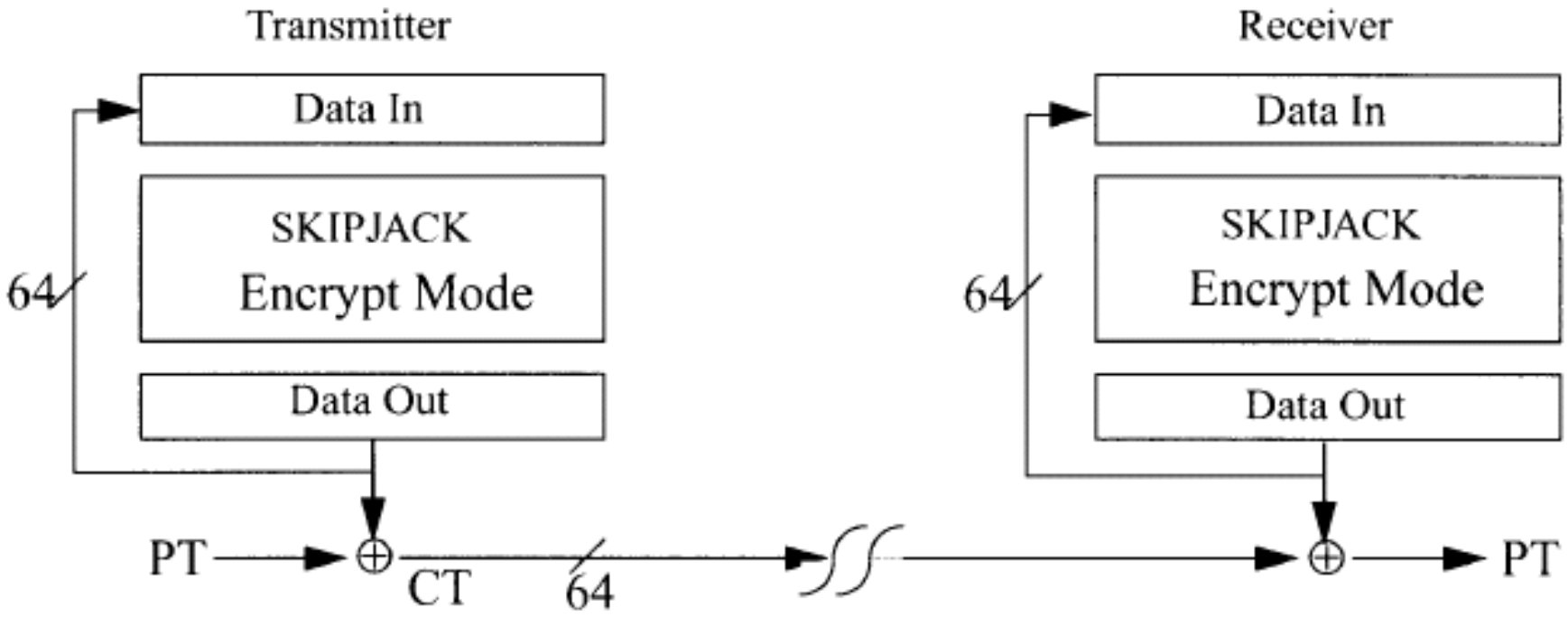


Figure 1. "Output Feed-Back Modes Diagram"