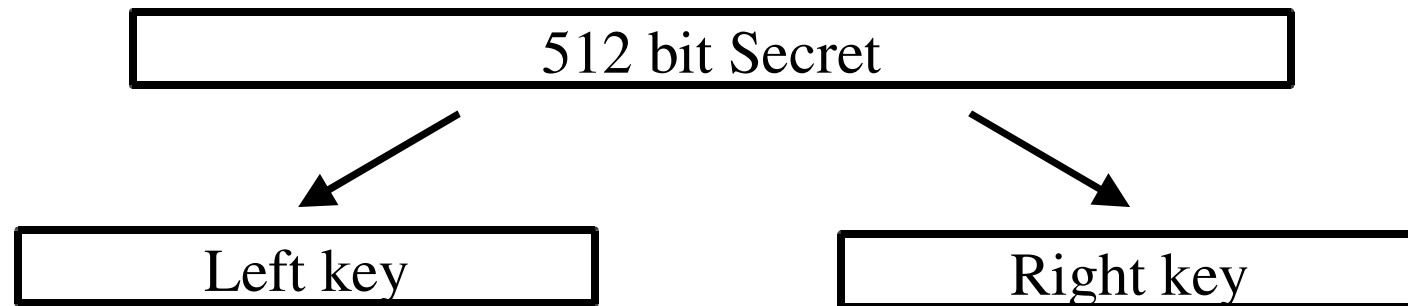


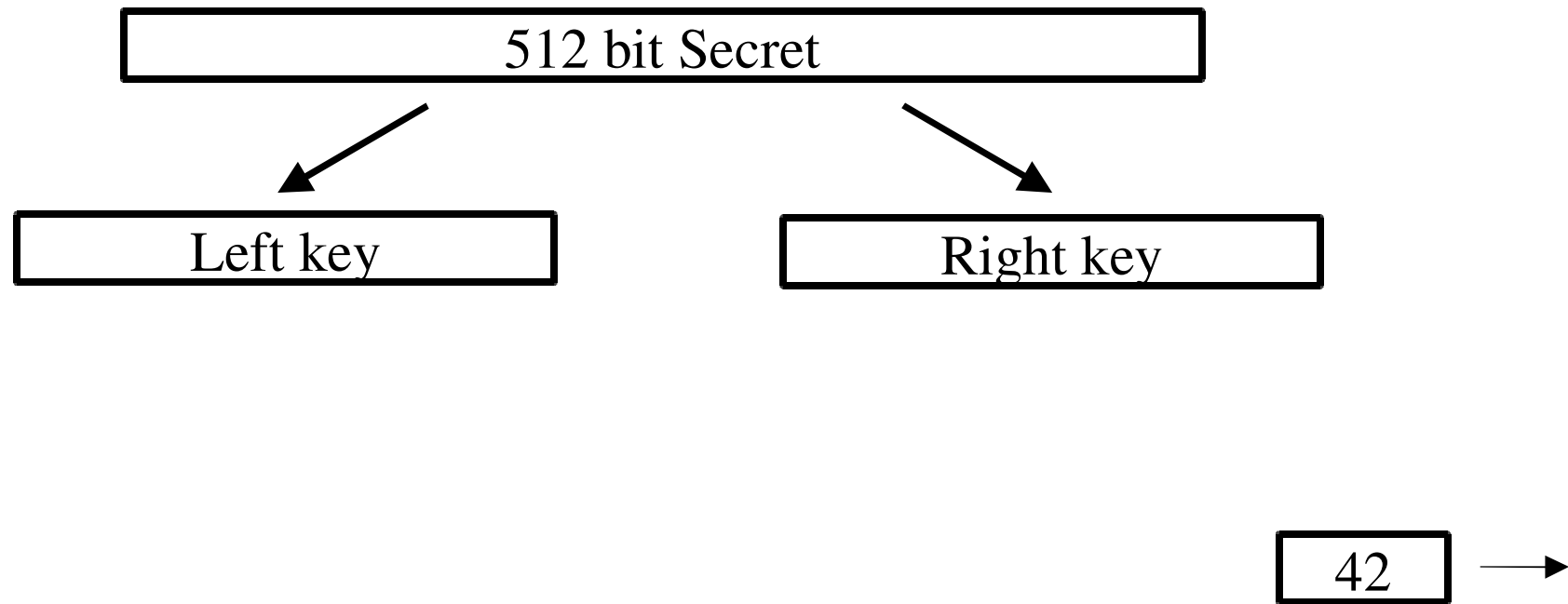
# Monitor's Secret Key Crypto - KARN, encrypt

512 bit Secret

# Monitor's Secret Key Crypto - KARN, encrypt

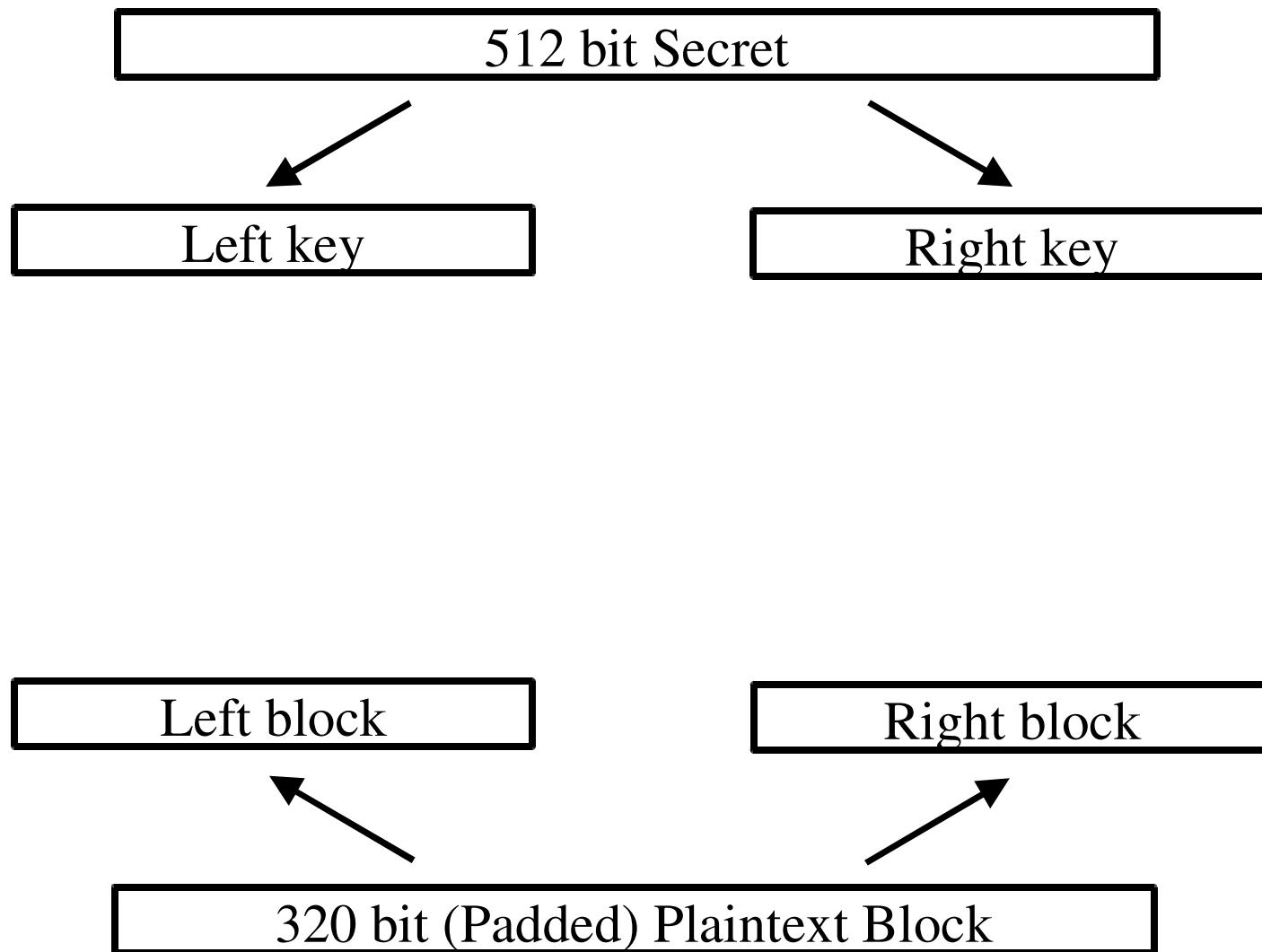


# Monitor's Secret Key Crypto - KARN, encrypt



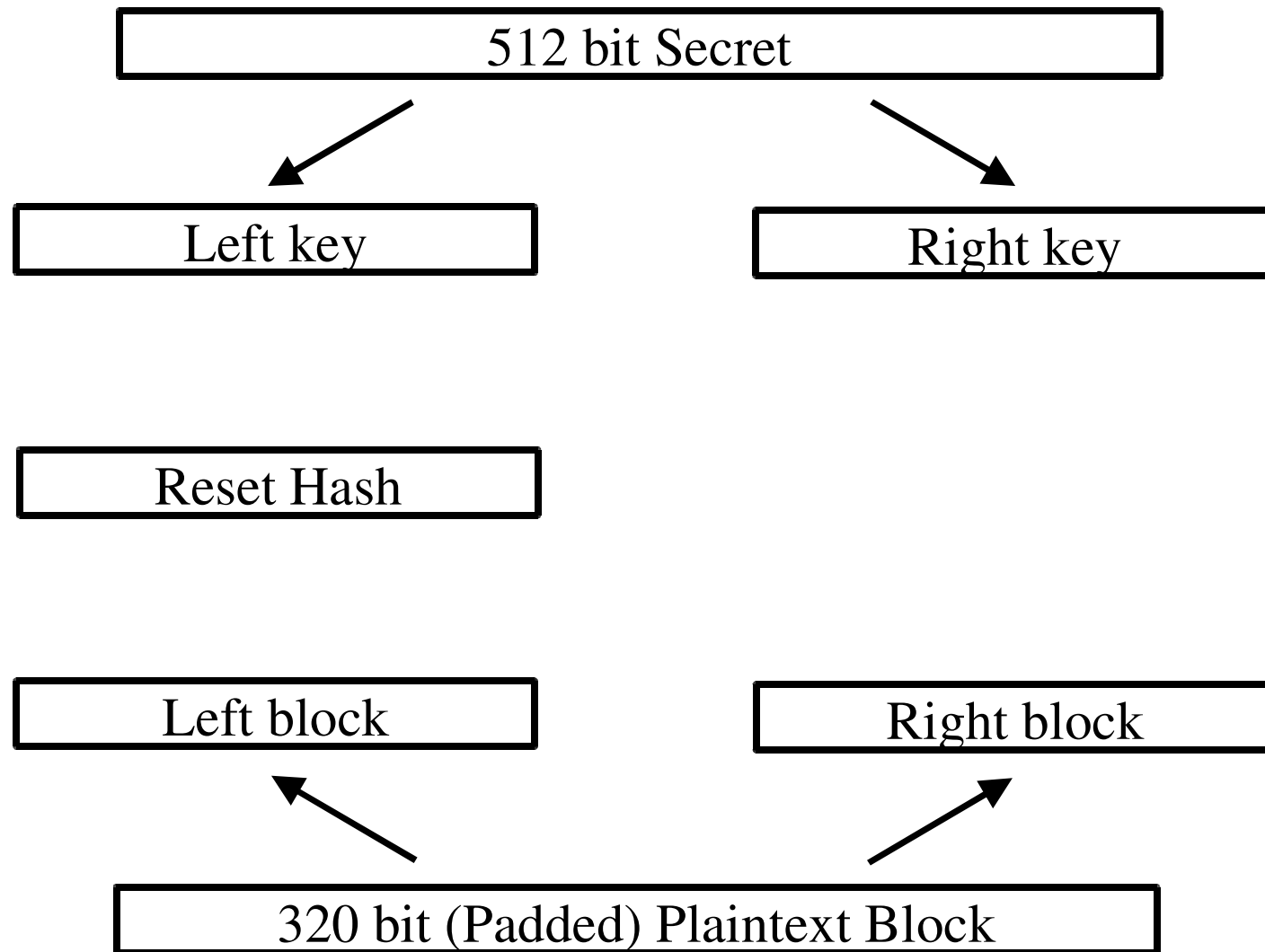
First: send out "guard byte" - the number 42 (00101010)

# Monitor's Secret Key Crypto - KARN, encrypt



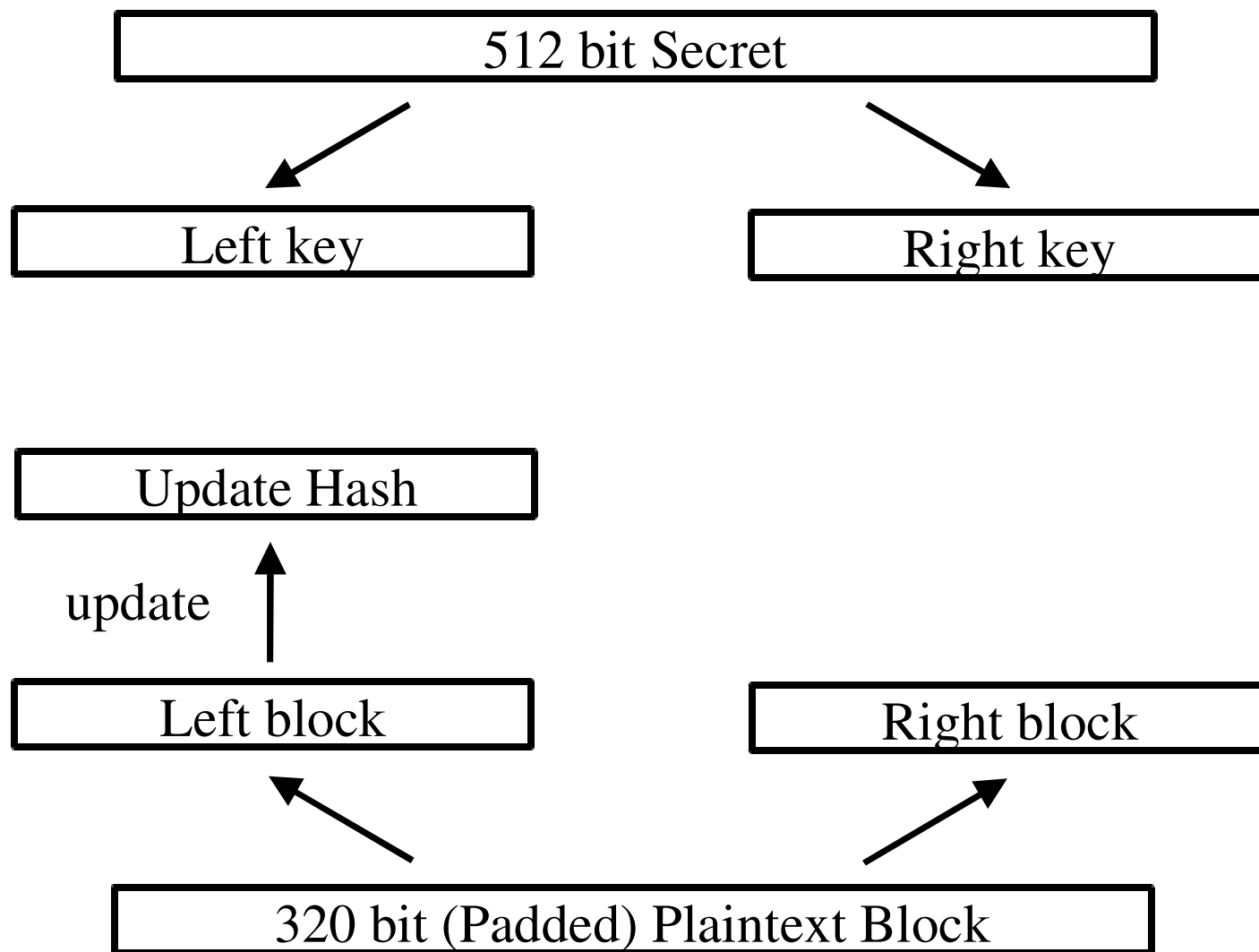
Split plaintext block into two halves

# Monitor's Secret Key Crypto - KARN, encrypt



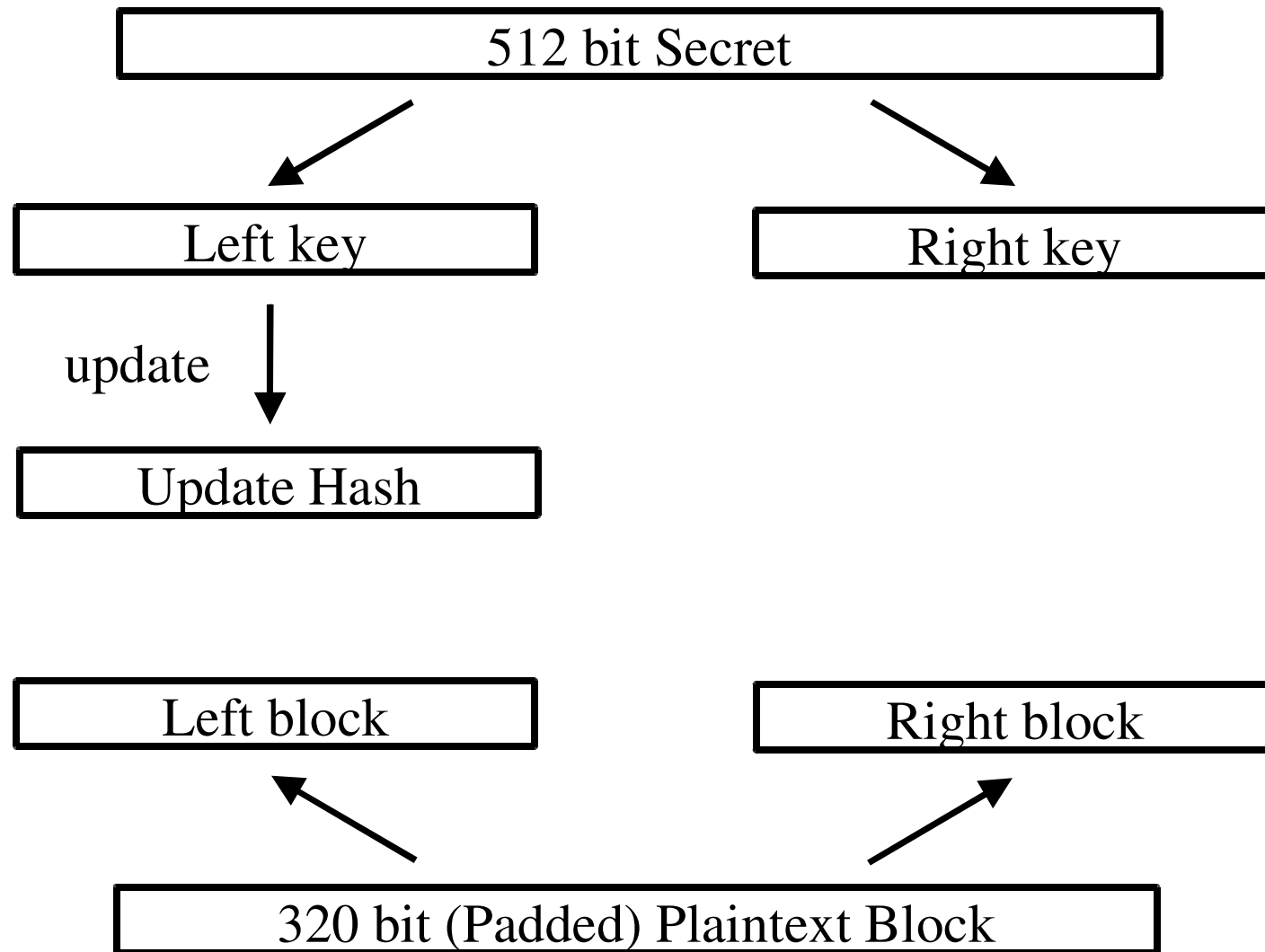
Reset a SHA message digest

# Monitor's Secret Key Crypto - KARN, encrypt



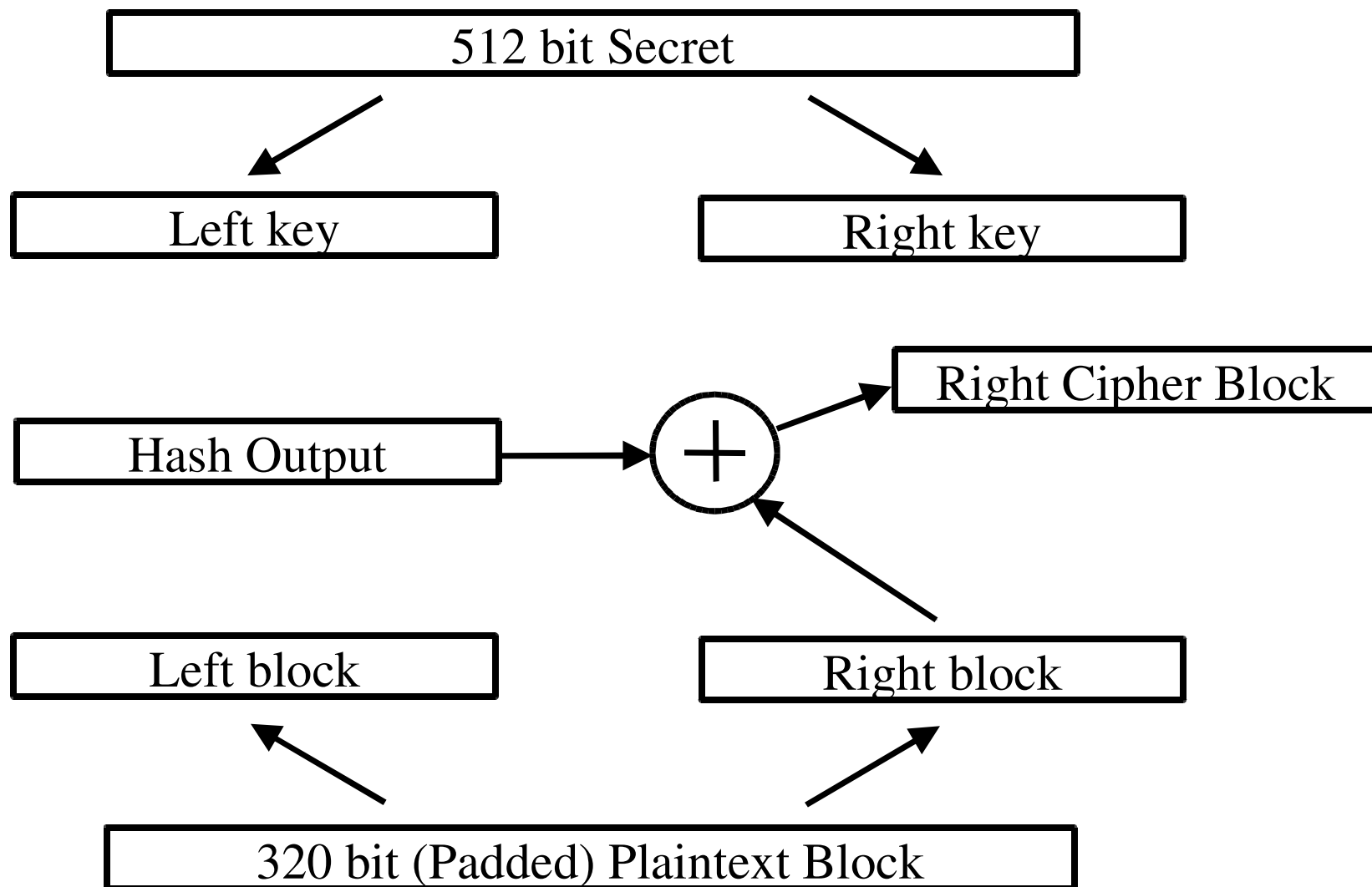
Update hash with plaintext left block

# Monitor's Secret Key Crypto - KARN, encrypt



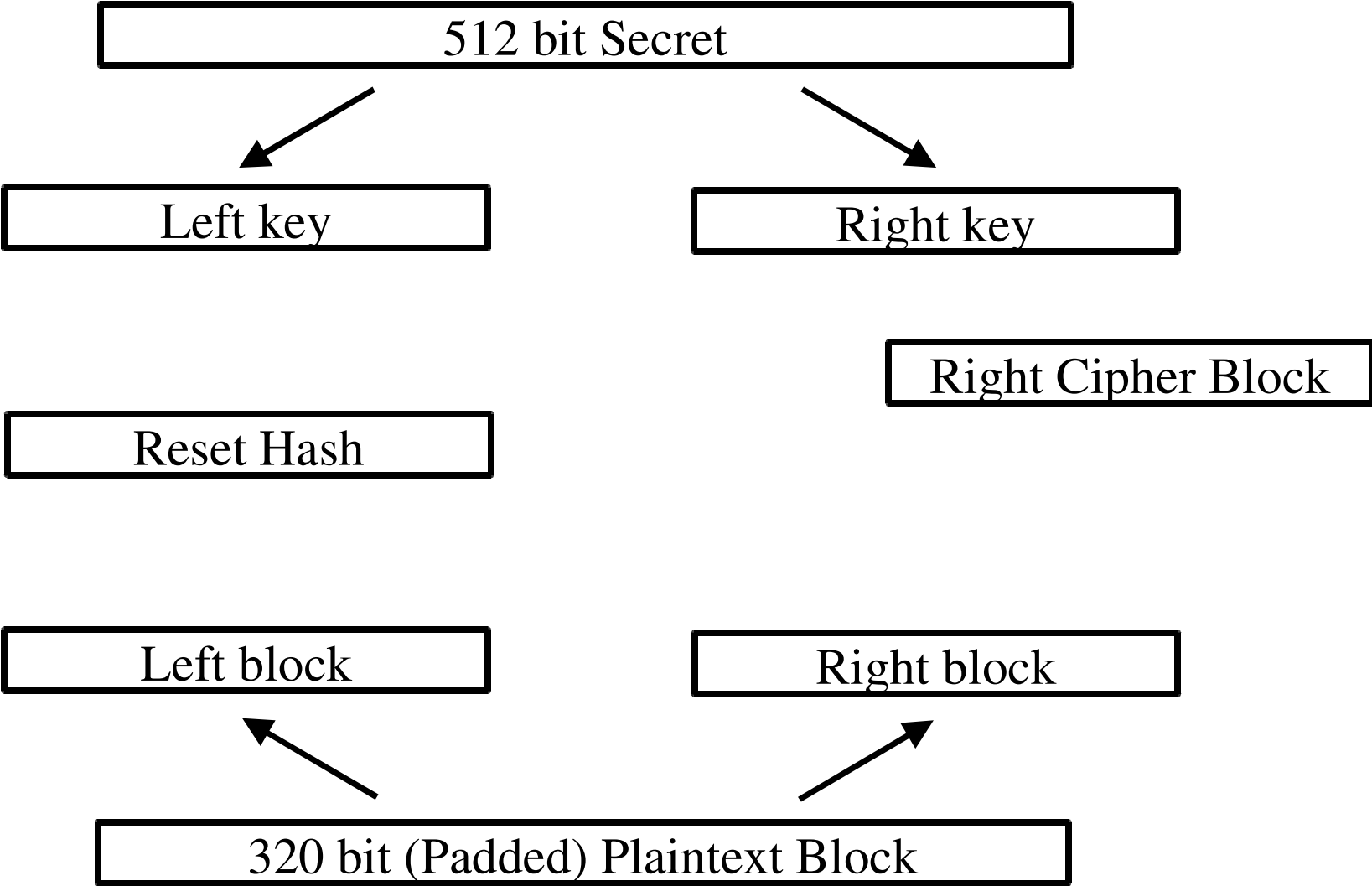
Update hash with left key

# Monitor's Secret Key Crypto - KARN, encrypt



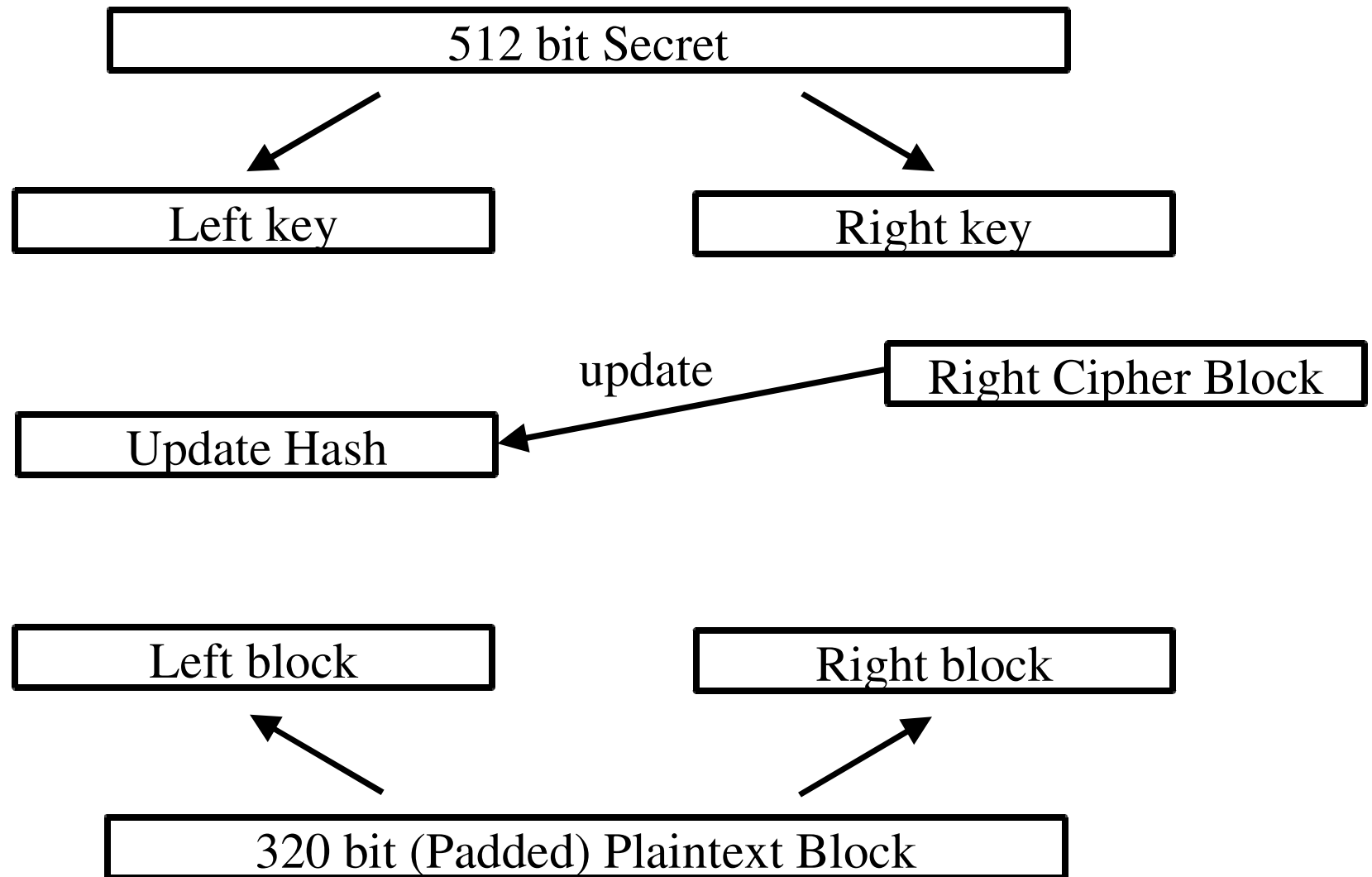
Create right cipher block

# Monitor's Secret Key Crypto - KARN, encrypt



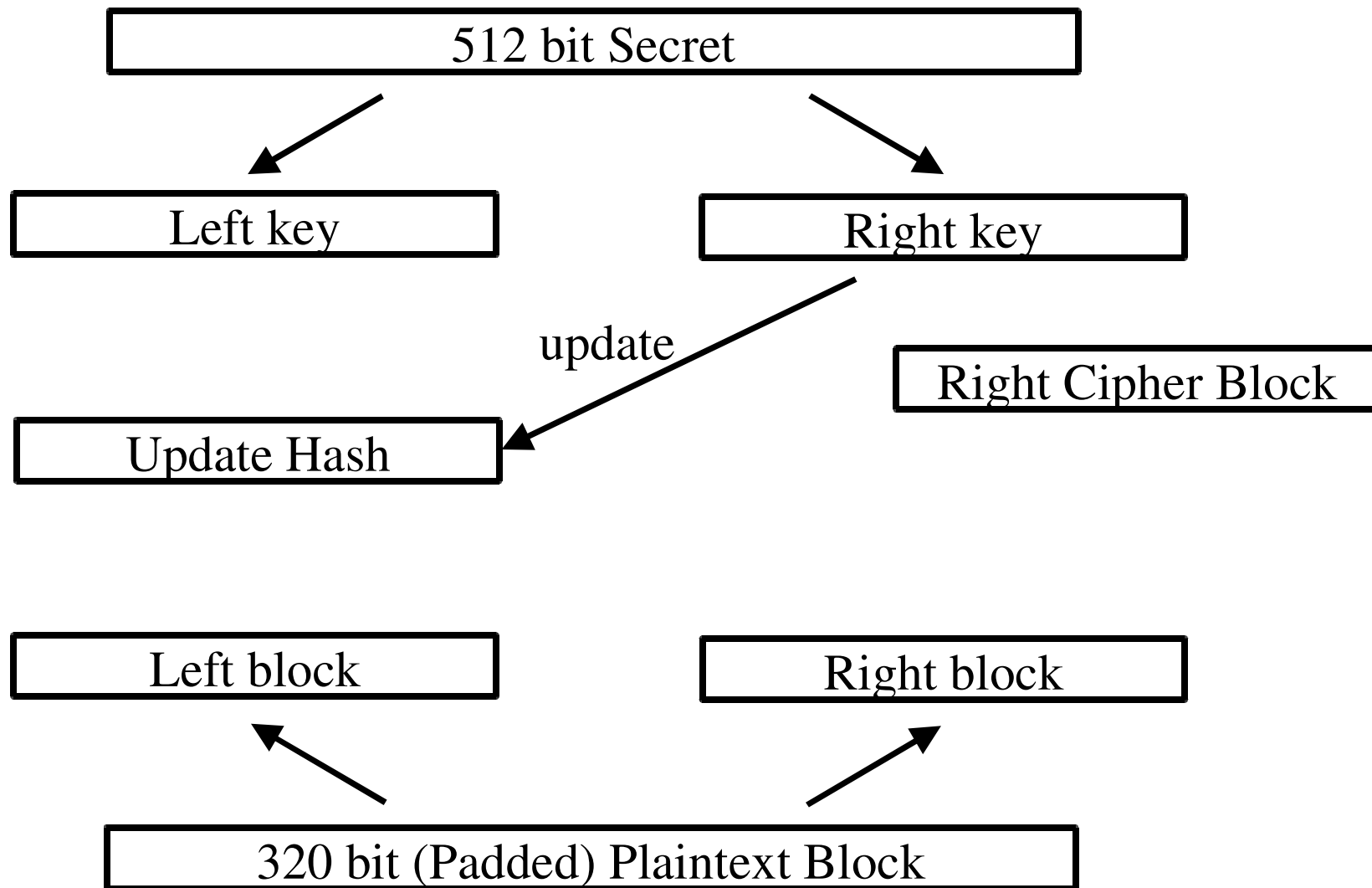
Reset Hash

# Monitor's Secret Key Crypto - KARN, encrypt



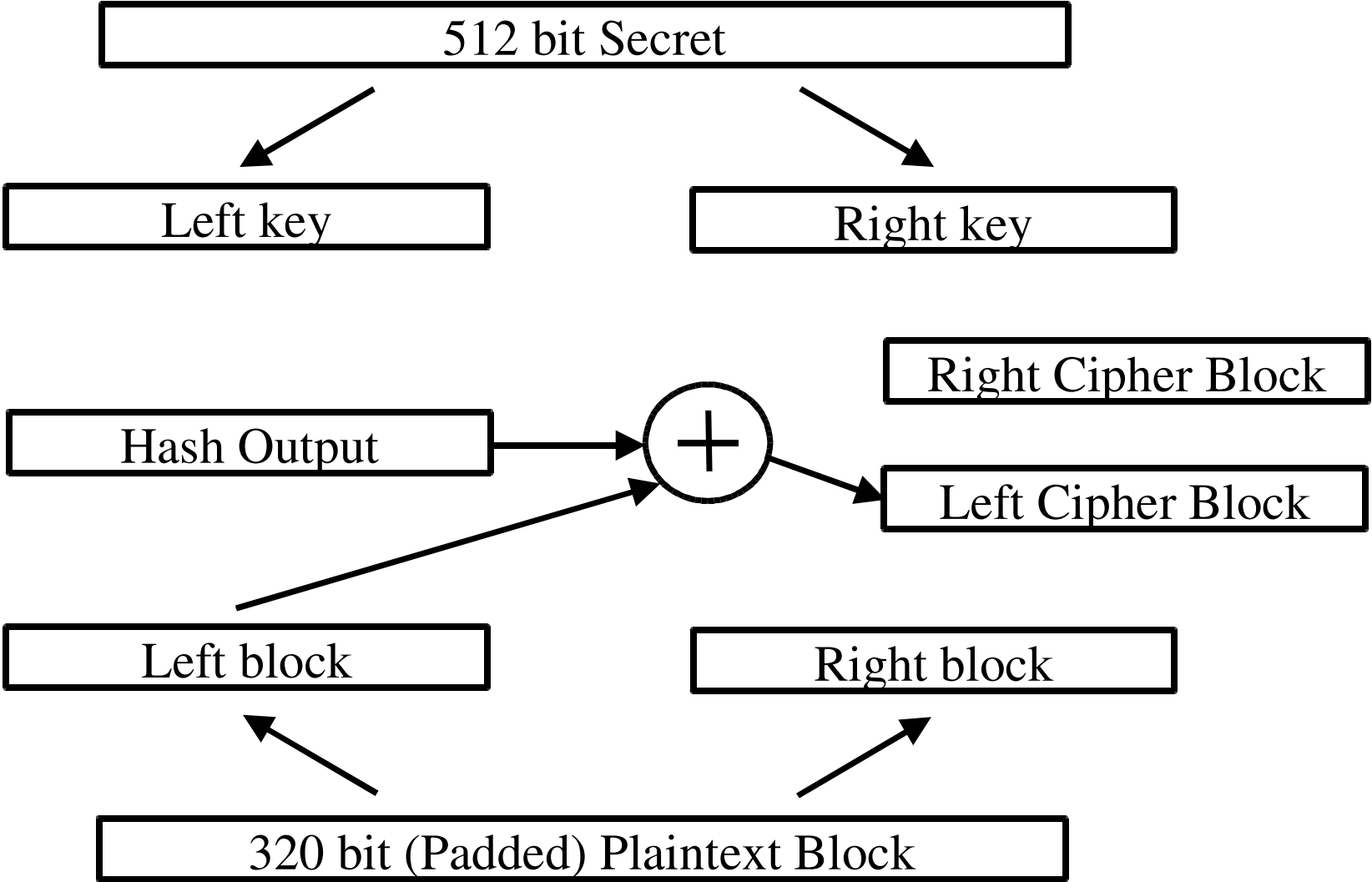
Update Hash with right cipher block

# Monitor's Secret Key Crypto - KARN, encrypt



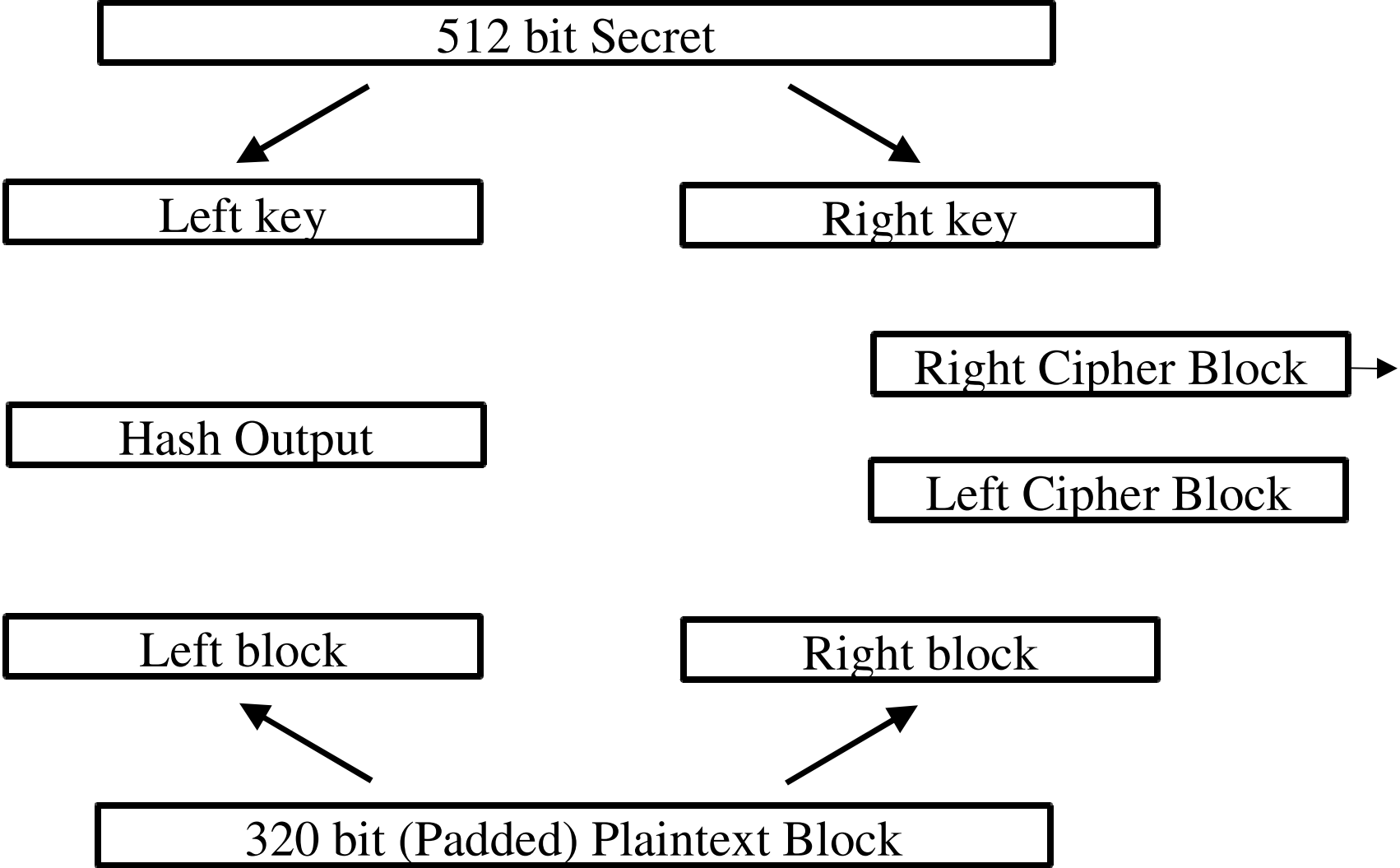
Update Hash with right key

# Monitor's Secret Key Crypto - KARN, encrypt



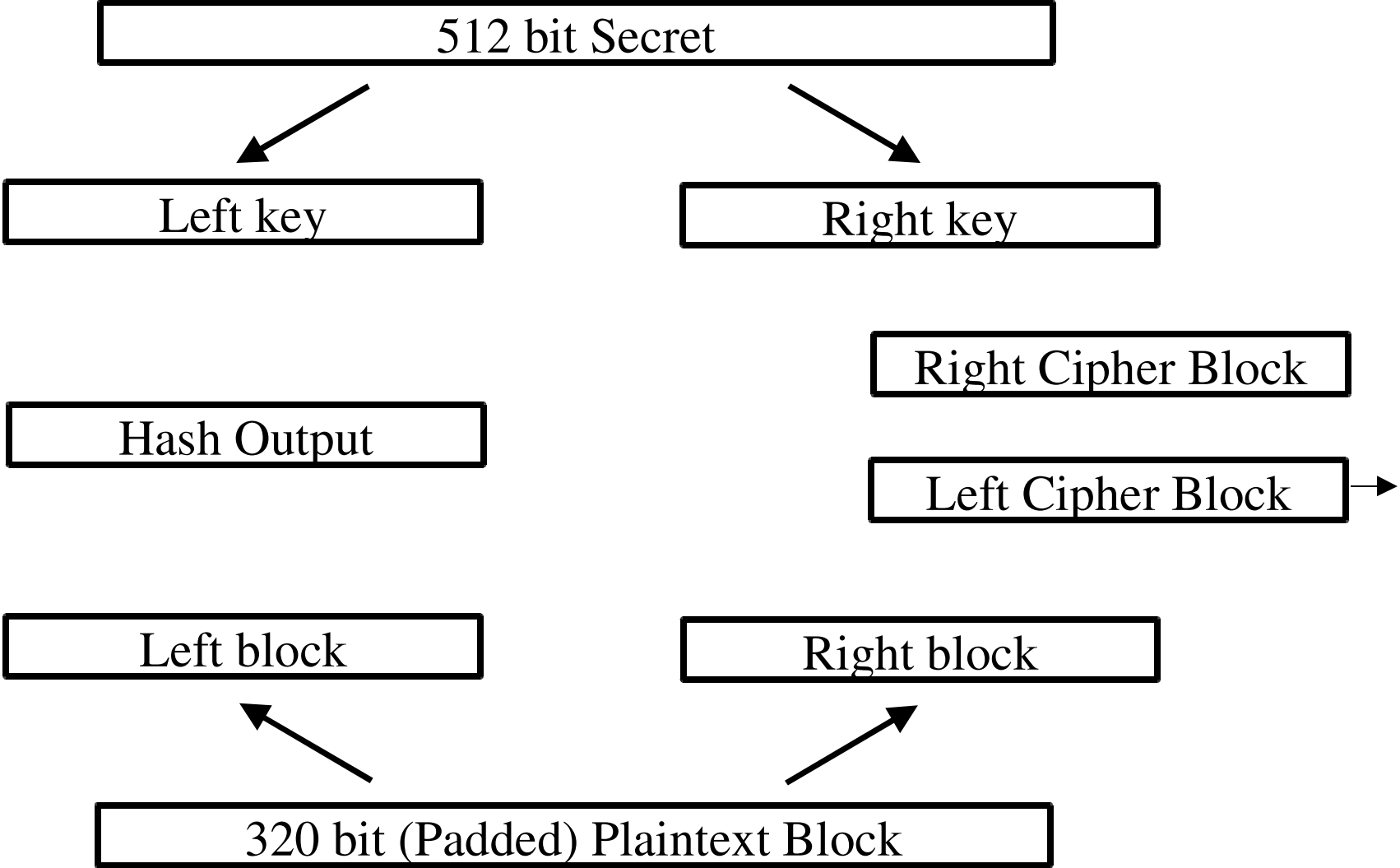
Create left cipher block - XOR digest with left plaintext block

# Monitor's Secret Key Crypto - KARN, encrypt



Output left cipher block

# Monitor's Secret Key Crypto - KARN, encrypt



Output right cipher block

# Monitor's Secret Key Crypto - KARN, padding

```
ByteArrayOutputStream buffer =  
    new ByteArrayOutputStream();  
  
String input = "The plaintext message to pad";  
byte scratch[] = input.getBytes();  
int len = input.length();  
buffer.write(scratch, 0, len);
```

< 320 bit Last Plaintext Block

Pad to last block, or pad a whole block

# Monitor's Secret Key Crypto - KARN, padding

```
buffer.write(0);
```



Stick a 0 byte on the end

# Monitor's Secret Key Crypto - KARN, padding

```
int padlen = PADSIZ - ((len + 1) % PADSIZ);  
scratch[] = new byte[padlen];  
SecureRandom sr = new SecureRandom();  
sr.nextBytes(scratch);  
buffer.write(scratch, 0, padlen);
```

< 320 bit Last Plaintext Block	0	Random #
--------------------------------	---	----------

< 320 bit Last Plaintext Block	0
--------------------------------	---

< 320 bit Last Plaintext Block
--------------------------------

Remaining bytes are derived from random #