Monitor's Secret Key Crypto - KARN, encrypt

512 bit Secret
Monitor's Secret Key Crypto - KARN, encrypt

512 bit Secret

Left key

Right key
Monitor's Secret Key Crypto - KARN, encrypt

First: send out "guard byte" - the number 42 (00101010)
Monitor's Secret Key Crypto - KARN, encrypt

512 bit Secret

Left key

Right key

Left block

Right block

320 bit (Padded) Plaintext Block

Split plaintext block into two halves
Monitor's Secret Key Crypto - KARN, encrypt

512 bit Secret

Left key

Right key

Reset Hash

Left block

Right block

320 bit (Padded) Plaintext Block

Reset a SHA message digest
Monitor's Secret Key Crypto - KARN, encrypt

512 bit Secret

Left key

Right key

Update Hash

update

Left block

Right block

320 bit (Padded) Plaintext Block

Hash sequence: left plaintext block then left key
Monitor's Secret Key Crypto - KARN, encrypt

512 bit Secret

Left key

Update Hash

Right key

Left block

Right block

320 bit (Padded) Plaintext Block

Hash sequence: left plaintext block then left key
Monitor's Secret Key Crypto - KARN, encrypt

512 bit Secret

Left key

Right key

Hash Output

Right Cipher Block

Left block

Right block

320 bit (Padded) Plaintext Block

Form right cipher block from right plaintext block and hash
Monitor's Secret Key Crypto - KARN, encrypt

- 512 bit Secret
  - Left key
  - Right key
  - Reset Hash
  - Left block
  - Right block
  - 320 bit (Padded) Plaintext Block
  - Reset Hash
Monitor's Secret Key Crypto - KARN, encrypt

- 512 bit Secret
  - Left key
  - Right key
  - Update Hash
  - Right Cipher Block
  - Left block
  - Right block
  - 320 bit (Padded) Plaintext Block

Hash sequence: right cipher block then right key
Monitor's Secret Key Crypto - KARN, encrypt

512 bit Secret

Left key

Right key

Update Hash

Right Cipher Block

Left block

Right block

320 bit (Padded) Plaintext Block

Hash sequence: right cipher block then right key
Monitor's Secret Key Crypto - KARN, encrypt

- 512 bit Secret
  - Left key
  - Right key
  - Hash Output

- 320 bit (Padded) Plaintext Block
  - Left block
  - Right block
  - Right Cipher Block
  - Left Cipher Block

Form left cipher block from left plaintext block and hash
Monitor's Secret Key Crypto - KARN, encrypt

- 512 bit Secret
  - Left key
  - Right key
    - Hash Output
      - Left block
        - Right Cipher Block
        - Left Cipher Block
      - Right block
        - 320 bit (Padded) Plaintext Block

Output right cipher block
Monitor's Secret Key Crypto - KARN, encrypt

- 512 bit Secret
  - Left key
  - Right key
  - Hash Output
    - Right Cipher Block
      - Left Cipher Block
    - Left block
      - Right block
      - 320 bit (Padded) Plaintext Block

Output left cipher block
Monitor's Secret Key Crypto - KARN, padding

```java
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);`

< 320 bit Last Plaintext Block | 0

< 320 bit Last Plaintext Block

Stick a 0 byte on the end
Monitor's Secret Key Crypto - KARN, padding

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

< 320 bit Last Plaintext Block

<table>
<thead>
<tr>
<th>0</th>
<th>Random #</th>
</tr>
</thead>
</table>

Remaining bytes are derived from random #
Monitor's Secret Key Crypto - KARN, decrypt

512 bit Secret

- Left key
- Right key

Right Cipher Block

Left Cipher Block

Input right cipher block
Monitor's Secret Key Crypto - KARN, decrypt

- 512 bit Secret
  - Left key
  - Right key
  - Reset Hash
  - Right Cipher Block
  - Left Cipher Block
Monitor's Secret Key Crypto - KARN, decrypt

512 bit Secret

Left key

Right key

Update Hash

Right Cipher Block

Left Cipher Block

Hash sequence: right cipher block then right key
Monitor's Secret Key Crypto - KARN, decrypt

512 bit Secret

Left key

Right key

Update Hash

Right Cipher Block

Left Cipher Block

Hash sequence: right cipher block then right key
Monitor's Secret Key Crypto - KARN, decrypt

512 bit Secret

Left key

Right key

Right Cipher Block

Left Cipher Block

Input left cipher block
Monitor's Secret Key Crypto - KARN, decrypt

512 bit Secret

Left key

Right key

Output Hash

Left Cipher Block

Right Cipher Block

Form left plaintext block from left cipher block and hash
Monitor's Secret Key Crypto - KARN, decrypt

512 bit Secret

- Left key
- Reset Hash
- Left block

- Right key
- Right Cipher Block
- Left Cipher Block
Monitor's Secret Key Crypto - KARN, decrypt

- 512 bit Secret
  - Left key
  - Right key
    - Update Hash
      - Left block
    - Right Cipher Block
    - Left Cipher Block

Hash sequence: left plaintext block then left key
Monitor's Secret Key Crypto - KARN, decrypt

512 bit Secret

Left key

Right key

Update Hash

Left block

Right Cipher Block

Left Cipher Block

Hash sequence: left plaintext block then left key
Monitor's Secret Key Crypto - KARN, decrypt

- 512 bit Secret
  - Left key
  - Right key

Output Hash

Left block

Right Cipher Block

Left Cipher Block

Right block

Form right plaintext block from right cipher block and hash
Monitor's Secret Key Crypto - KARN, decrypt

- 512 bit Secret
  - Left key
  - Right key
  - Output Hash
    - Left block
    - Right block
  - Right Cipher Block
  - Left Cipher Block
- 320 bit (Padded) Plaintext Block

Output Plaintext block