

```

import java.util.Scanner;

public class IS_L6 {

    private static final int INIT_A = 0x67452301;
    private static final int INIT_B = 0xEFCDAB89;
    private static final int INIT_C = 0x98BADCFE;
    private static final int INIT_D = 0x10325476;

    private static final int[] SHIFT_AMTS = { 7, 12, 17, 22, 5, 9, 14, 20, 4, 11,
16, 23, 6, 10, 15, 21 };

    public static void main(String[] args) {
        Scanner scanner = new Scanner(System.in);
        System.out.print("Enter the message: ");
        String message = scanner.nextLine();
        scanner.close();

        String hash = md5(message);
        System.out.println("MD5 Hash: " + hash);
    }

    public static String md5(String message) {
        int[] state = new int[] { INIT_A, INIT_B, INIT_C, INIT_D };

        byte[] msgBytes = message.getBytes();
        int msgLen = msgBytes.length * 8;

        // Append single 1 bit
        byte[] paddedMessage = appendPadding(msgBytes);

        // Append original length in bits
        paddedMessage = appendLength(paddedMessage, msgLen);

        // Process message in 512-bit blocks
        for (int offset = 0; offset < paddedMessage.length; offset += 64) {
            int[] M = new int[16];
            for (int i = 0; i < 16; i++) {
                M[i] = bytesToInt(paddedMessage, offset + i * 4);
            }

            int A = state[0];
            int B = state[1];
            int C = state[2];
            int D = state[3];

            for (int i = 0; i < 64; i++) {
                int F, g;
                if (i < 16) {
                    F = (B & C) | (~B & D);

```

```

        g = i;
    } else if (i < 32) {
        F = (D & B) | (~D & C);
        g = (5 * i + 1) % 16;
    } else if (i < 48) {
        F = B ^ C ^ D;
        g = (3 * i + 5) % 16;
    } else {
        F = C ^ (B | ~D);
        g = (7 * i) % 16;
    }

    int temp = D;
    D = C;
    C = B;
    B += Integer.rotateLeft(A + F + M[g] + getT(i), SHIFT_AMTS[i % 4]);
    A = temp;
}

state[0] += A;
state[1] += B;
state[2] += C;
state[3] += D;
}

// Concatenate state variables to form final hash
return String.format("%08x%08x%08x%08x", state[0], state[1], state[2],
state[3]);
}

private static byte[] appendPadding(byte[] input) {
    int initialLength = input.length;
    int newLength = initialLength + 1;
    while (newLength % 64 != 56) {
        newLength++;
    }
    byte[] padded = new byte[newLength];
    System.arraycopy(input, 0, padded, 0, initialLength);
    padded[initialLength] = (byte) 0x80;
    return padded;
}

private static byte[] appendLength(byte[] input, int length) {
    byte[] output = new byte[input.length + 8];
    System.arraycopy(input, 0, output, 0, input.length);
    for (int i = 0; i < 8; i++) {
        output[input.length + i] = (byte) ((length >>> (i * 8)) & 0xFF);
    }
    return output;
}

```

```

private static int bytesToInt(byte[] input, int offset) {
    int value = 0;
    for (int i = 0; i < 4; i++) {
        value |= (input[offset + i] & 0xFF) << (i * 8);
    }
    return value;
}

private static int getT(int i) {
    return (int) (long) (Math.pow(2, 32) * Math.abs(Math.sin(i + 1)));
}
}

```

**\*\*output\*\***

```

PS C:\Users\saura\Desktop\3rd year study matrial\TE SEM 6\LP2\IS LAB> cd
"c:\Users\saura\Desktop\3rd year study matrial\TE SEM 6\LP2\IS LAB\" ; if ($?) {
javac IS_L6.java } ; if ($?) { java IS_L6 }
Enter the message: Hello World
MD5 Hash: c7ffd9684366267956915fb97fb4e5b1

```