

Debugging Examples

Here are some debug examples for the cipher:

- $M = 01010111001000111000010011010100$, $K = 11100000011100110010110010001000$,
 $C = 10100111100011110110110111000011$.
- $M = 10010101110101000001101101101000$, $K = 11001110111001001001011011000011$,
 $C = 10100100111101101101010101110000$.
- $M = 00111001010010111011110101010010$, $K = 00000100100011001101010001111100$,
 $C = 01101100111000000110001011101001$.

Here are some debug examples for CFB mode with the cipher:

- $M = 10110010111101101011000100100111$ 01101001101001001000001101000001
11100100000100100011110001010110,
 $K = 10000001100001100110011010100011$,
 $IV = 11110000101010001011000100001001$,
 $C = 00100001000011001010011011101001$ 00000101110100000010001100000111
01000101101001110110111010010111.
- $M = 10010100101110011001001110101010$ 10001100000101100101000100110100
00101000011101100111011000111100,
 $K = 01101100010101001000110010001111$,
 $IV = 11110101100101000001111101100001$,
 $C = 11100011111000001101010101110111$ 00001001101000100001100001111100
11000111101110001101000001011011.
- $M = 00100110001110000010000111001010$ 00111010111010111000001000000010
01000001111011000000111110000100,
 $K = 00100011011111001110010000101110$,
 $IV = 11000011000000001101000100011011$,
 $C = 01110001101000000010011010101000$ 01111111000111101011011110010101
11110001010000001100000001110111.