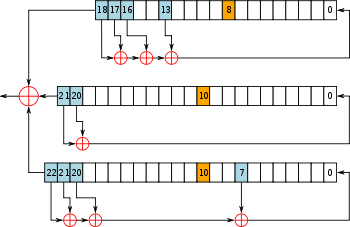
A5/1

**Theory:**

A5/1 consists of 3 shift registers.

X: 19 bits

Y: 22 bits Z: 23 bits



**Procedure:**

**Encrypt the following plaintext:**

|  |  |  |
| --- | --- | --- |
| **Plaintext** | **64-Bit Key** | **Ciphertext** |
| It is alive | 0011000001111111011110001  011011010011010000001000  011101101101011 | 001100011111010101101111111100101  00000010000000001111110110000110  000101110011111101101101000011101  0001 |
| Snap out of it | 111001101010101001110110  101000000100110011101101  1000001011001010 | 00110011101000100111100100000001  101000111111001101111110001101101  01100000001000111101000001101011  111111000000011101111101100011110  100 |
| I am as mad as hell and I am  not going to take this anymore | 001110101100110001000111  110111000111001100101101  1010100111001011 | 1110010100111000101010111001100  1101101111111001101011100000001  0011010000010101010001101110101  1010010111110110100000111000111  1010101110101010111000001111000  1001001111110110110010011010011  0000010001010001110000000010101  0011011010010110000010101011000  1110101011001000000000010101001  0001001111001110010101000101010  0010100101001100101011011010111  0010110011101100111000101011000  0110111011011010001001011111000  1110110110001001010011111010110  1111001101100111001010011000101  0111011111111100001000001101101  1111010111111101000101011111010  0111110001100010001000111110100  100110000011 |
| Bond James Bond | 110100000011110011001111  000000110011100100110000  0010110011100111 | 11101111000000100101011101001110  110011111101111101000111110100100  11011100011000011001011010110110  10111000000101000101111010111001  10110 |
| Love means never having to say you're sorry | 011111000010101100001010  111110011100000111000000  0001001101110110 | 1011011000100111010100101111010  1011111111010001000000010001110  0010110011110110101001001010000  0100011100000011100000111010110  0110010110101011010111101110111  0000100111110001111110001011101  1001000000100010000100001001101  0000011000101010000111011101101  0010110100111011011101000010001  0101011000011110100111100001000  1001010010000011110101110000001  0110001111111100110010100111110  1110110000000111010001011001 |

**Decrypt the following Ciphertext:**

|  |  |  |
| --- | --- | --- |
| **Ciphertext** | **64-Bit Key** | **Plaintext** |
| 101100001100101111010100  100100100010111010100001 | 100000000111100100000011  101011000011110010010100  1011001111000111 | **Nobody** |
| 01100001010000010000001  011101011000101000110011  00111111100100011 | 1100010111111111101000001  000110011010100100100111  011001000001100 | **KillBill** |
| 101001110100100101101011  01110111 | 001011001001100111100101  1100010100111010111011111  000010100010010 | **Bond** |
| 100011110111100000010000  111001000000110011111000  101011111001010000100110  101011101001010001011001  111110101100100 | 0001101101111111100111011  101010100000100111111100  011010010111010 | **Optimus@@ äÒÚ** |
| 1010111111111001100101000  100000111110010011000000  011010011010000111001010  0010010 | 111000000001100010111011  000010101110110101110000  1110110110000100 | **Darthvader** |