- The algorithm implements a block cipher where each block is of length 64.
- It reads plain text stream bitwise in blocks of 64 bits.
- The key is taken as input and is divided into blocks (each of 64 bit) and each block is XORed to get a single 64 bit block (call it keyBlock)
- Similar to the keyBlock generation , a paraphraseBlock is generated using a paraphrase string.
- Each block of plain text is encrypted by XORing it with keyBlock and previously encrypted plain text block (except first plain text block)
- In case of first plain text block , the XORing is done with keyBlock and paraphraseBlock
- At the end we have a bit stream which is converted into hexadecimal format for transmitting purposes