Bit-Manipulation Ciphers

- According to Shannon's work, there are two traits of secure ciphers: **confusion** and **diffusion**.

- Confusion means that the relationship between the symmetric key and ciphertext should be complex. In other words, it should be very difficult to work out the key given the ciphertext.

- Diffusion means the relationship between the plaintext and the ciphertext “diffuse”. In other words, a cipher that exhibits good diffusion will produce completely different ciphertext even with very similar plaintexts. It can be thought of as "diffusing" bits of the plaintext throughout the ciphertext.

- Bitshifts and especially rotations are so widely used because they promote good diffusion. Almost all modern-day ciphers implement the concept of **rounds**, where the plaintext is subjected to several rounds of some operations on it to convert it to ciphertext.

- If those rounds include **rotations**, then bits of the plaintext are directly carried to other locations. Once they are in their new locations, other operations take place which further **increases diffusion**, such as **modular addition**.

- Other operations may add security, like performing an **XOR** operation between a segment of a derived key with a buffer containing plaintext/ciphertext.

- As the number of rounds increases, the rotations increase, and the bits from the plaintext end up "spread out" throughout the ciphertext.

- MD5 is a very good example of a cipher which uses rotation heavily. Even a single bit change in the input to the algorithm results is a completely different hash.

- The following example illustrates the concept of diffusion (Note that ASCII uppercase and lowercase characters differ only by a single bit):

```
[root]# echo -n foobar | md5sum | awk '{print $1}'
3858f62230ac3c915f300c664312c63f
[root]# echo -n foobaR | md5sum | awk '{print $1}'
942f269a772cab5c7e971d99a4616f3e
```

- Bit-manipulation ciphers are ideally suited for computer use since they employ operations that are easily performed by machines.

- Unlike the previous substitution ciphers, the ciphertext generated by this cipher tends to look an unintelligible block of binary code.

- Bit-manipulation ciphers are applicable primarily to file I/O, especially given the fact that the encryption process produces non-printable ciphertext.

- This type of a cipher converts plaintext into ciphertext by altering the actual bit pattern of each character through the use of one or more of the following logical operators:

- AND (&&)
- OR (||)
- NOT (!)
- XOR (^)
- 1's Complement (~)

- The basic technique is very simple since most modern languages have built in operators required for bit manipulation.

- The sample Linux executable provided illustrates the use of a simple XOR cipher.

- The encryption portion reads a key word and two filenames from the command line. The algorithm is quite simple, 64-bit blocks are read from the input file, and then an exclusive OR of the block and the keyword. The ciphertext is then written in blocks to an output file.

- To decryption portion reads a block of ciphertext from encrypted file and essentially runs it against the same encryption program using the same password.

- Visually the encrypted file simply contains a series random byte values. This algorithm is a significant improvement over the simple character substitution encryption schemes discussed previously because each character's modification is a function of its position in the 8-byte block and the corresponding character in the keyword.

- This technique is not immune to code-breaking techniques, but it will require a lot more work and time.