An introduction to Block Ciphers

Saša Radomirović

April 2000

1 What is a Block Cipher?

A block cipher is an example of a *symmetric* crypto system. The word "symmetric" here means that the same key is used for encryption and decryption. One of the most famous block ciphers is *DES*. But there are many more.

2 Why use Block Ciphers?

Using the same key for encryption and decryption might seem like a drawback after having learned about RSA and Diffie–Hellman, but in fact RSA and Diffie–Hellman are only useful together with block ciphers. The important point is that block ciphers are much faster than public key crypto systems.

3 How are Block Ciphers used ?

For now, think of a block cipher as a big black box that needs a key in order to operate. If you feed in some plaintext, then something encrypted, depending on the key, will come out the other side. And if you feed in something encrypted, then the plaintext will show up again.
Recall that Diffie–Hellman allowed Alice and Bob, who might have never met before, to establish a secret which is only known to them and nobody else. This secret is used as the key for a block cipher which encrypts the secret messages Alice and Bob want to exchange.
The combination of RSA and a block cipher works in a similar way. Recall that in RSA everybody who has Alice's public key can send secret messages to Alice, but only Alice can decipher the messages and nobody else. In the real world, the RSA public key is being used to encrypt a key for the block cipher and the secret message is being encrypted with the block cipher.

4 How does a Block Cipher work now?

First, what requirements does the block cipher have to fulfill?

- It must be able to deal with inputs of various length.
- It must be reversible.

- It must be fast.
- It is hopefully hard to break.

Letters

Although a block cipher encrypts a message which consists of 0's and 1's, I will explain everything first in terms of letters. Suppose you want to encrypt the message "PROFESSOR GREENFIELD" with a block cipher.
The first thing a block cipher does is to divide the message into blocks of a given length – hence the name *block* cipher! If we take for example blocks of 4 letters in our message, then the first block would be "PROF" the second block would be "ESSO" and so on.
Each block is encrypted separately using exactly the same procedure and key. Essentially, there are only two simple procedures used for encryption: permutation and substitution. Permutation means changing the order, for example writing "ROPF" instead of "PROF". Substitution means replacing some parts with others, say writing "GNOF" instead of "PROF" and thereby replacing "PR" with "GN". A real block cipher won't actually have a table which tells what to replace with what. Instead it will use additions, multiplications, XOR's, and the like to compute the cipher text from the key and the plain text. Notice that permutations and substitutions are reversible.
Since a small number of permutations and substitutions is not likely to be very secure, a block cipher usually repeats that process a certain number of times for each block. Each repetition is called a "round".
The following is a simple example of a block cipher:

1. Divide the text into blocks of 4 letters.
2. Do the following for each block:
   (a) Switch the first two letters with the last two letters.
   (b) Shift the first letter by one, i.e. write 'B' for an 'A', etc.
   (c) Shift the second letter by two, i.e. write 'C' for an 'A' etc.
   (d) Shift the third letter by three.
   (e) Shift the fourth letter by four.
   (f) Repeat (a) – (e) 16 times (16 "rounds").

To keep things simple we haven't used a key in our block cipher, but one could for example make the shifting of the letters key–dependent. Notice that although the steps (a) – (e) are simple to break. But after repeating them 16 times it might not be that obvious what is happening.

Numbers

Now that we know how block ciphers work in principle, let's have a look at how they work in the real world. Messages will be strings of 0's and 1's. Today's block ciphers usually have 64 bit blocks. Permutations are done on selected groups of bits. Substitutions are done with mathematical functions like multiplications and additions mod 2, or XOR's and others. But since these operations are relatively easy to reverse, as pointed out they will be done many times to increase security.