DES Decryption Demistified

January 27, 2009

1 Introduction (INCOMPLETE)

DES provides an excellent sample of symmetric encryption for the student. We provides theoretical and practical instruction for the implementation of DES in Java. For instruction purposes we use 56-bit and 64-bit data blocks. However, we do not consider block chaining.

2 Theory from the outside in

The number of rounds in DES is not important to see that decryption works exactly the same way except with inverted key order.

First the Data D is permuted

$$D' = IP(D)$$

Then it is seperated into two parts such that

$$D' = L0||R0$$

These go through the rounds in DES as shown below where rows labeled e_i are encryption and d_i are decryption.

e_0	$L0$	$R0$
e_1	$R0$	$F(R0, K0) \oplus L0$
e_2	$F(R0, K0) \oplus L0$	$F(F(R0, K0) \oplus L0, K1) \oplus R0$
$\ldots$	$\ldots$	$\ldots$
$swap$	$F(F(R0, K0) \oplus L0, K1) \oplus R0$	$F(R0, K0) \oplus L0$
$\ldots$	$\ldots$	$\ldots$
d_0	$F(F(R0, K0) \oplus L0, K1) \oplus R0$	$F(R0, K0) \oplus L0$
d_1	$F(R0, K0) \oplus L0$	$F(F(R0, K0) \oplus L0, K1) \oplus F(F(R0, K0) \oplus L0, K1) \oplus R0$
d_1	$F(R0, K0) \oplus L0$	$R0$
d_2	$R0$	$F(R0, K0) \oplus R(R0, K0) \oplus L0$
d_2	$R0$	$L0$
$Swap$	$L0$	$R0$

The left and right sides are combined to get D' and the decrypted dated is given by

$$D = IP^{-1}(D')$$

Including more rounds will produce much more complicated expressions at each level, but the decryption process is identical. More rounds may be added in the ellipses Adding more rounds would require an elipses before and after the swap ending the encryption part of table.