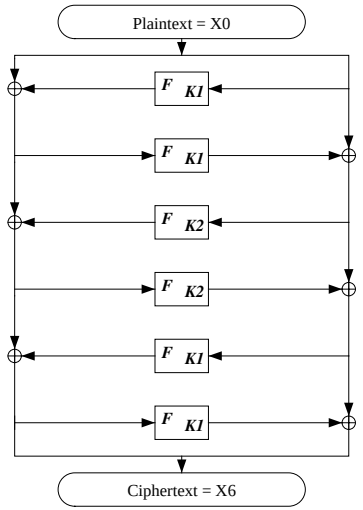
Cryptanalysis of Magenta

Eli Biham
Alex Biryukov
Niels Ferguson
Lars R. Knudsen
Bruce Schneier
Adi Shamir

March 23, 1999

Magenta



The Attack

We first present a chosen plaintext attack using 2^{64} chosen plaintexts and requiring 2^{64} steps of analysis.

This attack is independent of the choice of the F function.

1. Choose an arbitrary plaintext X_0.
2. Request the ciphertext X_6 of X_0 under the unknown key K.

The Attack (cont.)

3. Try all 2^{64} possible values K_1', and for each compute the following:
   (a) Partially encrypt X_0 for the first two rounds to get a candidate for X_2.
   (b) Choose an arbitrary X_2' such that $X_2'^T = X_2^T$.
   (c) Partially decrypt X_2' under the trial subkey K_1' to get X_0'.
   (d) Request the ciphertext X_6' of X_0' under the unknown key K.
   (e) Partially decrypt X_6 and X_6' under the trial subkey K_1' to get X_4 and X_4'.
   (f) From X_2 and X_4 compute the output of the E function of round 3, and similarly for X_2' and X_4'.
   (g) Reject the trial subkey K_1' if the outputs are different.
4. Once K_1 is found, try all 2^{64} possibilities of K_2.

The Attack (cont.)

This attack can be converted into a known plaintext attack using only 2^{33} known plaintexts but 2^{97} steps of analysis.

The same attacks apply to the larger key sizes with the same reduction in complexity over brute force.