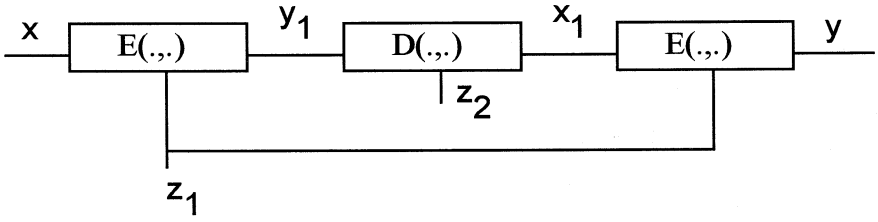
[The following report was made for, and at the request of, Cylink Corporation of Sunnyvale, California. Cylink Corporation has authorized the author to release this report to other interested parties.]

Analysis of Two-Key Triple DES Encryption

James L. Massey
April 2, 1994

The situation to be considered is shown in the following diagram:



Let z_1* and z_2* be the actual values of the keys z_1 and z_2. Let $k_1, k_2, k_3, \ldots$ denote the ordered list of all 2^{56} possible values of a key.

Chosen-Plaintext Attack to Find z_1* and z_2*:

a. Choose a value y_1* of y_1 arbitrarily (e.g., all zeroes).

b. For i = 1 to 2^{56}, DO:

1) Decrypt y_1* with the key k_i to obtain $x := D(y_1^*, k_i)$.

2) Submit x as a chosen plaintext and receive y as the resulting ciphertext, i.e., $y := E(D(E(x, z_1^*), z_2^*), z_1^*)$.

3) Decrypt y with the key k_i to obtain $x_1 := D(y, k_i)$.

4) Insert the pair (x_1, k_i) into an "(x_1, z_1) list" indexed on the first entry .

[One of the entries in this list of 2^{56} pairs is (x_1^*, z_1^*) where $x_1^* = D(y_1^*, z_2^*)$. Let $m_1, m_2, m_3, \ldots$ denote the ordered list of first entries in this (x_1, z_1) list. Note that there may be a small number of duplicate first entries since it is possible that y_1* decrypts to the same x for two or more keys.]

c. For j = 1 to 2^{56}, DO:

1) Decrypt y_1* with the key k_j to obtain $x_1 := D(y_1^*, k_j)$.

2) If x_1 is equal to a first entry m_h in the (x_1, z_1) pair list, say the entry (m_h, k_i), then $(z_1^*, z_2^*) = (k_i, k_j)$ is possible and indeed probable. Check this possibility on two known (x, y) pairs for the triple encryption. If $y = E(D(E(x, k_i), k_j), k_i)$ for both pairs, announce $(z_1^*, z_2^*) = (k_i, k_j)$ and stop. Do this for all h with $m_h = x_1$ in case there is more more than one such h.

Computational Requirements:

- We need 2^{56} chosen plaintext/ciphertext pairs for the triple encryption.
- We need to perform at most $2 \cdot 2^{56} + 2^{56} = 3 \cdot 2^{56}$ single DES encryptions or decryptions.
- We need storage for a table of 2^{56} plaintext/key pairs and we need to order this table on the first entry of the pair.

What makes this attack succeed is the fact that, *because we are able to choose plaintexts* for the triple encryption, we are able to create (y_1, x_1) pairs [in the notation of the above diagram] for each possible value of z_1, *all of which have the same value of* y_1, namely y_1*. *If we are restricted to a known-plaintext attack, this is not possible.* If we choose $y_1 = y_1$*, we can indeed find the corresponding plaintext x for any choice of z_1 as in step b.1) above, but we cannot find the corresponding ciphertext y for the triple encryption and hence cannot find x_1 as in step b.3) above. We could indeed form a table of 2^{56} (y_1, x_1, z_1) triples for the 2^{56} possible values of z_1, one of which is indeed $(y_1$*, x_1*, z_1*) such that x_1* = D(y_1*, z_2*), but the values of y_1 will appear random in this table. Hence, we will not be able to eliminate an incorrect value of z_2 by a single decryption as we can do when all entries in this table have the same value of y_1.

The chosen-plaintext attack described above cannot be used against true triple encryption (where all three keys are independently chosen) because, in step b.3), we would not know the decrypting key for converting y to x_1.

We make the following conclusions:

- Two-key triple DES encryption appears to be roughly as strong against a *known-plaintext* attack as is three-key triple DES encryption.

- Two-key triple DES encryption is definitely weaker than three-key triple DES encryption against a *chosen-plaintext* attack.

- Two-key triple DES encryption is definitely stronger than two-key double DES encryption for which (in the Merkle-Hellman "meet-in-the-middle" attack) only 2 known ciphertext/plaintext pairs, a sorted table of 2^{56} plaintext/ key pairs, and at most $2 \cdot 2^{56}$ encryptions suffice to determine the 112-bit key (cf. R.C. Merkle and M.E. Hellman, "On the Security of Multiple Encryption," *Comm. ACM*, vol. 24, no. 7, pp. 465-466, July 1981).

In our analysis, we have for convenience and practicality considered the embedded cipher to be the DES. It should be clear, however, that our analysis applies unchanged to any non-expanding block ciphers, such as SAFER K-64, IDEA, etc.