## 1.4 Triple Ciphers

The last section unveiled a principal weakness of double encryption. Therefore, to get a real improvement, we move on to triple encryption. An often used scheme is "EDE" (Encryption, Decryption, Encryption)

$$f_g \circ f_h^{-1} \circ f_k \quad \text{for } g, h, k \in K.$$

Why is $f_h$ inverted? The advantage of this scheme is its compatibility with simple encryption by choosing keys $g = h = k$.

The Meet in the Middle attack also applies to this scheme. Thus the effective key length (for exhaustion) is not tripled but only doubled, but that's OK for 56 or 64-bit keys.

Often the scheme is somewhat simplified as "two-key triple encryption":

$$f = f_k \circ f_h^{-1} \circ f_k \quad \text{for } h, k \in K.$$

This scheme has a weakness under an attack with *chosen* plaintext that however worries only paranoiacs. Consider the scenario

$$\begin{array}{ccccccc} \Sigma^* & \xrightarrow{f_k} & \Sigma^* & \xrightarrow{f_h^{-1}} & \Sigma^* & \xrightarrow{f_k} & \Sigma^*, \\ a & \mapsto & b & \mapsto & b' & \mapsto & c. \end{array}$$

**Step 1:** Using $\#K$ encryptions and $\#K$ memory cells precalculate the table

$$\{f_h^{-1}(b_0) \mid h \in K\}$$

for a fixed intermediate value of $b_0$.

**Step 2:** Then calculate for all keys $k \in K$:

$$\begin{array}{rcll} a_k & := & f_k^{-1}(b_0) & \text{(the chosen plaintext)}, \\ c_k & := & f(a_k), & \\ b_k & := & f_k^{-1}(c_k). & \end{array}$$

The second assignment is possible in an attack with chosen plaintext, which implies that we can evaluate $f$ with any plaintexts. The expenses are $5 \cdot \#K$ simple encryptions. If $b_k = f_h^{-1}(b_0)$, then we keep the pair $(h, k)$ of keys for further examination.

$$\begin{tikzcd}
\Sigma^* \arrow[r, "f_k"] & \Sigma^* \arrow[r, "f_h^{-1}"] & \Sigma^* \arrow[r, "f_k"] & \Sigma^* \\
 & b_0 \arrow[r, mapsto, "f_h^{-1}"] \arrow[ddl, "f_k^{-1}"'] & b_k \arrow[dl, dash] & \\
 & f_h^{-1}(b_0) \overset{?}{=} f_k^{-1}(c_k) & & \\
a_k \arrow[rrr, mapsto, "f"'] & & & c_k \arrow[uul, "f_k^{-1}"']
\end{tikzcd}$$

The most efficient known attack is described in:

- Van Oorschot/Wiener: A known plaintext attack on two-key triple encryption. Eurocrypt 90.