Algorithm 1: KDF overview

```
Data: K, M
Result: K'
$counter \leftarrow 1$
while output a key do
    $i \leftarrow random() \bmod 16$
    $K \leftarrow M \times K$
    if $M[i] = counter$ then
        swap(M[i], M[counter])
    end
    $M \leftarrow M^2$
    $counter \leftarrow (counter + 1) \bmod 16$
    output : $K$
end
```