Algorithm for IBDBP

Swapnil Ghosh

March 16, 2021

Algorithm 1 3-Layer Inverse Diffusion with Internal Permutation

```
Data: $cipher_{bits}$, $key_{bits}$
Result: $permuted_{bits}$
procedure IBDBP($ci, ke$)                      ▷ Decrypts the diffusion of a matrix
    for $q$ = $1$ to $l$ do                        ▷ Reverses Level 3 Diffusion
        for $d$ = $1$ to $8$ do
            if $d \leq 4$ then
                b1$_{(q,d)}$ = ci$_{(q,d+4)}$ $\oplus$ ke$_{(q,d)}$
            else
                b1$_{(q,d)}$ = ci$_{(q,d-4)}$ $\oplus$ ke$_{(q,d)}$
            end if
        end for
    end for
    for $q$ = $1$ to $l$ do                        ▷ Reverses Level 2 Diffusion
        for $d$ = $1$ to $8$ do
            if $d$ = $1, 2, 5, 6$ then
                b2$_{(q,d)}$ = b1$_{(q,d+2)}$ $\oplus$ ke$_{(q,d)}$
            else
                b2$_{(q,d)}$ = b1$_{(q,d-2)}$ $\oplus$ ke$_{(q,d)}$
            end if
        end for
    end for
    for $q$ = $1$ to $l$ do                        ▷ Reverses Level 1 Diffusion
        for $d$ = $1$ to $8$ do
            if $d$ = odd number then
                per$_{(q,d)}$ = b2$_{(q,d+1)}$ $\oplus$ ke$_{(q,d)}$
            else
                per$_{(q,d)}$ = b2$_{(q,d-1)}$ $\oplus$ ke$_{(q,d)}$
            end if
        end for
    end for
    return $per$                               ▷ Permuted Bits returned as matrix
end procedure
```