

# Incorrect use of a Trapdoor Function (TDF)

**Never** encrypt by applying  $F$  directly to plaintext:

$E(pk, m)$  :

output  $c \leftarrow F(pk, m)$

$D(sk, c)$  :

output  $F^{-1}(sk, c)$

Problems:

- Deterministic: cannot be semantically secure !!
- Many attacks exist (next segment)