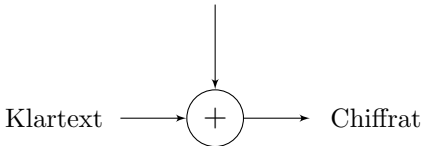


pseudo-random number generator zum key  $k$

$PRNG_k$



bitweise XOR