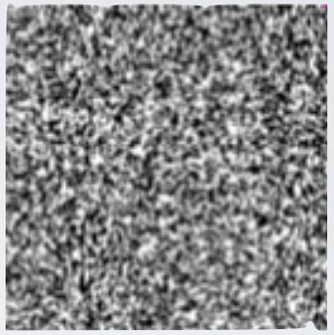
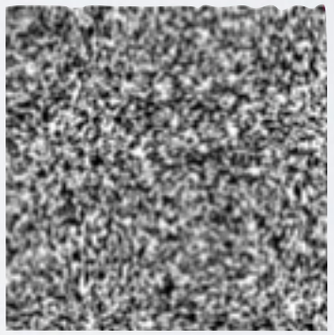
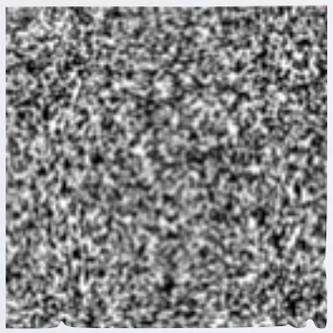
Key-reused attack on CTR

$\oplus$ K =

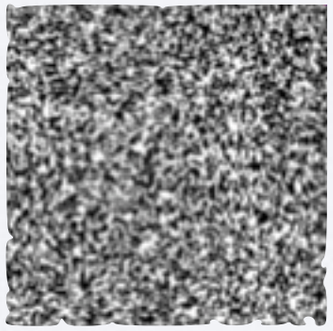


$\oplus$ K =





$\oplus$



=

Symmetric Encryption

Stream Cipher vs Block Cipher