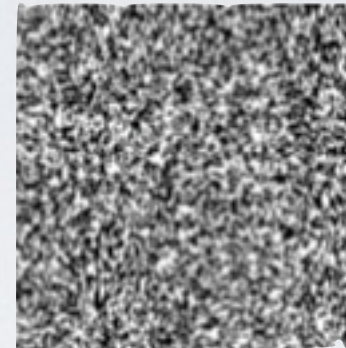


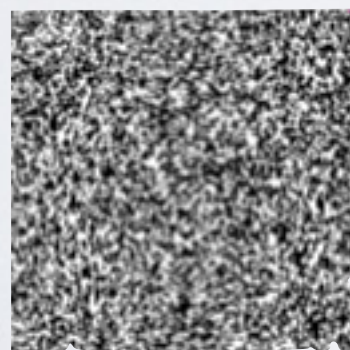
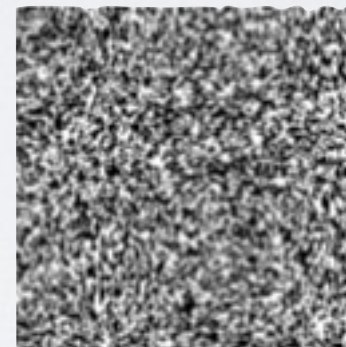
# Key-reused attack on CTR



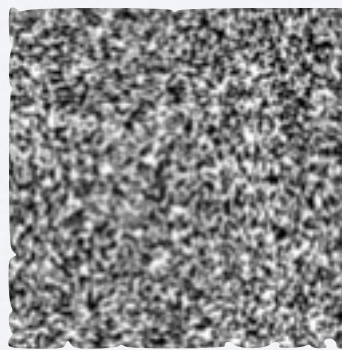
$$\oplus K =$$



$$\oplus K =$$



$$\oplus$$



$$=$$



# Stream Cipher vs Block Cipher