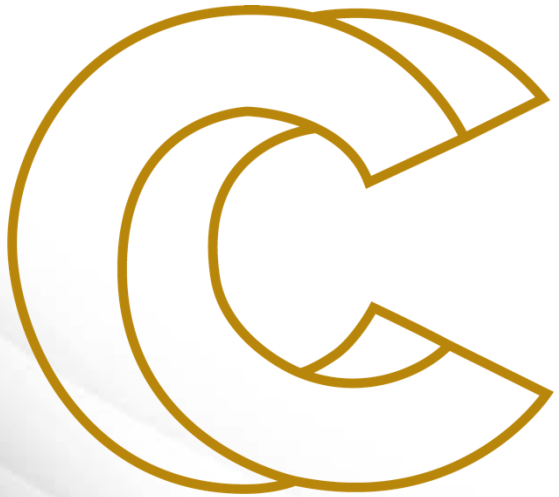


EURO^2

GPU Optimization of Advanced Encryption Standard

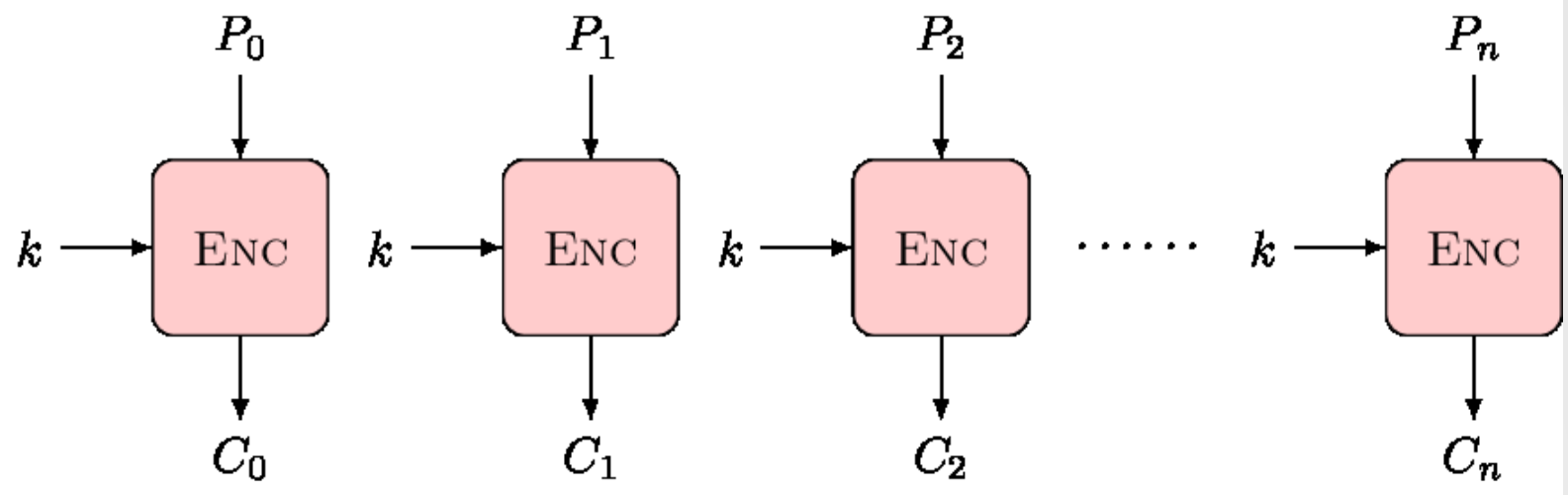
Cihangir Tezcan, PhD

Graduate School of Informatics, METU, Ankara

ncc@ulakbim.gov.tr

Lesson 3: Mode of Operation

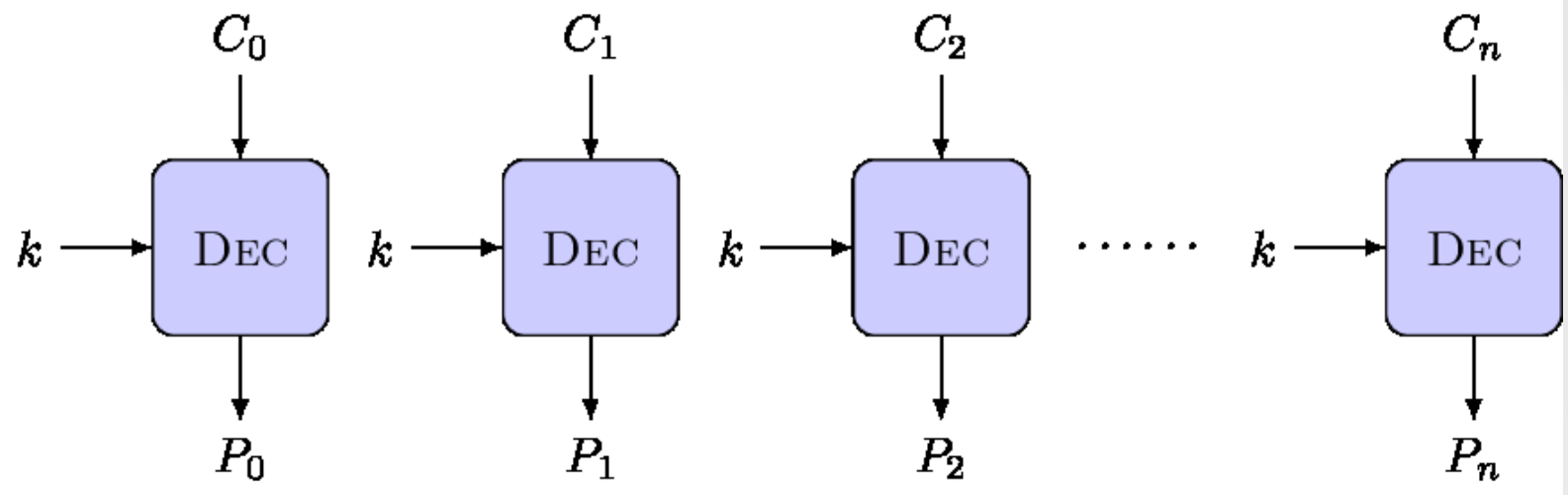
How to encrypt a plaintext larger than a single block?



This is called Electronic Code Book (ECB) mode of operation.

Lesson 3: Mode of Operation

How to encrypt a plaintext larger than a single block?



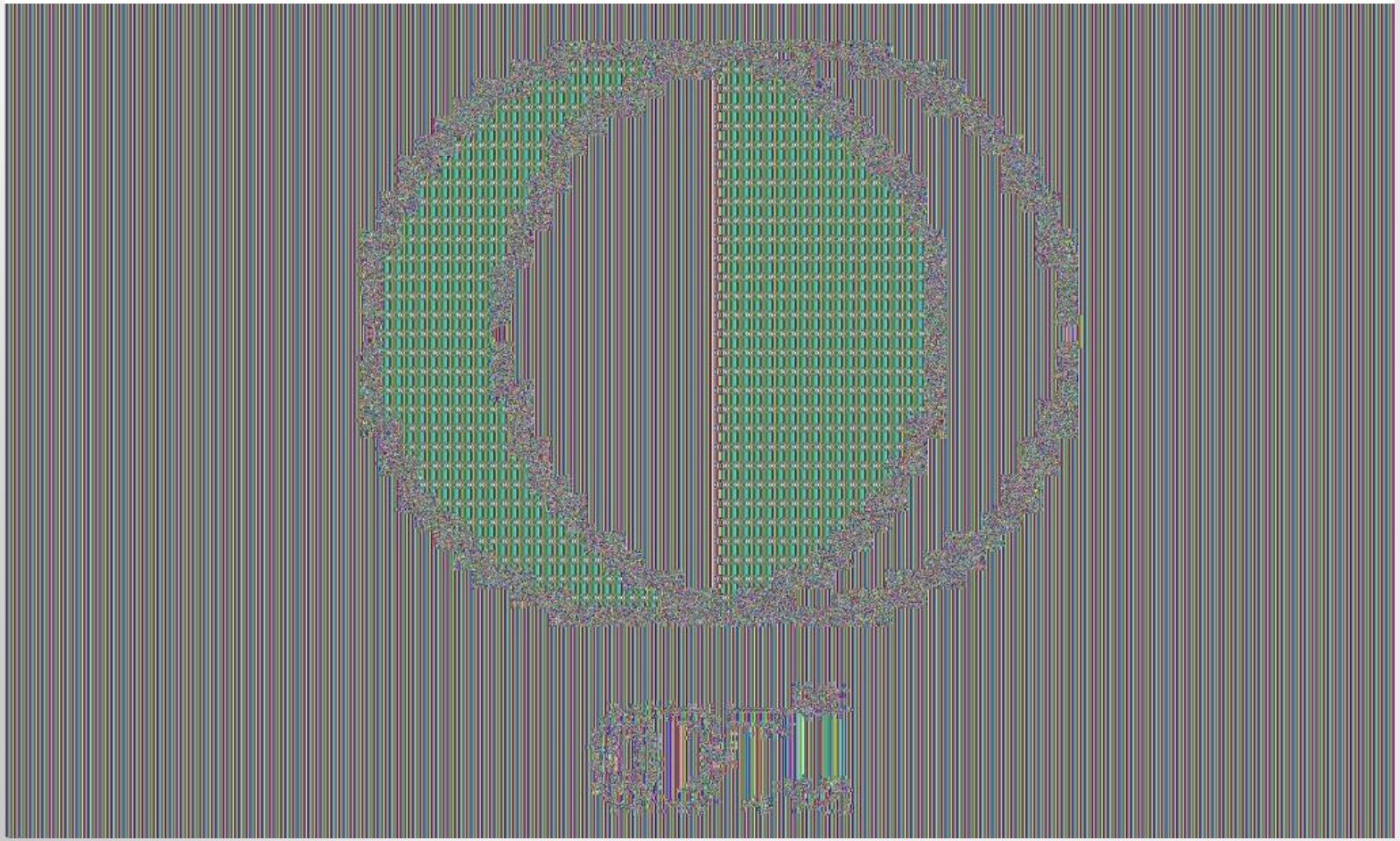
Decryption for Electronic Code Book (ECB) mode of operation.

Lesson 3: Mode of Operation

BMP File Example

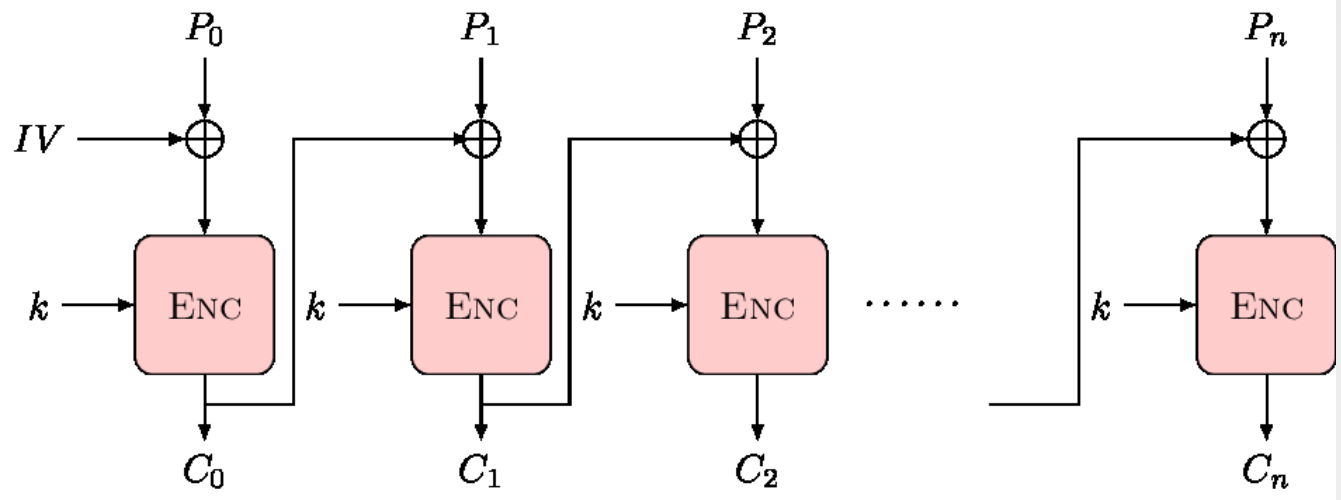
Lesson 3: Mode of Operation

BMP File Encrypted with AES-128 ECB



Lesson 3: Mode of Operation

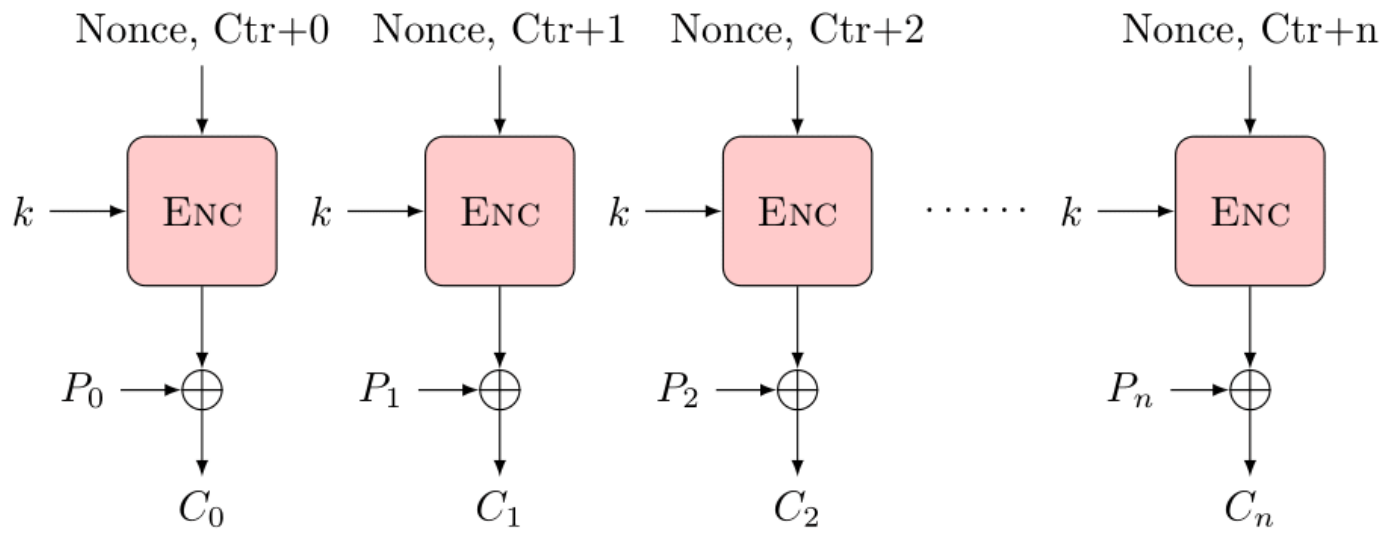
How to encrypt a plaintext larger than a single block?



Cipher Block Chaining (CBC) mode of operation solves the problem of ECB but it is not parallelizable.

Lesson 3: Mode of Operation

How to encrypt a plaintext larger than a single block?



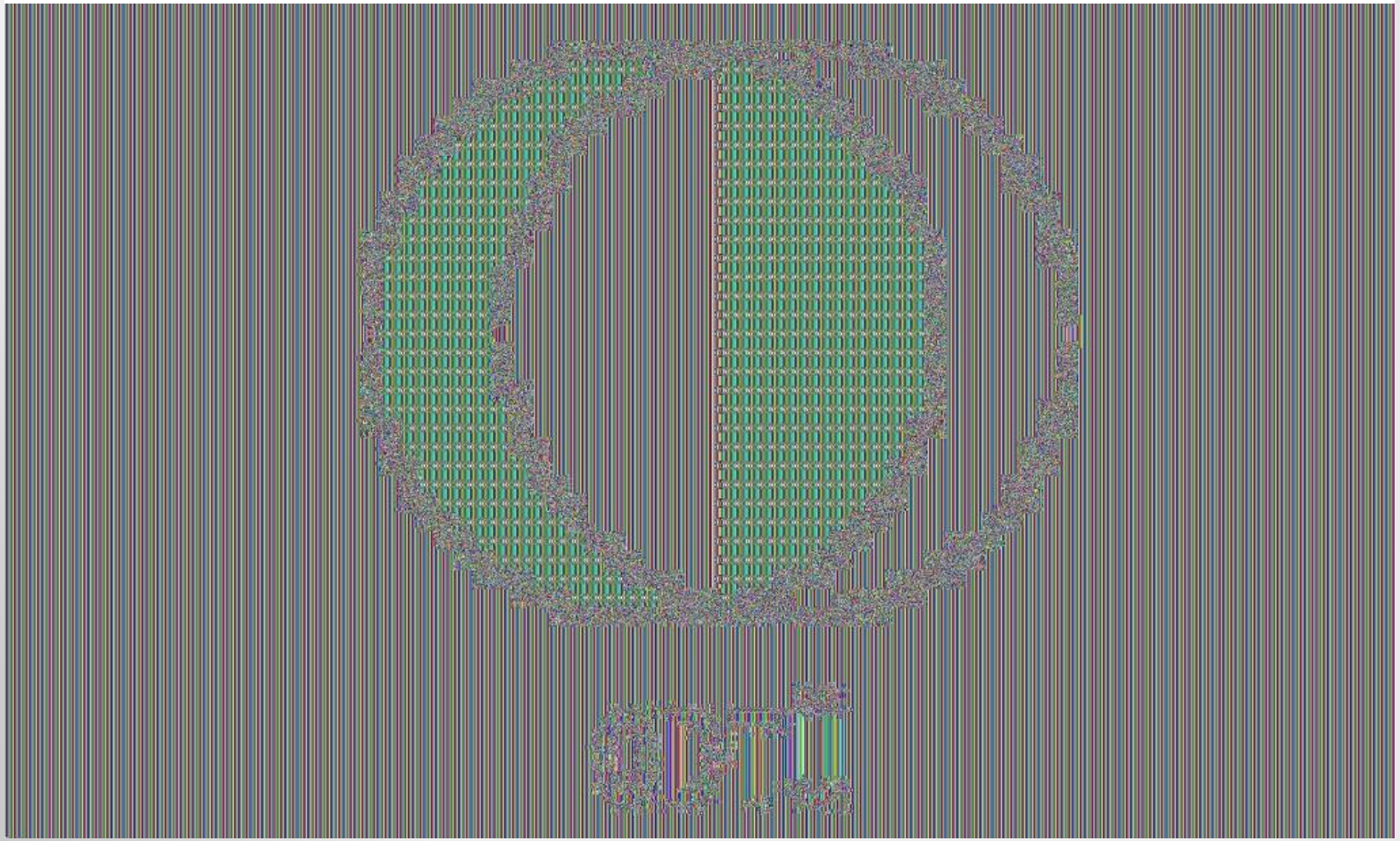
Counter (CTR) mode of operation solves the problem of ECB and it is also parallelizable.

Lesson 3: Mode of Operation

BMP File Example

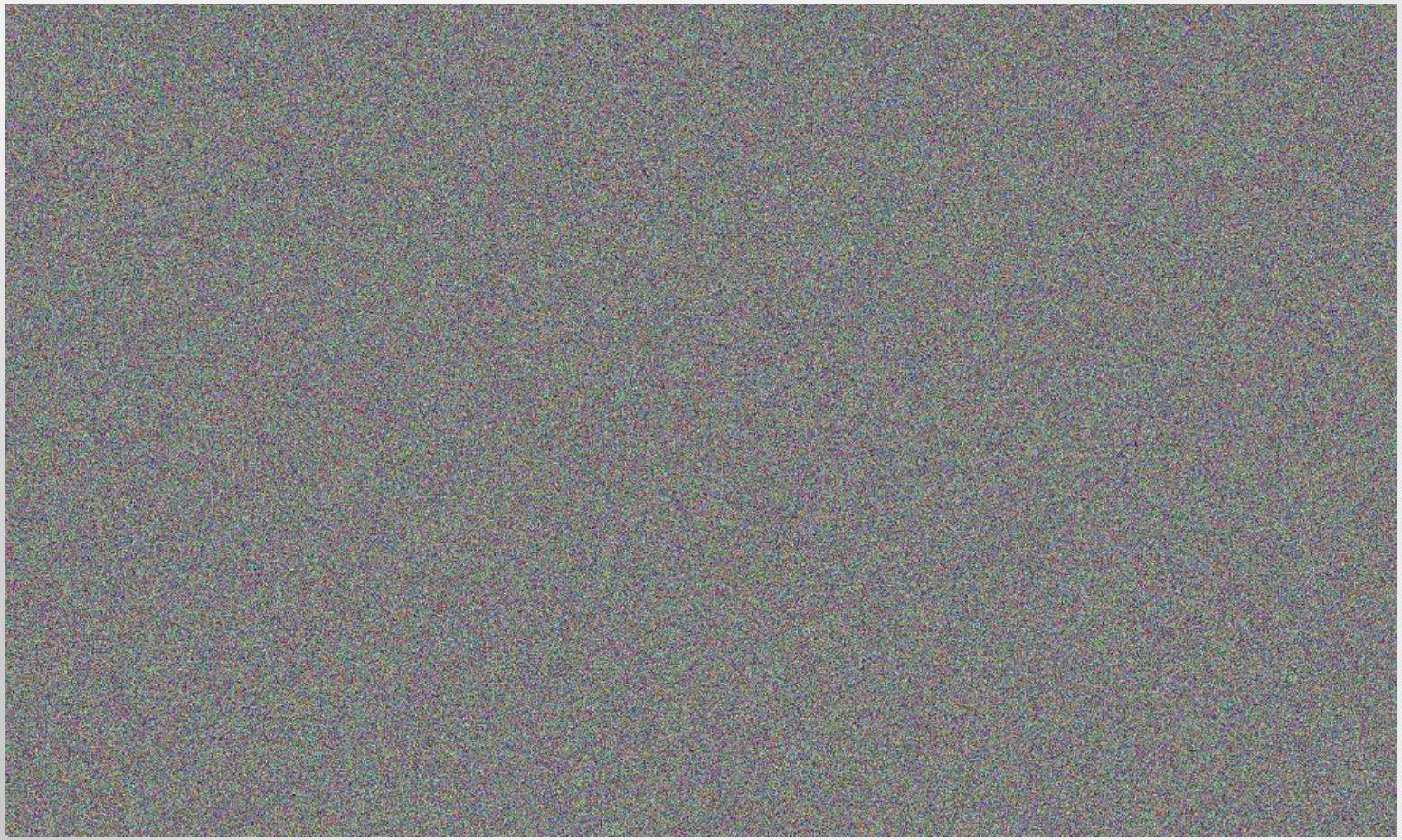
Lesson 3: Mode of Operation

BMP File Encrypted with AES-128 ECB



Lesson 3: Mode of Operation

BMP File Encrypted with AES-128 CTR



Next lecture

Reference C and CUDA Implementation of AES

- Before CUDA optimization, we are going to implement AES using C and CUDA

Thanks

This project has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101101903. The JU receives support from the Digital Europe Programme and Germany, Bulgaria, Austria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Italy, Lithuania, Latvia, Poland, Portugal, Romania, Slovenia, Spain, Sweden, France, Netherlands, Belgium, Luxembourg, Slovakia, Norway, Türkiye, Republic of North Macedonia, Iceland, Montenegro, Serbia