Carlos Martinez
Computer Security
Computer Science 4440
Cryptography In Java
Exercise 1

3.3 (f):

Oh no! javax.crypto.AEADBadTagException: mac check in GCM failed
Oh no! java.lang.NullPointerException

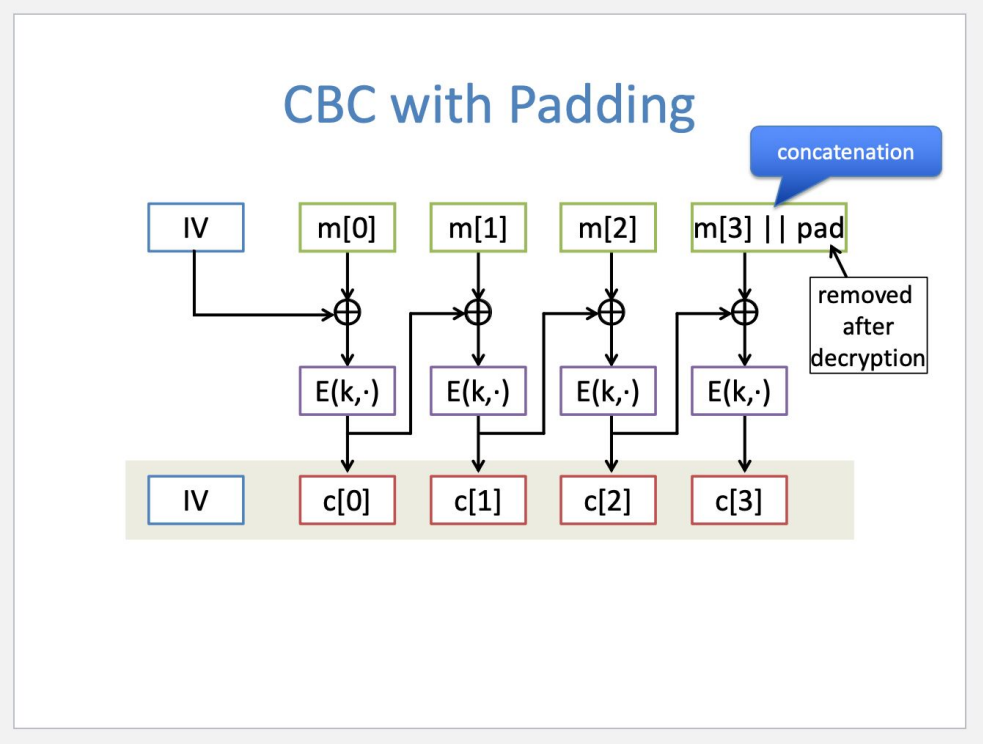
In cryptography, **Galois/Counter Mode** (**GCM**) is a mode of operation for symmetric-key cryptographic block ciphers widely adopted thanks to its performance. GCM throughput rates for state-of-the-art, high-speed communication channels can be achieved with inexpensive hardware resources.[1] The operation is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality. GCM is defined for block ciphers with a block size of 128 bits. **Galois Message Authentication Code** (**GMAC**) is an authentication-only variant of the GCM which can form an incremental message authentication code. Both GCM and GMAC can accept initialization vectors of arbitrary length.

GCM is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality, we got this because the integrity was violated and GCM was able to detect it

3.3 (g) (a): 43 Bytes

3.3 (g) (b): 48 Bytes

3.3 (g) (c): CTR does not require a full block, CBC does and adds padding to get the full block which is why it is larger



3.3 (g) (d): 59 Bytes

3.3 (g) (e): GCM has stuff in it that allow authentication, which makes the file larger than CTR. MAC is appended to the message to ensure integrity. GMC just handles the MAC for you so that we don’t have to check when writing the encryption code.

3.3 (h) (a): 0x01
3.3 (h) (b): 0x01
3.3 (h) (c): 0x03
3.3 (h) (d): Improperly Padded
3.3 (h) (e): Improperly Padded
3.3 (h) (f): Improperly Padded