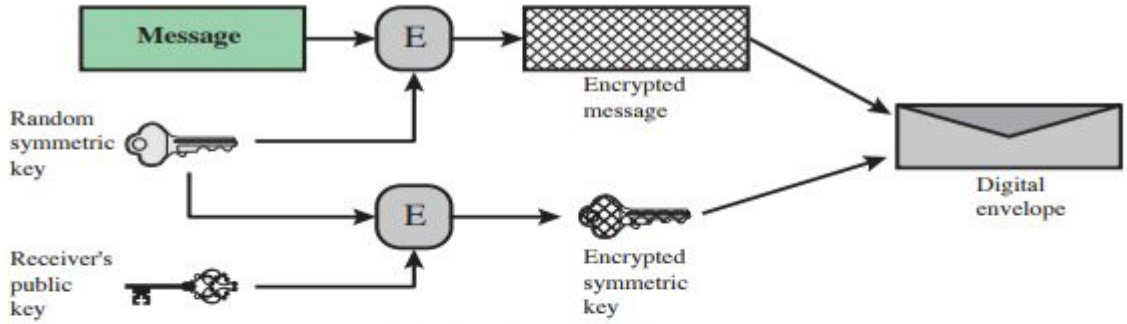
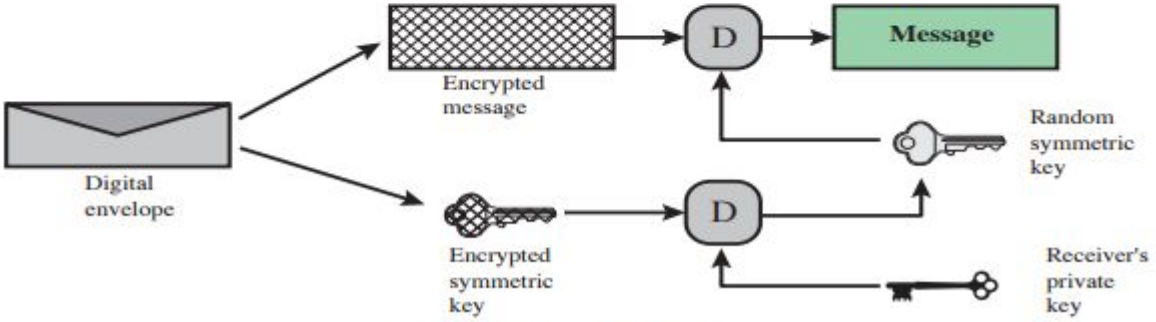
Option 3

...

Chris Brodski



(a) Creation of a digital envelope



(b) Opening a digital envelope

Sender

Sends these byte files::

- Hash number: $H(K_{xy} \,||\, M \,||\, K_{xy})$
- Encrypted message: $En(M,K_{xy})$
- Encrypted Key: $En(K_{xy},K_{y+})$

Receiver

Receives:

- Hash number: $H(K_{xy} \,||\, M \,||\, K_{xy})$
- Encrypted message: $En(M,K_{xy}) = C_M$
- Encrypted Key: $En(K_{xy},K_{y+}) = C_k$

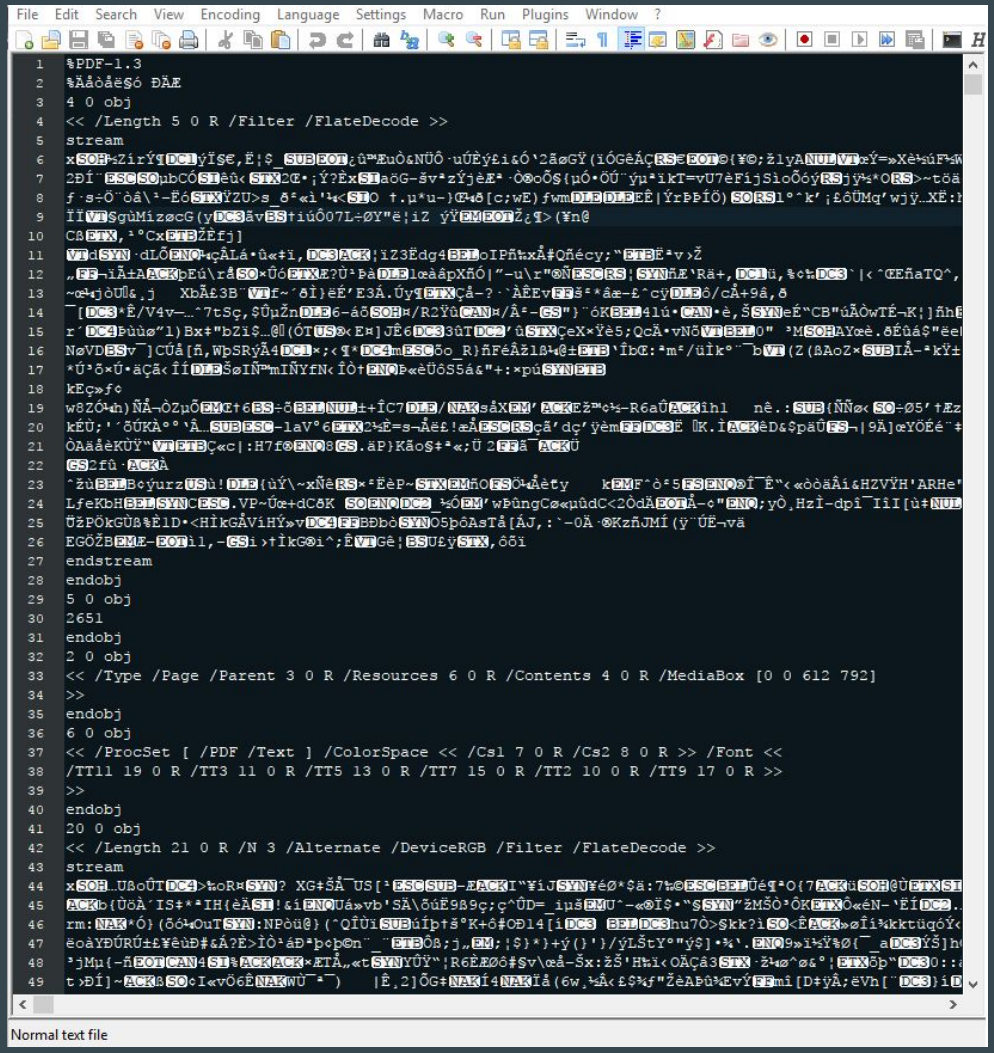
Decrypts

- $D(C_M,K_{y-}) = M$
- $D(C_k, K_{k-}) = K_{xy}$
- Calculates $H(K_{xy} \,||\, M \,||\, K_{xy})$ and compares with received hash value.

“Intro_01.pdf” byte file

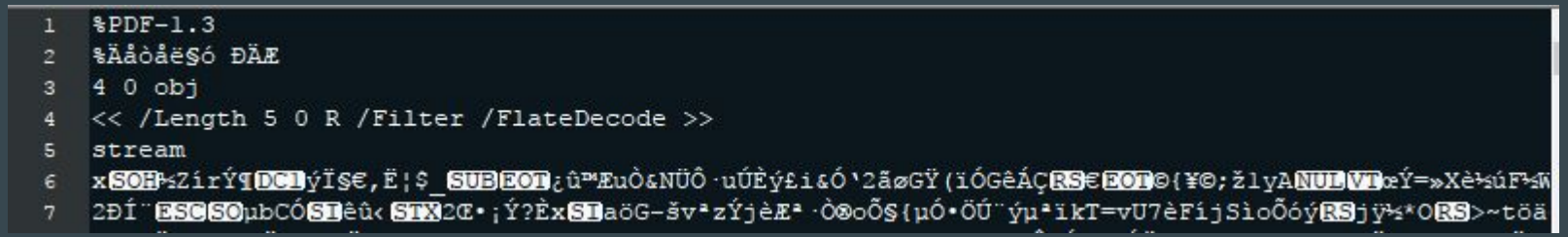
- I converted the file “Intro_01.pdf” to a byte file (taken from blackboard)
- This is what a text editor sees (next page):
  First 50 lines

“Intro_01.pdf” byte file

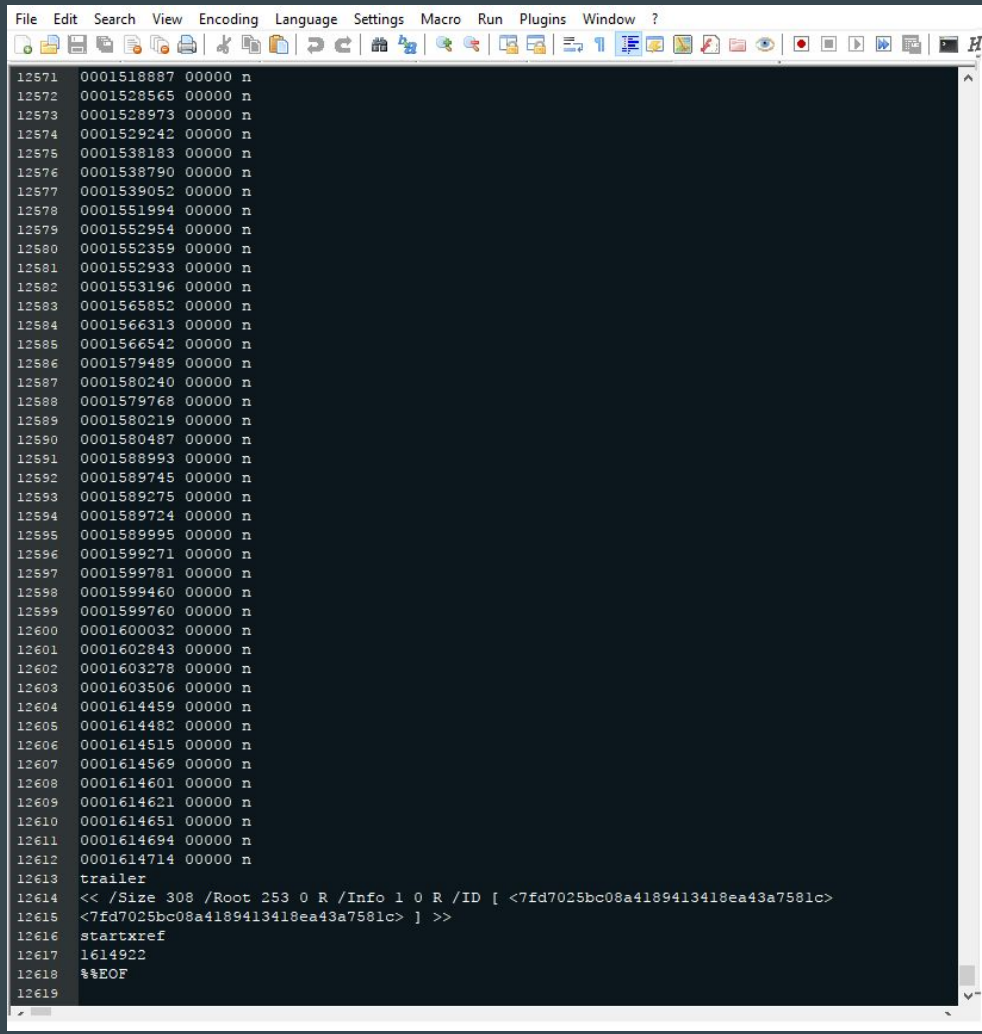


“Intro_01.pdf” byte file (top of file)

Observe first few lines



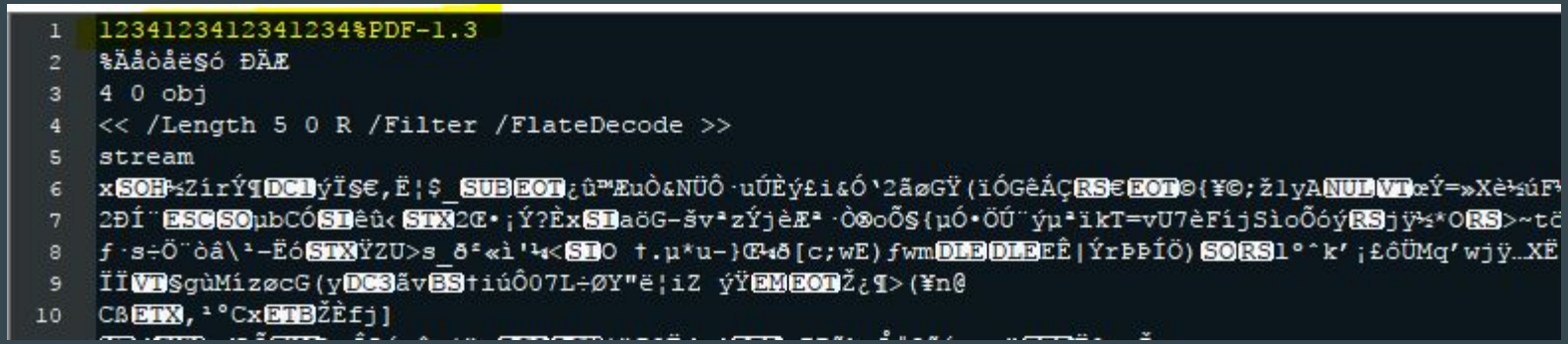
“Intro_01.pdf” byte file (end)



“Intro_01.pdf” byte file (end of file)

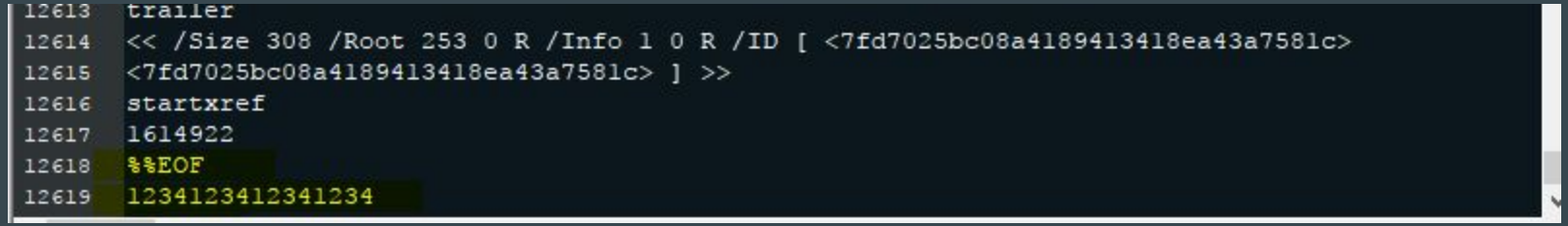
(K || M || K) top of file

- 1234123412341234 = Key



(K || M || K) bottom of file

- 1234123412341234 = Key



message.aescipher

- Message after encryption