

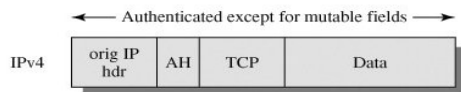


# Assignment #2 (2 points)

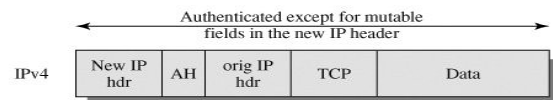
Due on: April 20th

End-to-end authentication and encryption are desired between two hosts. We have studied the following figures of simple Security Associations (SA) :

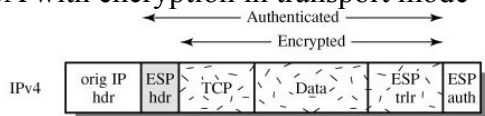
## SA with authentication in transport mode



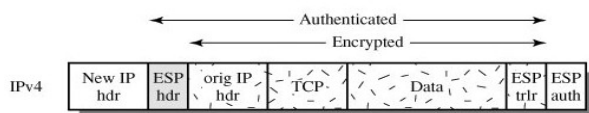
## SA with authentication in tunnel mode



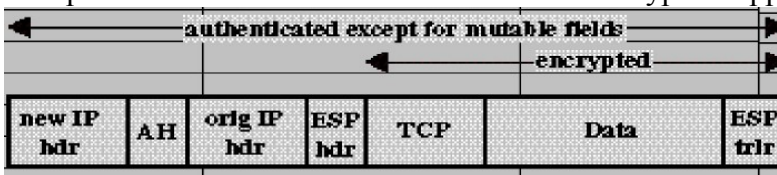
## SA with encryption in transport mode



## SA with encryption in tunnel mode



Security Associations can be combined. For example, the following figure depicts a transport SA bundled inside a tunnel SA with encryption applied before authentication.



Draw similar figures for the following **combinations** of Security Associations:

1. Transport adjacency, with authentication applied before encryption
2. A transport SA bundled inside a tunnel SA, with authentication applied before encryption
3. A transport SA bundled inside a tunnel SA both bundled inside a third tunnel SA, with the following order: encryption then authentication then encryption