

IK2206 – Internet Security and Privacy

Chapter 21 – PEM & S/MIME

21.1 Introduction (READ)

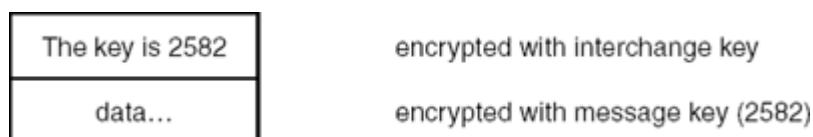
21.2 Structure of a PEM Message (READ)

- What are the different components that can be combined into a PEM message? (This is similar to S/MIME.)
 - Ordinary, unsecured data
 - Integrity-protected (unmodified data)
 - Integrity-protected encoded data
 - Encoded encrypted integrity-protected data

21.3 Establishing keys (READ BRIEFLY)

- Why did PEM specify both public key and secret key for interchange keys?

The per-message key used to encrypt a message is just a randomly selected number. But there is also a long-term key which PEM refers to as an interchange key. When public keys are used, the interchange key is Bob's public key. When secret keys are used, the interchange key is a key Alice and Bob share. **The interchange key is used to encrypt the per-message key.**



21.4 Some PEM History (READ BRIEFLY)

- Consider the high visions behind PEM, and if those visions actually were obstacles for practical deployment of the protocol?

21.5 PEM Certificate Hierarchy (READ)

- What was the certificate hierarchy proposed for PEM?
- How was it intended to be implemented?

21.6 - 21.16 (SKIP)

21.17 Differences in S/MIME (READ)

- What are the MIME extensions introduced for S/MIME?
- How are S/MIME headers encoded?
- What is the "smime.p7m" file? What does it contain?

- What is PKCS #7? (Suggestion: use Google or Wikipedia)

21.18 S/MIME Certificate Hierarchy (READ)

- Does S/MIME anticipate a specific kind of PKI organization?
- What are the three main ways of authenticating certificates?