Listen

Required Resources

Textbook: *Introduction to Cryptography With Coding Theory,* Chapter 15 through section 15.7: SSL and TLS

The reading this week provides insights into implementation and authentication challenges associated with public key communication schemes. It highlights the challenges of authenticating the legitimacy of websites and other information sources that imposters may create to steal sensitive information.

One technique that may attempt to steal or alter information is known as the "man-in-the-middle attack," in which an attacker intercepts and possibly alters the communication between two parties, making it appear as though they are communicating directly with each other. The goal of the various security protocols discussed in this chapter is to create real-world implementations that provide both strong security and authentication to attacks such as this.

Some of the specific protocols examined include Kerberos, a symmetric cryptography protocol designed to provide strong authentication and secure key exchange between users and servers in a networked environment, and Pretty Good Privacy (PGP), a decentralized cryptographic system that uses a web of trust to authenticate users and encrypt email messages.

Webpage: Advanced Encryption Standard (https://www.formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng.swf)
This webpage gives a step-by-step explanation of the AES algorithm, including an animation of the encryption process.

Video: The NSA and Surveillance... Made Simple - Animation (https://www.youtube.com/watch?v=GoM4jIZbTtQ) (2:52)

A captioned version of this video is available: The NSA and Surveillance... Made Simple - Animation (CC) (https://urldefense.com/v3/__https:/youtu.be/VMQhipM11lk__;!!BeImMA!7oEVIJrIYNNmlSUVYIKx_WMQfchhG0IKa9GjepszgaLJLhqRtfVlEi9IwoX6uERDkJMHdu5AJAh93GIKlOza87WbyovnnPA9SQ$)

A video transcript is available: Transcript for The NSA and Surveillance... Made Simple - Animation (https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?sourcedoc=%7BDAD591A0-C0D0-46B4-B423-85EE125CE109%7D&file=MAT%20260%20Transcript%20for%20The%20NSA%20and%20Surveillance...%20Made%20Simple%20-%20Animation.docx&action=default&mobileredirect=true)

Video: The Golden Key: FBI vs Apple iPhone (https://www.youtube.com/watch?v=6RNKtwAGvqc) (14:49)
This video features a discussion about the implications of unlocking an iPhone, and the concept of a "golden key" for encryption, which could have wide-ranging consequences for digital security and privacy, and the potential global ramifications of such actions.

A captioned version of this video is available: The Golden Key: FBI vs Apple iPhone (CC) (https://urldefense.com/v3/__https:/youtu.be/iWn5yu981q4__;!!BeImMA!7oEVIJrIYNNmlSUVYIKx_WMQfchhG0IKa9GjepszgaLJLhqRtfVlEi9IwoX6uERDkJMHdu5AJAh93GIKlOza87WbyotDSqHstw$)

A video transcript is available: Transcript for The Golden Key - FBI vs Apple iPhone (https://snhu.sharepoint.com/:w:/r/sites/LearningScienceAssessment/_layouts/15/Doc.aspx?sourcedoc=%7B7CE78517-107A-4A6E-829F-E04D7AF999F4%7D&file=MAT%20260%20Transcript%20for%20The%20Golden%20Key%20-%20FBI%20vs%20Apple%20iPhone%20-%20Computerphile.docx&action=default&mobileredirect=true)