Writing assignment: Public Key Cryptography

eSoc 488: Information Privacy with Applications

Due: 15 November 2018

Total Homework/Assignment Points: 100

Read Whitfield Diffie and Martin Hellman, 'New Directions in Cryptography.' Provide some historical context for the article, and a brief introductory paragraph on some of the main topics discussed in it. In the remainder of your writing, include answers to the following questions:

- The difference between "classical" and "public key" cryptography, as described in the article.
- What are the classes of threats that a cryptosystem may face? Give examples for each.
- What are the two approaches to securely transmitting keying material over an insecure channel? Describe each in detail.
- Which assumption about computational difficulty does the Diffie-Hellman key agreement protocol depend upon?
- Describe what a digital signature is.
- Describe what one-way authentication is. Give an example of it.