# CSci 4554 Assignment 11

**Due Friday, May 9 in class**

For this problem set you are asked to research the use of cryptographic algorithms in real-life applications. Specifically, you should focus on:

- What algorithms are used in the application? Please relate them to the algorithms that we studied in class. For instance, if the application uses digital signatures, what kinds of signature implementations and algorithms are acceptable for this protocol (DSS, ElGamal, etc.)? If it uses key agreement, what protocols and algorithms are used (STS, Diffie-Hellman, etc?)?
- How commonly is the application used? For instance, some secure versions of applications may be recommended or even mandated, but not commonly used, and less secure versions are used.
- What can you say about security of these applications, based on the above?

You may also discuss legal issues related to these applications if they mandate, restrict, or regulate certain algorithms or uses. For instance, if digital signatures are accepted as legally binding signatures, what conditions are mandated and why?
Requirements:

- You need to submit a 1-2 page paper on the subject. Don't forget a title and a bibliography (web references OK). The paper must be well-organized, well-written, and grammatically correct.
- The purpose of the application and the services it provides need to be explained. You may focus only on one aspect of the application. For instance, if it provides both data integrity and encryption, you may cover only one of the two.
- The work of the application should be described in detail (the algorithms used by each of the participants, in which order they are used, how are the keys determined, etc.). You may refer to algorithms and protocols covered in class without going into any details.
- Give a brief history of the application.
- Make sure to justify your claims about the security of the application by the known properties of the algorithms used. It is also OK to refer to articles on security of the application, but you need to give the summary of the argument in your own words.
- You need to prepare a 5-10 minutes presentation (slides are optional) to summarize your findings; be prepared to answer questions.

Some topic suggestions (feel free to choose your own):

- “Web of trust” systems, such as PGP and GnuPG.
- Public key infrastructure (PKI).
- LDAP (Lightweight Directory Access Protocol) authentication.
- X.509 or X.500 authentication.
- Random number generators used in practice.

These are just suggestions, you may consider very different applications, as long as you you satisfy the key points of the requirements.

Please enter your topic on the Wiki page so that there is no duplications. **Important:** the topics have to be chosen by Monday, May 5 at midnight. I will check them on Tuesday morning and may ask you to modify your topic. If you would like me to comment on your topic choice earlier, please email me.