6/15/16 - Quiz 1 - Erik Buschardt (CSSS 5260 WED)

1. Outline the case of Mary, Queen of Scots to include the factors related to the type of encryption methods used, the mistakes of Mary and her cohorts, the importance of this case to the field of encryption, and the lessons learned.

The case of Mary, Queen of Scots was one of the first military applications of encryption of its kind. Its failure was principally the result of a successful intervention between trusted cohorts, resulting in the beheading of Mary herself. The plot was to overthrow the queen of England while simulating an invasion by France, in order to establish Catholicism as the primary religion of the British Isles.

In Mary's desire to overthrow her government, she was overzealous and overlooked each level of detail required in the successful implementation of her plan, trusting aides and subordinates to figure out how to achieve the overall mission. In retrospect, this should have not been her plan of action, because each chain of events, each person trusted, each action taken, represents a vulnerability that eventually was exposed and defeated.

The importance to the field of encryption is its obvious military application between trusted parties within a planned coup d'etat.

2. Explain and outline the concept of Cryptanalysis, what it is, its linkage to the greater field of encryption, its sub-components, and its relevance in the modern field of digital encryption.

To the best of my understanding, cryptanalysis is the field of study that focuses specifically on the technical nature of decryption, and methodologies that emerge as a result of signature recognition, frequency analysis and other related linguistic and mathematical patterns that emerge from said analysis of encoded data or ciphertexts. Taking the verbiage apart, we get crypt, or hidden or vaulted message, with analysis, the careful and painstaking reverse engineering of encrypted messages.

In relation to the greater concepts of encryption, it does not deal with the encryption processes that can be strengthened as a result of the computation of decryption, but cryptanalysis can serve as lessons learned within the broader field of cryptology by providing examples of how easily a ciphertext can be decoded.

In that way, cryptanalysis makes the field of study of cryptology continuously stronger and more robust going forward.