**I have solicited McKinley Harmon to review my project and revised my work based off his feedback.**

**2. A textual summary of any interesting differences or common features that you observe:**

The Transport Layer Security properties of my ten selected websites show both common practices and notable differences. Most sites use RSA 2048-bit cryptographic keys, reflecting a strong and consistent security standard, though YouTube and X.com stand out for employing Elliptic Curve (EC 256-bit) keys, which provide equivalent security with greater computational efficiency. Nearly all sites use the SHA256withRSA authentication algorithm, but MyUTK and Microsoft Teams use SHA384withRSA, offering enhanced hash strength. Encryption is typically AES128GCM, except for, again, MyUTK and Microsoft Teams, which adopt AES256GCM, implying stronger encryption levels. All sites guarantee confidentiality, integrity, and forward secrecy, and none show revoked certificates. Issuers vary, with Amazon appearing most frequently, showing reliance on a major certificate authority. Overall ratings range from A to B, with most sites achieving A or A+, suggesting widespread adherence to modern TLS standards and only minor variation in cryptographic configurations or certificate issuers.

**3. List questions about any information you don’t understand or would like to know more about.**

A. Some sites use stronger or more secure encryption/hashing functions. Shouldn’t all sites be using stronger algorithms?

B. What are the risks of a revoked or expired certificate?

C. How often should organizations audit or update their TLS configurations?