2. The method by which I examined my websites was first using the openssl command and then matched the found cipher suite using the SSL labs for any missing information. All of my information is based on which cipher suite was used for my own connection. For the 10 websites I examined there were many commonalities between them; all of them used Elliptic Curve Diffie-Hellman, though three of them were ECDHE rather than just ECDH. The difference between these two was that for ECDH only one key is generated and used for the entire duration of the connection while with ECDHE a new key is used for every exchange made during this connection. Excluding most of Facebook, the rest of the cipher suites were nearly identical. Differences in the cipher suite only arrived when looking at the key sizes, where three had a key size of 128 with the rest at 256, and in hashing algorithm, where it was split down the middle using SHA256 and SHA384. They all used RSA in addition to Diffie-Hellman and, excluding Facebook and my.utk, they all used AES in GCM mode. My.utk also used AES but their encryption mode was in CBC instead of GCM. To discuss the outlier that is Facebook, they used a different encryption algorithm and mode from all of the rest with that being CHACHA20-POLY1305. Moving on from the cipher suite, there are a couple other things I noted for each website. To start off, I want to mention the rating given by SSL labs to each of the websites. Only a few got a rating of B and these sites were my.utk, Youtube, Amazon, and Facebook. The reason for all of them to have a lower rating than the rest is due to their continued support for TLS 1.0 and TLS 1.1, which are much more vulnerable in comparison to TLS 1.2 and beyond. The rest got a rating of A+, except for Steam which got an A for reasons that were not listed. Another item I listed was the version of TLS used to make my connection. All of them used TLS 1.3, except for my.utk, Stackoverflow, and Zoom which do not yet support TLS 1.3 and instead use TLS 1.2 which is still acceptable today.

3. The first website I would like to examine for this section is Facebook. They were the exclusive users of CHACHA20-POLY1305 which is known for being an algorithm that provides integrity, confidentiality, and authentication from its POLY1305 portion. POLY1305 uses MAC which allows it to send one time messages that give it the aforementioned qualities.
The second website I am going to examine is Discord, which is very similar to the remaining websites in that it uses Diffie-Hellman (Facebook also used Diffie-Hellman) and AES. Diffie-Hellman provides an algorithm that allows for a secure connection by allowing two parties to send each other values to calculate a set of keys for communication between them, it gives a near guarantee in authenticating information sent. The AES used here is 256-bit giving it both integrity and confidentiality as these large keys are incredibly hard to attack.
The third and final site I would like to discuss is my.utk. Their TLS is nearly identical to the way that discord and most of the other sites with a couple of key differences. First of all, they use ECDHE which is a little different from ECDHE in which every exchange creates a new key which in turn guarantees authenticity to a greater degree. The second is that they use CBC rather than GCM, this negatively affects it as a whole with authentication in particular being affected.

4.

- Why is CHACHA20 not as popular as AES? I've seen some comparisons online saying that in some cases it is better for TLS cipher.

- I noticed more cites than I would have thought supporting TLS 1.0 and 1.1, why would some high profile websites still be supporting this?
- Why does UTK use CBC rather than GCM? I would think that a college site would want to be as secure as possible. Is it just something that comes from the age of the site?

Peer Review: Ziad Tabet