Anthony Constantino
Project 6 TLS

Site	Key Exchange Method	Authentication Algorithm	Encryption Algorithm	Key Size	Mode	Cipher
Facebook	ECDHE	ECDSA	AES128	256	GCM	ECDHE-ECDSA-AES128-GCM-SHA256
Gmail	ECDHE	RSA	AES128	2048	GCM	ECDHE-RSA-AES128-GCM-SHA256
Wells Fargo	TLSv1/SSLv3		AES256	2048		AES256-SHA256
Citi	TLSv1/SSLv3		AES128	2048		AES128-SHA
Amazon	ECDHE	RSA	AES128	2048	GCM	ECDHE-RSA-AES128-GCM-SHA256
GitHub	ECDHE	RSA	AES128	2048	GCM	ECDHE-RSA-AES128-GCM-SHA256
Hotmail	ECDHE	RSA	AES256	2048		ECDHE-RSA-AES256-SHA384
Learning Suite	ECDHE	RSA	AES256	2048	GCM	ECDHE-RSA-AES256-GCM-SHA384
Twitch	ECDHE	RSA	AES256	2048	GCM	ECDHE-RSA-AES256-GCM-SHA384
DayBreak Games	ECDHE	RSA	AES256	2048	GCM	ECDHE-RSA-AES256-GCM-SHA384

It is interesting seeing that most sites are using public key sizes of 2048 bits other than Facebook. I am not sure why Facebook uses a smaller key size. This is good that they are choosing large key sizes so that they might last longer than shorter ones with the rate at which technology advances. Another thing I found interesting is that most all the Ciphers are almost all the same other than the MAC at the end which it seems that there are two popular SHA algorithms people are using SHA256 and SHA384. Most of the Ciphers that banks are using are much smaller than the other sites. Which doesn't contain the mode or the Authentication Algorithm. I am assuming this is because the information dealing with bank accounts is a little more important and for this reason maybe they are using some different technologies that don't give out as much information about what they are using.