Transport Layer Security

Website	Cipher Suite Name	Auth	KX	Cipher	MAC	PRF
booklist.byu.edu	ECDHE-RSA-AES256-SHA384	RSA	ECDHE	-	-	SHA384
google.com	ECDHE-RSA-AES128-GCM-SHA256	RSA	ECDHE	AES128-GCM	-	SHA256
zionsbank.com	ECDHE-RSA-AES256-GCM-SHA384	RSA	ECDHE	AES256-GCM	-	SHA384
cia.gov	ECDHE-RSA-AES256-GCM-SHA384	RSA	ECDHE	AES256-GCM	-	SHA384
inbox.google.com	ECDHE-RSA-AES128-GCM-SHA256	RSA	ECDHE	AES128-GCM	-	SHA256
facebook.com	ECDHE-ECDSA-CHACHA20-POLY1305	ECDSA	ECDHE	CHACHA20	POLY1305	
twitter.com	ECDHE-RSA-AES128-GCM-SHA256	RSA	ECDHE	AES128-GCM	-	SHA256
gamestop.com	ECDHE-RSA-AES128-GCM-SHA256	RSA	ECDHE	AES128-GCM	-	SHA256
amazon.com	ECDHE-RSA-AES128-GCM-SHA256	RSA	ECDHE	AES128-GCM	-	SHA256
fbi.gov	ECDHE-ECDSA-CHACHA20-POLY1305	ECDSA	ECDHE	CHACHA20	POLY1305	-

Observations

- All of the examples I researched use ECDHE as their key exchange method. From what I learned online, it is a variant of and significantly faster than the regular Diffie-Hellman key exchange algorithm.
- Facebook and the FBI websites use ChaCha20, which comes from the ChaCha family of ciphers. It is fairly new, published in 2008, and it aims to increase the diffusion per round while possibly achieving better performance than other stream ciphers.
- Along with ChaCha20, they also use Poly1305 as their Message Authentication Code. It is used to verify the data integrity and authenticity of a message. Because it uses AES, it is very secure.
- The aforementioned websites also use an Elliptic Curve Digital Signature Algorithm (ECDSA), which is a variant of DSA.
- Websites that deal with more valuable assets (banks, government, personal data, etc) tend to use pseudorandom functions with a larger quantity of bits.
- Most websites use GCM as their symmetric key cryptographic block cipher. This is because of its high efficiency and performance, since it takes advantage of parallel processing, among other things.
- I wonder at what point companies decide to move from one type of security protocol to another. What makes it so that there is a need to make something more secure?