Task 4.4

**TSL\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256**

Authentication:

* RSA for key exchange and signing
* ECDHE states that the elliptic curve diffie-hellman algorithm is used for the key exchange

Encryption:

* Symmetric encryption with AES 128 GCM
* 128 is the key size
* GCM states the mode used for encryption

Integrity:

* Hash function SHA256 is used to obtain integrity
* 256 states the size of the output

**TLS\_RSA\_RC4\_128\_MD5**

Authentication:

* RSA (see above)

Encryption:

* Symmetric encryption with RC4
* 128 bit long key is used

Integrity:

* Hash function MD5 is used

Three reason why the first suite is more secure:

1. RC4

RC4 takes a key and transforms it into a long random string, which is XORed with the plain text. At this point, it was detected that the random generator isn’t that random and with the help of a large amount of connection of the same encrypted data, this data can be decrypted by obtaining resembling pattern. Therefore an amount of connections is needed.

Source: http://www.heise.de/security/meldung/Erneuter-Krypto-Angriff-auf-SSL-TLS-Verschluesselung-1822963.html

1. MD5

With the help of a collision attack it is possible to get the same output from MD5 for two different inputs. Such that for the MD5 hash algorithm computes . The attack could enforce a collision at digital certificates.

Source: http://www.heise.de/security/artikel/Konsequenzen-der-erfolgreichen-Angriffe-auf-MD5-270106.html

1. RC4

Various sources claim that the NSA decrypt RC4 encryption in real time. These experts advises to stop using the RC4 algorithm, because it isn’t safe anymore.

Source: http://www.heise.de/security/meldung/Erneuter-Krypto-Angriff-auf-SSL-TLS-Verschluesselung-1822963.html