Here I will upload screenshots and provide explanations for the different certification authorities providing verification that the [www.uib.no](http://www.uib.no) website is secure. For each of them show what digital signature algorithm was used to authenticate them, what their public key is, and what the public parameters that were used in the algorithm (e.g. the prime number p for RSA).

There will be screenshots showing how and where for the different information, including my name in the screenshot.

To find the certificate we can click on the lock-icon next to the URL:

Et bilde som inneholder Nettsted

Automatisk generert beskrivelse

Onwards, you click “Connection secure” and “More information” (could not use the snippet tool while clicking through this part). And you end up with this window:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Here we click “View certificate” and we end up with a page in the web browser showing us different kinds of information related to the certificate for the website.

At the top, it is showing us the hierarchy of verification where left-most is at the bottom and right at the top:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

For **www.uib.no** itself, this was the signature algorithm used:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Their public key:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

For the public parameters used in RSA, you can see on the screenshot above that the prime number used is the modulus value in hexadecimal there. You could translate this into decimal, but it would be a really big number so I chose not to write it down. The modulus is made up of two prime numbers.

The certificate authority above uib.no that verified UiB is Sectigo RSA Organization Validation Secure Server CA.

Similarly for this authority, it used RSA. But this time with SHA-384:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

The public parameters for the RSA algorithm:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

With modulus being the combined (multiplied) number of two smaller primes P and Q.

The last and larger certificate authority that verified the first certificate authority mentioned above, is USERTrust RSA Certification Authority.

Similar signature algorithm as with the certificate authority below.

Et bilde som inneholder tekst

Automatisk generert beskrivelse

And the RSA public parameters:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

It has a bigger key size than the certificate authority below, with a key size of 4096.

Modulus being the combination of the prime numbers, p and q.