Oppgave 1 - AES a little history

Since May 26, 2002, the AES (Advanced Encryption Standard) describes the official standard of the US government.

1. The evolutionary history of AES differs from that of DES. Briefly describe the differences of the AES history in comparison to DES.

The evolutionary history of AES differs significantly from that of DES.

AES, which is a variant of the Rijndael block cipher, was developed by two Belgian cryptographers as part of the NIST “AES selection process”. DES was exclusively developed by IBM and was subsequently adopted as a federal standard in the United States.

One of the most critical distinctions lies in key length. AES provides support for longer key sizes while DES is limited to a short 56-bit key. The relatively short key size of DES is a big factor in why it is no longer considered secure for modern cryptographic applications.

2. What is the name of the algorithm that is known as AES?

The original name for the algorithm known as AES is Rijndael.

3. Who developed this algorithm?

AES was developed by two Belgian cryptographers named Joan Daemen and Vincent Rijmen during the NIST AES selection process.

4. Which block sizes and key lengths are supported by this algorithm?

AES supports block size of 128 bits with key lengths 128, 192, and 256 bits