

Data Security 27.3.2009

- What is authentication? (2p)
 - How time demanding is it to compute the greatest common divisor of two n digit numbers? (2p)
 - What is discrete logarithm? (2p)
 - What is Kerberos used for? (2p)
- What phases does the AES (or Rijndael) consist of? (4p)
 - Compute $2F \bullet A5$ in $GF(2^8)$, as it is done in AES. (4p)
- Construct $EC_5(2, 1)$ and compute $2P$ and $3P$ for $P = (0, 1)$. (8p)
- Sign message "YES". Hash the message by splitting it to 4-bit blocks and bitwise XORing the blocks. In signing use RSA constructed of the primes $p = 3$ and $q = 11$, and the public encryption key $e = 3$. The ASCII codes of Y, E, and S in hexadecimal are 59, 45 and 53. (8p)
- What is the zero information proof and for what can it be used? (8p)