Homework 2
Due: 23:59, Monday, 04/02/2018

1. (20 points) In this problem, we want to compare the computational performance of symmetric and asymmetric algorithms. Assume a fast public-key library such as OpenSSL (http://www.openssl.org/) that can decrypt data at a rate of 100 Kbit/sec using the RSA algorithm on a modern PC. On the same machine, AES can decrypt at a rate of 17 Mbit/sec. Assume we want to decrypt a movie stored on a DVD. The movie requires 1 GByte of storage. How long does decryption take with either algorithm?

2. (15 points) Encrypt and decrypt by means of the RSA algorithm with the following system parameters: $p = 3$, $q = 11$, $d = 7$, $x = 5$.

3. (15 points) Compute the two public keys and the common key for the DHKE scheme with the parameters $p = 467$, $\alpha = 2$, $a = 400$, and $b = 134$.

4. (30 points) We state that sender (or message) authentication always implies data integrity. Why? Is the opposite true too, i.e., does data integrity imply sender authentication? Justify both answers.

5. (20 points) Compute the output of the first round of stage 1 of SHA-1 for a 512-bit input block of (1) $x = \{0...00\}$ and (2) $x = \{10...00\}$ (i.e., the 1st bit is one). Ignore the initial hash value H_0 for this problem (i.e., $A_0 = B_0 = ... = 00000000_{hex}$).