*IV054 Coding, Cryptography and Cryptographic Protocols*
**2011 - Exercises V.**

1. Determine the last digit of $7^{(7^7)}$. Explain your reasoning.

2. Let $(n, e_1)$ and $(n, e_2)$ be public keys for the RSA cryptosystem. Let $n = 4019989$, $e_1 = 831391$ and $e_2 = 363173$. Bob encrypts his message $m$ with both public keys to obtain $c_1$ (using $(n, e_1)$) and $c_2$ (using $(n, e_2)$):
$$c_1 = 3198255,\ c_2 = 2125927$$
Without factorization, find Bob's message $m$.

3. To establish their common key, Alice and Bob use the Diffie-Hellman protocol with $p = 863$ and $q = 5$. Let $x = 27$ and $y = 33$ be secret exponents used by Alice and Bob, respectively. Perform in detail steps of the protocol and determine $X$, $Y$ and $K$.

4. Consider the RSA cryptosystem. Let $e = 551$ and $n = 1517$. Decrypt the following cryptotext:
$$1374,\ 1278,\ 682,\ 809,\ 890,\ 380,\ 0,\ 57$$

5. Consider the Knapsack cryptosystem with modulus $m = 701$, $u = 200$ and the following superincreasing sequence:
$$(1, 4, 9, 25, 41, 82, 170, 333).$$
   (a) Determine the public key.
   (b) Encrypt message 10010101 and decrypt the result.

6. Alice, Bob and Eve use the RSA cryptosystem with $n = 99443$. Let $e_A = 7883$, $e_B = 5399$ and $e_E = 1483$ be the corresponding public key exponents. Messages are written in ASCII, divided into blocks of length 5, each block is encrypted separately. Imagine that you are Eve and you have captured the following message intended for Bob which was sent by Alice:
```
16278490204355400279
```
You know your $d_E = 3931$. Decrypt the cryptotext (Do not use brute force).