2007 - Exercises V.

1. Consider the following assignment of numerical equivalents to a 40-letter alphabet. The letters A, B, ..., Z are given their numerical equivalents 0 to 25, respectively, a blank space = 26, . = 27, ? = 28, \$ = 29 and the numerals 0, 1, ..., 9 are assigned 30, 31, ..., 39, respectively. Using this alphabet, a message is encoded into a string of numbers by taking each pair of symbols in the message, converting the pair to their numerical equivalents, say a and b, and replacing the pair by the number $40a + b$. If this method is used to convert a message to a numerical sequence and then the sequence is encrypted by the RSA cryptosystem, explain how the message could be decrypted without knowing the factorization of the public modulus.

2. Suppose that $n = 1363$ in the RSA cryptosystem and it has been revealed that $\varphi(n) = 1288$. Use this information to factor n.

3. Suppose that $X' = (1987, 439, 1394, 724, 339, 2303, 1256, 810, 650)$ and $m = 2503$ in the Knapsack cryptosystem. Decrypt the cryptotext $c = 3155$.

4. Suppose that Alice, Bob and Charles have the same encryption exponent $e = 3$ for the RSA cryptosystem. Let their moduli be n_A, n_B and n_C. Suppose that $\gcd(n_i, n_j) = 1$ for each $i, j \in \{A, B, C\}$. Suppose that Dennis sends the same message m to all of them. This means he sends the cryptotexts $c_A = m^3 \bmod n_A$, $c_B = m^3 \bmod n_B$ and $c_C = m^3 \bmod n_C$. Show how it is possible to compute m from the public information without factoring the moduli.

5. Let $(n = pq, e)$ be a public key and let d be the corresponding secret key for the RSA cryptosystem. Let m be a plaintext of the form $m = kp + 1$ for some $k \in \mathbb{N}$. Show how one can efficiently compute d knowing only the cryptotext $c = m^e \bmod n$.

6. Two users, Ari-Pekka and Saku, use the RSA cryptosystem with the same modulus n and encryption exponents e_A and e_S with $\gcd(e_A, e_S) = 1$.
   Hannu sends the message m to both Ari-Pekka and Saku. Olli intercepts $c_A = m^{e_A} \bmod n$ and $c_S = m^{e_S} \bmod n$. Olli then computes $x_1 = e_A^{-1} \bmod e_S$ and $x_2 = (x_1 e_A - 1)/e_S$.
   (a) How can Olli compute m from intercepted ciphertexts c_A, c_S using x_1 and x_2?
   (b) Use the proposed method to compute m if $n = 18721$, $e_A = 43$, $e_S = 7717$ and you intercept ciphertexts $c_A = 12677$ and $c_S = 14702$.

7. (a) Consider a Diffie-Hellman scheme with $q = 3$ and $p = 353$. Alice chooses $x = 97$ and Bob chooses $y = 233$. Compute X and Y and the key k.
   (b) Consider a Diffie-Hellman scheme with $q = 2$, $p = 11$, $X = 9$ and $Y = 3$. Compute x and y.
   (c) Design the extension of the Diffie-Hellman key exchange that allows three parties Alice, Bob and Charlie to generate a common secret key.