IV054 Coding, Cryptography and Cryptographic Protocols

2008 – Exercises V.

1. Which of the following pairs is a good choice for the Diffie-Hellman protocol. Explain your reasoning. Omit the fact that the numbers are very small:
   (a) $q = 1$, $p = 179$;
   (b) $q = 2$, $p = 181$;
   (c) $q = 14$, $p = 197$.
2. Suppose that Alice wants to send a message 1001111001 to Bob using the Knapsack cryptosystem with $X = (3, 6, 10, 22, 43)$, $m = 97$ and $u = 13$.
   (a) Find Bob's public key X'.
   (b) What is the cryptotext c computed by Alice?
   (c) Perform in detail Bob's decryption of c.
3. Suppose that the RSA cryptosystem is used. Angela sends $m^e \equiv c \pmod{n}$ to Bert. However, malicious Manfred intercepts c, selects a random $y \in \mathbb{Z}_n$ and sends $cy^e \equiv c' \pmod{n}$ to Bert. Not knowing this, Bert computes $m' = c'^d \pmod{n}$ and sends m' to Angela.
   How can Manfred retrieve m from m'?
4. Let n be an odd number. Consider the following version of the Miller-Rabin primality test. The number $n-1$ is written as $n - 1 = 2^s m$ where m is odd. Then a number $a \in \{1, \dots, n-1\}$ is chosen and the numbers

$$\begin{aligned} x_0 &= a^m \bmod n, \\ x_{k+1} &= x_k^2 \bmod n, \end{aligned}$$

   where $k \in \{0, \dots, s-1\}$, are computed. Show that if n is prime, then either $x_0 = 1$ or $x_k = n - 1$ for some $k < s$.
5. Suppose that Bob uses the RSA cryptosystem with a large modulus n for which the factorization cannot be found efficiently. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer from the set $\{0, \dots, 25\}$ and then encrypting each character separately. Describe how Eve can decrypt a message which is encrypted in this way.
6. Let (n, e) be a public key for the RSA cryptosystem. Prove that there exists an integer r such that $m \equiv c^{e^r} \bmod n$ for every plaintext m and its corresponding ciphertext c.
7. Consider the RSA cryptosystem where q is much larger than p. Assume that a message being encrypted is smaller than p so that one can efficiently decrypt a message by computing $m' = c^d \bmod p = m$.
   Show that a single chosen-ciphertext attack is sufficient to break this version of the RSA cryptosystem.