IV054 Coding, Cryptography and Cryptographic Protocols

2009 – Exercises V.

1. Let (n, e) be a public key for the RSA cryptosystem.
   An integer $m \in \{1, 2, \dots, n-1\}$ is called a fixed point if $m^e = m \pmod{n}$.

   Show that if m is a fixed point then $n - m$ is also a fixed point.

2. Let $n = pq$ where p, q are large primes. Show that there is an integer $e > 1$ such that $gcd(e, (p-1)(q-1)) = 1$ and for any integer m it holds that $m^e = m \pmod{n}$, *ie.* each m is a fixed point.

3. Let $n = 54105049$. Suppose that Eve was able to determine the value $\varphi(n) = 54090036$. How can Eve determine the prime factors of n.

4. Let $n = pq$ where p, q are large primes. Consider a file system with n files $F_1, F_2, \dots, F_n$. Let $e_1, e_2, \dots, e_n$ be integers such that $gcd(e_i, e_j) = 1$ and $gcd(e_i, (p-1)(q-1)) = 1$ for any $i \neq j$. These integers are made public.

   For each i the file F_i is encrypted somehow and the decryption key is $k_i = r^{\frac{1}{e_i}} \pmod{n}$ where r is an integer. Let $S \subseteq \{1, \dots, n\}$ and $b = \prod_{i \in S} e_i$. Suppose that Alice is given $k_A = r^{\frac{1}{b}} \pmod{n}$ and she knows the set S. Show that she can decrypt any file F_i such that $i \in S$.

5. Alice and Bob want to establish a common secret key using the Diffie-Hellman key establishment protocol with $p = 1511$ and $q = 97$. Alice has chosen $x = 126$, Bob $y = 534$. Compute X, Y and a shared key K.

6. Bob sets up the Knapsack cryptosystem with $X = (2, 5, 8, 17, 35, 70)$, $m = 191$, $u = 34$ so that Alice can send him messages.

   a) Determine Bob's public key X'.

   b) Encode messages 101010 and 100010.

   c) Decode in detail cryptotexts $c_1 = 370$ and $c_2 = 383$.

7. Alice and Bob share a secret large prime s. They are using the RSA cryptosystem and the following scheme for encrypting a secret message $m = m_1 m_2 ... m_k$ where m_i are alphabetic characters. Each character m_i is represented as a digit, *eg.* 'a' $= 0$, 'b' $= 1, \dots,$ 'z' $= 25$. Encryption proceeds as follows.

   $$c_1 = s \oplus e(m_1),$$

   $$c_{i+1} = c_i \oplus e(m_{i+1}),$$

   where $0 < i < k$.

   Is the proposed scheme secure?

8. Consider the RSA scheme with $n = 1073$ and $e = 949$. You know the following plaintext-ciphertext pairs:

   $$e(157) = 12, \quad e(2) = 533, \quad e(933) = 970$$

   Without factoring or brute-force attack decrypt the ciphertext $c = 893$. Explain your reasoning. (Hint: One of the exercises above.)