T-79.4501 Cryptography and Data Security
2007 / EXAM
Monday, October 29, 2007, SOLUTIONS

1. (6 pts) The operation of the *Atbash cipher* on the English alphabet (A=0, B= 1 ,...,Z=25) is as follows: $C(x) = 25 - x \bmod 26$, for $x \in \{0, 1, 2, ..., 25\}$. Denote the key of the shift cipher by K. Then the ciphers commute if and only if $(25-x)+K \equiv 25-(x+K) \pmod{26}$, for all $x \in \{0, 1, 2, ..., 25\}$. This happens exactly if $2K \equiv 0 \pmod{26}$. We get two solutions $K = 0$ or $K = 13$, from which $K = 13$ is the non-trivial one. If $K = 0$ then the Shift cipher has no effect, and the ciphers commute trivially.

2. See lectures.

3. (6 pts) The 8-bit constants C_i, $i = 8, 9, 16$ are computed in polynomial arithmetic modulo $m(x) = x^8 + x^4 + x^3 + x + 1$, as

$$\begin{aligned} C_8 &= 2^7 = 10000000_2 = 128 \\ C_9 &= 2^8 = 00011011_2 = 27 \\ C_{16} &= 2^{15} = x^7 \cdot x^8 = x^7(x^4 + x^3 + x + 1) = x^5 + x^3 + x^2 + x + 1 = 00101111_2 = 47. \end{aligned}$$

4. Consider the RSA cryptosystem with modulus $n = 101 \cdot 131 = 13231$.

   (a) (2 pts) $\phi(13231) = 100 \cdot 130 = 13000$ and $\gcd(4563, 13000) = 13$. Therefore 4563 cannot be used as the encryption exponent for RSA with modulus 13231.

   (b) (2 pts) The private decryption exponent d using $e = 1323$ is computed as $d = e^{-1} = 6387 \bmod 13000$ using the Extended Euclidean Algorithm.

   (c) (2 pts) $x_1 = c^d = 202^{6387} \bmod 101 = 0 \bmod 101$ and $x_2 = c^d = 202^{6387} \bmod 131 = 71^{17} \bmod 131$, where 202 is reduced modulo 131 and the exponent 6387 is reduced modulo 130. Using Square-and-Multiply Algorithm, we get that $x = 92 \bmod 131$. Since $x_1 = 0$, the Chinese Remainder Theorem gives $x = x_2 \cdot (M_2^{-1} \bmod m_1)m_2 \bmod M = 92 \cdot 48 \cdot 101 \bmod 13231 = 9393$, where we used $(M_2^{-1} \bmod m_1) = 101^{-1} \bmod 131 = 48$ computed using the Extended Euclidean Algorithm.

5. (6 pts) Now Alice computes the shared key as $K = 660^a \bmod 1031$ and Bob computes it as $K = 619^b \bmod 1031$. Knowing the subgroup consisting of 5 elements $\{1, 518, 264 = 518^2, 660 = 518^3, 619 = 518^4\}$ Carol gets that $K = 518^{3a} = 518^{4b} \bmod 1031$. Hence K is also in the small subgroup, and the only integers $a, b \in \{0, 1, 2, 3, 4\}$ that satisfy $3a = 4b \bmod 5$ are $a = 4$ and $b = 3$, from which Carol gets $K = 518^{12} = 518^2 = 264$.