T-79.4501 Cryptography and Data Security
2006 / Homework 5
Mon 20.2 and Wed 22.2

1. Show that the multiplicative order of $g = 8 = 2^3$, in modulo 19 arithmetic, is equal to 6.

2. Consider polynomial arithmetic with polynomial $x^3 + x + 1$ on the set of three-bit integers. Determine the discrete logarithm of $6 = \texttt{110}$ to the base $2 = \texttt{010}$.

3. Consider the polynomial arithmetic of four-bit numbers using the polynomial $x^4 + x + 1$. Then, all non-zero numbers form a cyclic group of order 15. Alice and Bob use Diffie-Hellman in this cyclic group with the generator element $g = 3 = \texttt{0011}$. Alice's secret exponent $a = 7$ and Bob's secret exponent $b = 5$. Compute the Diffie-Hellman key K.

4. Alice is using a toy version of the DSS signature scheme with a prime modulus $p = 47$ and generator $g = 2$ of order $q = 23$. By accident, Alice generates signatures for two different messages with the same per-messages random number k. The hash codes of the two signed messages are 2 and 3 and the signatures are (4, 21) and (4, 19), respectively. Compute Alice's private key.

5. Alice and Bob use Diffie-Hellman Key Exchange to establish a shared secret key for their encrypted email application. After they computed the shared secret Diffie-Hellman key $K = g^{ab}$ they verify that they have got the same value for K. For this purpose they compute a four digit hash value $h(K)$ and compare the computed values by phone to ensure that they are equal. Suppose there is a man-in-the-middle C. Show how C can perform the man-in-the-middle attack in such a way that $h(g^{ac}) = h(g^{bd})$, with some values c and d chosen by C, that is, the attack is successful and remains undetected. What kind of computations C must do, and what is the expected amount of computations it must do to make the attack succeed? Consider the following two cases:

   (a) Alice sends her public value first, and Bob sends his public value only after he received Alice's value.

   (b) Alice and Bob send their public values in any order.