Deadline: April 7th

Name:

Exercises

1) Write the scheme of the baby-step giant-step algorithm to solve $2^x \equiv 15 \pmod{19}$.

2) Suppose that a wise attacker A has invented a machine to solve Diffie-Hellman problem, i.e. A knows an efficiently computable function f such that $f(g^a, g^b) = g^{ab}$. Show that A can break the ElGamal cryptosystem using the public key.

3) Write the computations to get $5^{101} \pmod{127}$ by the repeated squaring method (fast powering algorithm).

4) Suppose you know that a message has been encryted with the ElGamal cryptosystem using a random exponent less than 20. How would you try to cryptanalyze it? Note: We assume that g, p and the public key are public domain.

5) Consider $\mathbb{F}_8$ in the form $\mathbb{F}_2[X]/\langle X^3 + X + 1\rangle$. Check that X is a generator of $\mathbb{F}_8^*$ and write the complete table of logarithms of the elements of $\mathbb{F}_8^*$ to base X.