Cryptography

Problem set 10 - 11-12 VI 2015

1. Present a proof of GMW algorithm [1] with "NAND" gate.
2. Fermat factored a positive integer n by writing it as $n = x^2 - y^2 = (x - y)(x + y)$. Factor $n = 13199$ by this method. Is this a general facoring that works for all composite integers? What is the running time of the algorithm – use $L_n[u, v]$ notation.
3. Use the $p - 1$ method to factor:
   (a) $n = 138277151$,
   (b) $n = 18533588383$.
4. The *random square* method of Dixon is similar to the *quadratic sieve* factoring method. The major difference is that the relations are found by factoring $x^2 \bmod n$, where x is a random number in $\{1, \ldots, n - 1\}$. Use the random square method to factor n with the smallest possible factor base.
5. Factor 11111 using the quadratic sieve.
6. Draw the function $f(k) = L_{2^k}[1/2, 1]$ for $k \in \{1, 2, \ldots, 2048\}$.
7. Solve the DL problem $3^x = 693 \bmod 1823$ using the baby-step giant-step algorithm.
8. Use the baby-step giant-step algorithm to compute the discrete logarithm of 15 to the base 2 mod 239.

References

[1] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 218–229. ACM, 1987.