Dartmouth College Department of Mathematics
Math 75 Cryptography
Spring 2022

Problem Set # 7 (upload to Canvas by Tuesday, May 24, 12:00 pm EDT)

Problems:

1. For the following integers either provide a witness for the compositeness of n or conclude that n is probably prime by providing 5 numbers that are not witnesses. Recall that a witness for the compositeness of n is an integer $a \in \mathbb{Z}$ such that, if we write $n-1 = 2^k u$, where u is odd, then a satisfies $a \not\equiv 0 \pmod{n}$ and $a^u \not\equiv 1 \pmod{n}$ and $a^{2^i u} \not\equiv -1 \pmod{n}$ for all $i = 0, \ldots, k-1$.

(a) $n = 1009$.

(b) $n = 2009$.

2. Using big-O notation, estimate the number of bit operations required to perform the witness test on $n \in \mathbb{Z}_{>0}$ enough times so that, if n passes all of the tests, it has less than a 10^{-m} chance of being composite.

3. Factor 53477 using the Pollard rho algorithm.

4. Fermat and sieving.

(a) Find three nontrivial factors of $n = 99999999999999999999999999999999919$ by hand.

(b) Let $n = 2^{29} - 1$. Given that

$$\begin{aligned} 258883717^2 &\equiv -2 \cdot 3 \cdot 5 \cdot 29^2 \pmod{n} \\ 301036180^2 &\equiv -3 \cdot 5 \cdot 11 \cdot 79 \pmod{n} \\ 126641959^2 &\equiv 2 \cdot 3^2 \cdot 11 \cdot 79 \pmod{n} \end{aligned}$$

discover a factor of n.

5. Discrete logarithms.

(a) Let $p = 101$. Compute $\log_2 11$ (using complete enumeration by hand).

(b) Let $p = 27781703927$ and $g = 5$. Suppose Alice and Bob engage in a Diffie-Hellman key exhange; Alice chooses the secret key $a = 1002883876$ and Bob chooses $b = 21790753397$. Describe the key exchange: what do Alice and Bob exchange, and what is their common (secret) key? *[You may want to use a computer!]*

(c) Let $p = 1021$. Compute $\log_{10} 228$ using the baby step-giant step algorithm. Show the output of, and explain all steps in, your computation.

(d) Let $p = 1801$. Compute $\log_{11} 249$ using the Pohlig–Hellman algorithm. Show the output of, and explain all steps in, your computation. You'll want to remind yourself of how to solve systems of congruence equations using Sunzi's theorem: To find $x \in \mathbb{Z}$ satisfying $x \equiv a_i \pmod{n_i}$ for $i = 1, \ldots, k$, first define integers $N_i = \prod_{j \neq i} n_i$ and $M_i \equiv N_i^{-1} \pmod{n_i}$ for all $i = 1, \ldots, k$, and then $x = \sum_{i=1}^{k} a_i N_i M_i$ works.