Dartmouth College Department of Mathematics
Math 75 Cryptography
Spring 2020

Problem Set # 7 (upload to Canvas by Friday, May 22, 11:30 am 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 $i = 1, \dots, k-1$.

(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. Sieving.

(a) Find a nontrivial factorization of $n = 999999999999999919$ by hand.

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

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

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!]*

6. Let $p = 1021$. Compute $\log_{10} 228$ using the baby step-giant step method.