

Midterm practice

These are sample problems similar to what you might find on the Midterm.

Instructions: *Show all of your work. Answers without sufficient justification will receive little or no credit.*

1. *Define the following concepts*

(a) *A primitive root modulo a prime p*

(b) *The Jacobi symbol*

(c) *The RSA Algorithm*

(d) *Diffe-Hellman key exchange algorithm*

2. *State and prove the Chinese Remainder Theorem.*

3. Prove that if p is a prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

4. Describe the Baby Step-Giant Step and Pohlig-Hellman algorithms for computing discrete logarithms. Illustrate their use by computing $L_5(10)$ for $p = 23$ and $L_3(12)$ for $p = 17$.

5. Describe how to factor $n = pq$ if you know $\phi(n)$. Factor $n = 254333$ using $\phi(n) = 253308$.

6. Compute the first four convergents of the continued fraction of $\sqrt{5}$

7. Solve the congruence $2x^2 + 7 \equiv 1 \pmod{11}$

8. Find the four-term recurrence relation defining the LFSR

10100111010011101...

and find its period.

9. Other problems similar to the Homework.