Cryptography 3/2

Reagan Shirk

March 2, 2020

Midterm Practice

Problem 1

- Find a prime factor of $(5^{15}-1)/4$

$$5^{15}-1 = \frac{5-1}{4}(5^{14}+5^{13}+\cdots)$$
$$(5^3)^5-1 = \frac{5^3-1}{4}(5^{12}+5^9+\cdots)$$
$$\frac{5^3-1}{4} = \frac{5-1}{4}(5^2+5+1) = 31$$

- $x^n-1 = (x-1)(x^{n-1}+x^{n-2}+\cdots)$ is a useful equation
- You want to make sure you're working with the smallest exponent possible to reduce the amount of time you're spending on the problem
  - i.e. reducing 5^3 instead of 5^5 which would've given the same answer but taken more time
- Remember polynomial factorization

Problem 2

- If a group in G, an element g has order 169. What is the order of g^{51}?

$$g^a = \frac{ord(g)}{gcd(a, ord(g))}$$

$$ord(g^{51}) = \frac{ord(g)}{gcd(51, ord(g))}$$

$$= \frac{169}{gcd(51,169)}$$
$$= 169$$

Problem 3

- Calculate the subgroup generated by x in $(\mathbb{F}_2[x]/(x^3+x+1))*$

$$
\begin{aligned}
&x \\
&x^2 \\
&x^3 = x + 1 \\
&x^4 = x^2 + x \\
&x^5 = x^3 + x^2 = x^2 + x + 1 \\
&x^6 = x^3 + x^2 + x = x^2 + 1 \\
&x^7 = x^3 + x = 1
\end{aligned}
$$

Problem 4

- Compute the multiplicative inverse of $x^6 + 1$ modulo $x^8 + x^4 + x^3 + x + 1$ over $\mathbb{Z}/2\mathbb{Z}$ using Extended Euclidean Algorithm. You need to show steps

$$
\begin{aligned}
x^8 + x^4 + x^3 + x + 1 &= x^2(x^6 + 1) + (x^4 + x^3 + x^2 + x + 1) \\
100011011 &\div 1000001 \\
x^6 + 1 = (x^2 + x)(x^4 + x^3 + x^2 + x + 1) &+ (x + 1)
\end{aligned}
$$

Problem 5

- Compute $18^{20^{20}} \bmod 28$
- Use the chinese remainder theorem

$$
\begin{aligned}
28 &= 4 \times 7 \\
18^{20^{20}} \bmod 4 &= 2 \\
2^{20^{20}} &= 0 \\
\text{Uh oh, zero divisor. Try mod 7} \\
18^{20^{20}} \bmod 7 &= 4 \\
&= 4^{2^{20} \bmod 6} \\
&= 4^4 \bmod 7 \\
&= 4
\end{aligned}
$$