Cryptology - Week 8 solutions

Here are worked solutions to all except for question 4.

1. (a) As 9 has order 50, we need to compute $a \pmod{50}$. The baby-step (up to $\lfloor\sqrt{50}\rfloor$) gives

$$\begin{aligned}
9^0 &= 1\\
9^1 &= 9\\
9^2 &= 81\\
9^3 &= 22\\
9^4 &= 97\\
9^5 &= 65\\
9^6 &= 80\\
9^7 &= 13
\end{aligned}$$

(computed in SageMath). The SageMath command GF(101)$(9^8)^{-1}$ returns 19, so the giant step gives

$$\begin{aligned}
17 \cdot 19^0 &= 17\\
17 \cdot 19^1 &= 20\\
17 \cdot 19^2 &= 77\\
17 \cdot 19^3 &= 49\\
17 \cdot 19^4 &= 22 = 9^3.
\end{aligned}$$

Therefore $a = 3 + 4 \cdot 8 = 35$.

2. (a) Using SageMath, I compute that the order of 3 in $\mathbb{F}_{17}$ is 16, so a is defined mod 16. Hence G_i is defined mod 17, and b_i and c_i are

defined mod 16. Then

$$\begin{aligned}
(G_0, b_0, c_0) &= 3, 1, 0\\
(G_1, b_1, c_1) &= 9, 2, 0\\
(G_2, b_2, c_2) &= 10, 3, 0\\
(G_3, b_3, c_3) &= 12, 3, 1\\
(G_4, b_4, c_4) &= 2, 4, 1\\
(G_5, b_5, c_5) &= 4, 8, 2\\
(G_6, b_6, c_6) &= 15, 8, 3\\
(G_7, b_7, c_7) &= 11, 9, 3\\
(G_8, b_8, c_8) &= 2, 2, 6.
\end{aligned}$$

We stop here as $G_4 = G_8$, which in turn implies that $b_4 + ac_4 \equiv b_8 + ac_8 \pmod{16}$, hence $a = 10$.

3. (a) The multiplicative order of 31 (mod 107) is 106 (checked in SageMath), so I need to compute $a \pmod{106}$. By searching over increasing powers of $31 \pmod{107}$ in SageMath, I find the equations

$$31^3 \equiv 3^2 \cdot 5 \pmod{107} 31^{10} \equiv 3 \cdot 5^2 \pmod{107} 31^{17} \equiv 2 \cdot 3^2 \pmod{107},$$

which taking discrete logs base 31 gives

$$\begin{aligned}
3 &\equiv 2\log_{31}(3) + \log_{31}(5) \pmod{106}\\
10 &\equiv \log_{31}(3) + 2\log_{31}(5) \pmod{106}\\
17 &\equiv \log_{31}(2) + 2\log_{31}(3) \pmod{106}.
\end{aligned}$$

Solving this system gives

$$\begin{aligned}
\log_{31}(3) &= 34\\
\log_{31}(2) &= 55\\
\log_{31}(5) &= 41.
\end{aligned}$$

Then

$$39 \cdot 31 \equiv 2^5 \pmod{107},$$

so

$$a + 1 \equiv 5 \cdot 55 \pmod{106},$$

hence $a = 62$.

(b) There are multiple answers to this. Possibly the easiest (but not necessarily the most efficient) is to always choose the factor base made up of the first $\log_2(p)$ primes.

4. (not included, see individual feedback).

5.* (a) $f(0) = f(1) = 1$, so f has no roots mod 2 and hence is irreducible, so this is valid.

(b) f factors as $x \cdot x$, so this is invalid.$p = 2$ and $f(x) = x^2$.

(c) $f(1) = 0$, so $(x - 1)$ is a factor of f, hence this is invalid.

(d) $f(1) = 0$, so $(x - 1)$ is a factor of f, hence this is invalid.

6.* Consider the finite field

$$\mathbb{F}_{2^9} = \left\{ \sum_{i=0}^{8} a_i x^i : a_i \in \mathbb{Z}/2\mathbb{Z},\, x^9 + x^4 + 1 \equiv 0 \pmod 2 \right\}.$$

Let $g = x$; then g generates $\mathbb{F}_{2^9}^*$ as a multiplicative group (you do not have to prove this).

Using index calculus with a factor base of

$$\{x + 1, x^4 + x + 1, x^2 + x + 1\},$$

compute $a \pmod{2^9 - 1}$ such that $g^a = x^4 + x$.

I define the given finite field $F29$ and its generator x in SageMath with the commands

```
P.<y> = PolynomialRing(GF(2))
F29.<x> = GF(2).extension(y^9 + y^4 + 1)
```

Then using the SageMath commands

```
PZ.<X> = PolynomialRing(ZZ)
for a in range(70):
    a,PZ(x^a).factor()
```

I find that

$$\begin{aligned} x^{19} &= x^4 + x + 1 \\ x^{39} &= (x + 1)^2(x^2 + x + 1) \\ x^{69} &= (x^2 + x + 1)^2. \end{aligned}$$

Taking discrete logs and solving mod $2^9 - 1$ gives

$$\begin{aligned} \log_x(x^2 + x + 1) &= 290 \\ \log_x(x + 1) &= 130 \\ \log_x(x^4 + x + 1) &= 19. \end{aligned}$$

Then observe that $g^a = x(x + 1)(x^2 + x + 1)$, which we now know $= x \cdot x^{130} \cdot x^{290}$, so $a = 421$.