Solutions for TMA4160 Cryptography, 2012 exam

Problem 1 Notice that the pattern of letter repetitions in `baboons` is repeated only at one position in the ciphertext, namely `olobbyn`. If our hypothesis is correct, `b` should go to `o` and `a` to `l`. Converting letters to numbers, we get that 0 should go to 11 and 1 should go to 14, giving us the equations

$$\begin{aligned} k_1 \cdot 0 + k_2 &\equiv 11 \pmod{26} \\ k_1 \cdot 1 + k_2 &\equiv 14 \pmod{26} \end{aligned}$$

from which we easily get that $k_2 = 11$ and $k_1 = 3$.

Since 9 is an inverse of 3 modulo 26, the decryption equation is $9(c - 11)$. Decrypting the ciphertext is now easy (spaces inserted for readability):

```
a thousand baboons made this exam
```

Problem 2

a. There are many ways to proceed. It is easy to see that 1 is a zero of the polynomial.

We can now observe that 3 is a second zero of the polynomial, and that it must therefore have three rational zeros. We know that this polynomial cannot have repeated zeros, since then the curve would be singular and not an elliptic curve. Therefore, it has three distinct zeros.

Alternatively, we can divide the polynomial by $(x - 1)$ to get $x^2 + x + 49$. Again, we may observe that 3 is a zero of this polynomial, or we may attempt to use the usual formula:

$$\frac{-1 \pm \sqrt{1^2 - 4 \cdot 49}}{2},$$

and observe that $1 - 4 \cdot 49 \equiv 49 \pmod{61}$, which is a square. Therefore, the quadratic polynomial has two zeros, both of which are easily computed and seen to be distinct.

It follows that there are three points of order 2 (and therefore a subgroup with 4 elements).

b. This is a simple computation. Either one computes $2Q$ and $3Q = 2Q + Q$ (one doubling and one addition) and observes that they are inverses, or $4Q = 2(2Q)$ (two doublings) and observes that it is the inverse of Q.

c. From the two previous tasks, we know that 4 and 5 must divide the group order N. From Hasse's theorem, we know that

$$62 - 2\sqrt{61} \leq N \leq 62 + 2\sqrt{61}.$$

The only number in that range that is divisible by 20 is 60, so $N = 60$.

The group is not cyclic, since there are three points of order 2 (which means that the group must contain a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$).

Problem 3

a. First note that

$$e_i(x_l) = \begin{cases} 1 & i = l, \\ 0 & i \neq l. \end{cases}$$

Let

$$u(x) = \sum_{i \in S} a_i e_I(x).$$

Observe that the degree of $u(x)$ is at most $|S| - 1$. Also note that $u(x_l) = a_l$, so for $l \in S$, $f(x_l) = u(x_l)$. The polynomial $f(x) - u(x)$ therefore has degree at most $|S| - 1$, but has at least $|S|$ zeros. Therefore, $f(x) - u(x) = 0$.

b. If $|S| > t$, the previous result shows that we can recover $f(x)$ by interpolation, and then we can compute $f(0)$.

If $|S| \leq t$, say $|S| = t$, then we can choose any value a_0, and by the above argument, we can find a polynomial $f(x)$ fitting all the values a_i for $i \in S$, and also $f(0) = a_0$. Since our knowledge fits any value for $f(0)$, we know nothing about it.

c. We first want to compute $f(0)$. For $S = \{1, 2, 3\}$, we compute

$$\begin{aligned} e_1(0) &= \frac{(-2)(-3)}{(1-2)(1-3)} = 3, \\ e_2(0) &= \frac{(-1)(-3)}{(2-1)(2-3)} = -3, \\ e_3(0) &= \frac{(-1)(-2)}{(3-1)(3-2)} = 1. \end{aligned}$$

Then $f(0) = 1 \cdot 3 + 10 \cdot (-3) + 1 \cdot 1 = 7$.

Since $g(x)$ has degree 1, the result from above means that we only need to use two b_i-values to recover $g(x)$. Since Bob and Carol may be lying, we cannot use those values. But we can still interpolate using $S = \{3, 4\}$. Happily, David's contribution is 0, which means we only have to compute Eve's contribution:

$$7 \cdot e_4(0) = 7 \frac{-3}{4-3} = 1 = l.$$

Problem 4

a. Let $p' = (p-1)/2$ and $q' = (q-1)/2$. Since g has maximal order, it has order $2p'q'$.

Suppose $h(x) = h(y)$, $x > y$. Then

$$g^x = g^y \Leftrightarrow g^{x-y} = 1,$$

which implies that the order of g divides $x-y$, that is, $2p'q'|x-y$.

Let $x-y=2^ts$, s odd. Then $s=p'q's'$, s' odd. Let $u=g^s\neq 1$. Then $u^2=1$. Since g and u have the same Jacobi symbol, and the Jacobi symbol of -1 is 1, we have that $u^2=1$ while $u\neq\pm 1$, which means that

$$\gcd(u-1,n)$$

is a proper divisor of n.

b. We compute:

$$\begin{aligned}
2^1 &\equiv 2 \pmod{517}\\
2^2 &\equiv 4 \pmod{517}\\
2^{2^2} \equiv 2^4 &\equiv 16 \pmod{517}\\
2^{2^3} \equiv 2^8 &\equiv 256 \pmod{517}\\
2^{2^4} \equiv 2^{16} &\equiv 394 \pmod{517}\\
2^{2^5} \equiv 2^{32} &\equiv 136 \pmod{517}\\
2^{2^6} \equiv 2^{64} &\equiv 401 \pmod{517}\\
2^{2^7} \equiv 2^{128} &\equiv 14 \pmod{517}\\
2^{2^8} \equiv 2^{256} &\equiv 196 \pmod{517}
\end{aligned}$$

So $h(256)=196$, while

$$h(26)\equiv g^{26}\equiv g^{16}g^8g^2\equiv 394\cdot 256\cdot 4\equiv 196 \pmod{517}.$$

c. The difference of the two collisions is 230, so we shall raise g to 115'th power:

$$g^{115}\equiv g^{64}g^{32}g^{16}g^2g^1\equiv 401\cdot 136\cdot 394\cdot 4\cdot 2\equiv 142 \pmod{517}.$$

Now it is easy to compute that $\gcd(142-1,517)=47$ and $517/47=11$.